

RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

UNIVERSITÉ MOULOUD MAMMERI DE TIZI-OUZOU
FACULTÉ DE GENIE ELECTRIQUE ET DE L' INFORMATIQUE
DÉPARTEMENT D'AUTOMATIQUE

THÈSE DE DOCTORAT

Présentée pour obtenir le diplôme de

DOCTORAT

Spécialité : AUTOMATIQUE

Par :

Ouerdia MEGHERBI

THEME

**Synchronisation des systèmes chaotiques
discrets d'ordre fractionnaire pour la sûreté de
communication à base d'observateurs impulsifs**

SOUTENUE PUBLIQUEMENT DEVANT LE JURY :

Président	KARA Redouane	Professeur, Université Mouloud Mammeri de Tizi Ouzou
Rapporteur	HAMICHE Hamid	M.C.A, Université Mouloud Mammeri de Tizi Ouzou
Co/Rapporteur	DJENNOUNE Saïd	Professeur, Université Mouloud Mammeri de Tizi Ouzou
Examineur	LADACI Samir	Professeur, Université de Constantine
Examineur	KEMIH Karim	Professeur, Université de Jijel
Examineur	MELLIT Adel	Professeur, Université de Jijel
Invité	BETTAYEB Maâmar	Professeur, Université de Sharjah, Emirats Arabes Unis.

ANNÉE : 23 JUIN 2018

Dédicace

Je dédie ce travail de thèse à la mémoire de ma défunte mère qui aurait été, sans doute, très fière de moi.

Remerciements

Ce travail de thèse a été effectué au Laboratoire de Conception et Conduite des Systèmes de Production (L2CSP) de la faculté de Génie Electrique et Informatique de l'université Mouloud Mammeri de Tizi-Ouzou.

Il est vrai qu'une thèse de doctorat résume une expérience de recherche scientifique, de longues journées et nuits de réflexion et un tas de difficultés qu'il a fallu surmonter. Cependant, elle est avant tout un parcours humain qui ne peut être réussi sans aides et conseils. C'est effectivement le cas pour moi. L'aboutissement de ce travail et l'ampleur de notre contribution auraient en effet été impossibles sans la participation de près ou de loin des personnes et des institutions qui m'ont facilité les choses pour que ce travail soit mené à terme. Pour cette raison, c'est un vrai plaisir pour moi d'utiliser cet espace pour leur exprimer mes sincères remerciements.

Je tiens d'abord à remercier mon directeur de thèse, Monsieur Hamid HAMICHE, Maître de Conférences Classe A. C'était un honneur et un plaisir de travailler sous sa direction lors de ces dernières années. Je lui serai toujours reconnaissante pour la confiance qu'il m'a accordée en acceptant d'encadrer ce travail doctoral, pour ses multiples et précieux conseils et pour toutes les heures qu'il a consacrées à diriger cette thèse. Par sa persévérance et sa patience, il a su me guider dans chacune des étapes lors de mes recherches. J'aimerai également lui dire à quel point j'ai apprécié sa grande disponibilité et son respect sans faille des délais serrés de relecture des documents que je lui ai adressés malgré ses nombreuses responsabilités. Enfin, j'ai été extrêmement sensible à ses qualités humaines d'écoute et de compréhension tout au long de ce travail de thèse.

Je tiens également à exprimer ma profonde gratitude à mon co-directeur de thèse le Professeur Saïd DJENNOUNE. Depuis le début de ma thèse, il a été très présent et m'a accueillie avec gentillesse et patience à chaque fois que je venais le consulter pour lui poser des questions. Ses réponses m'ont toujours éclairci les idées et permis d'avancer dans mes travaux de recherche. J'admirerai toujours son savoir ainsi que sa capacité à l'exposer et à le partager. Il a aussi consacré beaucoup de son temps, en dépit de son emploi du temps chargé, à discuter à propos de notre travail et je lui en suis très reconnaissante.

Je remercie infiniment Monsieur Maâmar BETTAYEB, Professeur et Vice-recteur de l'université de Sharjah pour sa précieuse collaboration. Je ne peux oublier sa générosité et celle des membres de sa famille, sa patience et ses encouragements. Nous avons énormément apprécié sa présence durant mon stage scientifique tant sur le plan scientifique

que sur le plan humain. Je garderai toujours beaucoup de plaisir à discuter avec lui et à bénéficier de ses conseils et de son savoir. Ces quelques lignes ne suffiront certainement pas à lui décrire toute la mesure de ma gratitude pour les ressources intellectuelles et matérielles qu'il met à la disposition de ses étudiants pour leur permettre d'avancer dans leurs travaux. Je le remercie également d'avoir accepté notre invitation pour assister à ma soutenance de Doctorat.

Je tiens à remercier chaleureusement les membres du jury qui nous honorent par leur présence et ont accepté de juger nos travaux. Je leur suis reconnaissante d'avoir répondu présents pour juger notre travail et d'avoir consacré du temps à lire et à évaluer ce manuscrit de thèse.

Je tiens à remercier Monsieur KARA Redouane, Professeur à l'université Mouloud Mammeri de Tizi-Ouzou et Directeur du laboratoire L2CSP pour l'honneur et le plaisir qu'il m'a faits en acceptant de présider le jury et d'évaluer notre travail. Ses précieuses remarques et suggestions me permettront sans aucun doute d'améliorer la qualité de ce manuscrit. Qu'il trouve dans ces lignes l'expression de ma profonde gratitude.

Je remercie énormément Monsieur LADACI Samir, Professeur à l'université de Constantine ainsi que Monsieur KEMIH Karim et Monsieur MELLIT Adel, Professeurs à l'université de Jijel d'avoir accepté de faire partie de ce jury de soutenance et pour l'honneur qu'ils me font par leurs présences. Je leur suis infiniment reconnaissante de porter leurs regards d'experts sur notre travail et notre manuscrit de thèse. Leurs suggestions intéressantes, leurs remarques avisées et leurs discussions constructives m'aideront certainement à améliorer ce travail et me serviront à l'avenir pour en réaliser d'autres.

Je ne manquerai surtout pas de remercier tous les enseignants membres du laboratoire de Conception et Conduite des Systèmes de Production L2CSP qui grâce à leurs efforts et leurs expériences, m'ont offert l'opportunité et le plaisir de travailler dans un cadre de recherche convivial et riche en connaissances durant presque une décennie. Par leur rigueur scientifique, leur professionnalisme et leur enthousiasme pour leurs travaux de recherche, ils ont toujours été des exemples pour moi et je m'estime tout le temps chanceuse de travailler parmi eux au sein de ce laboratoire.

Mes vifs remerciements vont particulièrement à Mr Rafik SADDAOUI, Doctorant et enseignant en électronique, qui a mis à profit ses compétences en programmation et m'a aidée pour l'implémentation de notre travail sur les cartes Arduino.

Durant ces dernières années, j'ai eu le privilège et la chance d'effectuer des enseignements au département d'Automatique de la faculté de Génie Électrique et Informatique de l'université Mouloud Mammeri. Je tiens à adresser mes sincères et chaleureux remerciements au chef du Département Monsieur TOUAT Mohand ainsi qu'à l'ensemble des enseignants et fonctionnaires du département qui m'ont encouragée, guidée et facilité ma tâche. Je leur suis reconnaissante pour m'avoir fait profiter de leurs compétences et leurs riches expériences.

Je tiens également à exprimer ma reconnaissance au Vice-Doyen chargé de la post-Graduation le Professeur Mourad LAGHROUCHE ainsi qu'au personnel de la scolarité chargée de la Post-Graduation pour leur soutien permanent et leur accueil chaleureux à chaque fois que j'ai recours à eux. Je remercie aussi Monsieur le Doyen de la faculté de Génie Électrique et Informatiques Monsieur BELKAID Mohammed Saïd et tous les fonctionnaires de la faculté sans exception. Je leur suis redevable pour m'avoir permis d'étudier et d'effectuer mes travaux de recherche durant des années dans un endroit sûr et parmi des personnes sérieuses, compétentes et respectueuses.

Un grand merci à tous les enseignants et chercheurs du département de Génie Électrique et Informatique de l'université de Sharjah pour leur accueil chaleureux durant ma période de stage. Je serai toujours reconnaissante au Docteur Qassim NASIR, au Docteur Talal BONNY et à l'ingénieure Maha ALAA EDDIN pour le temps qu'ils m'ont consacré à répondre à mes questions techniques.

Mes remerciements seraient incomplets sans en adresser à mes amis et collègues du laboratoire L2CSP sans exception. Leurs riches connaissances, leurs qualités humaines et leur bonne humeur m'ont toujours permis d'avancer dans mes travaux dans une belle ambiance et de joindre ainsi l'utile à l'agréable. Merci à Sofiane HAMMOUCHE pour ses précieuses remarques, sa perspicacité et ses critiques positives, qui m'ont souvent aidée à faire mieux, à chaque fois que je le sollicite pour m'aider ou pour avoir son avis. Je remercie aussi Karima HAMMAR, Lamia, Sarah, Nabila, Karima TEBANI, Chahira, Nouara, Kahina, Karima HOUACINE, Tassadit, Hakima, Sassa, Samia, Saliha, Naima, Lynda, Aldjia, Ghania, Karima AMOURA, Rima, Katia, Nadia, Fatima, Zohra, Dyhia, Ahcène, Aghiles et Yacine. Je ne peux pas oublier mes amies hors du laboratoire qui m'ont toujours soutenue comme ma chère amie de longue date Samira, l'inoubliable Hakima du département des sciences de gestion et ma chère Nouara HAKEM.

La réalisation de ce travail n'aurait pu aboutir sans ma famille qui m'a toujours soutenue tout au long de mes études. Les mots ne peuvent exprimer combien je suis reconnaissante envers mon très cher père qui a veillé sur moi, m'a fait confiance et s'est toujours sacrifié pour sa famille. Je lui dois beaucoup l'aboutissement de mon travail. C'est aussi, grâce à ma douce et adorable belle-mère Fatima, grâce à son amour, à ses paroles apaisantes et à sa patience que j'ai réussi, souvent à vaincre le stress, surmonter les difficultés rencontrées et mener à terme ce travail de thèse. Je remercie aussi mes très chers frères Ouziane et Ouali qui m'ont constamment poussée et encouragée à avancer dans mes études et projets.

Je tiens aussi à remercier la famille Chachoua, parents de ma belle-mère, qui m'ont toujours réconfortée par leurs encouragements et par leur soutien infaillibles ces dernières années.

Je ne saurais clore ces pages sans remercier vivement mon oncle Mahammed MEGHERBI Professeur à la faculté Génie Électrique et Informatique à l'université Mouloud Mammeri de Tizi-Ouzou pour son aide et soutien indéfectibles tout au long de mes formations de graduation et de Post-graduation. Il m'a toujours motivée pour aller loin dans mes études. Qu'il trouve dans ces mots l'expression de ma profonde gratitude.

