République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

UNIVERSITE MOULOUD MAMMERI DE TIZI-OUZOU

FACULTE DU GENIE ELECTRIQUE ET D' INFORMATIQUE
DEPARTEMENT D'AUTOMATIQUE

Mémoire de Fin d'Etudes de MASTER PROFESSIONNEL

Domaine : **Sciences et Technologies**

Filière : **Automatique**

Spécialité : **Contrôle des Véhicules á Propulsion Électrique.**

Présenté par

ARROUCHE Yasmine

HADDAD Melissa

Thème

Conception d'un crypto-système à base de systèmes chaotiques d'ordre fractionnaire : Application au cryptage vidéo

Mémoire soutenu publiquement le 27/06/ 2024 devant le jury composé de :

M DJEGHALI Nadia
Grade Professeur ,UMMTO , Président

M HAMOUDI Ahcene
Grade MAB , UMMTO, Encadrant

M MEGHERBI Ouardia
Grade MCB ,UMMTO, Examinateur

M AMOURA Karima
Grade MCB , UMMTO, Examinateur

Remerciements

Nous souhaitons exprimer notre profonde gratitude à notre encadreur, Monsieur ***HAMOUDI Ahcene****, pour ses conseils précieux, son soutien tant scientifique que moral, ainsi que pour tous les encouragements et efforts qu'il nous a prodigués tout au long de cette période de travail.*

Nous tenons également à adresser nos sincères remerciements aux membres du jury : Professeur DJEGHALI NADIA, *Dr.****MEGHERBI Ouardia*** *et Dr.****AMOURA Karima****, qui ont généreusement accepté d'évaluer notre travail.*

Nous exprimons notre reconnaissance aux enseignants du département d'Automatique pour leur aide précieuse durant nos années de scolarité.

Enfin, nous remercions chaleureusement toutes les personnes qui, de près ou de loin, ont contribué à la réalisation de ce mémoire.

Dédicace

À la mémoire de ma chère mère, à qui je dois ce que je suis.

Je te dédie ce travail et ce diplôme, en hommage à tout ce que tu as fait pour moi.
À toi, ma binôme, avec qui j'ai eu l'occasion de mener à bien ce projet.

Mélissa

Dédicace

Je dédie ce modeste travail à mes chers parents, à qui je dois tout. Leur soutien indéfectible et leurs sacrifices ont été le fondement de mon parcours académique.

À la mémoire de mon défunt oncle, mon deuxième père, qui a toujours été là pour moi. Sache que j'ai réussi.

À mes sœurs et mon frère, dont la présence et le soutien sans failles ont été une source de force et de motivation à chaque étape de ma vie.

À mes cousins et cousines, pour leur appui continu et leurs encouragements qui m'ont accompagné tout au long de ce chemin.

À toi, ma binôme, avec qui j'ai mené à bien ce projet, sans aucun regret.

Enfin, à mes amis et à chaque personne qui a contribué, de près ou de loin, à la réussite de ce mémoire, je vous adresse ma profonde gratitude.

Yasmine

Résumé

Ce mémoire se concentre sur la conception d'un cryptosystème innovant reposant sur des systèmes chaotiques d'ordre fractionnaire, en particulier le système de Lozi et de Hénon modifié, appliqué au cryptage vidéo.

Le travail débute par une introduction aux systèmes chaotiques, suivie d'une exploration des principes de la cryptographie et de la synchronisation chaotique. Par la suite, une analyse des systèmes chaotiques d'ordre fractionnaire est effectuée. Enfin, le mémoire examine l'application du cryptosystème proposé pour le cryptage d'une vidéo.

Les résultats des simulations confirment que ce schéma de chiffrement assure une protection efficace contre les attaques potentielles, tout en garantissant une transmission sécurisée des données vidéo.

Mots clés : cryptosystème, systèmes chaotiques, ordre fractionnaire, Lozi, Hénon modifié, cryptage vidéo, synchronisation chaotique.

This thesis focuses on the design of an innovative cryptosystem based on fractional-order chaotic systems, specifically the Lozi and modified Hénon systems, applied to video encryption.

The work begins with an introduction to chaotic systems, followed by an exploration of the principles of cryptography and chaotic synchronization. Subsequently, a detailed analysis of fractional-order chaotic systems is conducted. Finally, the thesis examines the application of the proposed cryptosystem for video encryption.

Simulation results confirm that this encryption scheme provides effective protection against potential attacks while ensuring secure transmission of video data.

Keywords : cryptosystem, chaotic systems, fractional order, Lozi, modified Hénon, video encryption, chaotic synchronization.

Table des matières

Symboles et Notations

Introduction générale **1**

1 Systèmes chaotiques **5**

1.1 Introduction 5

1.1.1 Les systèmes dynamiques 6

1.1.2 Les systèmes autonomes 7

1.1.3 La théorie du chaos 7

1.1.4 Le chaos 7

1.1.5 Identification du chaos : 9

1.1.6 Exemple illustrant des systèmes chaotique : 13

1.1.7 Cas discret : 21

1.2 Conclusion : 23

2 Cryptographie et synchronisation chaotique **25**

2.1 introduction 25

2.2 Introduction á la cryptographie : 26

2.3 Principe de cryptographie : 26

2.3.1 Terminologie : 27

2.3.2 Principes de Kerckhoffs pour la cryptographie : 27

2.3.3 Principe de Shannon pour la cryptographie 28

2.3.4 Objectifs de la cryptographie 29

2.4 Méthodes de Chiffrement 30

2.4.1 Chiffrement classique 30

2.4.2 Chiffrement moderne : . . . 31
2.5 Cryptographie chaotique : . . . 34
2.6 Techniques de cryptage par chaos . . . 35
2.6.1 Cryptage par clé . . . 35
2.6.2 Cryptage par message . . . 36
2.7 Synchronisation chaotique . . . 39
2.7.1 Introduction . . . 39
2.7.2 Définition . . . 39
2.7.3 Régimes de synchronisation . . . 40
2.7.4 Modes de synchronisation . . . 42
2.7.5 Synchronisation à base d'observateurs . . . 42
2.8 conclusion : . . . 46

3 Systèmes chaotiques d'ordre fractionnaire 47
3.1 Introduction . . . 47
3.2 Théorie de la dérivation non entière . . . 47
3.2.1 Calcul fractionnaire . . . 47
3.2.2 Fonctions spécifiques à la dérivation fractionnaire . . . 48
3.2.3 Intégration fractionnaire . . . 49
3.2.4 Dérivation fractionnaire . . . 49
3.2.5 Propriétés des dérivées fractionnaires et intégrales fractionnaires . . . 51
3.3 Systèmes d'ordre fractionnaires . . . 52
3.3.1 Représentation des systèmes fractionnaires . . . 52
3.3.2 Systèmes d'ordre fractionnaires commensurables et non commensurables . . . 53
3.3.3 Observabilité et Stabilité des systèmes d'ordre fractionnaires . . . 54
3.4 Systèmes chaotiques d'ordre fractionnaires . . . 56
3.4.1 Exemple de synchronisation . . . 56
3.4.2 Synthèse de l'observateur discret retardé étape par étape . . . 58
3.5 Conclusion . . . 61

4 Conception d'un cryptosystème pour le cryptage vidéo 63
4.1 Introduction . . . 63

4.2 Définition de l'image 64
4.3 Définition de l'image numérique 64
4.4 Caractéristiques de l'image numérique 65
4.4.1 Le pixel 65
4.4.2 Dimension 66
4.4.3 Contours 66
4.4.4 Résolution 66
4.4.5 Luminance 66
4.4.6 Contraste 66
4.4.7 Voisinage 67
4.5 Types d'images numériques 68
4.5.1 Image en niveaux de gris 68
4.5.2 Image binaire 68
4.5.3 Image couleur 68
4.6 Définition d'une vidéo 69
4.7 Définition d'une vidéo numérique 70
4.8 Caractéristiques d'une Vidéo Numérique 71
4.8.1 Format du fichier 71
4.8.2 Codec 71
4.8.3 Résolution 71
4.8.4 Fréquence d'images (Frame Rate) 71
4.9 Analyse comparative entre les images et les vidéos 71
4.10 Outils d'évaluation de la sécurité 72
4.10.1 Cryptanalyse 72
4.10.2 Hypothèse de Kerckhoff 72
4.10.3 Analyse de l'espace des clés 73
4.10.4 Analyse de la sensibilité de la clé 73
4.10.5 Analyse statistique 74
4.10.6 Entropie d'information 76
4.11 Application au cryptage vidéo 76
4.12 Analyse des Résultats 78

4.13 Conclusion 82

Conclusion Générale **83**

Table des figures

1.1 Évolution dans le temps, pour deux conditions initiales très proches. 14

1.2 Aspect aléatoire des états du système de Lorenz. 15

1.3 L'attracteur de Lorenz 15

1.4 Exposants de Lyapunov du système de Lorenz 16

1.5 Spectre de puissance de la variabe x du système de Lorenz. 16

1.6 Diagramme de bifurcation de Lorenz. 17

1.7 Aspect aléatoire de l'état x du systéme de Rossler 18

1.8 Évolution dans le temps, pour deux conditions initiales très proches (sensibilité aux conditions initiales). 18

1.9 Attracteur de Rössler 19

1.10 Diagramme de bifurcation du système de Rössler. 19

1.11 Exposants de Lyapunov du système de Rössler. 20

1.12 Aspect aléatoire. 21

1.13 Sensibilité aux conditions initiales de l'état x du système de Hénon. 21

1.14 Attracteur de Hénon. 21

1.15 Bifurcation de Hénon 22

1.16 Exposants de Lyapunov du système de Hénon. 22

1.17 Spectre de puissance des variable x et y du système de Hénon. 22

2.1 Schéma général de la communication chiffrée entre un émetteur et un récepteur. 26

2.2 Décalage de César. 31

2.3 schéma du chiffrement symétrique. 32

2.4 Principe de chiffrement asymétrique 34

2.5 Cryptage par commutation 35

2.6 cryptage par addition 36
2.7 Cryptage par modulation paramétrique 37
2.8 Observateur à entrée inconnue 38
2.9 Décryptage par inversion 38
2.10 Schéma de couplage unidirectionnel 42
2.11 Schéma de couplage bidirectionnel 42

3.1 Région de stabilité des systèmes d'ordre fractionnaires avec $0 < \alpha < 1$. 55
3.2 Région de stabilité des systèmes d'ordre fractionnaires avec $1 < \alpha < 2$. 55
3.3 La figure suivante illustre la sensibilité aux conditions initiales du système de Hénon modifié d'ordres fractionnaires en comparant les valeurs de x_3 égales à $0,1$ et $0,10000001$. 57
3.4 La figure suivante illustre la sensibilité aux paramètres de la dérivée d'ordre fractionnaire du système de Hénon modifié d'ordres fractionnaires en comparant les valeurs de α_3 égales à $0,75$ et $0,750001$. 57
3.5 Synchronisation de l'état x_1 et son estimé $\hat{x}_1$ 60
3.6 Synchronisation de l'état x_2 et son estimé $\hat{x}_2$ 60
3.7 Synchronisation de l'état x_3 et son estimé $\hat{x}_3$ 60
3.8 Les états x_1, x_2 et x_3 du système sont parfaitement reconstruits comme le montrent les figures (5), (6), (7). 60

4.1 Un exemple concret d'image numérique. 65
4.2 Exemple de contraste 67
4.3 Une image en niveaux de gris est représentée par $I(i,j) \in [0,255]$. 68
4.4 Une image binaire est représentée par $I(i,j) \in \{0,1\}$. 68
4.5 Image couleur. 69
4.6 Les 3 constituants principaux d'une couleur(RVB). 69
4.7 Schéma de principe de crypto-système vidéo proposé 78
4.8 Synchronisation des états 79
4.9 Trames(1,15 et 40) vidéo originale, chiffrée et décryptée 79
4.10 Histogramme vidéo originale 80
4.11 Histogramme vidéo cryptée 80

4.12 Histogramme vidéo décryptée 80
4.13 Histogrammes vidéo originale, cryptée et décryptée 80
4.14 La corrélation entre les pixels de la vidéo originale et cryptée 80

Liste des tableaux

1.1 Différents régimes d'un système dynamique non linéaire. 11

4.1 Voisins horizontaux-verticaux de $p(x, y)$ 67

4.2 Voisins diagonaux de $p(x, y)$ 67

4.3 Coefficients de corrélation de la vidéo originale et cryptée 81

4.4 Les différentes variations appliquées et les valeurs correspondantes du NPCR . . 81

Symboles et Notations

$\mathbb{R}$:	Ensemble des nombres réels
$\mathbb{R}_+$:	Ensemble des nombres réels positifs ou nuls
$\mathbb{R}^n$:	Espace vectoriel de dimension n dans l'ensemble des réels
$\mathbb{R}^{n\times m}$:	Ensemble des matrices réelles de dimensions $n \times m$
$\mathbb{C}$:	Ensemble des nombres complexes
t :	Variable temporelle
$x \in \mathbb{R}$:	Variable d'état
x^T :	Transposée du vecteur x
$\mid x \mid$:	Valeur absolue de x
$\| x \|_2$:	Norme euclidienne de x
$\dot{x}(t)$:	Dérivée temporelle de l'état x
A^T :	Transposée de la matrice A
A^{-1} :	Inverse de la matrice A
I_n :	Matrice d'identité de dimension $n \times n$
$\mathcal{C}$:	Matrice de commandabilité
$\mathcal{O}$:	Matrice d'observabilité

${}_{t_0}^{RL}D_t^{\alpha} f(t)$:	Dérivée d'ordre α de la fonction $f(t)$ selon la définition de Riemann-Liouville
${}_{t_0}^{C}D_t^{\alpha} f(t)$:	Dérivée d'ordre α de la fonction $f(t)$ selon la définition de Caputo
D^{α} :	Opérateur de dérivation d'ordre non entier α
Γ :	Fonction Gamma d'Euler
$\binom{\alpha}{j}$:	$(\alpha \in \mathbb{R}_+)$, désigne le binôme de Newton généralisé à des ordres réels
$D^{\alpha} f(kh)$:	désigne la valeur de la $\alpha^{ème}$ dérivée de $f(t)$ à l'instant kh
E_{α} :	Fonction Mittag-Leffler
$D^{\alpha} x$:	$(x \in \mathbb{R}^n)$, tous les éléments du vecteur $x(t)$ sont dérivés au même ordre α
$D^{(\alpha)}(x)$:	$(\alpha \in \mathbb{R}_+^n,\ x \in \mathbb{R}^n)$, le $i^{ème}$ élément du vecteur $x(t)$ est dérivé à la $i^{ème}$ composante du vecteur α

LTI :	Linear Time Invariant
LTV :	Linear Time variant
$SISO$:	Single Input, Single Output
$BIBS$:	Bounded Input, Bounded State
LMI :	Linear Matrix Inequality
UIO :	Unknown Input Observer
TS :	Takagi-Sugeno
STA :	Super-Twisting Algorithm
DES :	Data Encryption Standard
RSA :	Rivest Shamir Adleman
$NPCR$:	Number of Pixels Change Rate
$UACI$:	Unified Averaged Changed Intensity

Introduction Générale

Avec l'essor rapide des systèmes de production multimédia, de la publication électronique et de la diffusion généralisée des données multimédias numériques sur Internet, la protection des informations numériques contre la copie et la distribution illégales est devenue cruciale, la sécurité est également apparue naturellement à la suite de la vulgarisation des échanges d'informations confidentielles.

Afin d'y remédier, nous faisons appel à la cryptographie, qui revêt une importance capitale dans la sécurisation et la fiabilité des systèmes de transmission de données.

Les techniques de cryptographie classiques sont principalement fondées sur la théorie des nombres, notamment sur la factorisation des entiers en nombres premiers. Ces méthodes ont servi pendant de nombreuses années à concevoir des systèmes de chiffrement robustes et fiables[40].

La cryptographie moderne se subdivise principalement en deux grandes catégories : le chiffrement symétrique et le chiffrement asymétrique tels que les protocoles RSA, DES.Bien que ces méthodes aient été considérées comme sûres pendant un certain temps, la majorité des protocoles classiques, ont fini par être cassés. Cette vulnérabilité est souvent due à des avancées dans les techniques de cryptanalyse, l'augmentation de la puissance de calcul, et parfois à des faiblesses intrinsèques dans les algorithmes eux-mêmes[40].

Les systèmes non linéaires chaotiques ont attiré l'attention des chercheurs en cryptographie en raison de leurs propriétés uniques qui peuvent améliorer la sécurité des systèmes de chiffrement.

Au cours des dernières décennies, les systèmes chaotiques non linéaires ont été utilisés en cryptographie pour améliorer la sécurité. L'étude de ces systèmes est liée à la théorie du chaos, qui a connu une évolution significative à partir des années 1960 grâce aux travaux du météorologue Edward Lorenz. Les systèmes chaotiques, avec leurs propriétés telles que la sensibilité aux conditions initiales, constituent de solides candidats pour les applications cryptographiques[25].

L'idée d'utiliser le chaos dans les systèmes de communication est née de la découverte de Pecora et Carroll en 1990. Ces chercheurs ont montré que deux systèmes chaotiques identiques, ayant des conditions initiales différentes, peuvent finir par se synchroniser s'ils sont couplés de manière adéquate. Depuis lors, de nombreuses techniques de cryptage ont été développées, telles que le cryptage par addition, le cryptage par commutation, le cryptage par modulation, etc., pour intégrer le message clair dans une porteuse chaotique. Grâce à un processus de synchronisation, le récepteur peut estimer l'état de l'émetteur, décrypter le message et restituer le message clair [34].

Les chercheurs ont également démontré que la synchronisation peut être étendue aux systèmes chaotiques à dérivées fractionnaires [18]. Ces systèmes chaotiques d'ordre fractionnaire ont été appliqués dans le domaine de la transmission sécurisée pour renforcer la protection des données et rendre la cassure de la clé presque impossible.

Notre travail vise à développer un cryptosystème innovant pour la synchronisation des systèmes chaotiques, en mettant à profit les propriétés des systèmes dynamiques chaotiques. Pour ce faire, nous employons la synchronisation par observateurs en temps discret. Afin de renforcer davantage la sécurité de ces cryptosystèmes, nous intégrons le calcul fractionnair dans ces systèmes dynamiques chaotiques. Finalement, cette approche sera appliquée au domaine du cryptage vidéo.

Pour entreprendre ce travail, nous avons structuré ce mémoire en quatre chapitres, dont : Le premier chapitre est dédié à l'introduction et à l'étude des systèmes chaotiques, en mettant en lumière leurs caractéristiques ainsi que les outils permettant d'identifier et d'analyser leurs comportements.

Le second chapitre expose les généralités sur la cryptographie et les diverses méthodes de chiffrement existantes. L'objectif de ce chapitre est d'introduire l'utilité et l'application du chaos en cryptographie. Il présente également l'approche de Pecora et Carroll concernant la synchronisation des systèmes chaotiques, ainsi que les différentes méthodes de synchronisation.

Dans le troisième chapitre, nous aborderons les différentes notions relatives au calcul fractionnaire, appliquées aux systèmes chaotiques en temps continu et en temps discret.

Le quatrième chapitre est consacré à l'étude et à la conception d'un schéma de transmission sécurisée en temps discret. Ce schéma comprend un émetteur composé de deux systèmes chaotiques d'ordre fractionnaire, à savoir le « Système de Lozi » et le « Système de Hénon modifié », ainsi que deux observateurs « retardés étape par étape » à la réception. Ces obser-

vateurs permettent de reproduire les signaux chaotiques générés par l'émetteur et de récupérer le message confidentiel, de type ≪ vidéo ≫

Enfin, nous terminons par une conclusion générale et en citant quelques perspectives d'avenir concernant nous recherches effectuer dans le domaine de la cryptographie a base de systèmes chaotiques,clôturant ainsi notre travail.

Chapitre 1

Systèmes chaotiques

1.1 Introduction

Pendant de nombreuses années, le terme ”chaos” a été associé à l'idée de désordre et de confusion, en contraste avec l'ordre et la prévisibilité qui caractérisent la science. Henri Poincaré a été parmi les premiers à envisager la théorie du chaos, mettant en lumière la sensibilité aux conditions initiales à travers l'étude de l'interaction de trois corps célestes.

Le ”chaos” est un concept qui décrit un état singulier d'un système, où son comportement est non répétitif, fortement influencé par les conditions initiales et difficile à prédire à long terme. Cette idée a captivé l'intérêt de chercheurs provenant de divers domaines, tous désireux de déterminer si des phénomènes tels que les arythmies cardiaques ou les fluctuations de populations animales sont soumis à des lois bien définies. De même, l'étude des mouvements commerciaux ou des variations sur les marchés financiers a soulevé des interrogations sur la possibilité de les modéliser.

Cette approche du chaos a trouvé de nombreuses applications, que ce soit dans les domaines physiques, biologiques, chimiques ou économiques. Ainsi, ce chapitre se concentrera principalement sur les systèmes dynamiques chaotiques, en examinant en détail les espaces de phase, les attracteurs étranges et les bifurcations (transitions vers le chaos). L'objectif est de fournir des notions fondamentales sur les systèmes dynamiques, permettant ainsi une meilleure compréhension du chaos : ses manifestations dans un système donné et les méthodes pour le quantifier.[39] [10] [26]

1.1.1 Les systèmes dynamiques

En général, un système dynamique décrit des phénomènes qui évoluent au cours du temps. Le terme "système" fait référence à un ensemble de variables d'état, dont les valeurs évoluent au fil du temps, ainsi qu'aux interactions entre ces variables. L'ensemble des variables d'état d'un système permet de construire un espace mathématique appelé "espace de phase". Ce dernier est une structure correspondant à toutes les trajectoires possibles du système considéré. Ces systèmes peuvent être classés en deux catégories distinctes :

Les systèmes dynamiques continus

Un système dynamique continu désigne un système dont l'évolution dans le temps est décrite de manière continue par des équations différentielles sans discontinuité ni saut. Les états du système varient de manière continue sur un intervalle non disjoint, déterminé par les variables d'état et les paramètres du système. Ce dernier est caractérisé par un ensemble d'équations différentielles ordinaires du premier ordre, généralement sous la forme suivante :

$$\dot{X} = (t, X(t)) \tag{1.1}$$

Ce qui est une écriture abrégée du système suivant :

$$\begin{cases} \dot{X}1 = f_1(t, x_1, ..., x_n) \\ . \\ . \\ . \\ \dot{X}_n = f_n(t, x_1, ..., x_n) \end{cases} \tag{1.2}$$

ou :

— $f : \mathbb{R}^+ \times \mathbb{R}^n \to \mathbb{R}^n$ désigne la dynamique du système.

— $x(t) \in \mathbb{R}^n$ c'est le vecteur d'état de dimension n.

— $t \in \mathbb{R}^+$ désigne le temps.

Les systèmes dynamiques discrets

Un système dynamique discret est un modèle mathématique qui décrit l'évolution d'un système au fil du temps, mais avec des pas de temps discrets.

$$X(k+1) = g(k, X(k)) \tag{1.3}$$

oú :

— $g : \mathbb{Z}^+ \times \mathbb{R}^n \to \mathbb{R}^n$ désigne la dynamique du système en temps discret.