Liste des abréviations

<i>AES</i> :	Advanced Encryption Standard. Algorithme de chiffrement symétrique.
<i>DEMUX</i> :	Démultiplexeur.
<i>DES</i> :	Data Encryption Standard. Algorithme de chiffrement symétrique.
<i>E₀</i> :	Algorithme de chiffrement par flot utilisé par le protocole Bluetooth pour protéger les transmissions.
<i>IDEA</i> :	International Data Encryption Algorithm. C'est un algorithme de chiffrement symétrique.
<i>ICSP</i> :	In-Circuit Serial Programming. Interface de programmation des microcontrôleurs pouvant être reprogrammé in-situ.
<i>MD5</i> :	Message Digest 5. C'est une fonction de hachage cryptographique qui permet d'obtenir l'empreinte numérique d'un fichier.
<i>MUX</i> :	Multiplexeur
<i>NPCR</i> :	Number of Changing Pixel Rate. Métrique pour évaluer la robustesse d'un schéma de transmission.
<i>PRNG</i> :	Pseudorandom Number Generator. Générateur de nombres pseudo-aléatoires
<i>PSNR</i> :	Peak Signal to Noise Ratio. Mesure de distorsion utilisée en image numérique.
<i>RAM</i> :	Random Access Memory. Mémoire à accès aléatoire.
<i>RGB</i> :	Red Green Blue. Systèmes de codage informatique des couleurs (Rouge, Vert, Bleu).
<i>RC4</i> :	Rivest Cipher 4. C'est un algorithme de chiffrement en continu.
<i>RSA</i> :	Rivest Shamir Adleman. Algorithme de cryptographie asymétrique.
<i>SHA – 1</i> :	Secure Hash Algorithm. Fonction de hachage cryptographique conçue par la National Security Agency des États-Unis.
<i>UACI</i> :	Unified Averaged Changed Intensity. Métrique pour évaluer la robustesse d'un schéma de transmission
<i>UART</i> :	Universal Asynchronous Receiver Transmitter. émetteur-récepteur asynchrone universel.
<i>UIO</i> :	Unknown Input Observer. Observateur à entrée inconnue.
<i>USB</i> :	Universal Serial Bus. Bus universel en série : bus informatique série qui sert à connecter des périphériques informatiques à un ordinateur ou à tout type d'appareil prévu à cet effet.

Notations mathématiques

$\mathbb{R}$:	Ensemble des nombre réels.
$\mathbb{Z}$:	Ensemble de nombres relatifs.
$\mathbb{R}^n$:	Vecteur de réels de dimension n .
C^∞ :	Classe de fonctions infiniment dérivables et continues sur un intervalle.
$\mathcal{L}$:	Opérateur de Laplace.
$(.)^T$:	Transposée d'un vecteur ou d'une matrice.
D^α :	Opérateur de dérivation d'ordre fractionnaire α .
I^α :	Opérateur d'intégration d'ordre fractionnaire α .
$\Gamma(.)$:	Fonction Gamma.
E_α :	Fonction Mittag-Leffler à un seul paramètre.
$E_{\alpha,\beta}$:	Fonction Mittag-Leffler à deux paramètres.
Δ^α :	Opérateur de différence d'ordre fractionnaire α .
$ \cdot $:	Valeur absolue d'un nombre réel ou module d'un nombre complexe.
$\ \cdot\ $:	Norme vectorielle ou matricielle.
I_n :	Matrice identité de dimension n .
$\mathcal{O}$:	Matrice d'observabilité

Table des matières

Table des figures	xx
Table des tableaux	xxii
Introduction générale	1
1 Les systèmes dynamiques chaotiques d'ordre fractionnaire	9
1.1 Introduction	9
1.2 Concepts fondamentaux sur la théorie des systèmes dynamiques non linéaires	10
1.2.1 Systèmes dynamiques continus	10
1.2.2 Systèmes dynamiques discrets	11
1.2.3 Systèmes dynamiques à retards	11
1.2.4 Espace de phase et attracteurs	12
1.3 Généralités sur les systèmes chaotiques	13
1.3.1 Propriétés des systèmes chaotiques	15
1.3.2 Les exposants de Lyapunov	20
1.3.3 Bifurcations et routes vers le chaos	23
1.4 Analyse de la complexité des systèmes chaotiques	28
1.4.1 Complexité par l'algorithme de l'entropie spectrale	29
1.4.2 Complexité par l'algorithme C_0	29
1.5 Test 0 – 1 des systèmes chaotiques	30
1.6 Concepts de base et définitions dans le calcul fractionnaire	32
1.6.1 Les systèmes dynamiques d'ordre fractionnaire continu	34

1.6.2	Les systèmes dynamiques discrets d'ordre fractionnaire	41
1.7	Les systèmes chaotiques d'ordre fractionnaire	49
1.7.1	Systèmes chaotiques d'ordre fractionnaire continus	49
1.7.2	Systèmes chaotiques d'ordre fractionnaire discrets	52
1.8	Conclusion	57
2	Synchronisation des systèmes chaotiques d'ordre entier	59
2.1	Introduction	59
2.2	Synchronisation des systèmes chaotiques d'ordre entier	60
2.2.1	Historique	60
2.2.2	Principe de synchronisation des systèmes chaotiques	61
2.2.3	Types de synchronisation	62
2.2.4	Techniques et stratégies de synchronisation	65
2.3	Notions de base sur les observateurs d'états	74
2.3.1	Principe d'un observateur	74
2.3.2	Observabilité des systèmes non linéaires	75
2.4	Synchronisation des systèmes chaotiques d'ordre entier à base d'observateurs impulsifs	79
2.4.1	Synchronisation impulsive des systèmes chaotiques continus	80
2.4.2	Synchronisation impulsive des systèmes chaotiques discrets	87
2.5	Conclusion	92
3	Synchronisation impulsive des systèmes chaotiques discrets d'ordre fractionnaire	95
3.1	Introduction	95
3.2	Méthodes de synchronisation des systèmes chaotiques d'ordre fractionnaire : État de l'art	96
3.2.1	Synchronisation par contrôle actif	96
3.2.2	Commande par rétroaction	97
3.2.3	Synchronisation par la commande backstepping	97

3.2.4	Synchronisation par la commande adaptative	98
3.2.5	Synchronisation à base d'observateurs	98
3.3	Synchronisation des systèmes chaotiques d'ordre fractionnaire à base d'ob- servateurs impulsifs	100
3.3.1	Synchronisation impulsive des systèmes chaotiques continus d'ordre fractionnaire	100
3.3.2	Synchronisation impulsive des systèmes chaotiques discrets d'ordre fractionnaire	109
3.4	Synchronisation impulsive de deux systèmes chaotiques de Lozi d'ordre fractionnaire	115
3.4.1	Analyse des dynamiques du système de Lozi d'ordre fractionnaire	116
3.4.2	Structure de l'observateur impulsif d'ordre fractionnaire	126
3.4.3	Résultats de simulations	127
3.4.4	Résultats expérimentaux	131
3.5	Conclusion	140
4	Application de la synchronisation impulsive des systèmes chaotiques discrets d'ordre fractionnaire à la transmission sécurisée de données	143
4.1	Introduction	143
4.1.1	Introduction à la cryptographie	145
4.2	Le chaos en cryptographie	146
4.2.1	Relation entre les systèmes chaotiques et les systèmes cryptogra- phiques	147
4.2.2	Techniques de cryptage à base de systèmes chaotiques	148
4.2.3	Schémas de transmission de données à base de systèmes chaotiques d'ordre fractionnaire	157
4.3	Transmission d'images à base de la synchronisation impulsive des systèmes chaotiques discrets d'ordre fractionnaire	159
4.3.1	Structure de l'émetteur	159
4.3.2	Structure du récepteur	162

4.3.3	Résultats de transmission	163
4.4	Conclusion	168
5	Etude de la robustesse et analyse de la sécurité du schéma de transmis-	
	sion	169
5.1	Introduction	169
5.2	Introduction à la cryptanalyse	170
5.3	Analyse de la robustesse du schéma de transmission proposé	171
5.3.1	Analyse statistique	171
5.3.2	Analyse de sensibilité des clés secrètes	174
5.3.3	Analyse de l'espace de clés	175
5.3.4	Analyse de la qualité de cryptage	175
5.3.5	Analyse de la rapidité	176
5.3.6	Robustesse vis à vis du bruit	176
5.4	Analyse de sécurité du système de transmission proposé	176
5.4.1	Résultats de l'analyse de l'histogramme	177
5.4.2	Résultats de l'analyse de corrélation entre pixels adjacents	180
5.4.3	Résultats de l'analyse de l'entropie	182
5.4.4	Résultats d'analyses de la sensibilité vis à vis des clés secrètes	182
5.4.5	Résultats de l'analyse de l'espace des clés	183
5.4.6	Qualité du cryptage	185
5.4.7	Résultats de l'analyse de la rapidité du système de transmission	186
5.4.8	Effet du bruit sur la transmission	186
5.5	Conclusion	187
	Annexe A : Observabilité des systèmes dynamiques d'ordre fractionnaire	189
	Conclusion Générale	199
	Bibliographie	203

Table des figures

1.1	Sensibilité de l'état x de la fonction logistique aux conditions initiales . . .	16
1.2	Spectre de fréquence de l'état x de la fonction logistique chaotique	17
1.3	Attracteur chaotique étrange de Lorenz	19
1.4	Attracteur chaotique étrange de Fold	19
1.5	Quantification de la divergence de trajectoires par les exposants de Lyapunov	20
1.6	Exposants de Lyapunov de la fonction logistique avec $x(0) = 0.1$	22
1.7	Diagramme de bifurcation de la fonction logistique	24
1.8	Intermittences vers le chaos dans le circuit de Chua	26
1.9	Route vers le chaos par quasi-périodicité dans un circuit électrique, (a) :	
	$p_1 = 2, (b) : p_1 = 8, (c) : p_1 = 8.8, (d) : p_1 = 9.6, (e) : p_1 = 10.8, (f) : p_1 = 15$	27
1.10	Route vers le chaos par doublements de périodes dans le système de Lorenz	28
1.11	Application du test 0 – 1 sur la fonction logistique : Plans de phases $p - s$	
	pour différentes valeurs de r	32
1.12	Valeurs des coefficients C_p pour différents ordres fractionnaires	47
1.13	Attracteur étrange de Rössler d'ordre fractionnaire avec $a = 0.5, b = 0.2,$	
	$c = 10$ et $\alpha_{11} = 0.9, \alpha_{12} = 0.85$ et $\alpha_{13} = 0.95$	51
1.14	Evolution chaotique des états x_1, x_2 et x_3 du système de Rössler d'ordre	
	fractionnaire avec $a = 0.5, b = 0.2, c = 10$ et $\alpha_{11} = 0.9, \alpha_{12} = 0.85$ et	
	$\alpha_{13} = 0.95$	51
1.15	Attracteur étrange de Chen d'ordre fractionnaire avec $\bar{a} = 35, \bar{b} = 3, \bar{c} = 28$	
	et $\alpha_{21} = \alpha_{22} = \alpha_{23} = 0.95$	52

1.16	Evolution chaotique des états x_1 , x_2 et x_3 du système de Chen d'ordre fractionnaire avec $\bar{a} = 35$, $\bar{b} = 3$, $\bar{c} = 28$ et $\alpha_{21} = \alpha_{22} = \alpha_{23} = 0.95$	53
1.17	Evolution chaotique de la fonction logistique d'ordre fractionnaire pour $r = 4$ $\alpha = 0.96$ et $L = 20$	54
1.18	Attracteur étrange de la fonction logistique d'ordre fractionnaire pour $r = 4$ $\alpha = 0.96$ et $L = 20$ en plan de phase $(x(k) - x(k-1))$	55
1.19	Attracteur étrange du système de Lozi d'ordre fractionnaire avec $a = 1.7$, $b = 0.5$, $\alpha_1 = \alpha_2 = 0.95$ et $L = 10$	56
1.20	Evolution chaotique des états x_1 et x_2 du système de Lozi d'ordre fractionnaire avec $a = 1.7$, $b = 0.5$ et $\alpha_1 = \alpha_2 = 0.95$	56
2.1	Principe de synchronisation par répartition du système	63
2.2	Principe de synchronisation à base d'observateurs	73
2.3	Principe de la méthode de synchronisation par observateur impulsif	79
2.4	Estimation des états du système de Lorenz par l'observateur impulsif	86
2.5	Erreurs de synchronisation impulsive entre deux systèmes chaotiques de Lorenz	87
2.6	Erreurs de synchronisation impulsive avec $\delta = 2.5$ entre deux systèmes chaotiques de Lorenz	87
2.7	Etats synchronisés x_1 et $\hat{x}_1$ du système de Lozi d'ordre entier	92
2.8	Etats synchronisés x_2 et $\hat{x}_2$ du système de Lozi d'ordre entier	92
2.9	Erreur de synchronisation impulsive $e_1 = x_1 - \hat{x}_1$ entre deux systèmes chaotiques de Lozi	93
2.10	Erreur de synchronisation $e_2 = x_2 - \hat{x}_2$ entre deux systèmes chaotiques de Lozi	93
3.1	Attracteur étrange du système chaotique de Lü d'ordre fractionnaire avec $\alpha = 0.95$	108
3.2	Estimation des états du système de Lü d'ordre fractionnaire par l'observateur impulsif	110

3.3	Erreurs de synchronisation impulsive pour le système de Lü d'ordre fractionnaire	111
3.4	Diagramme de bifurcation du système de Lozi pour différentes valeurs de a (Cas commensurable)	117
3.5	Diagramme de bifurcation du système de Lozi d'ordre fractionnaire pour différentes valeurs de α_1	117
3.6	Spectres de fréquences du signal x_1 du système de Lozi d'ordre fractionnaire pour différentes valeurs des paramètres a et b et des ordres α_1 et α_2	118
3.7	Spectres de fréquences du signal x_2 du système de Lozi d'ordre fractionnaire pour différentes valeurs des paramètres a et b et des ordres α_1 et α_2	119
3.8	Complexité SE du signal chaotique x_1 du système de Lozi d'ordre fractionnaire dans le cas commensurable. (a) : Valeurs de SE en fonction du paramètre a , (b) : Valeurs de SE en fonction de l'ordre α , (c) : Plan $(a - \alpha)$	120
3.9	Complexité C_0 du signal chaotique x_1 du système de Lozi d'ordre fractionnaire dans le cas commensurable. (a) : Valeurs de C_0 en fonction du paramètre a , (b) : Valeurs de C_0 en fonction de l'ordre α , (c) : Plan $(a - \alpha)$	121
3.10	Complexité SE du signal chaotique x_2 du système de Lozi d'ordre fractionnaire dans le cas non commensurable (a) : Valeurs de SE en fonction du paramètre a , (b) : Valeurs de SE en fonction de l'ordre α_1 , (c) : Plan $(a - \alpha_1)$	122
3.11	Complexité C_0 du signal chaotique x_2 du système de Lozi d'ordre fractionnaire dans le cas non commensurable. (a) : Valeurs de C_0 en fonction du paramètre a , (b) : Valeurs de C_0 en fonction de l'ordre α_1 , (c) : Plan $(a - \alpha_1)$	123
3.12	Résultats d'application du test 0 – 1 sur la séquence x_1 du système de Lozi d'ordre fractionnaire : Plans de phases $p - s$ pour différentes valeurs des paramètres et des ordres fractionnaires	124
3.13	Résultats d'application du test 0 – 1 sur la séquence x_2 du système de Lozi d'ordre fractionnaire : Plans de phases $p - s$ pour différentes valeurs des paramètres et des ordres fractionnaires	124

3.14 États synchronisés x_1 et $\hat{x}_1$ du système de Lozi d'ordre fractionnaire et de l'observateur impulsif d'ordre fractionnaire	128
3.15 États synchronisés x_2 et $\hat{x}_2$ du système de Lozi d'ordre fractionnaire et de l'observateur impulsif d'ordre fractionnaire	128
3.16 Erreurs de Synchronisation impulsive entre le système de Lozi d'ordre fractionnaire et l'observateur impulsif d'ordre fractionnaire	129
3.17 Estimation de l'état x_1 du système de Lozi par l'observateur impulsif dans le cas non commensurable	129
3.18 Estimation de l'état x_2 du système de Lozi par l'observateur impulsif dans le cas non commensurable	130
3.19 Erreurs de synchronisation dans le cas non commensurable	131
3.20 États synchronisés x_1 et $\hat{x}_1$ pour $\hat{x}_1(0) = -17$	131
3.21 États synchronisés x_2 et $\hat{x}_2$ pour $\hat{x}_1(0) = -17$	132
3.22 Erreurs de synchronisation pour $\hat{x}_1(0) = -17$	132
3.23 États synchronisés x_1 et $\hat{x}_1$ pour $\hat{x}_2(0) = 8$	133
3.24 États synchronisés x_2 et $\hat{x}_2$ pour $\hat{x}_2(0) = 8$	133
3.25 Erreurs de synchronisation pour $\hat{x}_2(0) = 8$	134
3.26 Carte à microncontrôleur Arduino-Mega	135
3.27 Code du système de Lozi d'ordre fractionnaire	136
3.28 Code de l'observateur impulsif d'ordre fractionnaire	137
3.29 Implémentation de la synchronisation impulsive sur cartes Arduino-Mega .	138
3.30 Attracteur étrange du système de Lozi d'ordre fractionnaire en utilisant la carte Arduino-Mega (x_1 en abscisse et x_2 en ordonnée)	138
3.31 Etats x_1 (signal supérieur) et x_2 (signal inférieur) du système de Lozi d'ordre fractionnaire	139
3.32 Résultats de la synchronisation impulsive : (du haut vers le bas) : état x_1 , état estimé $\hat{x}_1$, état x_2 , état estimé $\hat{x}_2$ et les impulsions de contrôle	139
3.33 Plan de phase des états synchronisés x_1 (en abscisse) et $\hat{x}_1$ (en ordonnée) obtenus par la carte Arduino-Mega	140

3.34 Plan de phase des états x_2 (en abscisse) et $\hat{x}_2$ (en ordonnée) obtenus par la carte Arduino-Mega	141
4.1 Principe du cryptage par addition	153
4.2 Principe du cryptage par commutation	154
4.3 Principe du cryptage par modulation chaotique	155
4.4 Cryptage par inclusion et décryptage par Observateur à entrées inconnues .	156
4.5 Cryptage par inclusion et décryptage par Inversion du modèle de l'émetteur	157
4.6 Diagramme bloc de l'émetteur du schéma de transmission proposé	159
4.7 Diagramme bloc du récepteur du schéma de transmission proposé	160
4.8 Les images tests utilisées : a : Image Cameraman.jpg, b : Image Peppers.jpg, c : Image Baboon.jpg	164
4.9 Erreurs de synchronisation impulsive	165
4.10 Transmission de l'image Cameraman.jpg. (a) : Image originale , (b) : Image chiffrée, (c) : Image reçue	165
4.11 Transmission de l'image Baboon.jpg. (a) : Image originale , (b) : Image chiffrée, (c) : Image reçue	166
4.12 Transmission de l'image Peppers.jpg. (a) : Image originale , (b) : Image chiffrée, (c) : Image reçue	166
4.13 Signal envoyé sur le canal lors de la transmission de l'image Cameraman .	166
4.14 Signal envoyé sur le canal lors de la transmission de l'image Peppers . . .	167
4.15 Signal envoyé sur le canal lors de la transmission de l'image Baboon . . .	167
4.16 Plans de phases des images originales et reçues. (a) : Image Cameraman, (b) : Image Pepper, (c) : Image Baboon	168
5.1 Image Cameraman originale et son histogramme	177
5.2 Image Cameraman chiffrée et son histogramme	177
5.3 Image Peppers originale et ses histogrammes	178
5.4 Image Peppers chiffrée et ses histogrammes	178
5.5 Image Baboon originale et ses histogrammes	179

5.6	Image Baboon chiffrée et ses histogrammes	179
5.7	Corrélation des pixels adjacents dans les images Cameraman originale et chiffrée dans les différentes directions	181
5.8	Sensibilité aux variations des clés en utilisant l'image Cameraman. (a) : Image Cameraman originale, (b) : Image Cameraman chiffrée, (c) : Image Cameraman déchiffrée avec une variation 10^{-16} du paramètre b	184
5.9	Sensibilité aux variations des clés en utilisant l'image Peppers. (a) : Image Peppers originale, (b) : Image Peppers chiffrée, (c) : Image Peppers déchif- frée avec une variation 10^{-16} du paramètre α_1	184