1.1.2 Les systèmes autonomes

Un système autonome est un système dynamique non linéaire qui ne dépend pas explicitement du temps. Il est donné comme suit :

$$\begin{cases} \dot{X} = f(x, y) \\ \dot{Y} = g(x, y) \end{cases} \tag{1.4}$$

Les systèmes autonomes sont indépendants du temps initial, alors que les systèmes non autonomes ne le sont pas. Dans un système autonome, tout moment peut être considéré comme un moment initial, et tout état x(t) du système peut être considéré comme un état initial

1.1.3 La théorie du chaos

La théorie du chaos, l'une des branches les plus récentes et avancées des sciences contemporaines, se concentre sur l'étude des systèmes dynamiques complexes et non linéaires. Cette discipline analyse les comportements dynamiques, non constants et non périodiques, à travers des récurrences et des algorithmes mathématiques. Elle englobe l'étude qualitative et quantitative des comportements instables, non périodiques et apparemment aléatoires des systèmes déterministes, offrant ainsi une perspective unique sur l'évolution de ces systèmes.[23] [28] [24]

1.1.4 Le chaos

Bien qu'il n'existe pas de définition universelle du chaos adoptée dans la littérature, on peut le décrire comme un phénomène qui peut se manifester dans les systèmes dynamiques déterministes non linéaires. Ces systèmes se caractérisent par une évolution qui semble aléatoire et par un aspect fondamental d'instabilité appelé sensibilité aux conditions initiales. Cette sensibilité signifie que de petites variations dans les conditions initiales peuvent conduire à des

résultats totalement différents à mesure que le système évolue dans le temps, ce qui le rend imprédictible en pratique à long terme.[23]

1.1.4.1.Propriétés des systèmes chaotiques

Pour approfondir la compréhension des systèmes chaotiques associés au phénomène du chaos, nous nous appuyons sur diverses définitions, propriétés et domaines d'application. Ces concepts sont essentiels pour explorer et analyser ces systèmes, qui remettent souvent en question nos intuitions concernant la prédictibilité et le comportement déterministe.[23] Un système dynamique chaotique inclut les caractéristiques, qui lui sont inhérentes, présentées comme suit :

*** Non-linéarité :** L'analyse détaillée des systèmes dynamiques non linéaires démontre de manière évidente que la caractéristique fondamentale du chaos exclut la possibilité d'un système linéaire d'être chaotique.

*** Le déterminisme :** Le déterminisme se réfère à la capacité de prédire le futur d'un phénomène en se basant sur son état passé ou présent. L'instabilité du comportement d'un système chaotique est directement liée à ses non-linéarités. Contrairement aux phénomènes aléatoires où il est absolument impossible de prédire la trajectoire d'une particule, un système chaotique suit des lois fondamentales déterministes, écartant toute notion de probabilité.

*** L'aspect aléatoire** Tous les états d'un système chaotique révèlent un aspect aléatoire en raison de la complexité inhérente de ces systèmes. Bien que déterministes, les systèmes chaotiques présentent une imprévisibilité dans leurs états successifs qui peut sembler aléatoire. Cette apparence de hasard provient de la sensibilité extrême aux conditions initiales, rendant toute tentative de prédiction précise pratiquement impossible à long terme. Ainsi, l'aspect aléatoire devient une caractéristique centrale, où chaque état semble se développer de manière imprévisible malgré les lois déterministes qui gouvernent le système.

*** Sensibilité aux conditions initiales** Une caractéristique fondamentale des systèmes chaotiques réside dans leur sensibilité aux conditions initiales. Cela signifie que deux points de départ, aussi proches soient-ils, auront des évolutions tellement divergentes qu'il sera impossible d'établir une relation entre leurs trajectoires. Même la plus petite erreur ou imprécision dans la condition

initiale rend impossible la prédiction précise de la trajectoire réelle du système, empêchant ainsi toute projection sur son évolution à long terme. Malgré le caractère déterministe de ces systèmes, leur comportement à long terme demeure imprévisible.[24]

Une propriété essentielle du chaos réside donc dans cette sensibilité aux conditions initiales, qui peut être caractérisée en mesurant les taux de divergence des trajectoires.

*** Attracteur étrange** Les attracteurs, fondamentaux en dynamique des systèmes, représentent les états vers lesquels convergent les trajectoires de l'espace des phases d'un système. Ils décrivent les configurations vers lesquelles le système évolue, indépendamment de ses conditions initiales. Dans un espace des phases bidimensionnel, les attracteurs peuvent être des points fixes ou des cycles limites.

Les attracteurs réguliers, présents dans les systèmes non chaotiques, maintiennent des trajectoires proches les unes des autres dans l'espace des phases, permettant ainsi des prédictions fiables à partir de conditions initiales précises. En revanche, les attracteurs étranges, caractéristiques des systèmes chaotiques, présentent une complexité infinie. Bien que les trajectoires convergentes vers un attracteur étrange semblent chaotiques, elles restent confinées dans un espace défini. Cependant, de légères variations initiales peuvent entraîner des divergences exponentielles avec le temps, rendant la prédiction à long terme impossible malgré des conditions initiales minutieusement définies. L'introduction d'une troisième variable dans un système à deux variables est nécessaire pour générer des mouvements chaotiques, et l'attracteur étrange joue un rôle central dans cette dynamique.

1.1.5 Identification du chaos :

Étant donnée la complexité inhérente à la résolution analytique des systèmes chaotiques, l'utilisation de méthodes numériques est courante. Dans cette section, nous examinerons plusieurs techniques permettant d'analyser l'évolution du comportement chaotique d'un système dynamique ainsi que ses caractéristiques.

1.5.1 Exposants Lyapunov : L'évolution d'un flux chaotique est complexe à appréhender en raison de la divergence rapide des trajectoires sur l'attracteur. C'est pourquoi l'estimation ou la mesure de la vitesse de divergence ou de convergence est souvent entreprise. Alexandre Lyapunov a développé une mesure permettant d'évaluer cette divergence des trajectoires initialement

proches. Cette mesure est appelée "exposant de Lyapunov". Les exposants de Lyapunov sont utilisés pour évaluer le niveau de stabilité d'un système et permettent de quantifier la sensibilité aux conditions initiales d'un système chaotique [30] [46]. Le nombre d'exposants de Lyapunov est égal à la dimension de l'espace des phases, et ils sont généralement classés du plus grand au plus petit, notés λ_1 ; λ_2 ; λ_3...

soit $f : \mathbb{R} \to \mathbb{R}$ une fonction de C^1. Pour chaque point x_0 on définit un exposant de Lyapunov $\lambda(x_0)$ comme suit :

$$\lambda(x_0) = \lim_{n\to\infty} \sup \frac{1}{n} \log(|f(n)'(x_0)|) = \lim_{n\to\infty} \sup \frac{1}{n} \sum_{i=0}^{n-1} \log(|f(x_j)|) \tag{1.5}$$

avec $x_j = f_j(x_0)$

Donc deux trajectoires dans le plan de phase initialement séparées par un taux Z_1,divergent après un temps $\Delta t = t_2 - t_1$ vers Z2 tel que :

$$|Z_2| \approx e^{\lambda \Delta t} \tag{1.6}$$

ou λ est l'exposant de Lyapunov.
C^1 fait référence à la classe de régularité de la fonction f.
Z_1 représente la distance initiale entre deux trajectoires dans le plan de phase.

Les exposants de Lyapunov généralisent le concept de valeurs propres pour les points fixes et celui des multiplicateurs caractéristiques pour les solutions périodiques. Dans le cas d'un attracteur non chaotique, tous les exposants de Lyapunov sont inférieurs ou égaux à zéro, avec une somme négative. En revanche, un attracteur étrange se caractérise par la présence d'au moins trois exposants de Lyapunov, dont au moins un est positif.Les différents éléments utilisés pour décrire la dynamique d'un système non linéaire sont résumés dans le tableau 1.1.

Régime permanent	Attracteur	Exposants de Lyapunov
Point d'équilibre	Point	$0>\lambda_1\geq...\geq\lambda_n$
Périodique	Courbe fermée	$\lambda_1=0, \quad 0>\lambda_2\geq...\geq\lambda_n$
Quasi-périodique	Tore	$\lambda_1=...=\lambda_i=0, \quad 0>\lambda_i+1\geq...\geq\lambda_n$
Chaotique	Fractal	$\lambda_1>0, \quad \lambda_2>0\geq...\lambda_n$
Hyperchaotiques	Fractal	$\lambda_1>\lambda_2>0, \quad 0>\lambda_3\geq...\geq\lambda_n$

TABLE 1.1 – Différents régimes d'un système dynamique non linéaire.

1.5.2 Spectre de puissance et fonction d'auto-corrélation : Selon les méthodes d'analyse des signaux temporels, la transformée de Fourier est largement utilisée pour caractériser les états chaotiques. Le spectre de puissance d'un signal $x(t)$ est défini comme le carré de son amplitude par unité de temps. Sa forme spectrale fournit des informations sur le type de comportement du système étudié. En régime chaotique, le spectre de puissance d'une variable du système dynamique présente une partie continue, indiquant une évolution désordonnée. Ce type de spectre est difficile à différencier de celui du bruit blanc, rendant cette méthode insuffisante pour identifier les états chaotiques. À l'inverse, un état périodique se distingue par un spectre de puissance constitué d'une raie de fréquence f, accompagnée de raies harmoniques à $2f$, $3f$, etc.

Pour évaluer le degré de désordre, il est utile d'introduire la fonction d'autocorrélation, définie comme suit :

$$C(\Gamma) = \frac{1}{t_2 - t_1} \int_{t_1}^{t_2} x(t) \cdot x(t-\Gamma)\, dt. \tag{1.27}$$

Cette fonction mesure la similarité entre la variable x à l'instant t et sa valeur à l'instant $(t+\Gamma)$. Elle évalue ainsi la similarité du signal avec lui-même au fil du temps. En régime chaotique,

$C(\Gamma)$ tend vers zéro à mesure que Γ augmente. La fonction d'autocorrélation temporelle du signal avec lui-même diminue, voire disparaît complètement, à des instants suffisamment éloignés. Cela traduit une perte progressive de la similitude interne, rendant le chaos imprévisible. .

1.5.3 Bifurcation : La théorie des bifurcations examine les changements qualitatifs d'un système dynamique suite à des modifications de ses paramètres. Les bifurcations peuvent entraîner des changements tant quantitatifs que qualitatifs dans les solutions, comme la disparition ou la modification de la stabilité d'une solution, ou l'apparition de nouvelles solutions. On distingue deux types de bifurcations : locales et globales, chacune caractérisée par des formes normales telles que la bifurcation pli, transcritique, fourche, flip, Neimark-Sacker, noeud-col et de doublement de période. L'évolution vers le chaos dans les systèmes dynamiques peut être observée en ajustant les paramètres, avec trois scénarios théoriques principaux qui décrivent ces transitions :[47]

1.Le doublement de période : Pour un système périodique, l'augmentation du paramètre peut conduire à un phénomène de doublement de sa période. Ce doublement se produit successivement, multipliant la période par 2, 4, 8, 16, et ainsi de suite. À chaque étape, l'incrément nécessaire du paramètre devient de plus en plus petit. Au-delà d'une certaine valeur critique du paramètre, le système bascule soudainement vers un comportement chaotique. Lorsque la période du système tend vers l'infini, les mouvements deviennent alors complètement chaotiques.

2.L'intermittence vers le chaos : Ce scénario décrit un phénomène où un mouvement périodique stable est interrompu par des épisodes de turbulence. En augmentant progressivement le paramètre de contrôle, ces épisodes de turbulence deviennent de plus en plus fréquents. À un certain seuil, la turbulence devient dominante et le système entre alors dans un état chaotique. Cela peut être illustré par des exemples tels que les systèmes météorologiques, où des périodes de calme sont suivies par des tempêtes de plus en plus fréquentes jusqu'à ce que la turbulence prédomine totalement.

3.La quasi-périodicité : Dans ce scénario, un système périodique peut présenter des signes de nouvelles fréquences qui ne sont pas rationnellement liées à la première. Lorsque le paramètre est ajusté, une troisième fréquence peut apparaître, et ainsi de suite. Ces fréquences supplémentaires

peuvent engendrer des motifs complexes dans le comportement du système. À mesure que le paramètre est davantage modifié, le système finit par basculer dans un état chaotique où les mouvements ne suivent plus de schéma périodique prévisible.

Ces scénarios représentent des mécanismes cruciaux pour comprendre comment les systèmes dynamiques évoluent vers le chaos.

1.1.6 Exemple illustrant des systèmes chaotique :

Dans la quête des signaux complexes et non linéaires, différents types de systèmes dynamiques sont employés pour engendrer des comportements chaotiques. Il est intéressant de souligner que, dans le cadre continu, un système chaotique autonome, c'est-à-dire sans entrée ni retard, doit posséder au moins trois états pour manifester des propriétés chaotiques. En revanche, dans le domaine discret, même un système dynamique à une seule variable d'état peut exhiber des comportements chaotiques, comme le démontre la fonction logistique.

Pour illustrer ces concepts, nous présentons ci-dessous des exemples de systèmes chaotiques en continu et en discret. Ces systèmes sont des modèles largement étudiés et utilisés pour appréhender le chaos.

1.6.1 Cas continu :

Système chaotique de Lorenz : Le modèle de Lorenz, élaboré dans les années 1960, représente une avancée significative dans la compréhension des systèmes dynamiques chaotiques, notamment dans le cadre de la modélisation des phénomènes météorologiques comme la convection atmosphérique. L'approche de Lorenz était intentionnellement axée sur la compréhension plutôt que sur la précision prédictive. Il a entrepris de simplifier les équations météorologiques complexes afin de créer un modèle plus accessible, tout en capturant toujours l'essence de la dynamique chaotique des masses d'air.

Le système chaotique de Lorenz est représenté par :

$$\begin{cases} \dot{x} = \sigma(y - x) \\ \dot{y} = x(\rho - z) - y \\ \dot{z} = xy - \beta z \end{cases} \tag{1.7}$$

avec :

— x,y et z : sont des variables respectivement proportionnelles aux amplitudes du champ de vitesse, et du champ de température.

— σ Le coefficient de Prandtl, qui est un nombre sans dimension utilisé pour caractériser la viscosité du fluide et le taux de transfert de chaleur par conduction par rapport au transfert de chaleur par convection.

— ρ : Le nombre de Rayleigh, un autre nombre sans dimension qui caractérise le gradient de température à travers le fluide.

— β : Un paramètre qui mesure le rapport des variations de densité du fluide à la température. C'est le coefficient de couplage du modèle.

On prend :$(\sigma = 10; \rho = 28; \beta = 8/3\ )$; d es valeurs pour lesquelles le système présente un comportement chaotique, et pour les conditions initiales suivantes :$x_0 = 10; y_0 = 10; z_0 = 20$.

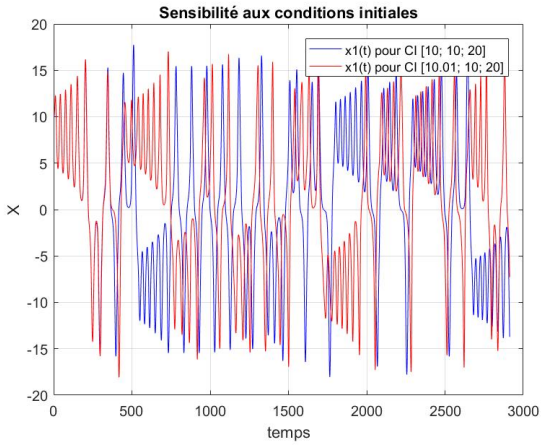

FIGURE 1.1 – Évolution dans le temps, pour deux conditions initiales très proches.

***Remarque :**Cette figure illustre la sensibilité extrême aux conditions initiales dans le système de Lorenz. Bien que les conditions initiales des trajectoires $x_1(t)$ et $x_2(t)$ soient très proches, une légère perturbation initiale entraîne une divergence rapide des trajectoires au fil du temps. Ce comportement, caractéristique des systèmes chaotiques, met en évidence l'imprévisibilité inhérente au modèle de Lorenz.

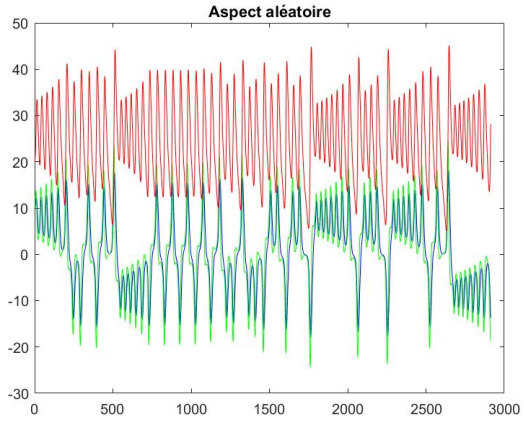

FIGURE 1.2 – Aspect aléatoire des états du système de Lorenz.

***Remarque :** La figure met en évidence l'aspect aléatoire du comportement chaotique dans le système de Lorenz. Bien que les trajectoires $x_1(t)$ et $x_2(t)$ démarrent à partir de conditions initiales très similaires, leur évolution diverge de manière imprévisible. Cette divergence rapide et apparemment aléatoire illustre l'incapacité à prédire précisément le comportement futur à long terme, même dans un système déterministe.

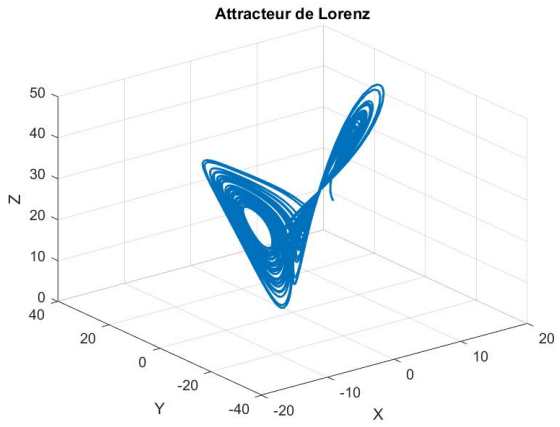

FIGURE 1.3 – L'attracteur de Lorenz

***Remarque :** La figure montre l'attracteur étrange du système de Lorenz, où les trajectoires, malgré des conditions initiales légèrement différentes, convergent vers une région confinée de l'espace des phases. Cet attracteur, de structure fractale, illustre la dynamique chaotique du système : les trajectoires ne se répètent jamais exactement, révélant un comportement complexe et imprévisible.

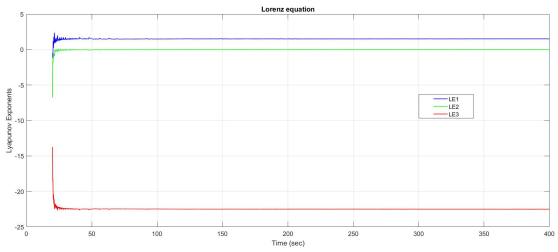

FIGURE 1.4 – Exposants de Lyapunov du système de Lorenz

***Remarque :** La figure montre les exposants de Lyapunov du système de Lorenz : $\lambda_1 = 1.50564$ (positif), $\lambda_2 = -0.000802294$ (près de zéro), et $\lambda_3 = -22.5048$ (négatif). L'exposant positif indique une divergence exponentielle des trajectoires, signe de chaos, tandis que l'exposant proche de zéro montre une stabilité limitée dans une direction. L'exposant négatif révèle une contraction rapide dans une autre direction, illustrant que le système reste confiné dans une région spécifique malgré sa nature chaotique. Ensemble, ces exposants caractérisent un attracteur étrange, avec des trajectoires se séparant rapidement tout en restant limitées.

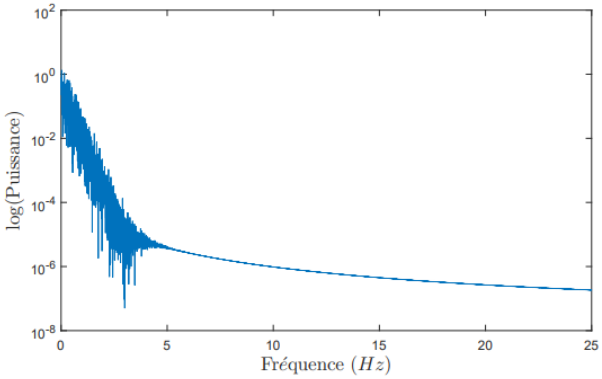

FIGURE 1.5 – Spectre de puissance de la variabe x du système de Lorenz.

***Remarque :** cette figure représente le spectre de puissance de la variable x du système de Lorenz révèle la complexité de son comportement chaotique. Contrairement à un spectre périodique, qui serait dominé par des raies discrètes correspondant à des fréquences harmoniques, le spectre de x présente une composante continue. Cette continuité est indicative d'une dynamique désordonnée, typique des systèmes chaotiques, où l'énergie est répartie sur une large bande de fréquences. Ce type de spectre rend difficile la distinction entre un signal chaotique et du bruit blanc, mettant en lumière l'imprévisibilité et la richesse dynamique du système de Lorenz.

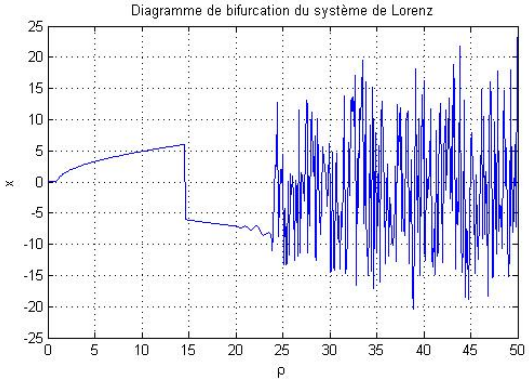

FIGURE 1.6 – Diagramme de bifurcation de Lorenz.

***Remarque :** La figure présente le diagramme de bifurcation du système de Lorenz, qui illustre les différentes dynamiques du système en fonction de la variation d'un paramètre, tel que le paramètre de contrôle r. À de faibles valeurs de r, le système tend vers des solutions stables, souvent représentées par une seule branche sur le diagramme. À mesure que r augmente, des bifurcations apparaissent, indiquant la transition vers des solutions périodiques, puis quasi-périodiques. Pour des valeurs plus élevées de r, le système entre dans un régime chaotique, caractérisé par une structure de bifurcation de plus en plus complexe et irrégulière. Ce passage progressif de l'ordre au chaos est typique des systèmes dynamiques non linéaires, et la figure met en lumière les points de bifurcation critiques où le comportement du système change radicalement.

Système chaotique de Rössler : Le système de Rössler, introduit par Otto Rössler en 1976, est un ensemble d'équations différentielles non linéaires conçu pour modéliser des dynamiques chaotiques simples. Initialement lié à l'étude des écoulements fluides et à la cinétique chimique, ce système est souvent utilisé pour illustrer les concepts de chaos déterministe et d'attracteurs étranges. Ses équations, bien que plus simples que celles du système de Lorenz, capturent néanmoins l'essence des comportements chaotiques, rendant le système de Rössler particulièrement utile pour l'analyse théorique et l'enseignement des dynamiques non linéaires.Les équations de ce système sont les suivantes :

$$\begin{cases} \dot{x} = -(y+z) \\ \dot{y} = x + ay \\ \dot{z} = b + z(x-c) \end{cases} \tag{1.8}$$

où :

— x, y, z est les variables d'état.

— a, b, c sont les paramètres du système de Rössler .

Le système de Rössler montre un comportement chaotique pour $a = 0.2, b = 5.7, c = 0.2$, avec les conditions initiales $x_0 = 0.1; y_0 = 0.1; z_0 = 0.1$.

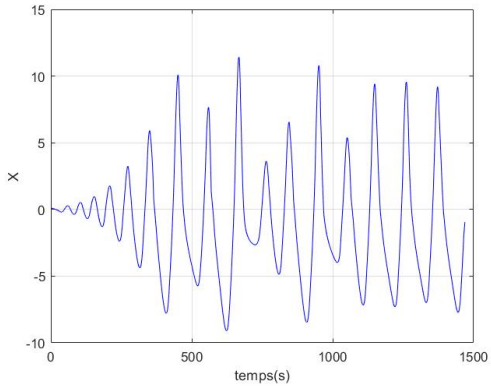

FIGURE 1.7 – Aspect aléatoire de l'état x du systéme de Rossler

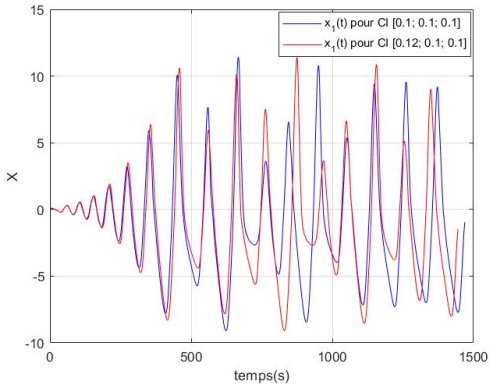

FIGURE 1.8 – Évolution dans le temps, pour deux conditions initiales très proches (sensibilité aux conditions initiales).

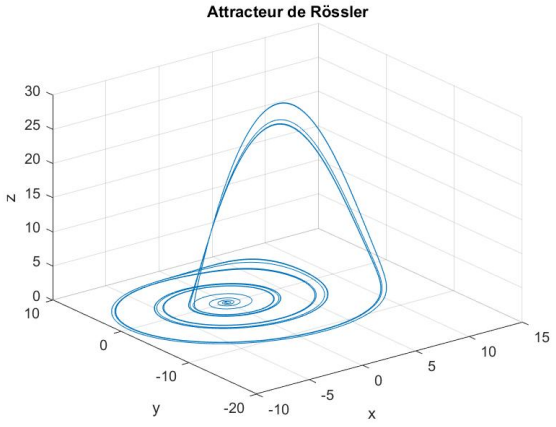

FIGURE 1.9 – Attracteur de Rössler

***Remarque :** La figure montre l'attracteur de Rössler, où les trajectoires, malgré des conditions initiales différentes, convergent et restent confinées dans une structure en spirale, illustrant la nature chaotique et imprévisible du système.

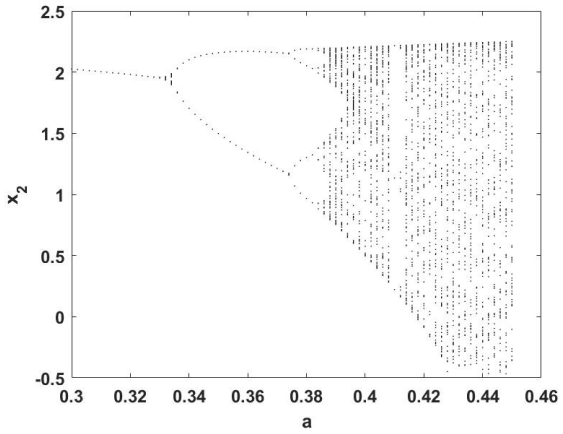

FIGURE 1.10 – Diagramme de bifurcation du système de Rössler.

***Remarque :** La figure montre le diagramme de bifurcation du système de Rössler, illustrant la transition du régime périodique au chaos à mesure que le paramètre de contrôle varie, soulignant la complexité croissante du système.

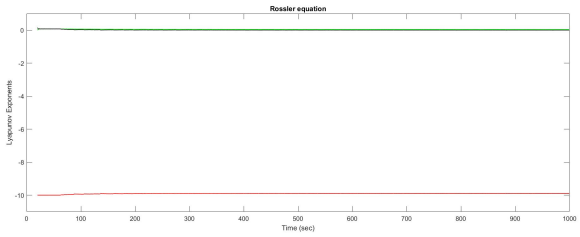

FIGURE 1.11 – Exposants de Lyapunov du système de Rössler.

***Remarque :** La figure montre que les exposants de Lyapunov du système de Rössler, avec $\lambda_1 = 0.039206$ (positif), $\lambda_2 = 0.0020676$ (proche de zéro), et $\lambda_3 = -9.8911$ (négatif), indiquent un comportement chaotique. Le système présente une divergence exponentielle des trajectoires, mais reste confiné dans une région limitée de l'espace des phases, confirmant la présence d'un attracteur étrange.

1.1.7 Cas discret :

Système de Hénon : Le système chaotique de Hénon est un exemple emblématique de la complexité que peut présenter un système dynamique non linéaire. Proposé par Michel Hénon en 1976, ce modèle se compose d'un ensemble d'équations itératives simples mais produisant des comportements extraordinaires. Les équations de Hénon sont les suivantes :

$$\begin{cases} x(k+1) = 1 - ax(k)^2 + y(k) \\ y(k+1) = bx(k) \end{cases} \tag{1.9}$$

où x et y représentent les coordonnées d'un point dans un espace bidimensionnel, et a et b sont des paramètres contrôlant le comportement du système. Ce modèle illustre comment de petites variations dans les conditions initiales peuvent conduire à des trajectoires complètement différentes, caractérisant ainsi le comportement chaotique.

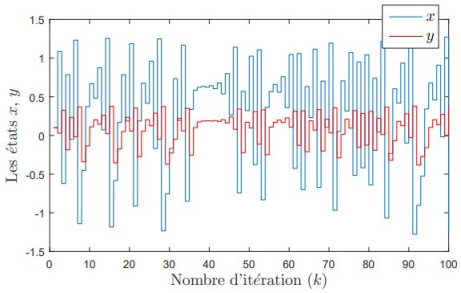

FIGURE 1.12 – Aspect aléatoire.

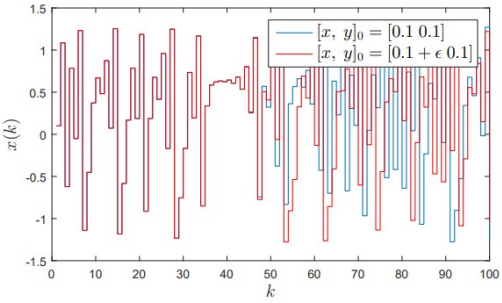

FIGURE 1.13 – Sensibilité aux conditions initiales de l'état x du système de Hénon.

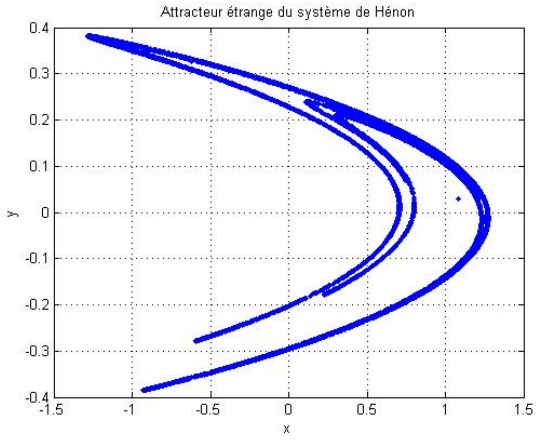

FIGURE 1.14 – Attracteur de Hénon.

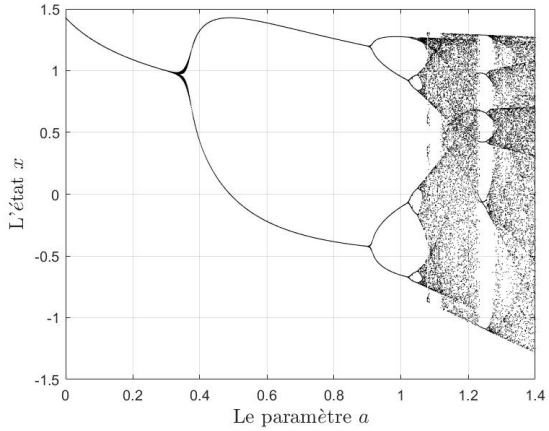

FIGURE 1.15 – Bifurcation de Hénon

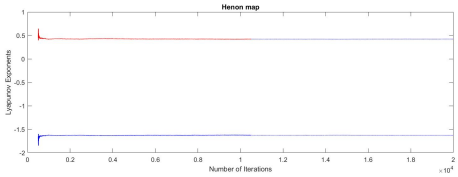

FIGURE 1.16 – Exposants de Lyapunov du système de Hénon.

La figure présente les exposants de Lyapunov du système de Rossler où λ_1 =0.42311, λ_2=-1.6271.

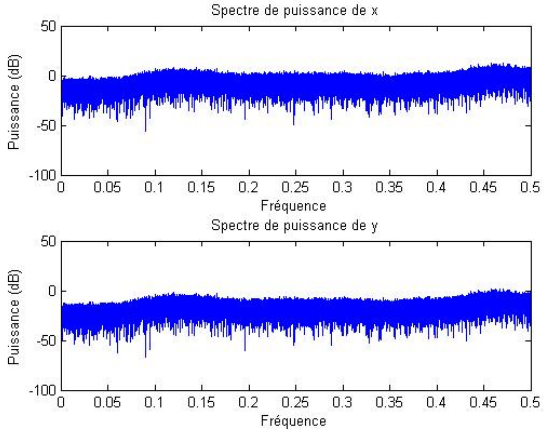

FIGURE 1.17 – Spectre de puissance des variable x et y du système de Hénon.

1.2 Conclusion :

L'étude des systèmes chaotiques dévoile un univers fascinant de dynamiques non linéaires, où de petites variations des conditions initiales peuvent entraîner des résultats totalement imprévisibles. Nous avons exploré les concepts clés du chaos, tels que la sensibilité aux conditions initiales, les attracteurs étranges, et les bifurcations, qui illustrent la complexité inhérente à ces systèmes. À travers les exemples des systèmes de Lorenz, Rössler, et Hénon, nous avons observé comment les paramètres et les conditions initiales influencent le comportement global des systèmes.

Nous avons également examiné les outils analytiques et numériques utilisés pour étudier le chaos, tels que les exposants de Lyapunov, les spectres de puissance, et les diagrammes de bifurcation. Ces outils permettent de quantifier et d'analyser le chaos, ainsi que d'observer les transitions vers des comportements chaotiques.

Le prochain chapitre abordera les analogies entre les systèmes cryptographiques et les systèmes chaotiques, ainsi que la synchronisation de ses derniers.

Chapitre 2

Cryptographie et synchronisation chaotique

2.1 introduction

Dans un monde de plus en plus numérique, la cryptographie est essentielle pour assurer la confidentialité, l'intégrité et l'authenticité des informations échangées. Les avancées récentes ont permis l'intégration des systèmes chaotiques dans les techniques cryptographiques, offrant de nouvelles perspectives pour la sécurité des communications. Ce chapitre explore l'intersection entre la cryptographie et la synchronisation chaotique, en examinant comment les propriétés uniques du chaos peuvent être exploitées pour renforcer la sécurité des échanges d'informations [8] [29].

Les systèmes chaotiques, détaillés dans le premier chapitre, sont caractérisés par une sensibilité extrême aux conditions initiales et un comportement apparemment aléatoire, rendant leur prédiction difficile sans une connaissance précise des conditions initiales. Ces propriétés sont particulièrement avantageuses pour la cryptographie, car elles permettent de générer des clés et des signaux de chiffrement complexes et robustes. De plus, la synchronisation chaotique, où deux systèmes chaotiques distincts évoluent de manière synchronisée sous certaines conditions, est une approche clé utilisée dans ces techniques.

Ce chapitre vise à approfondir la compréhension de la manière dont la cryptographie et la synchronisation chaotique peuvent être combinées pour développer des systèmes de communication à la fois sécurisés et efficaces.

2.2 Introduction á la cryptographie

L'échange de données, qu'il s'agisse de paroles, d'images ou de signaux, est devenu une nécessité fondamentale. Avec l'augmentation des échanges de données, la sécurité de ces opérations devient cruciale. Depuis l'époque de Jules César jusqu'à l'ère de l'informatique moderne, le chiffrement des messages est essentiel pour protéger les informations contre tout accès non autorisé et toute utilisation malveillante.

La cryptographie, étymologiquement "écriture secrète", est l'art de rendre les messages échangés entre deux entités via un canal non sécurisé incompréhensibles, sauf pour le destinataire légitime possédant la clé de déchiffrement. En parallèle, la cryptanalyse vise à déchiffrer ces messages ou à évaluer la robustesse des systèmes de chiffrement. Ces deux domaines, étudiés sous le terme de cryptologie, explorent les messages secrets.

Autrefois réservée aux militaires et aux services de renseignement, la cryptographie s'est démocratisée avec l'avènement des communications personnelles et la généralisation d'Internet. Aujourd'hui, avec la multiplication des transactions en ligne et l'utilisation croissante des réseaux publics, la sécurité est devenue essentielle. La cryptographie moderne offre des services cruciaux tels que l'intégrité des données, l'authentification des utilisateurs, l'identification des parties et la signature électronique, devenant ainsi un outil indispensable pour protéger les données sensibles.[40]

2.3 Principe de cryptographie :

Le concept de cryptographie peut être expliqué à l'aide d'un schéma représentatif illustré dans la figure ci dessous :

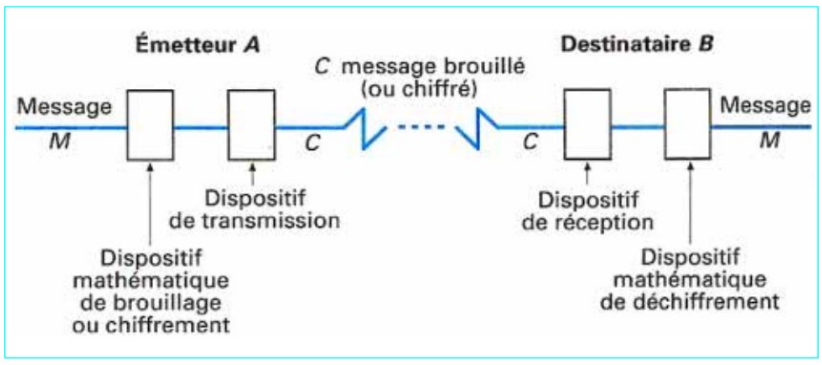

FIGURE 2.1 – Schéma général de la communication chiffrée entre un émetteur et un récepteur.

2.3.1 Terminologie

Cryptologie : La cryptologie est l'art de sécuriser les informations afin qu'elles ne soient accessibles qu'aux destinataires autorisés, que ce soit pour leur stockage ou leur transmission. Elle englobe à la fois la cryptographie, qui concerne le codage des informations, et la cryptanalyse, qui se concentre sur le décryptage des messages codés sans accès à la clé de cryptage.

Cryptographie : La cryptographie est le procédé consistant à rendre un message incompréhensible pour le protéger, en utilisant diverses techniques telles que les signes conventionnels, la modification de l'ordre ou de la disposition des signes, ainsi que le remplacement des signes. Ce processus est connu sous le nom de chiffrement ou cryptage. L'opération inverse, qui consiste à rendre le message chiffré à nouveau lisible en utilisant une clé spécifique appelée clé de déchiffrement, est appelée déchiffrement[8].

Cryptanalyse : Il s'agit de l'opposé de la cryptographie. La cryptanalyse consiste à étudier et à développer des techniques permettant de déchiffrer un message codé sans avoir accès à la clé de décryptage.

Cryptosystème : Un cryptosystème désigne l'ensemble des éléments impliqués dans le chiffrement et le déchiffrement de l'information. Il comprend l'espace de clés, c'est-à-dire toutes les combinaisons possibles de clés, ainsi que les textes en clair (les messages non chiffrés) et les textes chiffrés (les messages chiffrés) associés à un algorithme spécifique[8].

Cryptogramme : Message rendu inintelligible par une opération de cryptage.

Le déchiffrement : Le déchiffrement est l'action inverse du chiffrement, à condition que ce dernier soit réversible. En utilisant un algorithme cryptographique spécifique et la clé correspondante, il permet de restaurer le texte en clair à partir du texte chiffré.

Clé : Un élément crucial d'un algorithme de chiffrement ou de déchiffrement, sur lequel repose la confidentialité des données.

2.3.2 Principes de Kerckhoffs pour la cryptographie

Les systèmes cryptographiques civils actuellement en usage reposent sur plusieurs principes fondamentaux, dont ceux énoncés par Kerckhoffs dans son traité de cryptographie militaire. Parmi ces principes, celui qui revêt une importance particulière est que la sécurité d'un système ne doit pas reposer sur des éléments difficiles à modifier. En d'autres termes, aucun secret ne doit être incorporé dans l'algorithme lui-même, mais plutôt dans la clé utilisée. Cette approche

garantit qu'il serait pratiquement impossible de récupérer le texte en clair à partir du texte chiffré sans connaître la clé. Cependant, avec la connaissance de la clé, le déchiffrement peut être réalisé instantanément. Ce principe est l'un des six énoncés par Kerckhoffs et constitue un pilier essentiel de la sécurité cryptographique moderne [17].

- Une information codée ne doit en aucun cas pouvoir être déchiffrée sans la connaissance de sa clé.
- Les interlocuteurs ne doivent subir aucun dommage même si le système de codage est dévoilé.
- La clé doit être simple à utiliser et modifiable à souhait.
- Les cryptogrammes doivent être adaptés à la correspondance télégraphique.
- L'appareil de codage et les documents doivent être facilement transportables.
- Le système doit être simple d'utilisation.

2.3.3 Principe de Shannon pour la cryptographie

Le principe de Claude Shannon peut être considéré comme une reformulation de celui de Kerckhoffs. Ainsi, Shannon a énoncé que [6] [42] :

- Pour qu'un cryptosystème soit inconditionnellement sûr, la clé secrète doit être aussi longue que le texte clair, sinon tous les autres systèmes sont théoriquement cassables.
- La confusion doit dissimuler les structures algébriques et statistiques du texte.
- La diffusion doit permettre à chaque bit du texte clair d'influencer une grande partie du texte chiffré. Cela signifie que la modification d'un bit du bloc d'entrée doit entraîner la modification de nombreux bits du bloc de sortie correspondant.
- La sécurité pratique d'un cryptosystème repose sur le fait que la connaissance du message chiffré et de certains couples texte clair/texte chiffré ne permet pas de trouver ni la clé ni le texte clair en un temps humainement raisonnable.

Shannon a défini un cryptosystème comme étant un ensemble :

$$U = \{M, C, K\{E_k\}_{k \in K} \tag{2.1}$$

avec :

- M : représente l'ensemble des messages clairs.
- C : représente l'ensemble des messages chiffré.

— K : un espace de paramètres appelés clés cryptographiques.

— E_k : représente,pour tout $k \in K$, une transformation de chiffrement :
$M \xrightarrow{E_k} C$

— D_k : représente, pour tout $k \in K$,une transformation de déchiffrement.
$C \xrightarrow{E_k} M$

Pour tout message M, nous avons la propriété suivante :

$$D_{ko}E_k(M) = M \tag{2.2}$$

Ce modèle, à la fois simple, élégant et puissant, propose une description exhaustive de tous les systèmes de cryptographie modernes.

2.3.4 Objectifs de la cryptographie

En cryptographie, un système de communication sécurisé cherche à atteindre plusieurs objectifs pour assurer son efficacité. Ces objectifs peuvent être poursuivis simultanément ou individuellement selon les besoins de l'application. Voici une présentation des principaux objectifs de la cryptographie :

— **Confidentialité :** Préserver le caractère privé des données pour toute personne non autorisée à y accéder.

— **Intégrité :** Protéger les données contre toute altération non autorisée.

— **Authentification :** Établir le lien entre les données et leur source. L'authentification des entités garantit leur identité.

— **Non-répudiation :** Mécanisme qui établit de façon crédible que l'émetteur est bien l'auteur du message, évitant ainsi au destinataire de contester l'origine du message.

— **Signature :** Méthode visant à établir un lien entre les informations et une entité donnée, ou à prouver l'identité de cette entité.

— **Autorisation :** Permettre au propriétaire d'accorder la permission à quelqu'un d'effectuer une opération en son nom.

— **Contrôle d'accès :** Processus visant à empêcher l'utilisation non autorisée des ressources. Il contrôle les personnes autorisées à y accéder, les moments d'accès, les restrictions et conditions applicables, ainsi que le niveau d'autorisation accordé pour chaque accès.

2.4 Méthodes de Chiffrement

Les méthodes de chiffrement sont traditionnellement catégorisées en deux types distincts : le chiffrement classique et le chiffrement moderne. Le chiffrement classique repose sur l'utilisation des lettres et des caractères d'une langue donnée. Il utilise principalement des techniques de substitution et de transposition, modifiant l'ordre des caractères pour créer différents niveaux de difficulté. En revanche, le chiffrement moderne fait appel à des méthodes plus avancées, appelées algorithmes, rendues possibles par l'émergence de l'informatique. Ces algorithmes opèrent directement sur les bits, augmentant ainsi la complexité et la sécurité des systèmes de chiffrement. Cette évolution illustre l'adaptation des techniques de chiffrement aux progrès technologiques contemporains.

2.4.1 Chiffrement classique

Chiffrement par substitution Le chiffrement par substitution consiste à remplacer chaque caractère du texte clair par un autre caractère spécifique. Pour que le destinataire puisse lire le message, il doit appliquer la substitution inverse. La complexité de ces systèmes de substitution est déterminée par trois facteurs essentiels [40] :

— La composition spécifique de l'alphabet utilisé pour chiffrer ou communiquer.

— Le nombre d'alphabets utilisés dans le cryptogramme.

— La méthode spécifique de leur utilisation.

On distingue quatre types de chiffrement par substitution :

— **Substitutions mono-alphabétiques** : consistent à remplacer chaque lettre du message clair par une autre lettre ou un autre caractère.

— **Substitutions poly-alphabétiques** : consistent à remplacer chaque lettre du message clair par différentes lettres ou différents caractères selon des alphabets variés.

— **Substitutions polygrammiques** : à la différence des autres types de substitutions, elles consistent à chiffrer des groupes de lettres plutôt que des lettres individuelles.

— **Substitutions tomographiques** : commencent par des substitutions poly-alphabétiques, où chaque lettre est remplacée par plusieurs lettres ou symboles, puis ces groupes sont chiffrés séparément par des techniques de substitution ou de transposition.