Liste des tableaux

1.1	Exposants de Lyapunov pour différents attracteurs	22
3.1	Résultats du test $0 - 1$	125
3.2	Valeurs de l'exposant de Lyapunov maximal obtenues pour le système de Lozi d'ordre fractionnaire pour différents paramètres et ordre fractionnaire	126
4.1	Comparaison entre les propriétés des systèmes chaotiques et les propriétés des systèmes cryptographiques	148
5.1	Valeur de χ^2 obtenue pour l'image cameraman	180
5.2	Valeurs de χ^2 obtenues pour les images test Peppers.jpg et Baboon.jpg . .	180
5.3	Les résultats de corrélation entre pixels adjacents en utilisant l'image Ca- meraman	181
5.4	Résultats de corrélation entre pixels adjacents en utilisant l'image Peppers.jpg	182
5.5	Résultats de corrélation entre pixels adjacents en utilisant l'image Baboon.jpg	182
5.6	Les résultats d'entropie des images Cameraman originale et chiffrée	183
5.7	Valeur d'entropie en utilisant les images couleur	183
5.8	La sensibilité aux variations des clés en utilisant l'image Cameraman . . .	183
5.9	La sensibilité aux variations des clés en utilisant l'image Peppers	185
5.10	La sensibilité aux variations des clés en utilisant l'image Baboon	185
5.11	Taux $PSNR$ entre l'image Cameraman et l'images cryptée associée	186
5.12	Taux $PSNR$ en utilisant les images Peppers et Baboon	186
5.13	Résultats de l'analyse de la rapidité du système de transmission proposé .	187
5.14	Taux $PSNR$ après ajout du bruit à l'image Cameraman	187

5.15 Taux PSNR après ajout du bruit à l'image Peppers	188
---	-----

Introduction Générale

A l'ère numérique actuelle, avec l'émergence des nouvelles technologies de la communication tel l'Internet, les communications sans fil et par satellite, les vidéo conférences et la messagerie électronique, la sécurité des échanges d'informations est devenue une préoccupation majeure [1]. Ce besoin de protection et de confidentialité de l'information transmise est, de plus, évolutif et est appelé à croître de façon exponentielle dans le futur en raison de la hausse spectaculaire des achats et des transactions bancaires et commerciales en ligne et via des réseaux publics. Dans ce contexte, la cryptographie joue un rôle capital et le recours aux techniques de cryptage ou de chiffrement pour protéger les données devient incontournable [2].

La cryptographie est l'art et la science de protection d'une information ou d'un message secret, et ce en brouillant son allure ou sa structure de manière à la rendre insignifiante et incompréhensible aux yeux de personnes non autorisées à connaître son contenu [3]. Diverses approches et algorithmes ont été élaborés et mis en oeuvre pour chiffrer et sécuriser les données. On peut citer, entre autres, les algorithmes de chiffrement classiques tels le DES (Data Encryption Standard) et le RSA (Rivest Shamir Adleman) [4] qui ont été utilisés pour crypter des messages binaires ou textes et ont permis leur transmission en toute sécurité [5]. Toutefois, ces algorithmes peuvent ne pas être aussi efficaces et appropriés dans le cas de données multimédia complexes comme les images et vidéos [6]. Ces types de données sont, en effet, souvent volumineux et sont caractérisés par une haute redondance et une forte corrélation de pixels [7]. L'application de tels algorithmes engendrera un temps de calculs élevé et une implémentation coûteuse. La recherche d'une solution alternative pour sécuriser l'envoi de tels fichiers devient alors nécessaire et la théorie du

chaos représente, à cet effet, une option intéressante.

Le chaos est l'une des dynamiques les plus complexes que peuvent exhiber les systèmes dynamiques non linéaires. Le comportement chaotique a été observé dans plusieurs systèmes non linéaires évoluant aussi bien en temps continu comme les systèmes de Lorenz, Rossler et Chen qu'en temps discret comme les systèmes de Hénon et de Lozi [8]. Suite à de nombreuses études et analyses, il s'est avéré que les systèmes chaotiques présentent des propriétés importantes telles la reproductibilité à l'identique, l'aspect aléatoire et la sensibilité aux variations des paramètres et aux conditions initiales qui satisfont certaines exigences des systèmes cryptographiques [9]. Depuis, de nombreux algorithmes de cryptage et schémas de communication, fondés sur les propriétés des systèmes chaotiques, ont été proposés. Lorsqu'on évoque le cryptage ou chiffrement de données à base du chaos, il s'agit, en effet, de dissimuler un signal message en le noyant dans un signal chaotique à travers plusieurs étapes et combinaisons successives. Les paramètres du système chaotique utilisé constituent alors les clés de chiffrement secrètes.

Tout comme la théorie du chaos qui a permis de changer notre vision, d'interpréter différemment et même d'exploiter certains phénomènes physiques, qualifiés depuis des temps comme étant incohérents, la théorie du calcul fractionnaire basée, sur la généralisation des dérivées d'ordres entiers à des ordres non entiers a, en parallèle, le potentiel énorme de changer la manière dont nous percevons, nous décrivons et nous contrôlons la nature autour de nous.

La théorie du calcul fractionnaire date de plus de trois siècles. Elle a presque la même longue histoire que le calcul différentiel d'ordre entier. Toutefois, et en raison du manque du concept d'application, son développement est relativement lent [10]. En fait, plusieurs systèmes physiques tels les processus thermiques [11], la polarisation diélectrique [12] et les ondes électromagnétiques peuvent être décrits par des modèles d'ordre fractionnaire. Il s'est avéré de plus, que comparées aux équations différentielles d'ordre entier, les équations

tions d'ordre fractionnaire peuvent caractériser plus précisément le phénomène naturel dans les domaines de la science appliquée tels la mémoire et l'hérédité des processus et matériaux variés, les lignes de transmission [13], la caractérisation électrique, les amortisseurs viscoélastiques [14], les oscillateurs sinusoïdaux d'ordre fractionnaire [15], etc.

Récemment, il s'est révélé que le caractère chaotique de certains systèmes non linéaires comme les systèmes de Lorenz, de Chen, de Hénon et bien d'autres est toujours présent bien que l'ordre du système change de l'ordre entier à l'ordre fractionnaire. On parle alors de systèmes chaotiques d'ordre fractionnaires [16]. L'étude de ces derniers est devenue actuellement une thématique de recherche intensément traitée dans le domaine des systèmes dynamiques non linéaires.

L'étude du comportement chaotique d'un système d'ordre fractionnaire est essentiellement basée sur celle du système d'ordre entier. L'idée principale est d'observer si oui ou non le système présente toujours une dynamique chaotique lorsque son ordre est fractionnaire [17]. A ce jour, la détermination de l'ordre fractionnaire lorsque le système entre en régime chaotique et les caractéristiques du système chaotique d'ordre fractionnaire restent des sujets de recherche ouverts.

Actuellement l'application des systèmes chaotiques d'ordre fractionnaire devient une nouvelle direction de recherche appliquée en sciences non linéaires, notamment, dans les aspects de communication sécurisée. En effet, la complexité du système d'ordre fractionnaire, est un point clé de la performance et de la sécurité du système cryptographique [18]. On distingue deux formes de complexité dans un système chaotique d'ordre fractionnaire. La première complexité est celle reliée au terme non linéaire dans son équation et peut aussi être associée à l'ordre non entier. Cette complexité peut être mesurée par le calcul des fractales du système. La deuxième complexité est celle des séries temporelles générées par le système chaotique d'ordre fractionnaire. En outre, l'utilisation des systèmes chaotiques d'ordre fractionnaire présente l'avantage de renforcer l'algorithme de cryptage

puisque les ordres de dérivation peuvent être considérés comme clés secrètes supplémentaires [19].

Dans un schéma d'une transmission de données à base de systèmes chaotiques, un générateur chaotique identique à celui utilisé pour le cryptage, au niveau de l'émetteur, doit être reproduit au niveau du récepteur afin de récupérer l'information secrète. Toutefois et compte tenu de la sensibilité élevée et du caractère imprévisible des systèmes chaotiques ainsi que des éventuels bruits dans le canal de transmission, il n'est pas toujours facile de dupliquer exactement, au niveau du récepteur, les signaux chaotiques, utilisés lors du processus de chiffrement à l'émission. Pour surmonter ces difficultés, il devient primordial d'imposer au générateur chaotique du coté récepteur, par un couplage approprié, d'adopter de façon permanente le même comportement et de suivre la même dynamique que celle du système chaotique utilisé lors du chiffrement du message. On parle alors de synchroniser l'émetteur et le récepteur ou, plus correctement, de synchroniser les systèmes chaotiques exploités, respectivement, aux niveaux émetteur et récepteur.

La synchronisation est considérée, par conséquent, comme le pilier central de l'application des systèmes chaotiques pour sécuriser les communications, que ce soit dans le cas de systèmes d'ordre entier ou des systèmes d'ordre fractionnaire. La synchronisation fait référence à un processus où deux ou plusieurs systèmes chaotiques ajustent leurs dynamiques vers un comportement commun dû à un couplage ou forçage [20]. Pecora et Carroll ont été les premiers à proposer le concept de la synchronisation chaotique et à la réaliser, en utilisant le principe maître-esclave, en 1990 [21]. Ce progrès de recherche révolutionnaire a ainsi mis fin à l'idée traditionnelle selon laquelle le comportement chaotique est nuisible et incontrôlable. Durant la vingtaine d'années qui suit, la synchronisation chaotique s'est beaucoup développée. Plusieurs régimes de synchronisations comme la synchronisation projective [22], la synchronisation retardée [23] et la synchronisation généralisée [24] ont été établis et plusieurs méthodes de synchronisation ont été proposées. Parmi ces méthodes, on retrouve la synchronisation à base d'observateurs dont le principe est

de concevoir un système dit observateur permettant de restituer les états d'un système chaotique [25]. Les observateurs impulsifs sont une classe d'observateurs permettant de reconstruire les états d'un système chaotique en recevant ces derniers à des instants discrets. La synchronisation par observateurs impulsifs dite aussi synchronisation impulsive consiste en effet à utiliser des échantillons des états d'un système chaotique à des instants discrets pour établir la synchronisation entre ce système et un autre après un certain temps [26]. Cette approche présente plusieurs avantages, particulièrement dans les systèmes de transmission tels l'implémentation facile, la non redondance de signaux, et la non surcharge du canal de transmission [27].

Si les résultats de synchronisation obtenus dans le cas de systèmes d'ordre entier sont très nombreux, la recherche dans le cas d'ordre fractionnaire est encore à ses débuts, et ce, dû au manque d'outils mathématiques effectifs. En effet, si on applique les méthodes de synchronisation des systèmes d'ordre entier à un système chaotique d'ordre fractionnaire, les caractéristiques réelles seront ignorées. Pour ces raisons, l'étude des méthodes de synchronisation des systèmes chaotiques d'ordre fractionnaire devient pertinente pour leur application réelle. Dernièrement, quelques types de synchronisation cités auparavant tels la synchronisation généralisée, la synchronisation de phase, la synchronisation projective et quelques méthodes comme la synchronisation par observateurs ont été généralisés aux cas de systèmes chaotiques continus d'ordre fractionnaire [28].

Récemment, les définitions importantes des dérivées fractionnaires continues ont été discrétisées et ont conduit à un nouveau domaine de recherche et d'études qui est le calcul fractionnaire discret. Ce dernier se développe à un rythme accéléré et est appliqué dans divers champs [29].