Exemple :le chiffrement de César Le chiffrement de César est l'une des techniques de chiffrement les plus simples et anciennes. Elle consiste à décaler chaque lettre d'un certain nombre

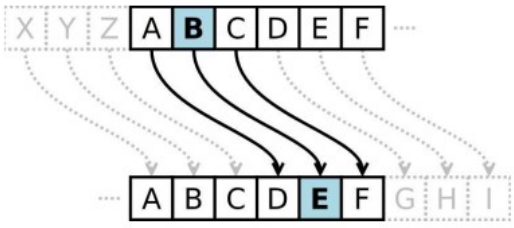

FIGURE 2.2 – Décalage de César.

de positions dans l'alphabet. Par exemple, avec un décalage de 3, "A" deviendrait "D", "B" deviendrait "E", et ainsi de suite, lexemple suivant illustre cela :
message clair : MASTER CVPE.
message chiffré : PDVWHU FYSH.
Pour déchiffrer un message, on applique simplement le décalage dans l'autre sens. Cependant, le chiffrement de César est très vulnérable aux attaques par force brute, car il y a seulement 25 décalages possibles avec un alphabet de 26 lettres.

2.4.1.2 Chiffrement par transposition Le chiffrement par transposition implique de réorganiser les caractères d'un message selon un schéma spécifique, plutôt que de les remplacer par d'autres caractères comme dans le chiffrement par substitution. Ainsi, le message chiffré conserve les mêmes caractères que le message clair, mais leur ordre est modifié selon une méthode particulière. Il existe diverses techniques de chiffrement par transposition, chacune utilisant des méthodes distinctes pour réorganiser les caractères :

- **Transposition simple par colonnes**
- **Transposition complexe par colonnes**
- **Transposition par carré polybique**

2.4.2 Chiffrement moderne

2.4.2.1 Cryptographie à clé secrète (symétrique) La cryptographie symétrique, également connue sous le nom de cryptographie conventionnelle ou de chiffrement à clé secrète, est un type de cryptosystème où une seule clé est utilisée à la fois pour le chiffrement et le déchiffrement des données. Cette clé est préalablement choisie par l'émetteur et le récepteur, et elle doit être gardée secrète, car la sécurité des algorithmes repose sur celle-ci.

Le principal défi du chiffrement symétrique réside dans la préservation du secret de la clé.

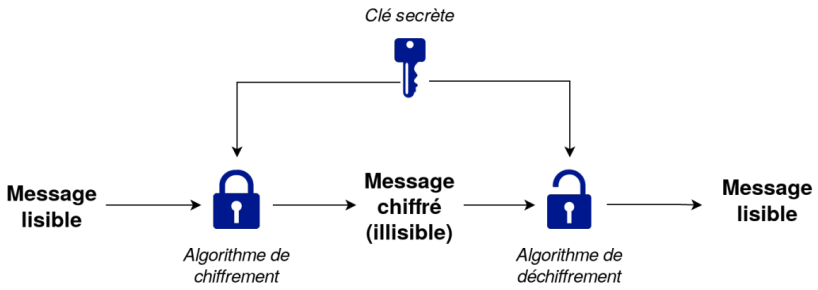

FIGURE 2.3 – schéma du chiffrement symétrique.

Ainsi, le processus de sélection et de transmission de la clé doit être hautement sécurisé. Un autre défi survient lorsqu'un grand nombre de personnes souhaitent communiquer simultanément, ce qui entraîne une multiplication du nombre de clés nécessaires pour chaque paire de communicateurs. Cela pose alors un problème de gestion des clés.

2.4.2.2 Chiffrement par blocs (block cipher) Le chiffrement par blocs consiste à diviser les données en blocs de taille fixe, généralement une puissance de 2. Chaque bloc est ensuite chiffré individuellement. La taille des blocs influence à la fois la sécurité et la complexité : des blocs plus grands offrent une meilleure sécurité mais sont plus difficiles à implémenter.Il est également recommandé d'utiliser une clé suffisamment longue pour minimiser les coûts de réalisation. Le chiffrement par blocs peut être utilisé pour obtenir le même résultat qu'un chiffrement par flux. Mathématiquement, le chiffrement par flux est plus simple à analyser. La majorité des applications cryptographiques symétriques basées sur les réseaux utilisent des chiffrements par blocs. L'idée générale du chiffrement par blocs est la suivante :

1. Convertir les caractères en code binaire.
2. Diviser cette chaîne binaire en blocs de longueur fixe.
3. Chiffrer chaque bloc en combinant chaque bit avec la clé.
4. Permuter certains bits du bloc.
5. Répéter les étapes 3 et 4 un certain nombre de fois, formant une ronde.
6. Passer au bloc suivant et reprendre à l'étape 3 jusqu'à ce que tout le message soit chiffré.

2.4.2.3 Chiffrement par flux Le chiffrement par flux crypte les données numériques en traitant un bit ou un octet à la fois. Ses principaux avantages résident dans sa capacité à

modifier la méthode de chiffrement pour chaque symbole du texte en clair, ainsi que dans sa grande rapidité. De plus, il se révèle particulièrement utile dans des environnements sujets à des erreurs fréquentes, car il prévient la propagation de ces erreurs. Si le flux de clé cryptographique est aléatoire, ce type de chiffrement est incassable, sauf si le flux de clé est intercepté. Cependant, ce flux de clé doit être distribué préalablement aux deux utilisateurs via un canal indépendant et sécurisé, ce qui peut poser des problèmes logistiques insurmontables lorsque le volume de données à chiffrer est très important. Par conséquent, pour des raisons pratiques, le générateur de flux binaire est généralement implémenté comme une procédure algorithmique, permettant aux deux utilisateurs de produire le même flux de bits cryptographiques. La structure d'un chiffrement par flux repose sur un générateur de clés produisant une séquence de clés K_1, K_2, ..., K_i. La sécurité du chiffrement dépend de la qualité de ce générateur. Par exemple, si K_i est toujours égal à 0 pour tout i, alors M est égal à C. En revanche, si la séquence des clés K_i est infinie et complètement aléatoire, on obtient un One-Time Pad. En pratique, on utilise souvent une séquence pseudo-aléatoire, qui se situe entre ces deux extrêmes. En ce qui concerne la propagation des erreurs, une erreur dans C_i n'affecte qu'un seul bit de M_i, mais la perte ou l'ajout d'un bit dans C_i affecte tous les bits suivants de M après déchiffrement. Le générateur de clés peut être considéré comme une machine à états finis. Un exemple typique de ce type de générateur est le registre à décalage à rétroaction (FSR, Feedback Shift Register).

2.4.2.4 Algorithme de chiffrement DES Le DES (Data Encryption Standard) est un algorithme de chiffrement utilisant une clé de 56 bits pour sécuriser des blocs de données de 64 bits. Il effectue une série d'étapes, notamment une permutation initiale, 16 itérations de transformations basées sur la clé, un échange de moitiés de bloc et une permutation inverse pour obtenir le texte chiffré. Les clés restent les mêmes pour chaque bloc, et l'algorithme peut chiffrer jusqu'à 1 Go de données par seconde, ce qui en fait une option efficace pour sécuriser les données. Les avantages de l'algorithme DES comprennent un niveau élevé de sécurité, une spécification complète et une facilité de compréhension, une dépendance à l'algorithme lui-même pour la sécurité, et l'utilisation d'une clé relativement petite de 56 bits, qui simplifie son implémentation tout en offrant une sécurité adéquate [40].

2.4.3 La cryptographie a clé publique (asymétrique) Le chiffrement asymétrique résout le problème du partage de clé secrète du chiffrement symétrique en utilisant une paire de clés

complémentaires : une clé privée pour décoder et une clé publique pour encoder. La clé publique est disponible sur un serveur authentifié, permettant aux expéditeurs d'envoyer des messages sécurisés sans avoir besoin de transmettre physiquement la clé. Cependant, les clés asymétriques sont beaucoup plus longues que celles du chiffrement symétrique, nécessitant généralement des clés d'au moins 4096 bits pour assurer une sécurité à long terme. Ces méthodes reposent sur la complexité de problèmes mathématiques difficiles à résoudre, tels que la factorisation d'entiers ou le calcul de logarithmes discrets.

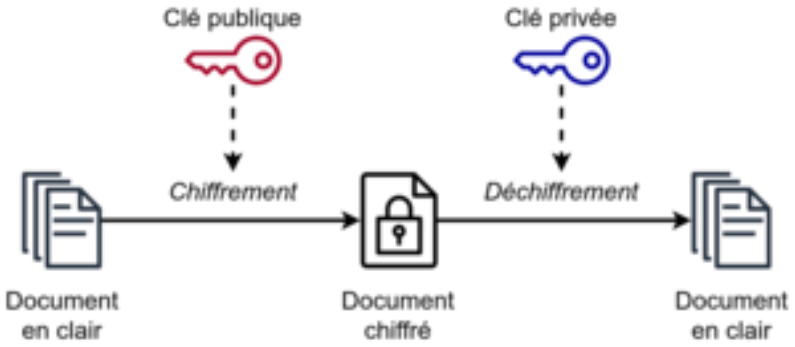

FIGURE 2.4 – Principe de chiffrement asymétrique

Les principaux algorithmes asymétriques à clé publique les plus utilisés sont :

— RSA

— DSA

— Diffie-Hellman

2.5 Cryptographie chaotique

Principe : La cryptographie chaotique, développée au cours de la dernière décennie, répond aux exigences de sécurité tout en offrant une grande résistance à la cryptanalyse. Elle conserve également les attributs nécessaires aux algorithmes de chiffrement traditionnels. Il existe deux types de fonctions chaotiques : celles au comportement purement chaotique, qui ne sont pas modélisables, et les fonctions chaotiques déterministes, qui peuvent être modélisées par des systèmes dynamiques non linéaires. Ce sont ces dernières qui sont utilisées en cryptographie chaotique, car leurs attracteurs fractals rendent les trajectoires totalement dépendantes des conditions initiales, ce qui rend leur prévision impossible sans connaître ces conditions initiales.

Cela assure une sécurité quasi totale. Pour les utiliser en chiffrement, il faut d'abord choisir une fonction chaotique, puis superposer le signal chaotique au flux de données à transmettre selon une technique de cryptage par chaos appropriée.

2.6 Techniques de cryptage par chaos

2.6.1 Cryptage par clé

Le cryptage chaotique par clé utilise les propriétés imprévisibles des systèmes chaotiques pour générer des clés de chiffrement robustes et sécurisées. Ces clés, sensibles aux conditions initiales, rendent le cryptage difficile à décrypter sans une connaissance précise des paramètres initiaux.

***Cryptage par commutation** Cette technique est réservée aux messages prenant un nombre fini de valeurs. L'émetteur utilise deux ou plusieurs systèmes chaotiques. Ces systèmes peuvent partager le même modèle dynamique avec des paramètres différents, ou bien avoir des modèles dynamiques totalement distincts [6] [20]. La figure ci-dessous illustre cette méthode de cryptage.

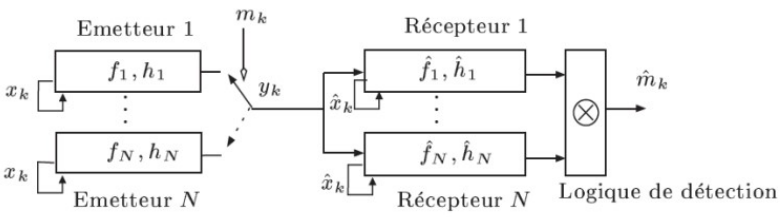

FIGURE 2.5 – Cryptage par commutation

À chaque symbole m_k de l'information correspond un signal y_k issu d'un système chaotique $\sum_K$ défini par :

$$\begin{cases} x_{k+1} = f_i(x_k) \\ y_{k+1} = f_i(x_k) \end{cases} \tag{2.3}$$

avec $i \in \{1, \ldots, N\}$ et $x_k \in \mathbb{R}^n$.

Le rôle du récepteur est de détecter le signal de sortie y_k émis par l'émetteur. Par conséquent, il est composé d'autant de systèmes que l'émetteur.

$$\begin{cases} \hat{x}_{k+1} = \hat{f}_i(\hat{x}_k) \\ \hat{y}_k = \hat{h}_i(\hat{x}_k) \end{cases} \tag{2.4}$$

$i = 1, \ldots, N$.

La détection peut être cohérente ou non cohérente. Dans le premier cas, une synchronisation d'un seul système du récepteur est effectuée pour pouvoir reconstruire ensuite l'information m_i associée à l'aide d'une logique de détection. Dans le cas de détection non cohérente, nous utilisons les outils statistiques basés sur la corrélation entre les signaux y_k et $\hat{y}_k$.

2.6.2 Cryptage par message

Le cryptage chaotique par message exploite la dynamique des systèmes chaotiques pour encoder directement les messages. Cette méthode encode les informations en les intégrant dans des signaux chaotiques, rendant le message difficilement déchiffrable sans synchronisation avec le système chaotique utilisé.

2.6.2.1 Cryptage par addition Cette méthode est la première à utiliser la synchronisation chaotique. Le concept repose sur l'observation des signaux chaotiques. Le principe est simple : il suffit d'ajouter directement le signal informationnel $u(t)$ au signal chaotique $Cx(t)$ et de le récupérer ensuite par synchronisation chaotique. Le même système est utilisé à la fois à l'émetteur et au récepteur, avec la différence que le récepteur est contrôlé par le signal émis pour obtenir la synchronisation.

Au niveau du récepteur, après synchronisation avec le signal reçu, le message original est récupéré par une simple soustraction. Par conséquent, un intrus ne soupçonnera pas qu'un message est transmis, même s'il intercepte le signal $y(t)$ (porteuse chaotique plus message), et il ne cherchera donc pas à appliquer des techniques de décryptage.

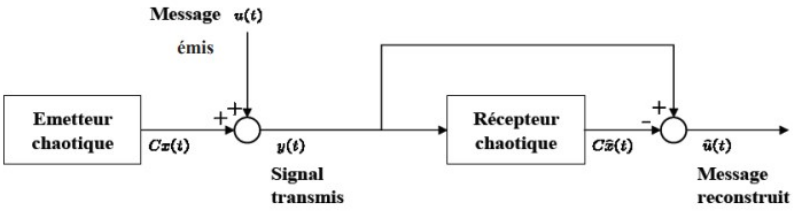

FIGURE 2.6 – cryptage par addition

Le principal avantage de cette méthode réside dans la simplicité du cryptage. Cette technique

peut être appliquée aussi bien à des messages continus qu'à des messages discrets. Cependant, pour garantir une synchronisation correcte, le message doit être au moins 20 à 30 dB en dessous du niveau de sortie de l'émetteur. En présence d'un bruit de canal d'une puissance similaire à celle du message, la détection de l'information devient difficile. De plus, cette méthode est vulnérable aux attaques extérieures et l'utilisation du canal de transmission est inefficace en termes d'énergie transmise par rapport à la qualité de l'information fournie.

2.6.2.2 Cryptage par modulation paramétrique L'approche de la modulation paramétrique implique l'utilisation du message contenant l'information pour moduler un ou plusieurs paramètres θ de l'émetteur chaotique. Un contrôleur adaptatif est chargé de maintenir la synchronisation au niveau du récepteur tout en suivant les changements du paramètre modulé. Le schéma correspondant est illustré à la figure (2.7)[6].

Au niveau de l'émetteur, la modulation d'un (ou plusieurs) paramètre(s) entraîne un changement continu de l'attracteur de la trajectoire. En conséquence, le signal transmis est plus complexe qu'un signal chaotique "normal". Cependant, la méthode d'injection du message et donc la fonction de démodulation des paramètres ne doivent pas supprimer le caractère chaotique du signal envoyé au récepteur.

Cette approche exploite intégralement les particularités et les caractéristiques des systèmes chaotiques, la distinguant ainsi clairement des méthodes de communication conventionnelles.

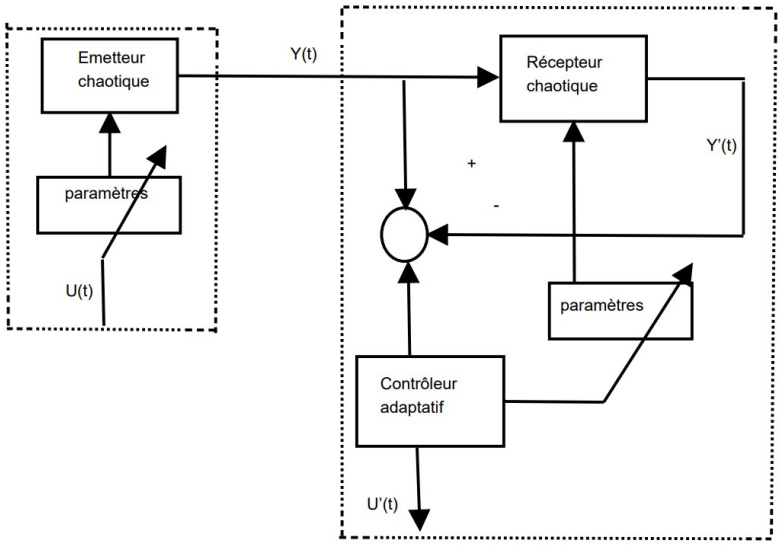

FIGURE 2.7 – Cryptage par modulation paramétrique

2.6.2.3 Cryptage par inclusion Cette technique de chiffrement implique l'intégration du message dans le flux dynamique de l'émetteur. La récupération de l'information se réalise principalement par deux méthodes : l'utilisation d'observateurs à entrées inconnues ou l'inversion du système émetteur. Cette approche présente de multiples avantages et demeure largement employée en pratique.

Observateurs a entrées inconnues : Le schéma de la figure (2.8) illustre un problème classique d'estimation d'état non linéaire à entrées inconnues :
La reconstruction de l'état $x(t)$ du système émetteur, ainsi que de l'entrée inconnue $m(t)$, est es-

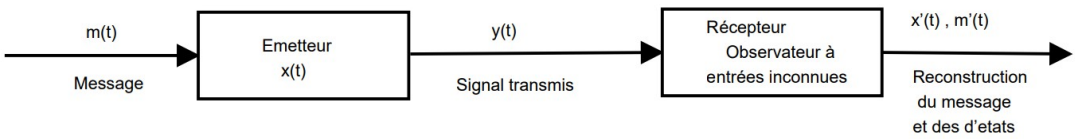

FIGURE 2.8 – Observateur à entrée inconnue

sentielle. Diverses méthodes de conception d'observateurs à entrées inconnues ont été examinées dans la littérature et peuvent être exploitées dans le contexte du décryptage. Plusieurs travaux de recherche ont utilisé ces observateurs pour déchiffrer les informations transmises.

Décryptage par inversion : Cette technique de cryptage par inclusion implique de retourner le modèle de l'émetteur pour obtenir celui du récepteur.

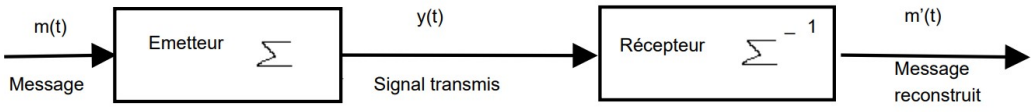

FIGURE 2.9 – Décryptage par inversion

2.7 Synchronisation chaotique

2.7.1 Introduction

Dans le domaine de l'étude des systèmes chaotiques, où l'imprévisibilité est une caractéristique intrinsèque, le concept de contrôle du chaos émerge comme crucial. Toutefois, il est fascinant de constater que cette imprévisibilité peut être transformée en une opportunité inattendue. En effet, cette propriété chaotique peut être exploitée pour créer des schémas de communication hautement sécurisés. Ces efforts reposent sur l'utilisation des techniques de synchronisation du chaos, ouvrant ainsi la voie à une nouvelle dimension dans les communications sécurisées[2].

2.7.2 Définition

Les phénomènes de synchronisation impliquent l'interaction de deux systèmes identiques qui peuvent être couplés de manière à ce que la solution d'un système converge toujours vers celle de l'autre, indépendamment des conditions initiales et des paramètres. Cependant, même si un système répond à l'autre, la réciprocité n'est pas toujours présente [1]. L'une des configurations les plus populaires est la configuration maître-esclave, dans laquelle un système dynamique, appelé système esclave, suit le rythme et la trajectoire imposés par un autre système dynamique, appelé système maître. Ainsi, nous pouvons donner la définition suivante [19] :
on dit qu'un système est esclave :

$$\dot{x}_s = f_s(x_s), \quad x_s \in \mathbb{R}^n \tag{2.5}$$

se synchronise avec un système maitre :

$$\dot{x}_m = f_m(x_m), \quad x_m \in \mathbb{R}^n \tag{2.6}$$

si pour toutes paires de conditions initiales (xm(0), xs(0)),

$$\lim_{t\to\infty} |\mathbf{x_s}(t) - \mathbf{x_m}(t)| = 0. \tag{2.7}$$

avec :

x_s : est l'état du système esclave.

x_m : est l'état du système maître.

2.7.3 Régimes de synchronisation

il existe différents régimes de synchronisation, nous allons citer dans cette partie les principales caractéristiques de ces derniers.

2.7.3.1 Synchronisation complète La synchronisation identique, aussi appelée synchronisation complète, est la forme la plus élémentaire de synchronisation entre des systèmes chaotiques couplés. Elle se caractérise par la reproduction précise des trajectoires de deux systèmes chaotiques après une période transitoire, grâce à un signal de couplage unidirectionnel. Ce type de synchronisation garantit que les systèmes demeurent en phase au fil du temps [36].

2.7.3.2 Synchronisation généralisée La synchronisation généralisée se produit lorsque deux systèmes chaotiques, appelés le système maître et le système esclave, présentent une relation fonctionnelle entre leurs états à long terme. Plus précisément, avec un couplage suffisamment fort, il peut exister une fonction $\mathbf{F}$ telle que l'état du système récepteur $\mathbf{x}_s(t)$ converge vers la transformation $\mathbf{F}(\mathbf{x}_m(t))$ de l'état du système émetteur $\mathbf{x}_m(t)$. Mathématiquement, cela se traduit par :

$$\lim_{t\to\infty} |\mathbf{x}_s(t) - \mathbf{F}(\mathbf{x}_m(t))| = 0.$$

Cela signifie que, bien que les états des deux systèmes ne coïncident pas exactement, ils deviennent de plus en plus proches, modulés par la fonction $\mathbf{F}$, à mesure que le temps t tend vers l'infini. La synchronisation complète est un cas particulier où $\mathbf{F}$ est l'identité, entraînant une synchronisation parfaite des états des deux systèmes.

— $\mathbf{x}_s(t)$: État du **système récepteur** (ou esclave) à l'instant t, influencé par le système émetteur via le couplage.
— $\mathbf{x}_m(t)$: État du **système émetteur** (ou maître) à l'instant t, qui guide le système récepteur à travers le couplage.
— $\mathbf{F}$: Fonction qui relie les états des deux systèmes. Elle transforme l'état du système émetteur $\mathbf{x}_m(t)$ pour le rapprocher de l'état du système récepteur $\mathbf{x}_s(t)$ en cas de synchronisation.

2.7.3.3 Synchronisation projective c'est une autre forme spéciale de la synchronisation généralisée, elle est établie s'il existe une fonction linéaires simple $F(x) = \pi x$ telle que [36] :

$$\lim_{t\to\infty} |\pi x_m(t) - \mathbf{x_s}(t)| = 0. \tag{2.8}$$

ou ces deux systèmes sont amenés à aligner leurs trajectoires dans un espace de référence commun, appelé espace projeté.

avec :

π : Représente la fonction de projection qui associe l'état du système émetteur $\mathbf{x}_m(t)$ à une forme qui est censée être similaire à l'état du système récepteur $\mathbf{x}_s(t)$ lorsqu'ils sont synchronisés.

2.7.3.4 Synchronisation retardée La synchronisation retardée se produit lorsqu'il y a un faible couplage entre deux systèmes chaotiques non identiques, où les variables dynamiques des deux systèmes convergent vers un même point, mais avec un décalage temporel. Ce phénomène se produit lorsque les variables d'état $x_s(t)$ du système chaotique esclave convergent vers les variables d'état $x_m(t)$ du système chaotique maître, mais avec un retard temporel. Ainsi, les états du système esclave convergent vers les états passés du système maître selon la relation suivante [36] :

$$\lim_{t\to\infty} |\mathbf{x_s}(t) - \mathbf{x_m}(t-\tau)| = 0. \tag{2.9}$$

avec :

$x_m(t)$:est l'état du système maître.

$x_s(t)$:est l'état du système esclave.

τ :est un retard positif.

2.7.3.5 Synchronisation de phase La synchronisation de phase entre un système maître et un système esclave est atteinte lorsque les phases ϕ_1 et ϕ_2 de ces deux systèmes peuvent être considérées comme équivalentes dans une certaine marge d'erreur.Cela signifie qu'il existe deux nombres entiers m et n, et un petit nombre positif ϵ, tels que [36] :

$$|\phi_1 - m \cdot \phi_2| < \varepsilon \tag{2.10}$$

la phase du système esclave converge vers celle du système maître mais leurs amplitudes peuvent ne pas être les mêmes.

2.7.4 Modes de synchronisation

D'une manière globale, l'ensemble des méthodes de synchronisation peuvent être classées selon deux modes distincts, définis par la relation entre le système maître et le système esclave.

2.7.4.1 Synchronisation par couplage unidirectionnel Dans la synchronisation unidirectionnelle, la rétroaction est appliquée de manière unilatérale, ciblant spécifiquement l'un des deux systèmes impliqués dans le processus de synchronisation, comme illustré dans la figure suivante :

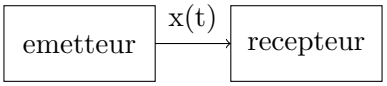

FIGURE 2.10 – Schéma de couplage unidirectionnel

2.7.4.2 Synchronisation par couplage bidirectionnel La synchronisation bidirectionnelle implique que deux systèmes disposent d'une boucle de rétroaction simultanée, appliquée simultanément à chaque système. Cela est illustré dans la figure ci-dessous :

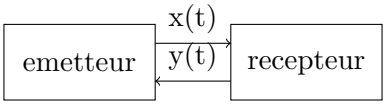

FIGURE 2.11 – Schéma de couplage bidirectionnel

2.7.5 Synchronisation à base d'observateurs

Précédemment, nous avons exploré la notion de synchronisation chaotique basée sur la commande, reposant sur la distinction entre un système maître et un système esclave. À présent, nous allons nous pencher sur une autre approche, celle de la synchronisation basée sur les observateurs, ou le maitre est un système chaotique et l'esclave est un observateur.

2.7.5.1 observabilité : Avant d'entreprendre la conception d'un observateur pour un système dynamique, il est important et nécessaire de s'assurer que l'état de ce dernier peut être estimé

à partir des informations d'entrée et de sortie, soit le système suivant :

$$\begin{cases} \dot{x} = Ax + Bu \\ y = Cx + Du \end{cases} \tag{2.11}$$

où A, B, C et D sont respectivement des matrices constantes

L'équation d'état (8) est dite observable si, pour tout état initial $x(0)$ inconnu, il existe un temps fini $t1 > 0$ tel que la connaissance de l'entrée u et de la sortie y sur l'intervalle [0, t1] suffise à déterminer de manière unique l'état initial $x(0)$. Sinon, l'équation est dite non observable [5].

2.8.5.2 Observabilité des systèmes linéaires : Pour un système linéaire parfaitement connu, où l'entrée $u(t)$ est donnée et la matrice B n'est pas impliquée dans les critères d'observabilité, l'analyse de l'observabilité peut être réduite à l'étude de la paire (A, C) [5].

Soit la matrice d'observabilité définie par :

$$O(A, C) = \begin{bmatrix} C \\ CA \\ CA^2 \\ \vdots \\ CA^{n-1} \end{bmatrix} \tag{2.12}$$

On dit qu'un système linéaire est observable si rang $O(A, C) = n$.

Avec : n dimension du système.

2.7.5.3 Observateurs linéaires : Dans la plupart des cas, la dimension du vecteur d'état est supérieure celle du vecteur de sortie ($l < n$). Ainsi, à un instant t donné, le vecteur $x(t)$ ne peut être pleinement mesuré ou déduit des sorties. Cependant, dans certaines circonstances, il est possible de reconstruire l'état à l'aide d'un observateur. Une conception habile de cet observateur devrait permettre une estimation précise et rapide des composantes du vecteur d'état $x(t)$.

Soit, de façon plus générale, le système dynamique SYS défini par :

$$SYS : \begin{cases} \dot{x}(t) = Ax(t) + Bu(t) \\ y(t) = Cx(t) \end{cases} \tag{2.13}$$

dont l'état $x(t)$ est estimé (ou reconstruit) par un système dynamique appelé observateur et noté OBS, dont la structure est donnée par :

$$OBS : \begin{cases} \dot{\hat{x}}(t) = A\hat{x}(t) + Bu(t) + Ly(t) \\ y(t) = C\hat{x}(t) + Dy(t) \end{cases} \tag{2.14}$$

Avec $x(t) \in \mathbb{R}^n$, $u(t) \in \mathbb{R}^m$ et $y(t) \in \mathbb{R}^l$ représentant respectivement l'état, l'entrée et la sortie du système. $\hat{x}(t) \in \mathbb{R}^n$ est le vecteur d'état de l'observateur, conçu pour que $\hat{x}(t)$ tende asymptotiquement vers $x(t)$ (l'état réel du système). La sortie $y(t)$ représente la sortie du système observateur.

Le système dynamique constituant l'observateur doit assurer que l'erreur de reconstruction, définie par $e(t) = x(t) - \hat{x}(t)$, tende asymptotiquement vers 0, soit [14] :

$$\lim_{t \to \infty} e(t) = x(t) - \hat{x}(t) = 0 \tag{2.15}$$

2.7.5.4 Observateur de Luenberger : La théorie de l'Observateur de Luenberger repose fondamentalement sur l'utilisation de méthodes de positionnement des pôles, visant à concevoir un observateur permettant une estimation précise de l'état interne d'un système donné.

$$\begin{cases} \dot{\hat{x}}(t) = A\hat{x}(t) + Bu(t) + L(y(t) - \hat{y}(t)) \\ \hat{y}(t) = C\hat{x}(t) \end{cases} \tag{2.16}$$

$\hat{y}(t)$ représente la sortie estimée. Le facteur L est le gain de l'observateur. Définissons l'erreur d'estimation sur l'état par :

$$e_x(t) = x(t) - \hat{x}(t) \tag{2.17}$$

2.8.5.5 Observateurs non linéaire : On considère le système non linéaire :

$$\begin{cases} \dot{x} = f(x,u) \\ y = h(x,u) \end{cases} \tag{2.18}$$

ou $f : \mathbb{R}^n \times \mathbb{R}^m \to \mathbb{R}^n$ et $h : \mathbb{R}^n \times \mathbb{R}^m \to \mathbb{R}^p$

Indistinguabilité : Soient $y_u^0(t)$ et $y_u^1(t)$ deux signaux de sortie générés par l'application du signal d'entrée $u(t)$ au système **(2.15)** avec les conditions initiales x^0 et x^1. Ils sont indistinguables si :

$$y_u^0(t) = y_u^1(t), \quad \forall t \geq 0, \quad \text{pour toute entrée } u.$$

Dans le cas contraire, on dit que x^0 et x^1 sont distinguables.

Observabilité : Le système **(2.15)** est dit observable en x^0 si x^0 est distinguable de tout $x \in \mathbb{R}^n$. De plus, le système **(2.15)** est observable si pour tout $x^0 \in \mathbb{R}^n$, x^0 est distinguable.

Pour cela, considérons h une fonction C^∞ de $\mathbb{R}^n$ dans $\mathbb{R}$. Nous définissons la dérivée de Lie dans la direction de f, notée $L_f(h)$, comme la dérivée de h le long de la courbe intégrale de f en $t = 0$.

$$L_f h(x) = \sum_{i=1}^{n} f_i(x) \frac{\partial h}{\partial x_i}(x) \tag{2.19}$$

Par définition on écrit :

$$L_f^0 h = h \text{ et } L_f^k h = L_f(L_f^{k-1} h), \quad \forall k \geq 1.$$

avec :

$$f(x) = \begin{pmatrix} f_1(x) \\ f_2(x) \\ \vdots \\ f_n(x) \end{pmatrix} \tag{2.20}$$

Le système **(2.15)** doit satisfaire la condition du rang d'observabilité [5], c'est-à-dire que $\text{rang}(O) = n$, où n représente le nombre d'états du système. La matrice d'observabilité O est définie comme :

$$O = \begin{pmatrix} dh \\ dL_f h \\ \vdots \\ dL_f^{n-1} h \end{pmatrix}$$

où dh représente la différentielle de la sortie h, et $L_f h$ désigne la dérivée de Lie de h le long du champ de vecteurs f. Le système est observable si et seulement si la matrice O a un rang égal à n.

exemples d'observateurs non linéaires Dans le cas des observateurs non linéaires, on peut citer l'observateur de Luenberger étendue et le filtre de Kalman étendu.

2.8 conclusion :

La sécurisation des communications et le cryptage représentent des domaines d'application prometteurs pour les systèmes chaotiques. La cryptographie chaotique offre plusieurs schémas possibles, chacun déterminant la méthode d'intégration du message lors de sa transmission. Ce chapitre explore les concepts de cryptographie et de transmission de données, en présentant les méthodes de chiffrement à clé privée et à clé publique, ainsi que le chiffrement basé sur le chaos, qui exploite les propriétés du comportement chaotique pour assurer une transmission sécurisée de données confidentielles. En examinant l'importance de la synchronisation chaotique dans le contexte de la transmission de données, nous avons étudié différents régimes et méthodes de synchronisation, y compris la synchronisation basée sur des observateurs. Cette exploration a mis en lumière leur contribution remarquable à la transmission de données.

Chapitre 3

Systèmes chaotiques d'ordre fractionnaire

3.1 Introduction

Le calcul fractionnaire, qui traite de la différenciation et de l'intégration d'ordres non entiers, remonte presque aussi loin que le calcul conventionnel. Des mathématiciens éminents tels que Leibniz, L'Hôpital, Jacob Bernoulli, Euler, Laplace et Fourier ont exploré ces idées, introduisant notamment la fonction Gamma d'Euler pour généraliser la factorielle. Euler a ainsi observé que la formule pour la dérivée n-ième d'une fonction puissance a du sens même lorsque l'ordre de la dérivée n n'est pas entier. Dans son article consacré à la généralisation du problème de la tautochrone et publié en 1823, Abel a introduit à la fois les intégrales fractionnaires, appelées aujourd'hui intégrales fractionnaires de Riemann-Liouville, et les dérivées fractionnaires, appelées aujourd'hui dérivées fractionnaires de Caputo. La dérivée et l'intégrale d'ordre fractionnaire offrent un excellent outil pour la description de la mémoire et des processus dynamiques.

3.2 Théorie de la dérivation non entière

3.2.1 Calcul fractionnaire

Un système fractionnaire est un système dynamique dont l'évolution est décrite par des équations intégrales-différentielles impliquant des opérateurs de dérivées et d'intégrales d'ordres non entiers. Ces systèmes se caractérisent par des comportements complexes et non linéaires,

souvent influencés par des phénomènes de mémoire à long terme, des dépendances non locales et des interactions à longue portée. L'opérateur intégral-différentiel ${}_aD_t^\alpha$ est un opérateur linéaire agissant sur une fonction, résultant de la composition d'un opérateur intégral et d'un opérateur différentiel. Cet opérateur est défini comme suit [18] :

$$ {}_aD_t^\alpha = \begin{cases} \frac{d^\alpha}{dt^\alpha} & \text{si } \alpha > 0 \\ 1 & \text{si } \alpha = 0 \\ \int_t^1 (d\tau)^{-\alpha} & \text{si } \alpha < 0 \end{cases} \tag{3.1} $$

Où :

Les bornes de l'opération sont a et t, et son ordre est $\alpha \in \mathbb{R}$.

3.2.2 Fonctions spécifiques à la dérivation fractionnaire

Ces fonctions sont les fondements essentiels du calcul fractionnaire :

La fonction Gamma La fonction gamma, notée $\Gamma(z)$, est définie par l'intégrale [43] :

$$ \Gamma(z) = \int_0^\infty e^{-t} t^{z-1} dt \tag{3.2} $$

Où : $z \in \mathbb{C}; \Gamma(z)$ est une fonction monotone et strictement décroissante pour $0 \prec z \leq 1$.

Une propriété importante de $\Gamma(z)$ est la relation de récurrence suivante :

$$ \Gamma(z+1) = z\Gamma(z) \tag{3.3} $$

qu'on peut démontrer par une intégration par parties :

$$ \Gamma(z+1) = \int_0^\infty t^z e^{-t} dt = \left[-t^z e^{-t}\right]_0^\infty + z \int_0^\infty t^{z-1} e^{-t} dt = z\Gamma(z) \tag{3.4} $$

et en particulier :

- La fonction Gamma d'Euler généralise la factorielle car $\Gamma(n+1) = n!, \forall n \in \mathbb{N}^*$.
- $\Gamma(1) = \int_0^\infty t^{1-1} e^{-t} dt = \int_0^\infty e^{-t} dt = 1$.
- $\Gamma(0_+) = +\infty$.

La fonction Bêta La fonction bêta, souvent appelée intégrale d'Euler de premier type, est définie pour $x > 0$ et $y > 0$ par l'intégrale suivante :

$$ \beta(x, y) = \int_0^\infty t^{x-1} (1-t)^{y-1} dt \tag{3.5} $$

Elle peut être liée avec la fonction Gamma $\Gamma(z)$ par la relation suivante :

$$\beta(x,y) = \frac{\Gamma(x)\cdot\Gamma(y)}{\Gamma(x+y)} \tag{3.6}$$

La fonction Mittag-Leffler La fonction de Mittag-Leffler est une généralisation de la fonction exponentielle e^z. Elle est couramment utilisée pour résoudre des problèmes physiques décrits par des équations différentielles ou intégrales fractionnaires. Une caractéristique notable de la fonction de Mittag-Leffler est qu'elle possède un nombre fini de zéros réels, ce qui est pertinent pour de nombreux problèmes physiques. La fonction de Mittag-Leffler à deux paramètres α et β est définie par la série suivante [18] :

$$E_{\alpha,\beta}(z) = \sum_{k=0}^{\infty} \frac{z^k}{\Gamma(\alpha k+\beta)} \tag{3.7}$$

où $\Gamma(z)$ est la fonction gamma d'Euler.
Pour $\beta = 1$, on obtient la fonction de Mittag-Leffler avec un seul paramètre :

$$E_{\alpha,1}(z) = \sum_{k=0}^{\infty} \frac{z^k}{\Gamma(\alpha k+1)} \tag{3.8}$$

Pour $\alpha = 1$ et $\beta = 1$, on obtient la fonction exponentielle :

$$E_{1,1}(z) = \sum_{k=0}^{\infty} \frac{z^k}{\Gamma(k+1)} = \sum_{k=0}^{\infty} \frac{z^k}{k!} = e^z \tag{3.9}$$

3.2.3 Intégration fractionnaire

Au sens de Riemann-Liouville l'opérateur intégral fractionnaire de Riemann-Liouville d'ordre $\alpha \in \mathbb{R}^+$ appliqué à une fonction $f(t)$ est défini comme suit [37] :

$${}_aI_t^{\alpha} f(t) = \frac{1}{\Gamma(\alpha)} \int_a^t (t-\tau)^{\alpha-1} f(\tau)\, d\tau \tag{3.10}$$

où $\Gamma(\alpha)$ est la fonction Gamma d'Euler.
a et t sont des limites de l'opération.

3.2.4 Dérivation fractionnaire

Il existe de nombreuses approches pour la dérivation fractionnaire. Parmi celles-ci, les méthodes les plus couramment employées dans les applications sont les suivantes :

Dérivées fractionnaires au sens de Riemann-Liouville La dérivée fractionnaire au sens de Riemann-Liouville est la plus réputée et la plus largement utilisée.

Soit f une fonction intégrable sur $[a,t]$. La dérivée fractionnaire d'ordre α est définie par [33] :

$$ {}_aD_t^{\alpha} f(t) = \frac{1}{\Gamma(n-\alpha)} \frac{d^n}{dt^n} \int_a^t (t-\tau)^{n-\alpha-1} f(\tau)\, d\tau \tag{3.11} $$

où Γ est la fonction Gamma d'Euler, et n est un entier positif tel que $n-1 < \alpha < n$.

Cette dérivée d'ordre fractionnaire peut également être définie à partir de l'équation (10) de la manière suivante :

$$ {}_aD_t^{\alpha} f(t) = \frac{d^n}{dt^n} \left({}_aI_t^{n-\alpha} f(t) \right) \tag{3.12} $$

où ${}_aI_t^{n-\alpha}$ représente l'intégrale fractionnaire d'ordre $n-\alpha$.

Dérivée fractionnaire au sens de Caputo La dérivée fractionnaire au sens de Caputo est une approche couramment utilisée pour la dérivation fractionnaire, particulièrement adaptée pour traiter des conditions initiales classiques. Deux formulations de cette dérivée sont largement utilisées, chacune ayant ses propres avantages et applications [18]. Nous présentons ici ces formulations :

La première formulation est donnée par l'équation suivante :

$$ {}_aD_t^{\alpha} f(t) = \frac{1}{\Gamma(n-\alpha)} \int_a^t (t-\tau)^{n-\alpha-1} f^{(n)}(\tau)\, d\tau \tag{3.13} $$

Transformée de Laplace inverse La deuxième formulation est donnée par l'équation suivante :

$$ {}_aD_t^{\alpha} f(t) = I^{n-\alpha} \left(\frac{d^n}{dt^n} f(t) \right) \tag{3.14} $$

où n est un entier positif tel que $n-1 < \alpha < n$, Γ est la fonction Gamma, et $f^{(n)}(\tau)$ est la n-ième dérivée entière de $f(\tau)$.

Dérivée fractionnaire au sens de Grünwald-Letnikov La définition de la dérivée fractionnaire au sens de Grünwald-Letnikov repose sur une approche basée sur les différences finies fractionnaires. La dérivée fractionnaire au sens de Grünwald-Letnikov d'une fonction $f(t)$ est définie par la relation suivante [12] :

$$ {}_aD_t^{\alpha} f(t) = \lim_{h \to 0} \frac{1}{h^{\alpha}} \sum_{k=0}^{[\frac{t-a}{h}]} (-1)^k \binom{\alpha}{k} f(t-kh) \tag{3.15} $$

où $\left[\frac{t-a}{h}\right]$ désigne la partie entière d'un nombre réel, h est la période d'échantillonnage, et $\binom{\alpha}{k}$ sont des coefficients binomiaux généralisés.

Les coefficients $\binom{\alpha}{k}$ sont donnés par :

$$\binom{\alpha}{k} = \frac{\Gamma(\alpha+1)}{\Gamma(k+1)\Gamma(\alpha-k+1)} \tag{3.16}$$

Le coefficient binomial de l'entier naturel α et de l'entier naturel k est défini comme étant l'entier naturel C_k^α

$C_k^\alpha = \binom{\alpha}{k} = \frac{\alpha!}{k!(\alpha-k)!}$ si $0 \leq k \leq \alpha$

et

$C_k^\alpha = \binom{\alpha}{k} = 0$ si $k < 0$ ou $k > 0$

$k!$ désigne la factorielle de k.

3.2.5 Propriétés des dérivées fractionnaires et intégrales fractionnaires

Les principales propriétés des opérateurs d'ordre fractionnaire sont les suivantes [31] :

1. Si $f(z)$ est une fonction analytique en z alors sa dérivée fractionnaire $D_z^\alpha f(z)$ est une fonction analytique en z et α.
2. Pour $\alpha = n$, où n est un nombre entier, l'opération $D_t^\alpha f(t)$ produit le même résultat que la dérivation classique d'ordre entier.
3. Pour $\alpha = 0$, l'opérateur D_t^α est l'opérateur identité

   $D_t^0 f(t) = f(t)$
4. La dérivation et l'intégration fractionnaires sont des opérations linéaires

   $$D_t^\alpha(\gamma f(t) + \delta g(t)) = \gamma D_t^\alpha f(t) + \delta D_t^\alpha g(t) \tag{3.17}$$

   où f et g sont deux fonctions continues, γ et δ des nombres réels.
5. La loi additive

   $$D_t^\alpha D_t^\beta f(t) = D_t^\beta D_t^\alpha f(t) = D_t^{\alpha+\beta} f(t) \tag{3.18}$$

   où α et β sont deux nombres réels.

6. Règle de Leibniz

$$aD_t^{\alpha}(f(t)\cdot g(t)) = \sum_{k=0}^{\infty}\binom{\alpha}{k} f^{(k)}(t) D_t^{\alpha-k} g(t) \tag{3.19}$$

Où $f(t)$ et $g(t)$ sont continues dans $[a,t]$.

3.3 Systèmes d'ordre fractionnaires

3.3.1 Représentation des systèmes fractionnaires

Il existe trois manières différentes de représenter les systèmes non entiers.

3.3.1.1 Équation différentielle fractionnaire

La représentation d'une équation différentielle fractionnaire est la suivante [4] :

$$\sum_{i=1}^{n} a_i D^{\alpha_i} y(t) = \sum_{j=0}^{m} b_j D^{\beta_j} u(t) \tag{3.20}$$

$$y(t) + a_1 D^{\alpha_1} y(t) + \ldots + a_n D^{\alpha_n} y(t) = b_0 D^{\beta_0} u(t) + b_1 D^{\beta_1} u(t) + \ldots + b_m D^{\beta_m} u(t) \tag{3.21}$$

Où :

α_j et $\beta_j \in \mathbb{R}^+$

$u(t)$, $y(t)$ désignent respectivement l'entrée et la sortie du système à l'instant t.

a_i, b_j sont les coefficients de l'équation différentielle.

3.3.1.2 Fonction de transfert fractionnaire

En appliquant la transformée de Laplace à l'équation (32), nous obtenons :

$$Y(s) + a_1 s^{\alpha_1} Y(s) + \cdots + a_n s^{\alpha_n} Y(s) = b_0 s^{\beta_0} U(s) + b_1 s^{\beta_1} U(s) + \cdots + b_m s^{\beta_m} U(s) \tag{3.22}$$

Pour obtenir la fonction de transfert à partir de cette équation, il suffit de diviser $Y(s)$ par $U(s)$:

$$H(s) = \frac{Y(s)}{U(s)}$$

nous obtenons donc :

$$H(s) = \frac{Y(s)}{U(s)} = \frac{\sum_{j=0}^{m} b_j s^{\beta_j}}{1 + \sum_{i=1}^{n} a_i s^{\alpha_i}} \tag{3.23}$$

[4]

3.3.1.3 Représentation d'état des systèmes d'ordre fractionnaire

La représentation d'état fractionnaire d'un système consiste à exprimer ses équations d'état sous forme matricielle, de manière similaire à la représentation d'état classique. Les matrices d'état sont déterminées en utilisant des dérivées fractionnaires [4].