Bien que plusieurs études ont été faites dans le cas des systèmes linéaires discrets d'ordre fractionnaire, ce n'est malheureusement pas le cas pour le cas de systèmes non linéaires qui n'est pas beaucoup abordé [30]. Comme les systèmes en temps discret sont

représentés par des équations aux différences, l'utilisation des équations aux différences d'ordre fractionnaire semble être un outil puissant pour la modélisation plus réaliste de la dynamique des systèmes complexes discrets. A cet effet, plusieurs définitions de dérivées discrètes ont été avancées par plusieurs chercheurs. Néanmoins, et contrairement au cas de systèmes continus, peu d'approches de synchronisation ont été proposées ou généralisées pour la synchronisations des systèmes chaotiques discrets d'ordre fractionnaire. En effet, et à ce jour, rares sont les méthodes de synchronisation qui ont été proposées pour les systèmes chaotiques d'ordre fractionnaires discrets [31]. Or dans des applications de transmission de données numériques, les systèmes discrets sont plus efficaces et appropriés que les systèmes continus. En effet, dû à plusieurs inconvénients comme les bruits du canal de transmission et la fluctuation des valeurs des composants électroniques utilisés, la synchronisation des systèmes chaotiques continus peut être altérée [32]. Pour toutes ces raisons, de nombreuses tentatives de transmission à base de circuits chaotiques analogiques sont vouées à l'échec. En outre, l'information telle qu'elle apparait de nos jours est de plus en plus numérisée, traitée et échangée par les calculateurs numériques [33]. Les schémas de communication à base de systèmes chaotiques discrets sont donc plus faciles à implémenter.

Dans l'ensemble, on peut dire que la recherche dans le domaine des systèmes chaotiques d'ordre fractionnaire, particulièrement dans le cas discret, est encore au stade initial. Il reste encore beaucoup de questions théoriques et pratiques qui nécessitent une étude plus approfondie.

Pour cette raison, et compte tenu des thèmes et problématiques abordés précédemment ainsi que des travaux pionniers déjà effectués, le travail présenté dans ce manuscrit de thèse, s'inscrit dans le cadre de la synchronisation des systèmes chaotiques discrets d'ordre fractionnaire pour la transmission sécurisées de données. Notre objectif dans ce travail de thèse est donc double. Il s'agit, d'une part, de proposer un schéma de synchronisation des systèmes chaotiques d'ordre fractionnaire discrets en utilisant un observateur d'ordre fractionnaire impulsif et, de l'autre part, de l'utilisation du schéma de synchroni-

sation conçu dans un système de transmission sécurisée de données.

Afin de faciliter la lecture de ce manuscrit, nous avons trouvé nécessaire de structurer notre travail de thèse en cinq chapitres. Ils sont, alors, organisés comme suit :

- Le premier chapitre de cette thèse consiste en l'étude de systèmes chaotiques d'ordre fractionnaire. Lors de ce chapitre nous rappellerons quelques définitions et caractéristiques des systèmes chaotiques en général. Nous fournirons par la suite des notions de base et définitions sur le calcul fractionnaire qui nous seront utiles pour la modélisation et l'étude des systèmes chaotiques d'ordre fractionnaire.
- Le deuxième chapitre consiste à l'étude de synchronisation de systèmes chaotiques d'ordre entier. Le principe de synchronisation ainsi que les approches utilisées y seront développés en détails en temps continu et discret. Nous nous focaliserons, par la suite, sur la méthode de synchronisation par observateurs et en particulier par les observateurs impulsifs.
- Dans le troisième chapitre, nous aborderons le problème de synchronisation des systèmes chaotiques d'ordre fractionnaire par observateurs impulsifs. Nous étudierons d'abord les différentes approches proposées dans le cas des systèmes continus puis présenterons notre contribution pour les systèmes chaotiques discrets d'ordre fractionnaire.
- Afin de montrer l'efficacité de notre schéma de synchronisation, nous présenterons, dans le quatrième chapitre, une application à la transmission sécurisée à base de la synchronisation de deux systèmes discrets d'ordre fractionnaire.
- Le cinquième et dernier chapitre de ce travail de thèse sera consacré à évaluer la robustesse et l'efficacité du système de transmission proposé. Il s'agit de vérifier que le système proposé dans le chapitre 4 peut résister aux différentes attaques et

tentatives d'intrusions.

- La conclusion générale et quelques perspectives ouvertes par le présent travail seront présentées à la fin de ce manuscrit de thèse.

Chapitre 1

Les systèmes dynamiques chaotiques d'ordre fractionnaire

1.1 Introduction

La théorie du chaos, en tant que nouvelle branche de la physique et des mathématiques, a fourni une nouvelle façon de voir l'univers et un outil important pour comprendre le comportement de plusieurs processus et systèmes physiques [34]. Cette théorie commence à prendre forme dans la seconde moitié du vingtième siècle après l'observation de différents systèmes qui, en dépit de la connaissance de leurs règles d'évolution et de leurs conditions initiales, leur futur semblait être arbitraire et imprévisible. La théorie du chaos a connu ces dernières années de multiples applications dans divers domaines de la science et de l'ingénierie tels la biologie [35], l'économie [36], la robotique [37], etc.

D'autre part, l'émergence récente des méthodes de dérivation et d'intégration d'équations d'ordre non entier a rendu les systèmes d'ordre fractionnaire de plus en plus attractifs [38]. En effet, et bien que le calcul fractionnaire a été introduit en 1695, il a été considéré pendant longtemps comme un domaine purement mathématique sans applications réelles [39]. Ceci a toutefois changé et le calcul fractionnaire s'est avéré très utile pour modéliser la viscoélasticité [40], les ondes électromagnétiques [41], l'évolution quantique de systèmes

complexes [42], etc.

Tous comme les systèmes d'ordre entier, les systèmes d'ordre fractionnaire, continus et discrets, peuvent aussi avoir des dynamiques complexes et même chaotiques. En effet, le comportement chaotique a été observé dans les systèmes d'ordre fractionnaire de Chua, Duffing, Lorenz, Chen, Rössler, Lü, Hénon, etc [43].

L'objectif de ce chapitre est donc de disposer des éléments théoriques nécessaires à l'étude des systèmes chaotiques d'ordre fractionnaire. Nous partirons de quelques définitions préliminaires permettant de comprendre les caractéristiques essentielles des systèmes dynamiques chaotiques, puis nous présenterons quelques notions de bases sur les systèmes d'ordre fractionnaire. Nous terminerons ce chapitre par l'étude de quelques exemples de systèmes chaotiques d'ordre fractionnaire.

1.2 Concepts fondamentaux sur la théorie des systèmes dynamiques non linéaires

Un système dynamique est un système dont l'état change avec le temps. Mathématiquement, un système dynamique consiste en un espace d'états et une loi appelée dynamique qui permet de déterminer quel état correspondra, dans un temps futur, à un état présent donné [44]. On distingue deux types de systèmes dynamiques : des systèmes continus et des systèmes discrets.

1.2.1 Systèmes dynamiques continus

Si le système évolue en temps continu, il est dit système continu. La description mathématique de son évolution est donnée par une équation différentielle ordinaire et un ensemble de conditions initiales [45, 46]

$$\begin{cases} \dot{x}(t) &= f(x(t)) \\ x(t_0) &= x_0 \end{cases} \quad (1.1)$$

où $x \in \mathbb{R}^n$ est le vecteur d'état, f est une fonction $\mathbb{R}^n \rightarrow \mathbb{R}^n$ appelée champ de vecteur. Si f est linéaire, le système est dit linéaire. Il est dit non linéaire dans le cas contraire. $x_0 \in \mathbb{R}^n$ représente le vecteur des états initiaux à l'instant initial t_0 . En outre, on définit la dimension d'un système n comme étant la dimension de son vecteur d'état.

On rappelle que la solution de (1.1) pour une condition initiale x_0 existe et est unique si la fonction f est Lipschitzienne.

1.2.2 Systèmes dynamiques discrets

Si un système prends ses valeurs uniquement à des instant régulièrement distribués, celui-ci est dit système en temps discret ou tout simplement système discret [46, 47]. Sa représentation mathématique est donnée par le système d'équations suivant.

$$\begin{cases} x(k+1) &= f(x(k)) \\ x(k_0) &= x(0) \end{cases} \quad (1.2)$$

avec k est l'instant discret, k_0 est l'instant discret initial et $x(0)$ est le vecteur des états initiaux.

Dans les deux types de systèmes dynamiques que nous venons de voir jusqu'à maintenant, l'évolution de l'état dépend seulement de l'état actuel (cas continu) ou du cas précédent (cas discret). Il existe toutefois des cas de système où l'évolution d'un état dépend aussi de son passé. Ces systèmes sont dits à *retards* [48].

1.2.3 Systèmes dynamiques à retards

Les systèmes à retards ont reçu un intérêt considérable grâce à leurs propriétés particulières comme le nombre infini de degrés de liberté et la dimension importante de son attracteur [48]. Mathématiquement, les systèmes à retards sont décrits par des équations

différentielles à retard comme suit :

$$\begin{cases} \dot{x}(t) = f(x(t), x(t - \tau)) & \text{pour } t > \tau \\ x = \phi(t) & \text{pour } t \in [0, \tau] \end{cases} \quad (1.3)$$

Avec $\phi : \mathbb{R} \rightarrow \mathbb{R}^n$ est une fonction vectorielle et τ un retard positif. La différence avec les systèmes sans retard est que les conditions initiales doivent être spécifiées sur un intervalle complet.

1.2.4 Espace de phase et attracteurs

Un espace de phase, en physique, est un espace contenant tout les états accessibles d'un système dynamique. Pour un système en temps continu, avec une dimension finie n , l'espace de phase est parcouru par les composantes de son vecteur d'état [49]. L'évolution d'un système dynamique est représentée par une trajectoire dans l'espace de phase, appelée *orbite*. Selon Ruelle et Takens [50], une évolution complexe dans le temps peut-être mieux représentée dans le plan de phase. Selon la dissipation d'un système donné, les trajectoires peuvent éventuellement converger vers un sous-ensemble A inclus dans l'espace de phase S et appelé *attracteur*.

Dans le cas des systèmes continus, la dissipation est définie par l'analyse de l'évolution d'un volume V de l'espace de phase autrement dit :

$$\dot{V}(t) = \int_V \nabla \cdot f dx \quad (1.4)$$

$\nabla \cdot f$ représente la divergence du champ de vecteur f . Elle est calculée par $\nabla \cdot f = \sum_{i=1}^n \frac{\partial f_i}{\partial x_i}$ avec f_i et x_i sont les composantes du champ de vecteur et du vecteur d'état respectivement [51].