Cas des systèmes en temps continu :

$$\begin{cases} D^{\alpha}x(t) = f(x(t), u(t)) \\ y(t) = \Psi(x(t)) \end{cases} \tag{3.24}$$

$x(t)$: est le vecteur d'état de dimension $(n \times 1)$.

f et Ψ : sont les fonctions non linéaires.

D^{α} : est l'opérateur de la dérivée d'ordre α.

Cas des systèmes en temps discret :

$$\begin{cases} \Delta^{\alpha}x(k+1) = f(x(k), u(k)) \\ y(k) = \Psi(x(k)) \end{cases} \tag{3.25}$$

$x(k) \in \mathbb{R}^n$, $u(k) \in \mathbb{R}^m$, $y(k) \in \mathbb{R}^p$ sont respectivement les vecteurs d'état, Δ^{α} étant l'opérateur de la différence d'ordre α.

3.3.2 Systèmes d'ordre fractionnaires commensurables et non commensurables

Systèmes d'ordre commensurables

Si les ordres de dérivation fractionnaires α_i sont des multiples entiers d'un ordre de base α, c'est-à-dire $\alpha_i = q \cdot \alpha$ pour tout i, alors le système est dit commensurable [35].

Systèmes d'ordre non commensurables :

Si les ordres de dérivation fractionnaires α_i ne sont pas des multiples entiers d'un ordre de base commun, alors le système est dit non commensurable [37].

En général, les systèmes non linéaires fractionnaires sont décrits comme suit :

$$D_t^{\alpha} x_i(t) = f_i(x_1(t), x_2(t), \ldots, x_n(t), t) \tag{3.26}$$

$$x_i(0) = c_i; \quad i = 1, 2, \ldots, n$$

Les variables c_i représentent les conditions initiales du système.
On peut également exprimer le système (3.26) de la manière suivante.

$$D^{\alpha} x = f(x) \tag{3.27}$$

$x \in \mathbb{R}^n, \quad \alpha_i = [\alpha_1 \alpha_2 \ldots \alpha_n]^T, \quad 0 \prec \alpha_i \prec 2, \quad (i = 1, 2, \ldots, n).$

3.3.3 Observabilité et Stabilité des systèmes d'ordre fractionnaires

3.3.1 Stabilité des systèmes d'ordre fractionnaires

Dans la théorie de la stabilité des systèmes linéaires à temps invariant et à dérivée d'ordre entier, il est bien établi qu'un système est stable si les racines du polynôme caractéristique ont des parties réelles strictement négatives, les plaçant ainsi dans la moitié gauche du plan complexe. Cependant, pour les systèmes fractionnaires linéaires à temps invariant, la définition de la stabilité diffère de celle des systèmes d'ordre entier. En effet, les systèmes fractionnaires, ou d'ordre non entier, peuvent parfaitement posséder des racines dans la moitié droite du plan complexe tout en restant stables [3].

$$\begin{cases} D^{\alpha} x(t) = Ax(t) + Bu(t) \\ y(t) = Cx(t) \qquad\qquad 0 < \alpha < 2 \\ x(0) = x_0 \end{cases} \tag{3.28}$$

$x(t) \in \mathbb{R}^n$, $u(t) \in \mathbb{R}^m$, et $y(t) \in \mathbb{R}^p$. Soit $\sigma(A) = \{\lambda_1, \ldots, \lambda_n\}$. Le système (3.28) avec comme entrée $u(t) = 0$ est stable si et seulement si :

$$|\arg(\lambda_i)| > \frac{\alpha\pi}{2}, \quad \lambda_i \in \sigma(A), \quad i = 1 \ldots n. \tag{3.29}$$

Selon ce théorème sur la stabilité, il est possible de déduire les diverses zones de stabilité et d'instabilité, voir figures 1 et 2 : Si $1 < \alpha < 2$, alors la relation (40) décrit une région convexe du plan complexe comme le montre la figure 2.

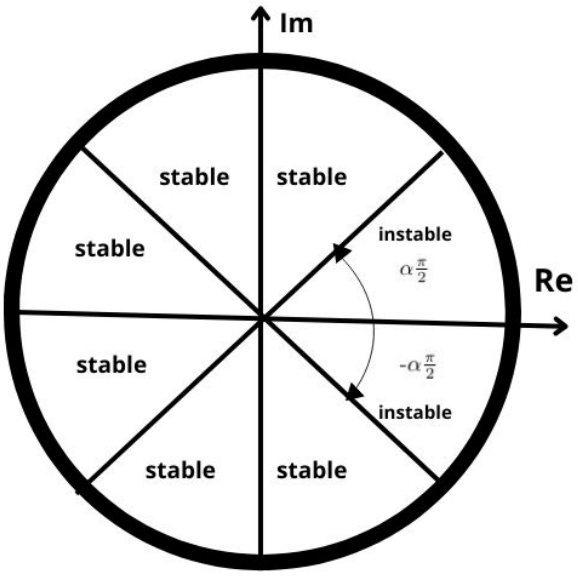

FIGURE 3.1 – Région de stabilité des systèmes d'ordre fractionnaires avec $0 < \alpha < 1$.

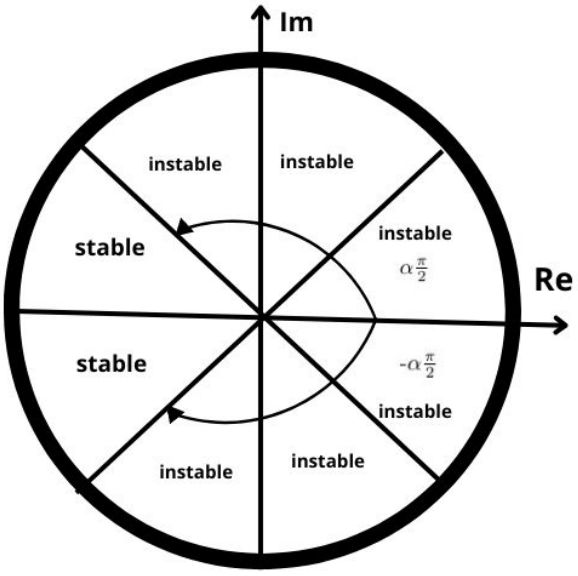

FIGURE 3.2 – Région de stabilité des systèmes d'ordre fractionnaires avec $1 < \alpha < 2$.

3.3.2 Observabilité des systèmes d'ordre fractionnaires Le système fractionnaire (28) d'ordre $0 < \alpha < 2$ est observable (ou la paire (C, A) est observable) si et seulement si l'une des deux conditions équivalentes suivantes est vérifiée [13] :

— Critère de Kalman :

$$\mathcal{O} = \begin{pmatrix} C \\ CA \\ CA^2 \\ \vdots \\ CA^{n-1} \end{pmatrix} \tag{3.30}$$

— Critère d'Hautus :

$$\operatorname{rang}\left(\begin{bmatrix} \sigma I_n - A \\ C \end{bmatrix}\right) = n = \dim(x) \tag{3.31}$$

3.4 Systèmes chaotiques d'ordre fractionnaires

L'une des applications importantes du calcul fractionnaire est la théorie du chaos. Les systèmes chaotiques d'ordre fractionnaire présentent des propriétés intrinsèques qui peuvent être exploitées dans les schémas de synchronisation et de cryptographie.

Contrairement aux systèmes dynamiques continus traditionnels, où le chaos ne peut se produire que lorsque l'ordre total est supérieur ou égal à trois, les systèmes fractionnaires permettent d'observer le chaos même avec un ordre total inférieur à trois. Cela est possible car l'ordre total est calculé comme la somme des ordres des dérivées fractionnaires des états du système.

3.4.1 Exemple de synchronisation

En discret :

Pour approfondir notre compréhension des propriétés des systèmes chaotiques fractionnaires, examinons une variation du système de Hénon modifié. Le système de Hénon modifié est présenté ci-dessous ; le modèle d'état de ce système est décrit comme suit :

$$\begin{cases} x_1(k+1) = a - x_2^2(k) - bx_3(k) \\ x_2(k+1) = x_1(k) \\ x_3(k+1) = x_2(k) \\ y(k) = x_2(k) \end{cases} \tag{3.32}$$

Avec :
$x = \begin{bmatrix} x_1 & x_2 & x_3 \end{bmatrix} \in \mathbb{R}^3$ sont les états du système (3.32) et $y(k)$ est la sortie.

Le système précédent présente un comportement chaotique lorsque les paramètres $a = 1,6$ et $b = 0,1$ sont utilisés, avec des conditions initiales choisies à l'intérieur du bassin d'attraction telles que $x_1(0) = 0,1$, $x_2(0) = -0,1$, et $x_3(0) = 0,1$.

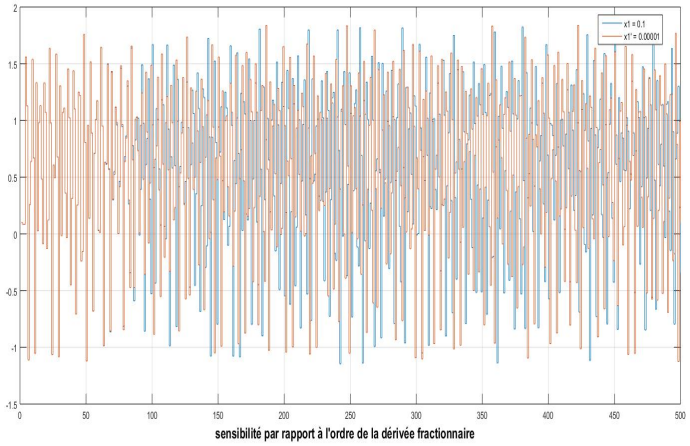

FIGURE 3.3 – La figure suivante illustre la sensibilité aux conditions initiales du système de Hénon modifié d'ordres fractionnaires en comparant les valeurs de x_3 égales à $0,1$ et $0,10000001$.

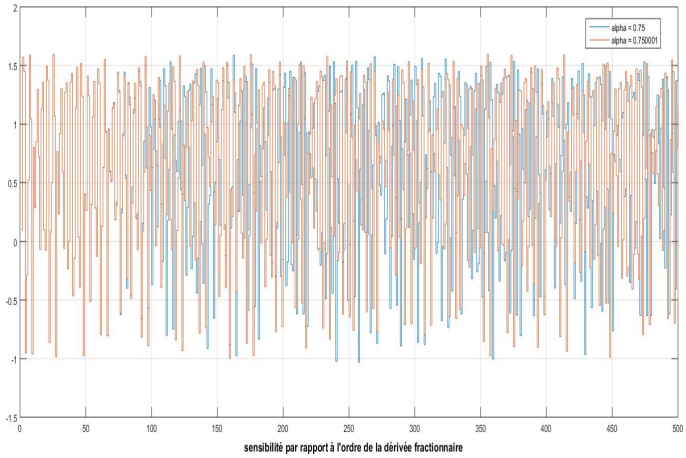

FIGURE 3.4 – La figure suivante illustre la sensibilité aux paramètres de la dérivée d'ordre fractionnaire du système de Hénon modifié d'ordres fractionnaires en comparant les valeurs de α_3 égales à $0,75$ et $0,750001$.

3.4.2 Synthèse de l'observateur discret retardé étape par étape

Dans cette section, un observateur discret retardé étape par étape est conçu. Cet observateur permet de reconstruire tous les états et l'entrée inconnue du système d'ordre fractionnaire à partir de la sortie du système transmise et de ses itérés. Dans un premier lieu, nous considérons que l'entrée est connue et nous nous intéressons à la reconstruction des états [15].

Soit le système de Hénon modifié d'ordre fractionnaire suivant :

$$\begin{cases} x_1(k+1) & = a - x_2^2(k) - bx_3(k) + (\alpha_1 - 1)x_1(k) + mx_1(k) \\ x_2(k+1) & = x_1(k) + (\alpha_2 - 1)x_2(k) + mx_2(k) \\ x_3(k+1) & = x_2(k) + (\alpha_3 - 1)x_3(k) + mx_3(k) \\ y(k) & = x_2(k) \end{cases} \tag{3.33}$$

Les mémoires du système d'ordre fractionnaire sont décrites par les équations suivantes :

$$\begin{cases} mx_1 & = \sum_{p=1}^{L} C_{p1}x_1(k-p) \\ mx_2 & = \sum_{p=1}^{L} C_{p2}x_2(k-p) \\ mx_3 & = \sum_{p=1}^{L} C_{p3}x_3(k-p) \end{cases} \tag{3.34}$$

avec :

$a = 1.6$, $b = 0.1$, $\alpha_1 = 0.85$, $\alpha_2 = 0.9$, $\alpha_3 = 0.75$

$L = 5$ désigne la longueur de la mémoire

$x_1(1) = 0.1$, $x_2(1) = 0.1$, $x_3(1) = 0.1$ sont les conditions initiales.

Reconstruction des états de l'observateur discret retardé étape par étape :

À partir de l'équation (3.33), nous obtenons :

$$\hat{x}_2(k) = y(k) \tag{3.35}$$

Estimation de l'état $\hat{x}_1(k)$:

De l'équation (3.33), on a :

$$\hat{x}_2(k+1) = \hat{x}_1(k) + (\alpha_2 - 1)\hat{x}_2(k) + m\hat{x}_2(k)$$

Ensuite, en appliquant un retard d'un pas, nous pouvons en déduire que :

$$\hat{x}_1(k-1) = y(k) + (\alpha_2 - 1)y(k-1) + m\hat{x}_2(k-1)$$

Estimation de l'état $\hat{x}_3(k)$:

De l'équation (33), on a :

$$\hat{x}_3(k) = \frac{1}{b}\left[a - \hat{x}_1(k+1) - \hat{x}_2^2(k) + (\alpha_1 - 1)\hat{x}_1(k) + m\hat{x}_1(k)\right]$$

Ensuite, en appliquant un retard de deux pas, nous pouvons en déduire que :

$$\hat{x}_3(k-2) = \frac{1}{b}\left[a - \hat{x}_1(k-1) - \hat{x}_2^2(k-2) + (\alpha_1 - 1)\hat{x}_1(k-2) + m\hat{x}_1(k-2)\right]$$

Donc, les équations de l'observateur sont données par :

$$\begin{cases} \hat{x}_1(k-1) = \hat{x}_2(k) + (\alpha_2 - 1)\hat{x}_2(k-1) + m\hat{x}_2(k-1) \\ \hat{x}_3(k-2) = \frac{1}{b}\left[a - \hat{x}_1(k-1) - \hat{x}_2^2(k-2) + (\alpha_1 - 1)\hat{x}_1(k-2) + m\hat{x}_1(k-2)\right] \\ y(k) = \hat{x}_2(k) \end{cases} \tag{3.36}$$

Avec :

$$\begin{cases} m\hat{x}_2 = \sum_{p=1}^{L} C_{p2}\hat{x}_2(k-p-1) \\ m\hat{x}_1 = \sum_{p=1}^{L} C_{p1}\hat{x}_1(k-p-2) \end{cases} \tag{3.37}$$

Les figures suivantes illustrent les résultats de la synchronisation du système de Hénon modifié d'ordre fractionnaire avec cet observateur :

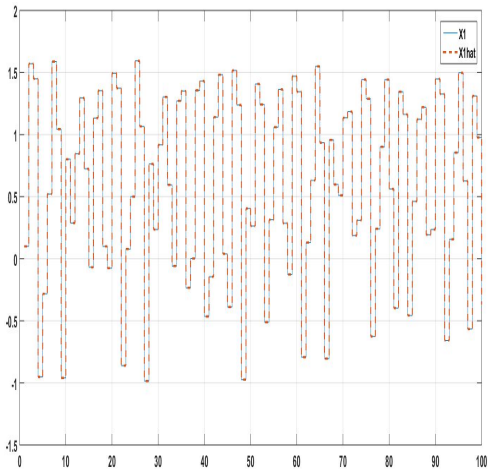

FIGURE 3.5 – Synchronisation de l'état x_1 et son estimé $\hat{x}_1$

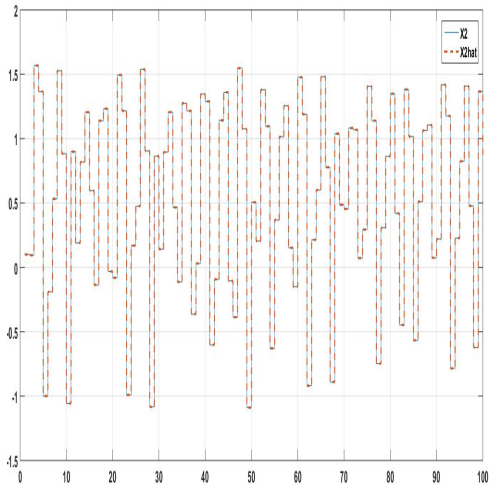

FIGURE 3.6 – Synchronisation de l'état x_2 et son estimé $\hat{x}_2$

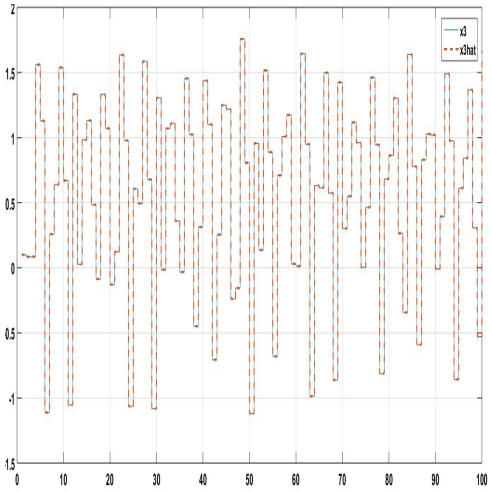

FIGURE 3.7 – Synchronisation de l'état x_3 et son estimé $\hat{x}_3$

FIGURE 3.8 – Les états x_1, x_2 et x_3 du système sont parfaitement reconstruits comme le montrent les figures (5), (6), (7).

3.5 Conclusion

Ce chapitre a mis en lumière la pertinence et les avantages des systèmes fractionnaires dans la modélisation de phénomènes complexes. La théorie de la dérivation non entière a été introduite, accompagnée de quelques rappels sur les fonctions de Gamma d'Euler et de Mittag-Leffler, ainsi que sur les différentes définitions et propriétés de la dérivée fractionnaire. Enfin, pour conclure ce chapitre, nous avons présenté les résultats fondamentaux sur la stabilité des systèmes linéaires fractionnaires, à la fois dans le cas où le domaine de stabilité est un domaine convexe (c'est-à-dire lorsque l'ordre de dérivation α est compris entre $1 < \alpha < 2$) et dans le cas où le domaine de stabilité est un domaine non convexe (avec $0 < \alpha < 1$). Le concept d'observabilité des systèmes linéaires fractionnaires a également été abordé. Ces résultats fondamentaux sur les systèmes fractionnaires seront utilisés dans le chapitre 4 pour mettre en ?uvre notre application de cryptographie vidéo.

Chapitre 4

Conception d'un cryptosystème pour le cryptage vidéo

4.1 Introduction

Les progrès technologiques ont radicalement transformé notre manière de vivre, de travailler et de communiquer. Cependant, ces avancées ont également soulevé des préoccupations majeures concernant la confidentialité et l'intégrité des informations échangées. La cryptographie est une mesure de sécurité essentielle pour répondre à ces préoccupations. Historiquement, des algorithmes de cryptographie comme AES et DES ont été largement utilisés pour sécuriser les données. Toutefois, ces algorithmes ne sont pas toujours adaptés aux caractéristiques spécifiques des données vidéo, en raison de leur grande capacité et de leur forte redondance.

Les vidéos sont un moyen de communication universel, permettant à des personnes de divers horizons et cultures de se comprendre mutuellement grâce à leur contenu riche. En tant que moyen de communication efficace, elles offrent la possibilité d'être analysées de manière unique, permettant d'en tirer des impressions et d'extraire des informations précises. Le traitement vidéo implique donc un ensemble de méthodes et de techniques visant à améliorer les aspects visuels des vidéos afin d'en extraire des informations pertinentes.

Pour sécuriser les vidéos numériques, il est nécessaire d'adopter des techniques de traitement vidéo avancées. Ces techniques ont pour objectif d'assurer la confidentialité et l'intégrité des

données vidéo. Dans ce chapitre, nous explorerons les notions fondamentales des images et des vidéos numériques, en abordant leurs caractéristiques et leurs types, avant de nous pencher sur les méthodes de sécurisation (cryptage). Pour illustrer ces concepts, nous présenterons également un exemple de décryptage appliqué à une vidéo, accompagné de sa simulation sous MATLAB.

4.2 Définition de l'image

Une image est une représentation visuelle ou mentale d'un objet, d'un être vivant ou d'un concept. Elle est obtenue par la capture et la transformation d'une scène réelle via un capteur, puis affichée sur un écran, permettant ainsi à l'œil humain de lui attribuer une signification. La formation d'une image peut être décrite de la manière suivante :

- **Formation de l'image** : Elle implique l'utilisation d'un dispositif physique capable de détecter les informations de la scène et de les encoder dans l'image.
- **Mesure physique** : L'image est obtenue à partir d'une mesure physique.
- **Quantité d'énergie** : Cette mesure physique correspond à la quantité d'énergie réfléchie, émise ou absorbée par l'objet.
- **Rôle du capteur** : Le capteur mesure cette énergie.

En général, une image est une représentation partielle d'une scène réelle à un moment donné dans un espace bidimensionnel. Elle est créée à l'aide de divers dispositifs de capture d'images, tels qu'une caméra, un appareil photo, une radiographie ou un scanner. Les images peuvent être sous forme analogique (par exemple, photographies, vidéos) ou numérique (par exemple, images numérisées dans divers formats, images compressées).

La numérisation d'une image, ou digitalisation, est le processus de conversion d'une image analogique (signal analogique) en une image numérique ou discrète. Cette conversion produit une série de bits visant à reproduire l'image aussi fidèlement que possible à l'original.

4.3 Définition de l'image numérique

Une image numérique est une représentation visuelle composée de pixels, qui sont des éléments de taille fixe organisés en une grille. Chaque pixel correspond à une position précise dans l'image ou la scène observée et possède une valeur de couleur ou de niveau de gris spécifique. Cette image est obtenue par la conversion de son état analogique, c'est-à-dire une distribution

continue d'intensité lumineuse dans un plan (x, y), en une image numérique représentée par une matrice bidimensionnelle de valeurs numériques $f(x, y)$. [11] [16]. Dans cette matrice :

— x et y représentent les coordonnées cartésiennes d'un point de l'image.

— $f(x, y)$ désigne le niveau de gris à ce point.