Dans le cas des systèmes discrets, la dissipation est définie par le module du déterminant de la matrice jacobienne associée au champ de vecteur et notée par $|\det(\nabla_x f)|$. Si le résultat est égal à 1, alors le système est conservatif. Dans le cas où $|\det(\nabla_x f)| < 1$, alors le système est dissipatif.

Un système dissipatif peut présenter, dans son plan de phase, des attracteurs avec quatre différentes géométries [52] :

Un point d'équilibre : Appelé aussi point fixe, c'est un point de l'espace de phase vers lequel tendent les trajectoire. Il est donc une solution stationnaire constante du système

Un cycle limite : Il s'agit d'une courbe fermée, dans le plan de phase, qui correspond à une évolution périodique dans le domaine temporel.

Un tore : Représente les mouvements résultant de deux ou plusieurs oscillations indépendantes que l'on appelle parfois "mouvements quasi périodiques".

Un attracteur étrange : Il s'agit d'une géométrie complexe de dimension fractale, associée souvent à une évolution imprévisible dans le domaine temporel. Nous développerons plus en détails ce type d'attracteur dans la partie où nous aborderons les systèmes chaotiques.

1.3 Généralités sur les systèmes chaotiques

En grec ancien, le chaos (Khaos) est défini en premier dans le Theogony d'Hésiode comme une profondeur béante qui précède l'origine du monde. On retrouve aussi ce terme dans les écrits de Christine de Pisan (Chemin de long estude) et dans les Elegies de Desportes qui définissent le chaos comme une confusion et un désordre indésirables [53]. Bien qu'elles datent de plusieurs siècles, ces descriptions connectent deux concepts clés de la théorie du chaos moderne : le désordre et l'ordre. D'autre part, le philosophe Aristote souligna une importante propriété des systèmes chaotiques en énonçant sa conclusion "Une moindre déviation de la vérité est multipliée par mille plus tard". Le philosophe décrit, en effet, une divergence exponentielle avec le temps d'une forme initiale [54].

Trouvant ses origines en mythologie grecque et en philosophie, le chaos est considéré, durant des siècles, comme étant un phénomène sans importance de point de vue scientifique. En 1860, en développant sa théorie cinétique, James Clerk Maxwell remarqua que les collisions entre molécules de la sphère dures pourraient mener à l'amplification progressive

des petites variations et causer un rendement microscopique aléatoire dans les gaz [55]. En ce moment là, le chercheur était persuadé que c'était la complexité du système, le nombre de variables étant important, qui était à l'origine de ce phénomène.

Dans le même contexte, et en 1890, le mathématicien français Henri Poincaré remarqua une dépendance aux conditions initiales dans un cas particulier du problème des trois corps et montra que les lois de Newton n'ont pas fourni de solutions pour la prédiction des états futurs [56]. En utilisant les méthodes de Poincaré, le mathématicien français Jacques Hadamard a étudié en 1898, le problème de divergence de trajectoires dans l'espace de courbures négatives et démontré la sensibilité aux conditions initiales [57]. Son étude a été reprise huit ans plus tard par Pierre Duhem. Entre 1920 et 1960, plusieurs autres mathématiciens et physiciens poursuivirent l'étude des systèmes hamiltoniens non linéaires en s'inspirant des travaux de Poincaré et ce domaine a commencé à fournir des caractérisations sur les différents comportements de ces systèmes régis par les équations différentielles.

A partir de 1960, la théorie du chaos a reçu une attention sans précédents, et ce, suite aux travaux d'Edward Lorenz [58]. Le météorologue travaillait sur un modèle numérique et simplifié de l'atmosphère terrestre et proposa une représentation graphique de la sensibilité aux conditions initiales. L'objectif de Lorenz était d'analyser les données produites par le modèle sur de larges séquences. La puissance des calculs étant limitée en cette période, il était indispensable de dérouler de multiples simulations séquentielles. En initialisant les prochaines simulations, avec une précision inférieure, Lorenz remarqua que le modèle ne génère pas l'évolution prévue. En effet et contrairement à ses attentes, les conditions initiales - avec moins de précision - ne sont pas sans conséquences sur la dynamique du système. C'est lors de la 139^{ième} rencontre de l'Association Américaine pour l'Avancement de la Science (AAAS) que le météorologue résuma cette sensibilité aux conditions initiales par la célèbre métaphore " Un battement d'ailes d'un papillon en Brésil peut-il causer une tornade au Texas ? " [59]. C'est à partir de là, que l'expression "effet papillon " a été utilisée pour caractériser la sensibilité aux conditions initiales des systèmes chaotiques.

Ces résultats, ont encouragé d'autres travaux et recherches sur la théorie du chaos. En

1971, D. Ruelle et F. Takens [50] ont proposé une explication alternative et mathématique concernant les turbulences dans la dynamique des fluides en se basant sur l'existence d'attracteurs étranges. Deux ans plus tard, Tien-Yien Li et James A. Yorke [60] évoquent le comportement chaotique pour décrire l'évolution imprévisible de certains systèmes non linéaires déterministes. Il s'agit des premiers chercheurs qui ont utilisé le terme chaos pour décrire ce phénomène. En 1978, Mitchell J. Feigenbaum interpréta le comportement de certains systèmes comme une transition vers le chaos et déduisit la constante de Feigenbaum [61]. L'attracteur chaotique a été observé pour la première fois dans un circuit électronique par T. Matsumoto et L.O. Chua en 1984 [62]. Le circuit a été réalisé avec seulement une résistance non linéaire caractérisée par une fonction linéaire par morceaux. Cette découverte a été un point de départ dans le développement des circuits électroniques chaotiques.

Après cet aperçu historique et pour mieux comprendre le comportement chaotique et les raisons de son exploitation dans notre travail de thèse, nous développerons plus en détails, dans ce qui suit, les propriétés essentielles des systèmes chaotiques

1.3.1 Propriétés des systèmes chaotiques

Il existe un ensemble de propriétés qui résument les caractéristiques observées dans les systèmes chaotiques. Elles sont considérées comme des critères mathématiques qui définissent le chaos. Les plus connues sont :

1.3.1.1 Sensibilité aux conditions initiales

La sensibilité aux conditions initiales constitue, sans aucun doute, la caractéristique essentielle du comportement chaotique d'un système. Cette propriété appelée aussi effet "Papillon" signifie que deux conditions initiales arbitrairement proches évoluent suivant des trajectoires significativement différentes et divergentes [63]. L'évolution est par conséquent imprévisible à long terme.

Pour mieux illustrer cette propriété, considérons la fonction logistique discrète utilisée par le biologiste Robert May pour décrire l'évolution de la population d'une espèce [64].

Elle est définie par l'équation suivante :

$$x(k+1) = rx(k)(1-x(k)) \quad (1.5)$$

où $x(k) \in [0, 1]$ est le vecteur d'état représentant la population à l'année k et $r \in \mathbb{R}$ représente le facteur de croissance de la population et satisfait la condition $0 \leq r \leq 4$, [65].

La figure (1.1) illustre l'effet d'une variation de 0.001 de la valeur initiale de l'état x sur l'évolution de ce dernier. Comme nous pouvons le voir, les deux courbes, avant et après variations, divergent complètement après les premières itérations.

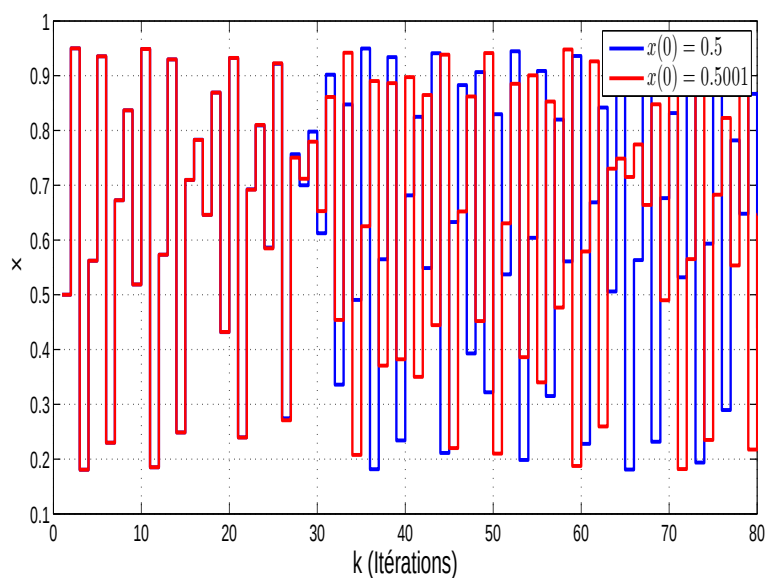


FIGURE 1.1 – Sensibilité de l'état x de la fonction logistique aux conditions initiales

1.3.1.2 Non périodicité

Un système présentant un comportement chaotique évolue dans une orbite qui ne se répète jamais sur elle-même. C'est à dire, les orbites ne sont jamais périodiques [66].

1.3.1.3 Déterminisme

Le déterminisme signifie que le système est non aléatoire et ne possède aucun paramètre ou entrée stochastique. Cette propriété est propre à tous les systèmes dont l'évolution est définie par un ensemble d'équations différentielles ou d'équations aux différences. Dans les phénomènes aléatoires, il est absolument impossible de prévoir la trajectoire d'une quelconque particule. À l'opposé, et bien qu'ils paraissent, à première vue, aléatoires, les systèmes dynamiques chaotiques sont régis par certaines équations rendant compte du phénomène, mais dont les solutions sont sensibles aux conditions initiales [67]. Le comportement irrégulier observé dans les systèmes chaotiques est dû à la non linéarité intrinsèque du système plutôt qu'au bruit [68].

1.3.1.4 Spectre à large bande

Le spectre de Fourier d'un signal chaotique est un spectre à large bande, analogue à celui d'un bruit blanc [69]. La figure (1.2) présente le spectre de la fonction logistique évoluant en régime chaotique.