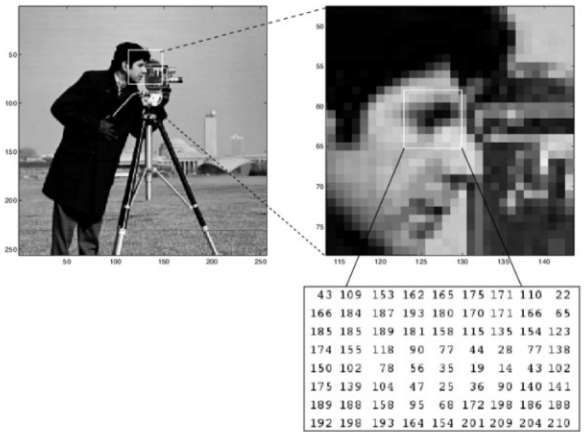

FIGURE 4.1 – Un exemple concret d'image numérique.

4.4 Caractéristiques de l'image numérique

L'image numérique est un ensemble structuré d'informations, caractérisé par les paramètres suivants [11] [21] :

4.4.1 Le pixel

Le terme *pixel* est l'abréviation de l'expression anglaise *Picture Elements*. Un pixel correspond au plus petit point carré d'une image et constitue l'entité calculable qui peut accepter la structure et la quantification. Étant donné qu'un bit est la plus petite unité d'information qu'un ordinateur peut gérer, un pixel représente le plus petit élément que le matériel ainsi que les logiciels d'affichage ou d'impression peuvent manipuler.

La quantité d'informations véhiculées par chaque pixel différencie une image monochrome d'une image couleur. Dans le cas des images monochromes, chaque pixel est généralement codé sur un bit, mais il peut également être codé sur plusieurs bits pour représenter différentes nuances de gris. Par conséquent, la quantité de mémoire nécessaire pour afficher une telle image est directement liée à la taille de cette dernière. En revanche, pour une image couleur (RVB),

un pixel est représenté par trois octets : un pour chaque composante de couleur, soit rouge (R), vert (V) et bleu (B).

4.4.2 Dimension

La dimension d'une image correspond à sa taille, exprimée sous la forme d'une matrice dont les éléments sont des valeurs numériques représentant des intensités lumineuses, ou pixels. Le nombre total de pixels dans l'image se calcule en multipliant le nombre de lignes par le nombre de colonnes de cette matrice.

4.4.3 Contours

Les contours définissent les limites entre des pixels adjacents présentant une différence notable de niveaux de gris.

4.4.4 Résolution

La résolution d'une image numérique désigne la finesse et la clarté des détails qu'un moniteur ou une imprimante peut produire. Pour les écrans d'ordinateur, la résolution est généralement exprimée en pixels par unité de mesure, soit par pouce (dpi) soit par centimètre.

4.4.5 Luminance

La luminance, également appelée brillance, désigne le niveau de luminosité des points d'une image. Elle se définit comme le rapport entre l'intensité lumineuse d'une surface et son aire apparente.

4.4.6 Contraste

Le contraste est la différence perceptible entre les zones claires et sombres d'une image. Il est déterminé par la variation de luminosité entre ces zones.

Le contraste, noté C, se calcule en comparant les niveaux de luminosité L_1 et L_2 de deux zones adjacentes de l'image. Mathématiquement, il est défini par le rapport suivant :

$$C = \frac{L_1 - L_2}{L_1 + L_2}$$

Un contraste excessivement élevé peut conduire à une diminution de la subtilité des dégradés de couleurs, entraînant ainsi des ombres très prononcées. À l'inverse, un contraste considérablement réduit crée un effet de voile gris.

Ces concepts sont illustrés dans les trois sections suivants : la photo de référence au centre, avec à gauche un contraste réduit (voile gris) et à droite un contraste augmenté (ombres accentuées).

FIGURE 4.2 – Exemple de contraste

4.4.7 Voisinage

Le voisinage se réfère à l'ensemble des pixels adjacents à un pixel donné de coordonnées (i, j) dans toutes les directions. En règle générale, chaque pixel $p(x, y)$ possède quatre voisins horizontaux-verticaux et quatre voisins diagonaux, comme illustré dans les figures suivantes :

	$(x, y+1)$	
$(x-1, y)$	$p(x, y)$	$(x+1, y)$
	$(x, y-1)$	

TABLE 4.1 – Voisins horizontaux-verticaux de $p(x, y)$

$(x-1, y+1)$		$(x+1, y+1)$
	$p(x, y)$	
$(x-1, y-1)$		$(x+1, y-1)$

TABLE 4.2 – Voisins diagonaux de $p(x, y)$

4.5 Types d'images numériques

Les images numériques se classent généralement en trois catégories principales : binaires, en niveaux de gris et en couleur. Nous les décrirons brièvement ci-dessous [21] :

4.5.1 Image en niveaux de gris

Les niveaux de gris indiquent l'intensité lumineuse d'un point, avec un éventail restreint de nuances intermédiaires, allant du noir au blanc. Dans ce mode, les pixels sont représentés par une valeur unique, exprimant la quantité de lumière émise. Habituellement, cette valeur est définie sur une échelle de 0 à 255, où 0 représente le noir et 255 le blanc. Ainsi, chaque pixel est codé sur un octet plutôt que sur plusieurs bits.

FIGURE 4.3 – Une image en niveaux de gris est représentée par $I(i, j) \in [0, 255]$.

4.5.2 Image binaire

Une image binaire se définit comme une matrice rectangulaire où les niveaux de gris se limitent à deux valeurs distinctes : 0 et 1.
Le niveau 0 correspond au noir absolu tandis que le niveau 1 représente le blanc.

FIGURE 4.4 – Une image binaire est représentée par $I(i, j) \in \{0, 1\}$.

4.5.3 Image couleur

Les images en couleur sont généralement codées en utilisant les trois couleurs fondamentales : le rouge, le vert et le bleu, formant ainsi ce qu'on appelle des images RVB (Rouge, Vert, Bleu). Chaque pixel est représentée par trois plans de couleur : un pour le rouge, un pour le vert et

un pour le bleu. Chaque plan est codé comme une image en niveaux de gris, avec des valeurs variant de 0 à 255.

Pour convertir une image couleur en une image en niveaux de gris, on utilise la fonction suivante :

$$G(i,j) = 0.299 \cdot R(i,j) + 0.587 \cdot V(i,j) + 0.114 \cdot B(i,j) \tag{4.1}$$

où :

— (i,j) : coordonnées du pixel situé à la ligne i et à la colonne j.

— $R(i,j)$: intensité de la composante rouge du pixel (i,j).

— $V(i,j)$: intensité de la composante verte du pixel (i,j).

— $B(i,j)$: intensité de la composante bleue du pixel (i,j).

FIGURE 4.5 – Image couleur.

Les couleurs en RVB sont composées de trois éléments fondamentaux : le rouge, le vert et le bleu, comme illustré dans la figure ci-dessous :

FIGURE 4.6 – Les 3 constituants principaux d'une couleur(RVB).

4.6 Définition d'une vidéo

Une vidéo est une succession d'images en mouvement, pouvant être enregistrée, diffusée ou stockée dans une variété de formats et de supports. Voici les éléments clés de la définition d'une vidéo :

— **Images en mouvement** : Une vidéo consiste en une séquence d'images fixes affichées

successivement à une cadence élevée, habituellement de 24 à 60 images par seconde. Cette succession rapide crée l'illusion de mouvement fluide et continu.

— **Enregistrement et diffusion** : Les vidéos peuvent être capturées à l'aide de divers appareils tels que des caméras, des smartphones, des caméras de surveillance, etc. Elles peuvent être diffusées en direct, comme c'est le cas des émissions de télévision en direct, ou enregistrées pour une diffusion ultérieure.

— **Formats et supports** : Les vidéos peuvent être stockées sur divers supports tels que des cassettes, des DVD, des disques Blu-ray, des disques durs, des clés USB, ou sous forme de fichiers numériques dans différents formats comme MP4, AVI, MOV, etc.

— **Utilisations diverses** : Les vidéos sont utilisées à diverses fins, notamment le divertissement (films, séries télévisées), l'éducation (documentaires, cours en ligne), la communication (vidéoconférences...), la surveillance, ainsi que dans de nombreuses autres applications.

4.7 Définition d'une vidéo numérique

Une vidéo numérique est une succession d'images en mouvement encodées sous forme de données numériques. À la différence des vidéos analogiques, les vidéos numériques sont constituées de bits et sont ainsi aisément manipulables par des ordinateurs et autres dispositifs numériques. Voici les points fondamentaux à retenir concernant la définition d'une vidéo numérique : [41] [44] [38] [45]

— **Codage Numérique** : Les images et le son sont convertis en données binaires (bits) grâce à des techniques de compression et d'encodage. Les formats de fichier courants pour la vidéo numérique incluent MPEG, AVI, MP4, MOV, etc.

— **Compression** : Pour réduire la taille des fichiers, on utilise des algorithmes de compression tels que H.264, HEVC, permettant de diminuer la taille sans compromettre significativement la qualité.

— **Stockage** : Les vidéos numériques peuvent être sauvegardées sur divers supports numériques tels que des disques durs, des SSD,...etc.

— **Qualité et Résolution** : Les vidéos numériques peuvent varier en résolution, allant des vidéos de basse résolution (SD) aux vidéos haute définition (HD).

4.8 Caractéristiques d'une Vidéo Numérique

Les caractéristiques techniques d'une vidéo numérique incluent plusieurs aspects fondamentaux qui influencent la qualité, la taille et la compatibilité des vidéos. Voici une liste détaillée de ces caractéristiques[32] [7].

4.8.1 Format du fichier

Les vidéos numériques sont stockées dans des formats spécifiques comme MP4, AVI, MOV, MKV, chacun offrant différents niveaux de compression et de compatibilité .

4.8.2 Codec

Les codecs comme H.264, HEVC (H.265), VP9, et AV1 sont utilisés pour encoder et décoder les vidéos. Ils déterminent la qualité et la taille du fichier vidéo.

4.8.3 Résolution

La résolution de la vidéo indique le nombre de pixels en largeur et en hauteur :

— **SD (Standard Definition)** : 480p

— **HD (High Definition)** : 720p, 1080p

— **4K (Ultra High Definition)** : 2160p

— **8K (Ultra High Definition)** : 4320p .

4.8.4 Fréquence d'images (Frame Rate)

Mesurée en images par seconde (fps), les fréquences d'images courantes sont 24fps, 30fps, 60fps, et 120fps. Une fréquence plus élevée offre un mouvement plus fluide .

4.9 Analyse comparative entre les images et les vidéos

— Une image représente un instant figé, capturant généralement un seul moment dans le temps, offrant ainsi un aperçu unique.

— Une vidéo est constituée d'une séquence d'images en mouvement, appelées images clés ou frames, qui sont affichées successivement à une vitesse suffisante pour créer l'illusion du mouvement.

4.10 Outils d'évaluation de la sécurité

La sécurité d'un schéma de chiffrement est validée par une étape essentielle, qui est la cryptanalyse.[22] [29]

4.10.1 Cryptanalyse

La cryptanalyse étudie les probabilités de réussite des attaques contre les systèmes cryptographiques afin de détecter leurs vulnérabilités. Son objectif est de déterminer si un adversaire peut déchiffrer un message ou récupérer une clé secrète. Elle progresse en parallèle avec la cryptographie, qui conçoit des systèmes de chiffrement plus robustes pour remplacer ceux qui sont compromis. Le défi de la cryptographie est d'assurer que le temps nécessaire pour compromettre un système soit plus long que sa durée de pertinence. La réussite d'une attaque dépend de plusieurs facteurs, tels que les connaissances préalables, l'effort requis et la qualité des informations disponibles. Divers types d'attaques peuvent être lancés contre les systèmes cryptographiques.

4.10.2 Hypothèse de Kerckhoff

La cryptanalyse des schémas de chiffrement repose sur diverses hypothèses. L'une de ces hypothèses clés, connue sous le nom de principe de Kerckhoff, stipule que l'adversaire possède une connaissance complète de l'algorithme de chiffrement, à l'exception de la clé secrète. Il est donc risqué de compter sur le secret des mécanismes de chiffrement pour assurer la sécurité d'un système, car la véritable protection réside dans la confidentialité de la clé secrète. Les attaques cryptanalytiques visent toutes à retrouver le texte en clair à partir du texte chiffré ou à déduire la clé secrète. Ces attaques se classent en différentes catégories selon les types de données nécessaires pour les exécuter.[29]

2.7.1.1 Différentes classes d'attaques

— **Attaque sur le texte chiffré uniquement (ciphertext only attack) :** L'adversaire dispose uniquement du texte chiffré et tente de retrouver le texte clair et/ou la clé secrète en analysant la fréquence des lettres utilisées.[29]

— **Attaque à texte en clair connu (known plaintext attack) :**Le cryptanalyste possède à la fois des messages chiffrés et leurs versions en clair. L'objectif est de déterminer la méthode de chiffrement pour déchiffrer de nouveaux messages chiffrés avec la même

clé.[29]

— **Attaque à texte en clair choisi (chosen plaintext attack) :** Le cryptanalyste a accès aux textes chiffrés et peut choisir des séquences spécifiques de texte clair à chiffrer. Cette méthode est plus efficace car elle permet de choisir des textes en clair fournissant plus d'informations sur la clé.[29]

— **Attaque adaptative à texte en clair choisi (adaptive chosen plaintext attack) :**Une variante de l'attaque à texte en clair choisi où le choix du texte clair peut dépendre des résultats obtenus précédemment.[29]

— **Attaque sur le texte chiffré choisi (chosen ciphertext attack) :**L'attaquant sélectionne des séquences de texte chiffré et analyse les séquences correspondantes en clair, utilisée contre les systèmes à clé publique pour découvrir la clé privée.[29]

— **Attaque adaptative à texte en chiffré choisi (adaptive chosen ciphertext attack) :** Une variante où le choix du texte chiffré peut dépendre des textes en clair précédemment reçus.

— **Attaque exhaustive ou attaque par force brute(brute force attack) :** L'adversaire teste toutes les clés possibles de manière exhaustive jusqu'à obtenir le texte clair. Cette méthode est très coûteuse en calcul et en mémoire en raison de sa nature exhaustive.[29]

4.10.3 Analyse de l'espace des clés

L'espace des clés d'un schéma de transmission sécurisée représente l'ensemble des clés uniques utilisables pour chiffrer et déchiffrer les données. Pour être efficace, un tel schéma doit présenter une sensibilité à la clé de chiffrement, impliquant que même de légères variations dans la clé produisent des résultats de chiffrement totalement différents. De plus, l'espace des clés doit être suffisamment vaste pour rendre les attaques par force brute impraticables.

4.10.4 Analyse de la sensibilité de la clé

L'analyse de la sensibilité à la clé permet de dévoiler des informations sur la clé secrète d'un schéma de transmission sécurisée. Dans ce type d'analyse, deux clés légèrement différentes sont utilisées pour chiffrer la même image. Les images chiffrées obtenues doivent être totalement indépendantes l'une de l'autre, indiquant une faible corrélation. De plus, une image chiffrée ne

doit pas pouvoir être correctement déchiffrée si la clé secrète est légèrement modifiée lors du déchiffrement. Pour vérifier cette sensibilité, on utilise le taux de changement du nombre de pixels (NPCR - Number of Pixels Change Rate) et la moyenne unifiée du changement d'intensité (UACI - Unified Averaged Changed Intensity). Ces critères sont définis comme suit :

$$\text{NPCR} = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} D(i,j) \times 100 \tag{4.2}$$

$$\text{UACI} = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} \frac{|C_1(i,j) - C_2(i,j)|}{255} \times 100 \tag{4.3}$$

Où M et N représentent respectivement la largeur et la hauteur de l'image. Les valeurs $C_1(i,j)$ et $C_2(i,j)$ sont les pixels à la position (i,j) des deux images chiffrées utilisant des clés de chiffrement légèrement différentes. Parfois, C_1 et C_2 sont utilisés pour désigner l'image originale et l'image chiffrée. $D(i,j)$ est une matrice de la même taille que C_1 et C_2 définie comme suit :

$$D(i,j) = \begin{cases} 1 & \text{si } C_1(i,j) \neq C_2(i,j) \\ 0 & \text{sinon} \end{cases}$$

4.10.5 Analyse statistique

L'analyse statistique peut permettre de déchiffrer plusieurs algorithmes de cryptage, comme mentionné par Shannon. Cette section est dédiée aux attaques statistiques, qui exploitent principalement une faiblesse dans la partie confusion du chiffrement. Nous allons donc décrire l'analyse des histogrammes , la corrélation des pixels adjacents et l'entropie.

Analyse des histogrammes L'histogramme d'une image représente la répartition des intensités de ses pixels, c'est-à-dire le nombre de pixels pour chaque niveau d'intensité lumineuse. Dans le contexte de la transmission d'images sécurisées, un système de chiffrement est considéré comme robuste contre cette analyse si l'histogramme de l'image chiffrée est uniformément réparti. Bien qu'un examen visuel soit souvent réalisé, il n'est pas suffisant en soi. Pour garantir cette uniformité, le test du χ^2 est appliqué pour confirmer statistiquement l'uniformité de l'histogramme [9] :

$$\chi^2 = \sum_{i=0}^{Q-1} \frac{(o_i - e_i)^2}{e_i} \tag{4.4}$$

Dans l'équation (4.4), Q est le nombre de niveaux, o_i est la fréquence d'occurrence observée de chaque niveau de couleur (0 – 255) sur l'histogramme de l'image chiffrée, et e_i est la fréquence d'occurrence attendue de la répartition uniforme, donnée par $e_i = \frac{M \times N \times P}{Q}$, où M et N présentent la taille de l'image. Pour un algorithme robuste, la valeur expérimentale du χ^2 doit être inférieure au χ^2 théorique, soit 293 pour $\alpha = 0.05$ (α présente le niveau de signification) et $Q = 256$.

Analyse de corrélation Les images numériques se caractérisent par des pixels adjacents très redondants et fortement corrélés. Un schéma de transmission d'image sécurisé efficace doit être capable de supprimer ce type de relation ; c'est-à-dire que les pixels adjacents dans l'image chiffrée doivent présenter une redondance et une corrélation aussi faible que possible. Par conséquent, il est nécessaire de tester la corrélation entre les valeurs de deux pixels adjacents de nos images. Nous calculons donc le coefficient de corrélation dans chaque direction selon l'équation suivante [27] :

$$r_{xy} = \frac{\mathrm{cov}(x, y)}{\sqrt{D(x)D(y)}} \tag{4.5}$$

Dans l'équation ci-dessus, x et y représentent les valeurs de niveau de gris des pixels situés au même indice dans les images I et C, où I et C représentent respectivement les images originale et chiffrée. La covariance et la variance sont définies par les équations suivantes :

$$\mathrm{cov}(x, y) = \frac{1}{N} \sum_{i=1}^{N} E(x_i - E(x))(y_i - E(y)) \tag{4.6}$$

L'expression pour $E(x)$ est donnée par :

$$E(x) = \frac{1}{N} \sum_{i=1}^{N} x_i \tag{4.7}$$

L'expression pour $D(x)$ est donnée par :

$$D(x) = \frac{1}{N} \sum_{i=1}^{N} (x_i - E(x))^2 \tag{4.8}$$

Avec N est le nombre de pixels utilisés.

4.10.6 Entropie d'information

L'entropie de l'information est une caractéristique cruciale du caractère aléatoire. Les valeurs des pixels d'une image varient généralement de 0 à 255. Dans un algorithme de chiffrement robuste, il est essentiel que la probabilité d'occurrence d'un pixel soit uniforme, ou du moins très proche de l'uniformité. L'évaluation du caractère aléatoire des informations cryptées peut être effectuée en utilisant l'entropie de l'information, définie par :

$$H(C) = -\sum_{i=0}^{n} p(c_i) \log_2 \frac{1}{p(c_i)} \tag{4.9}$$

L'entropie $H(C)$ représente l'incertitude associée à l'image chiffrée C, où $p(c_i)$ est la probabilité d'apparition de la valeur d'information x_i. Pour une source aléatoire réelle produisant des symboles 2^L, l'entropie devrait être L. Par exemple, pour des images en niveaux de gris de 256 niveaux, où les données de pixels ont 2^8 valeurs possibles, l'entropie d'une image réellement aléatoire devrait être de 8. Cependant, dans la pratique, l'entropie de l'information est généralement inférieure à l'idéale.

4.11 Application au cryptage vidéo

***Algorithme** Pour réaliser notre cryptosystème et l'appliquer au chiffrement d'une vidéo, nous avons suivi les étapes suivantes :

-Prétraitement de la vidéo

1. Extraire les images de la vidéo.
2. Convertir chaque image en niveaux de gris.
3. Transformer chaque image en un vecteur unidimensionnel pour le traitement.

-Génération de la séquence chaotique avec la carte de Lozi

1. Initialiser les paramètres chaotiques $\beta_1 = 0.95$ et $\beta_2 = 0.95$.
2. Calculer les séquences z_1, z_2 et w en utilisant les équations de la carte de Lozi :

$$z_1(j+1) = 1 - \beta_1 \cdot |z_1(j)| + \beta_2 \cdot z_2(j) \tag{4.10}$$

où $z_1(1) = 0.1$ et $z_2(1) = -0.1$.

3. Permuter les pixels de l'image en fonction de w, triée pour obtenir une réorganisation aléatoire des pixels.

-Chiffrement avec Lozi

1. Effectuer la permutation des pixels de l'image basée sur la séquence w.
2. Calculer la clé à partir de la séquence i générée par :

$$i(j+1) = 0.628 \cdot z_1(j) + |z_2(j)| \tag{4.11}$$

La séquence i est transformée en une clé key par l'opération suivante :

$$key = \text{bitxor}(i, \text{circshift}(i)) \tag{4.12}$$

3. Appliquer un XOR entre les pixels permutés et la clé pour obtenir une image brouillée :

$$timg = \text{bitxor}(key, timg) \tag{4.13}$$

-Chiffrement avec la carte de Hénon modifié

1. Initialiser les paramètres $\alpha_1 = 0.85$, $\alpha_2 = 0.9$, $\alpha_3 = 0.75$.
2. Générer une nouvelle séquence chaotique m_1 avec la carte de Hénon :

$$x_1(j+1) = \alpha_1 - (x_2(j))^2 - \alpha_2 \cdot x_3(j) \tag{4.14}$$

où $x_1(1) = -0.3$, $x_2(1) = 0.2$ et $x_3(1) = 0.4$.

3. Utiliser m_1 pour modifier davantage l'image brouillée.

-Déchiffrement

1. Appliquer l'inverse de la carte de Hénon pour obtenir l'image intermédiaire.
2. Utiliser l'inverse de la carte de Lozi pour restaurer l'image originale via la séquence w.
3. Effectuer le XOR inverse avec la clé key pour récupérer l'image originale :

$$timg_decrypt = \text{bitxor}(key, timg_decrypt) \tag{4.15}$$

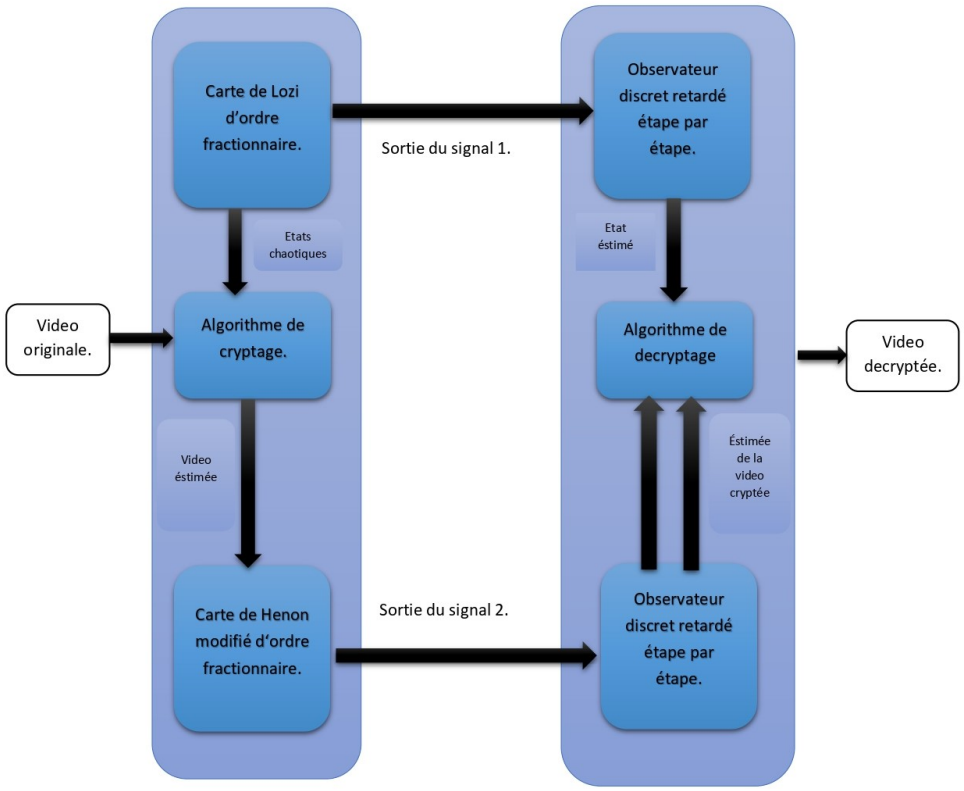

FIGURE 4.7 – Schéma de principe de crypto-système vidéo proposé

4.12 Analyse des Résultats

— Le schéma de chiffrement proposé (figure 4.7) a été appliqué pour chiffrer une vidéo composée de 46 trames, de largeur 256 et de hauteur 240.

— Les résultats de simulation concernant la synchronisation des deux systèmes et des observateurs sont présentés dans les figures (4.8). Ces résultats démontrent que les états du système ont été correctement reconstruits.

— Des images sélectionnées de la vidéo originale, chiffrée et déchiffrée sont illustrées dans les figures (4.9).

— Les histogrammes correspondants sont également présentés dans la figure (4.13[4.10,4.11,4.12]).L'histogramme de la vidéo chiffrée présente une distribution quasi uniforme, ce qui contraste nettement avec celui de la vidéo originale, qui correspond exactement à celui de la vidéo déchiffrée.

— La distribution de la corrélation entre deux pixels voisins (horizontalement, verticalement et diagonalement) dans la vidéo originale et la vidéo chiffrée est illustrée dans la figure

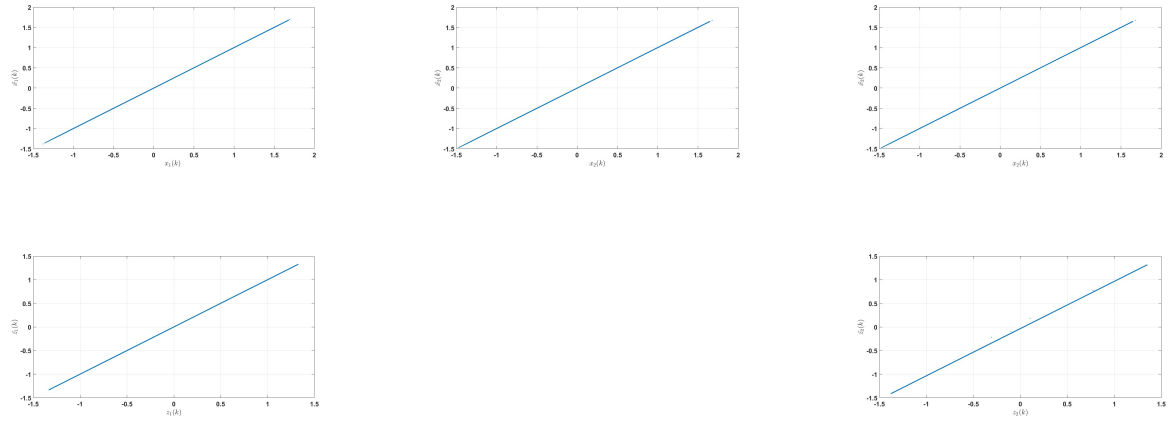

FIGURE 4.8 – Synchronisation des états

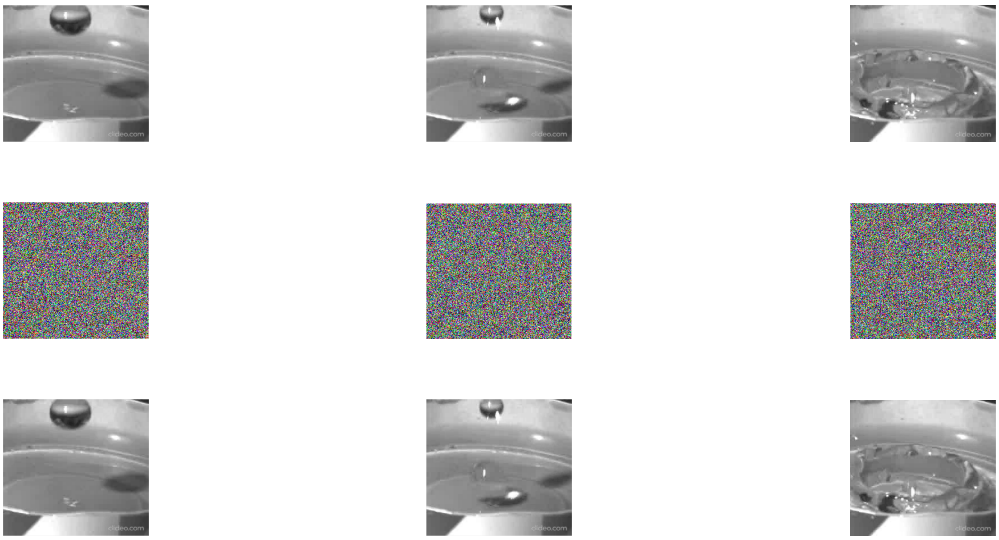

FIGURE 4.9 – Trames(1,15 et 40) vidéo originale, chiffrée et décryptée

(4.14). Cette analyse montre une nette différence entre les vidéos, soulignant l'efficacité du chiffrement pour brouiller les structures internes de la vidéo.

— Les coefficients de corrélation de la vidéo sont présentés dans le tableau (4.3). Ces résultats, indique que le schéma proposé est hautement sécurisé contre les attaques statistiques.

— La moyenne unifiée du changement d'intensité (UACI - Unified Averaged Changed Intensity) est de 32.66 %

— Le taux de changement du nombre de pixels est de NPCR=99.5 %.Un score élevé de

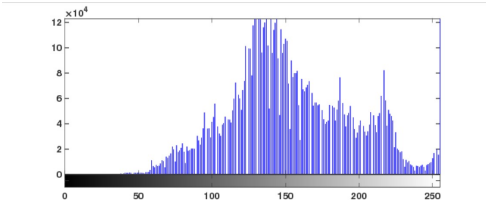

FIGURE 4.10 – Histogramme vidéo originale

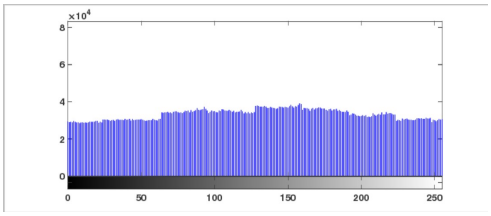

FIGURE 4.11 – Histogramme vidéo cryptée

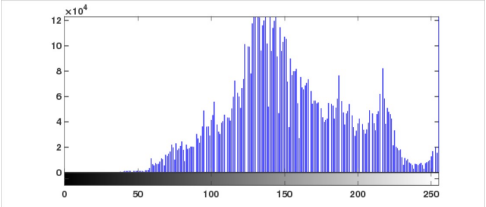

FIGURE 4.12 – Histogramme vidéo décryptée

FIGURE 4.13 – Histogrammes vidéo originale, cryptée et décryptée

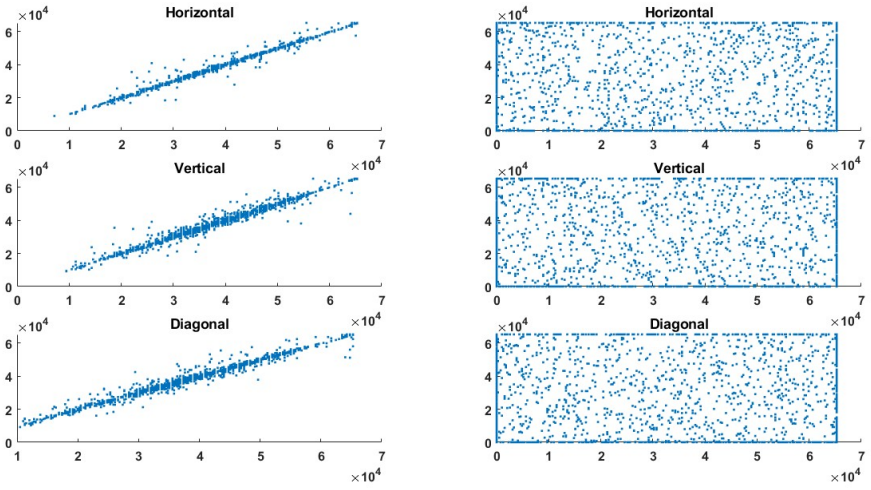

FIGURE 4.14 – La corrélation entre les pixels de la vidéo originale et cryptée .

NPCR indique une forte capacité à résister à diverses attaques.

— Le tableau suivant présente les différentes variations que nous avons apportées à notre système ainsi que les valeurs correspondantes du NPCR :

	Vidéo originale	Vidéo cryptée
Horizontale	0.9925	-6.3821 $\times 10^{-4}$
Verticale	0.9852	-0.0013
Diagonale	0.9802	-0.0034

TABLE 4.3 – Coefficients de corrélation de la vidéo originale et cryptée

	Variations	**NPCR**
Hénon modifier	$a - 10^{-5}$ et $b + 10^{-5}$	98.28 %
Observateur de Hénon modifié	$\alpha_{o1} + 10^{-8}$ et $\alpha_{o3} + 10^{-8}$	98.21 %
Observateur de Lozi	$\beta_{o1} + 10^{-8}$ et $\beta_{o2} - 10^{-8}$	99.08 %
	$0.628 + 10^{-7} \times z_1 + z_2$	99.53 %

TABLE 4.4 – Les différentes variations appliquées et les valeurs correspondantes du NPCR

4.13 Conclusion

Ce chapitre introduit les concepts fondamentaux des images et des vidéos, ainsi que les principes de base du traitement numérique de ces médias. Par la suite, nous appliquons notre approche basée sur les systèmes chaotiques fractionnaires au cryptage vidéo. Pour démontrer l'efficacité de notre méthode, nous présentons plusieurs tests et analyses approfondies illustrant la sécurité offerte.

Les coefficients de corrélation ainsi que le NPCR (Number of Pixels Change Rate) sont utilisés pour évaluer la robustesse du schéma face à diverses attaques. Les résultats obtenus attestent de la résilience de notre méthode face à ces menaces potentielles, soulignant ainsi sa fiabilité et sa capacité à sécuriser efficacement les données vidéo.

Cette étude met en lumière non seulement l'application des systèmes chaotiques fractionnaires dans le domaine du cryptage vidéo, mais aussi leur potentiel à fournir des solutions de sécurité robustes face aux défis de la protection des données.

Conclusion Générale

L'importance croissante de la protection des informations numériques dans un monde où la production multimédia et la diffusion électronique sont omniprésentes a conduit à des avancées significatives dans le domaine de la cryptographie. Nous avons exploré l'utilisation des systèmes chaotiques, en particulier ceux d'ordre fractionnaire, pour améliorer la sécurité des transmissions de données. Notre approche repose sur la synchronisation par observateurs en temps discret, qui a démontré son efficacité dans le cryptage vidéo.

Notre travail a pour objectif de concevoir un schéma innovant de transmission sécurisée de vidéos, utilisant des systèmes chaotiques comme le système de Lozi et le système de Hénon modifié. Nous avons démontré que ces systèmes, lorsqu'ils sont couplés et synchronisés de manière adéquate, offrent une robustesse accrue contre les attaques de cryptanalyse.

Le premier chapitre est consacré à l'introduction et à l'étude des systèmes chaotiques, en mettant en lumière leurs caractéristiques ainsi que les outils permettant d'identifier et d'analyser leurs comportements.

Le second chapitre expose les généralités sur la cryptographie et les diverses méthodes de chiffrement existantes. L'objectif de ce chapitre est d'introduire l'utilité et l'application du chaos en cryptographie.

Dans le troisième chapitre, nous abordons les différentes notions relatives au calcul fractionnaire, appliquées aux systèmes chaotiques en temps continu et en temps discret.

Le quatrième chapitre est consacré à l'étude et à la conception d'un schéma de transmission sécurisée en temps discret. Ce schéma comprend un émetteur composé de deux systèmes chaotiques d'ordre fractionnaire, à savoir le système de Lozi et le système de Hénon modifié, ainsi que deux observateurs "retardés étape par étape" à la réception. Ces observateurs permettent de reproduire les signaux chaotiques générés par l'émetteur et de récupérer le message confidentiel, de type vidéo.

Dans ce schéma, la vidéo originale est cryptée à l'aide de clés générées à partir des systèmes chaotiques d'ordre fractionnaire. La synchronisation basée sur des observateurs retardés étape par étape est mise en oeuvre pour estimer la clé lors du déchiffrement. Nous avons également effectué une analyse approfondie de la robustesse du schéma proposé face à diverses attaques de cryptanalyse.

Ainsi, notre mémoire a démontré le potentiel des systèmes chaotiques d'ordre fractionnaire dans le domaine du cryptage vidéo, ouvrant la voie à de nouvelles avancées technologiques pour la protection des données audiovisuelles.

En guise de perspectives, nous proposons les axes suivants :

— Élaboration de nouvelles méthodes de synchronisation fondées sur des observateurs pour les systèmes d'ordre fractionnaire.

— Application de ces nouvelles méthodes dans les protocoles de transmission sécurisée de données, images, vidéos et sons.

— Implémentation sur des circuits numériques tels que Arduino et Raspberry Pi.

Bibliographie

[1] R. Aguilar-Lopez, R. Martinez-Guerra et C. Perez-Pinacho. “Nonlinear observer for synchronization of chaotic systems with application to secure data transmission”. In : *European Physics Journal Special Topics* 223 (2014), p. 1541-1548.

[2] Taher Azar Ahmad et Vaidyanathan Sundarapandian. *Fractional Order Control and Synchronization of Chaotic Systems*. Springer, 2017.

[3] Author(s). “Stabilization and Synchronization of Discrete-time Fractional Chaotic Systems”. In : *Advances in Continuous and Discrete Models* (2022).

[4] Ahmad Taher Azar. *Fractional-Order Nonlinear Systems : Modeling, Analysis and Simulation*. Springer, 2018.

[5] Driss Boutat et Gang Zheng. *Observer Design for Nonlinear Dynamical Systems : Differential Geometric Methods*. Springer, 2012.

[6] E. Cherrier. “Estimation de l’état et des entrées inconnues pour une classe de systémes non linéaires”. Thèse de doct. France : Institut national polytechnique de Lorraine, 2006.

[7] Frédéric Dufaux. “Compression d’images et de vidéos pour les applications de communication”. Thèse de doct. Suisse : école Polytechnique Fédérale de Lausanne, 2007.

[8] R. Dumont. *Introduction á la cryptographie et á la sécurité informatique*. Note de cours, Université de Liége, 2006-2007. 2006.

[9] Jean Dupont. “Analyse des histogrammes et techniques de cryptanalyse des images”. Thése de doctorat. Thèse de doct. Paris, France : Université de Paris, 2010. url : https://tel.archives-ouvertes.fr/tel-01234567/document.

[10] Jean Dupont. “étude des attracteurs étranges dans les systémes dynamiques chaotiques”. Thèse de doct. Université Paris-Diderot, 2015. url : https://example.com/dupont2015.

[11] Yann Gaudeau. “Contributions en compression d’images médicales 3D et images naturelles 2D”. Thèse de doct. France : Université Henri Poincaré de Nancy 1, 2006.

[12] Alfred Grünwald et Aleksei Letnikov. “On the theory of differentiation and integration of variable order”. In : *Fract. Calc. Appl. Anal.* 1.1 (1997), p. 1-28.

[13] S. Guermah, S. Djennoune et M. Bettayeb. “Controllability and Observability of Linear Discrete-Time Fractional-Order Systems”. In : *International Journal of Applied Mathematics and Computer Science* 18.2 (2008), p. 213-222.

[14] V. Guerra, J. Smith et M. Lopez. “Linear Observers Design and Implementation”. In : *IEEE Transactions on Industrial Electronics* 67.5 (2020), p. 4205-4213.

[15] H. Hamiche. “Inversion á Gauche des Systémes Dynamiques Hybrides Chaotiques. Application á la Transmission Sécurisée de Données”. Thése de Doctorat. Université Mouloud Mammeri de Tizi-Ouzou (UMMTO), 2013.

[16] N. Hamrene, D. Idir et L. Hamoudi. “Codage d’images en sous bande par fractales : appliqué aux images médicales”. Thèse d’ingénieur d’état en électronique. UMMTO, 2005.

[17] A. Kerckhoffs. “La cryptographie militaire”. In : *Journal des sciences militaires* 9 (1883), p. 2-38, 161-191.

[18] Anatoly A. Kilbas, Hari M. Srivastava et Juan J. Trujillo. *Fractional Calculus and Fractional Processes with Applications to Financial Economics : Theory and Application.* Elsevier, 2006.

[19] M. Kolumban, M. P. Kennedy et L. O. Chua. “The role of synchronization in digital communications using chaos - part II : chaotic modulation and chaotic synchronization”. In : *IEEE Transactions on Circuits and Systems I : Fundamental Theory and Applications* 45.11 (1998), p. 1129-1140.

[20] M. L’Hernault, J.P. Barbot et A. Ouslimani. “Feasibility of Analog Realization of a Sliding-Mode Observer : Application to Data Transmission”. In : *IEEE Transactions on Circuits and Systems I : Regular Papers* (mar. 2008), p. 614-624.

[21] Kahina Lemikchi, Fatiha Ousmaal et Aldjia Rahali. *Segmentation Markovienne des images multispectrales MSG.* Mémoire d’ingénieur. Proposé et dirigé par Sadia Alkama. 2007.

[22] S. Li, G. Chen et G. Alvarez. “Return-map cryptanalysis revisited”. In : *International Journal of Bifurcation and Chaos* 16 (2006), p. 1557-1568.

[23] Edward N. Lorenz. “Deterministic Nonperiodic Flow”. In : *Journal of the Atmospheric Sciences* 20.2 (1963), p. 130-141. doi : 10.1175/1520-0469(1963)020<0130:DNF>2.0.CO;2.

[24] Edward N. Lorenz. *The Essence of Chaos*. Seattle, WA : University of Washington Press, 1993.

[25] Edward N Lorenz et K Haman. “The essence of chaos”. In : *Pure and Applied Geophysics* 147.3 (1996), p. 598-599.

[26] Marie Martin. “Analyse des bifurcations dans les systémes non linéaires : Applications au chaos”. Thèse de doct. Université Pierre et Marie Curie, 2018. url : https://example.com/martin2018.

[27] Marie Martin. “Étude des méthodes de corrélation pour l’analyse de la sécurité des images chiffrées”. ThÃ¨se de doctorat. Thèse de doct. Lyon, France : Université de Lyon, 2015. url : https://tel.archives-ouvertes.fr/tel-08901234/document.

[28] Robert M. May. “Simple Mathematical Models with Very Complicated Dynamics”. In : *Nature* 261 (1976), p. 459-467. doi : 10.1038/261459a0.

[29] Ouerdia Megherbi. “Etude et réalisation dâun système sécurisé à base de systèmes chaotiques”. Thèse de doct. Université Mouloud Mammeri, 2013.

[30] A. J. Michaels. “Digital Chaotic Communications”. PhD thesis. Georgia Institute of Technology, 2009.

[31] Kenneth S. Miller et Bertram Ross. *An Introduction to the Fractional Calculus and Fractional Differential Equations*. Wiley-Interscience, 1971.

[32] Jean-Luc Morin. “Compression vidéo : qualité subjective et méthodes de mesure”. Thèse de doct. France : Université de Rennes 1, 2009.

[33] Keith B. Oldham et Jerome Spanier. *The Fractional Calculus : Theory and Applications of Differentiation and Integration to Arbitrary Order*. Academic Press, 1974.

[34] Thomas L Pecora Louis M et Carroll. “Synchronisation dans les systÃ¨mes chaotiques”. In : *Lettres de rÃ©vision physique* 64 (), p. 821.

[35] Ivo PETRÁ. *Fractional-Order Nonlinear Systems : Modeling, Analysis and Simulation*. Springer, 2011.

[36] Arkady PIKOVSKY, Michael ROSENBLUM et Jürgen KURTHS. *Synchronization : A Universal Concept in Nonlinear Sciences*. Cambridge University Press, 2001.

[37] Igor PODLUBNY. *Fractional Differential Equations : An Introduction to Fractional Derivatives, Fractional Differential Equations, Some Methods of Their Solution and Some of Their Applications*. Academic Press, 1999.

[38] Ken C. POHLMANN. *Principles of digital audio*. 6th. New York, NY : McGraw-Hill Education, 2010.

[39] Henri POINCARÉ. "Sur le probléme des trois corps et les équations de la dynamique". Thèse de doct. Université Paris, 1890. URL : https://example.com/poincare1890.

[40] Louiza REZKALLAH. "De la cryptographie classique à la cryptographie moderne théorie et application". Thèse de doct. Alger, 2007.

[41] Iain E. G. RICHARDSON. *The H.264 advanced video compression standard*. Chichester, West Sussex, U.K. : Wiley, 2010.

[42] J.M.M. RODRIGUES. "Transfert sécurisé d'images par combinaison de techniques de compression, cryptage et marquage". Thèse de doct. France : Université Montpellier II, 2006.

[43] Michael SIPSER. *Introduction to the Theory of Computation*. 3rd. Cengage Learning, 2012.

[44] A. Murat TEKALP. *Digital video processing*. 2nd. Upper Saddle River, NJ : Pearson, 2015.

[45] Thomas WIEGAND et al. "Overview of the H.264/AVC video coding standard". In : *IEEE Transactions on Circuits and Systems for Video Technology* 13.7 (2003), p. 560-576. DOI : 10.1109/TCSVT.2003.815165.

[46] T. YANG. *Impulsive Control Theory*. Lecture Notes in Control and Information Sciences. Springer Verlag, 2001.

[47] H. ZHANG. "Chaos synchronization and its application to secure communication". Thèse de doct. Canada : University of Waterloo, 2010.