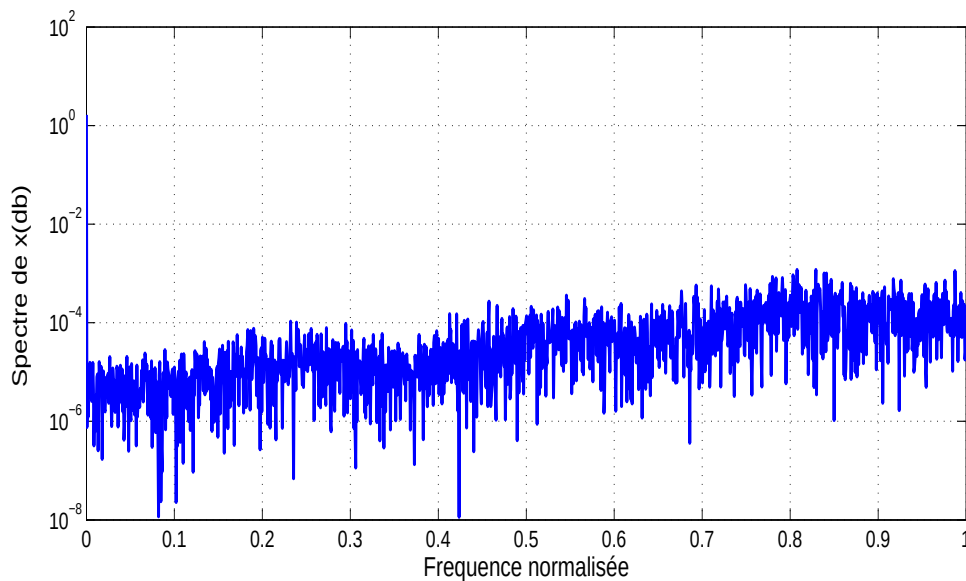


FIGURE 1.2 – Spectre de fréquence de l'état x de la fonction logistique chaotique

1.3.1.5 L'attracteur étrange

Les trajectoires d'un système dynamique chaotique sont attirées vers un attracteur dit étrange [70]. Ce dernier est caractérisé par

- a) un volume nul ;
- b) une séparation exponentiellement rapide de trajectoires initialement proches ;
- c) une dimension souvent fractale (non entière)[71].

La naissance d'un attracteur étrange est liée à l'existence de deux processus, à savoir

- *L'étirement*, responsable de l'instabilité et de la sensibilité aux conditions initiales
- *Le repliement*, responsable du côté étrange et fractal de l'attracteur.

Considérons deux exemples de systèmes chaotiques : Le système chaotique continu de Lorenz et le système chaotique discret de Fold. Le système de Lorenz est un système tridimensionnel présentant un comportement chaotique. Il doit son nom au chercheur et météorologue Édouard Lorenz. Le système de Lorenz est décrit par les équations suivantes [58].

$$\begin{cases} \dot{x}_1 &= \sigma(x_2(t) - x_1(t)) \\ \dot{x}_2 &= x_1(t)(\rho - x_3(t)) - x_2(t) \\ \dot{x}_3 &= x_1(t)x_2(t) - \beta x_3(t) \end{cases} \quad (1.6)$$

où $x = [x_1, x_2, x_3]^T \in \mathbb{R}^3$ est le vecteur d'état du système et σ , ρ et β sont les paramètres du système.

Le système de Fold est un systèmes discret. Il est défini par les deux équations suivantes [72] :

$$\begin{cases} x_1(k+1) &= ax_1(k) + x_2(k) \\ x_2(k+1) &= x_1^2(k) + b \end{cases} \quad (1.7)$$

où $[x_1 \ x_2]^T \in \mathbb{R}^2$ est le vecteur d'état et a , b sont deux paramètres constants.

Pour les valeurs $\sigma = 10$, $\rho = 28$ et $\beta = \frac{8}{3}$, le système de Lorenz présente un comportement chaotique. La figure 1.3 illustre l'attracteur chaotique étrange obtenu en plan de phase des

états x_1 et x_3 en considérant les conditions initiales $(x_1(0), x_2(0), x_3(0)) = (0.1, 0.1, 0.1)$. Le système discret de Fold donné par (1.7) présente une évolution chaotique pour les

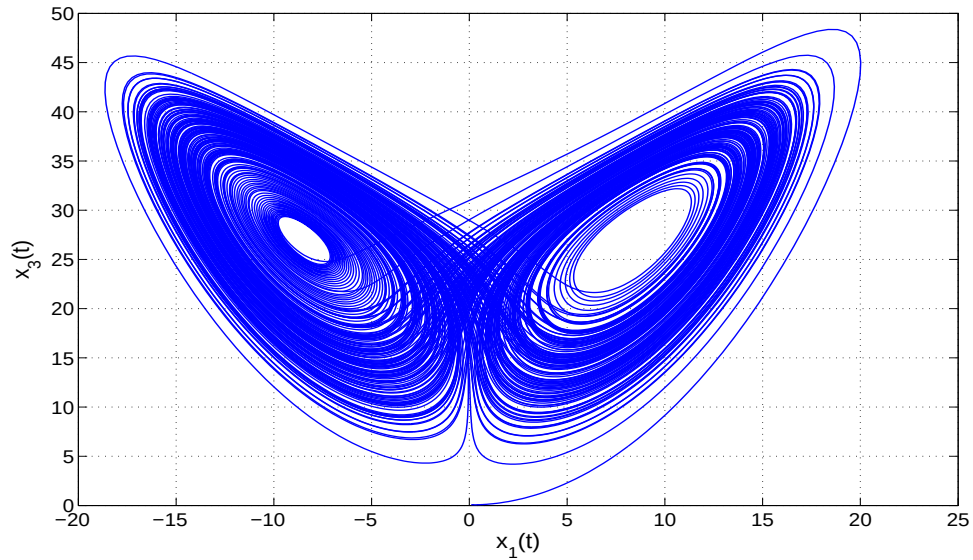


FIGURE 1.3 – Attracteur chaotique étrange de Lorenz

valeurs $a = -0.1$ et $b = -1.7$. L'attracteur étrange obtenu en plan de phase des états x_1 et x_2 et pour les valeurs initiales $(x_1, x_2) = (0, 0)$ est représenté dans la figure 1.4.

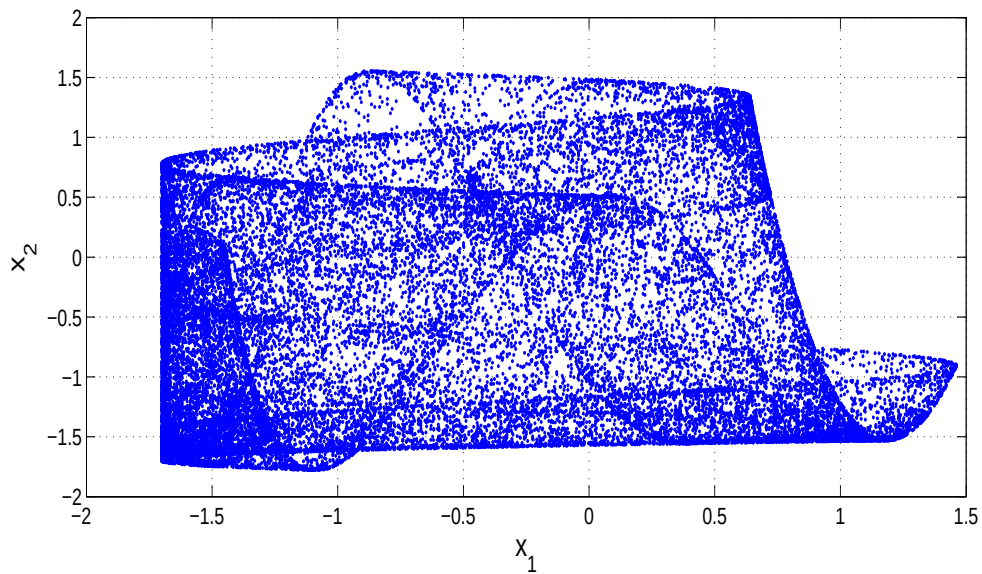


FIGURE 1.4 – Attracteur chaotique étrange de Fold

1.3.2 Les exposants de Lyapunov

L'exposant de Lyapunov noté λ peut-être considéré comme une mesure quantitative de la sensibilité aux conditions initiales [73]. Pour deux états initiaux légèrement différents x_0 et $x_0 + \epsilon$, leur divergence après n itérations peut-être caractérisée comme suit

$$|f^n(x_0 + \epsilon) - f^n(x_0)| = \epsilon e^{n\lambda(x_0)} \quad (1.8)$$

Comme le montre la figure 1.5, l'exposant de Lyapunov donne le taux moyen de diver-

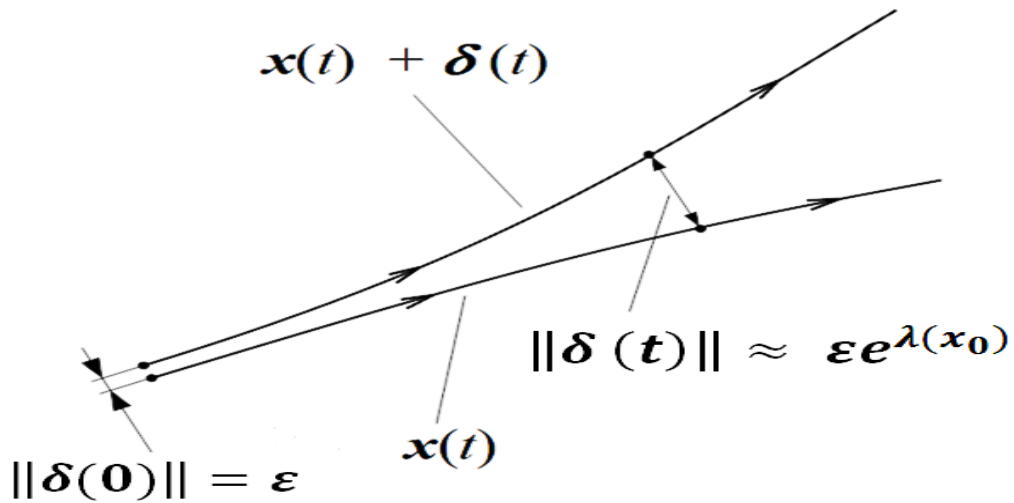


FIGURE 1.5 – Quantification de la divergence de trajectoires par les exposants de Lyapunov

gence de deux trajectoires et dépend des conditions initiales. Pratiquement, l'exposant de Lyapunov peut-être obtenu par le calcul de limite suivant [74] :

$$\begin{aligned} \lambda(x_0) &= \lim_{n \rightarrow \infty} \lim_{\epsilon \rightarrow 0} \frac{1}{n} \log \frac{1}{\epsilon} \frac{|f^n(x_0 + \epsilon) - f^n(x_0)|}{\epsilon} \\ &= \lim_{n \rightarrow \infty} \frac{1}{n} \log \frac{df^n x(0)}{dx_0} \end{aligned} \quad (1.9)$$

ou bien

$$\begin{aligned}
 \lambda(x_0) &= \lim_{n \rightarrow \infty} \frac{1}{n} \log \frac{df^n(x_0)}{dx_0} \\
 &= \lim_{n \rightarrow \infty} \frac{1}{n} \log \prod_{k=0}^{n-1} |f'(x_k)| \\
 &= \lim_{n \rightarrow \infty} \frac{1}{n} \sum_{k=0}^{n-1} \log |f'(x_k)|
 \end{aligned} \tag{1.10}$$

Le nombre d'exposants de Lyapunov est égal à la dimension de l'espace des phases et ils sont souvent rangés du plus grand au plus petit : $\lambda_1 > \lambda_2 > \dots$. La valeur du plus grand exposant quantifie le degrés du chaos.

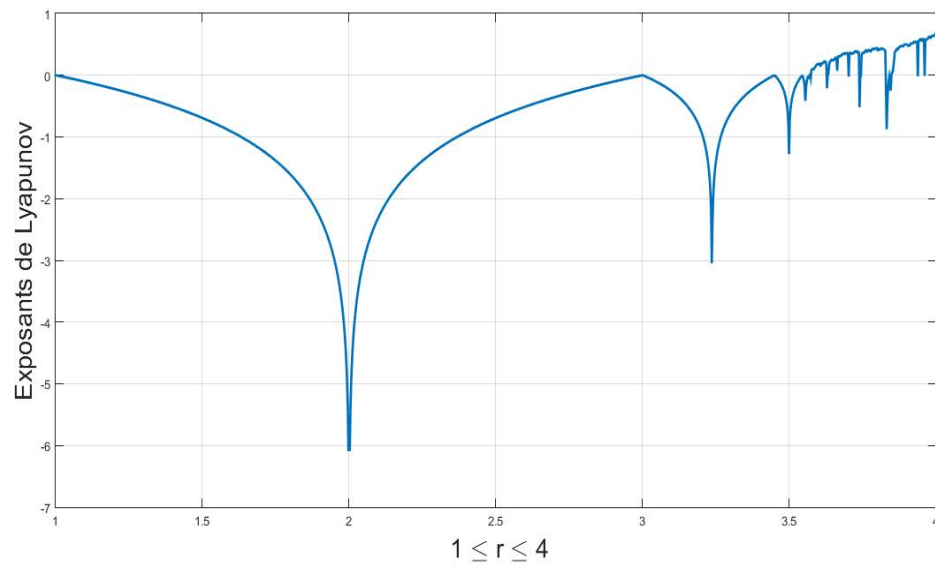
Les conditions suivantes sont nécessaires pour l'apparition du chaos dans un système dynamique [75].

- Au moins l'un des exposants de Lyapunov est positif pour expliquer la divergence des trajectoires.
- Au moins l'un des exposants de Lyapunov est négatif pour justifier le repliement des trajectoires.
- La somme de tous les exposants est négative pour indiquer qu'un système chaotique est dissipatif, c'est-à-dire qu'il perd en énergie.

Exemple : la fonction logistique

Considérons la fonction logistique précédemment donnée par l'équation (1.5). L'exposant de Lyapunov de la fonction logistique pour différentes valeurs du paramètre r et en choisissant la valeur initiale $x(0) = 0.1$ a été calculé en utilisant la toolbox Matlab LET et l'algorithme de Wolf [76]. Comme nous pouvons le voir sur la figure 1.6, pour la valeur $r = 4$ du paramètre de bifurcation, la simulation donne en résultat un exposant positif de valeur $\lambda = 0.6932$. Ceci implique que la fonction logistique présente un comportement chaotique.

Le tableau 1.1 illustre le lien entre les exposants de Lyapunov et les formes d'attracteurs et donne les signes des exposants de Lyapunov pour chaque type d'attracteur [77].

FIGURE 1.6 – Exposants de Lyapunov de la fonction logistique avec $x(0) = 0.1$

Attracteur	Exposants de Lyapunov
Point d'équilibre	$0 > \lambda_1 \geq \dots \geq \lambda_n$
Cycle limite	$\lambda_1 = 0, 0 > \lambda_2 \geq \dots \geq \lambda_n$
Tore d'ordre 2	$\lambda_1 = \lambda_2 = 0, 0 > \lambda_3 \geq \dots \geq \lambda_n$
Tore d'ordre k	$\lambda_1 = \dots = \lambda_k = 0, 0 > \lambda_{k+1} \geq \dots \geq \lambda_n$
Attracteur chaotique	$\lambda_1 > 0, \sum_{i=1}^n \lambda_i < 0$
Attracteur hyper-chaotique	$\lambda_1 > 0, \lambda_2 > 0, \sum_{i=1}^n \lambda_i < 0$

TABLE 1.1 – Exposants de Lyapunov pour différents attracteurs

1.3.3 Bifurcations et routes vers le chaos

Les systèmes chaotiques sont aussi sensibles aux variations des paramètres de contrôle. Cette dépendance peut causer que les dynamiques du système peuvent être complètement différentes (chaotique, périodique, ... etc) [78]. En effet, La génération d'une signal chaotique n'est pas immédiate. Autrement dit, le système n'évolue pas d'un état inexistant à un état chaotique sans passer par des transitions. Un tel changement dans les dynamiques du système est alors appelé *Bifurcation*. Les graphiques qui explicitent ces bifurcations, sont logiquement appelés diagrammes de bifurcation [79]. Cette notion est primordiale dans l'étude des systèmes chaotiques. Les diagrammes de bifurcation sont utilisés pour étudier les dynamique du système en fonction des paramètres de contrôle. Lorsque l'on établit un tel graphique, il faut faire attention aux axes. Sur un axe nous prenons le paramètre, et sur l'autre la variable d'état. Un diagramme de bifurcation délimite des zones de l'espace paramétrique dans lesquelles le comportement qualitatif du système est similaire. On voit apparaître aussi un enchaînement très rapide de doublements de période qui mène à une comportement chaotique.

Afin de mieux comprendre le phénomène de bifurcation, considérons, de nouveau, l'application logistique (1.5). La figure (1.7) représente le diagramme de bifurcation de l'application logistique. Pour les valeurs de r inférieures à 3, la trajectoire de l'état x converge vers un point fixe nul ou ne convergent pas. Dès que r est supérieure à 3, le système bifurque, c'est à dire qu'il oscille entre 2 valeurs autour du point fixe. On parle alors de cycle limite ou d'attracteur de période 2. En continuant à augmenter la valeur du facteur r , les 2 attracteurs s'écartent du point fixe jusqu'à ce qu'une nouvelle bifurcation ait lieu pour $r \approx 3.45$. Chaque point se dédouble et on obtient un cycle attracteur de 4 périodes. On dit qu'il y a doublement de périodes. C'est à partir de cet exemple que Feigenbaum pressentit l'existence d'une forme d'universalité dans cette transition vers le chaos sous forme d'une cascade de doublements de périodes.

Cette suite de bifurcations partant d'un attracteur stable jusqu'à un attracteur chaotiques est appelée route vers le chaos.

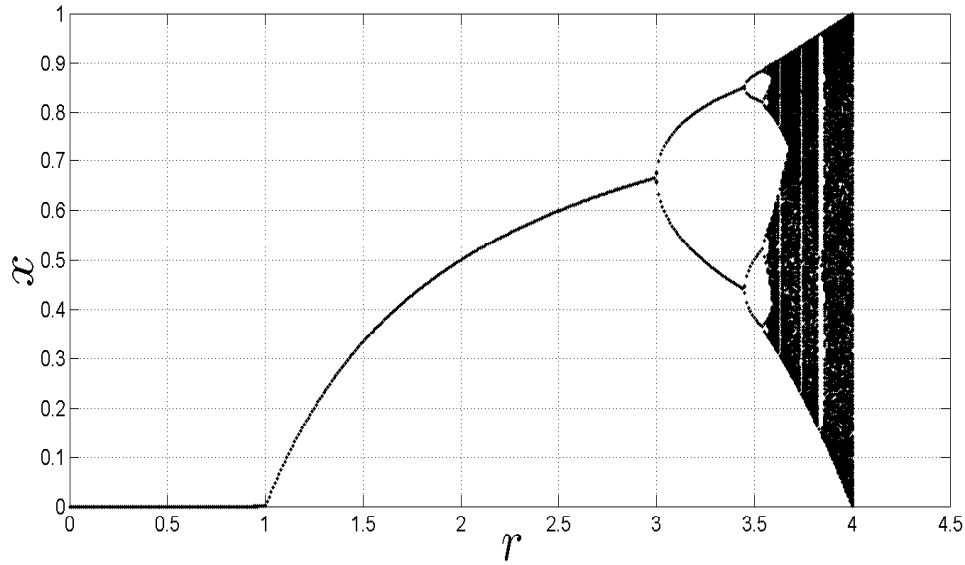


FIGURE 1.7 – Diagramme de bifurcation de la fonction logistique

Il existe une large variété de routes vers le chaos, trois scénarios ont souvent lieu et par conséquent sont considérés comme universels [80].

1.3.3.1 L'intermittence

Dans ce scénario, une seule bifurcation est responsable de l'alternance entre des zones de mouvement chaotique et des zones de mouvement régulier. Au fur et à mesure que le paramètre de bifurcation augmente, les zones où le comportement est chaotique durent plus longtemps et, éventuellement, au-dessus d'un seuil critique, le système reste chaotique [81]. L'intermittence est souvent connue comme la route de Pomeau-Manneville vers le chaos [82]. La figure 1.8 illustre une série d'intermittences survenues dans l'oscillateur de Chua donné par les équations d'états suivantes pour différentes valeurs des paramètres de bifurcation β et γ [83].

$$\begin{cases} \dot{x}_1 &= kc(x_2 - x_1 - f(x_1)) \\ \dot{x}_2 &= k(x_1 - x_2 + x_3) \\ \dot{x}_3 &= k(-\beta x_2 - \gamma x_3) \end{cases} \quad (1.11)$$

avec $x = [x_1 \ x_2 \ x_3]^T \in \mathbb{R}^3$ est le vecteur d'état. La fonction non linéaire f est définie comme suit :

$$f(x_1) = bx_1 + \frac{1}{2}(a - b)(|x_1 + 1| - |x_1 - 1|) \quad (1.12)$$

Pour illustrer le scénario d'intermittences vers le chaos, les valeurs des paramètres a , b , k et c sont fixées à $a = -0.98$, $b = -2.4$, $k = 1$ et $c = -75.018755$.

1.3.3.2 La quasi-périodicité

Appelé aussi la route de Ruelle-Takens-Newhouse vers le chaos, ce scénario consiste en une succession de trois bifurcations quand le paramètre de bifurcation augmente constamment [84]. La première bifurcation est une bifurcation de Hopf qui mène vers un cycle limite stable de période T . La seconde est une bifurcation de Tore qui résulte d'une dynamique quasi-périodique avec deux fréquences incommensurables associées à un attracteur torique T^2 . La dernière bifurcation transforme ce tore en un autre T^3 avec trois fréquences incommensurables qui se stabilise en attracteur étrange (chaotique). La figure 1.9 illustre un comportement quasi-periodique dans le circuit électrique proposé par Matsumoto, Chua et Tokunaga [85] et défini par les équations suivantes :

$$\begin{cases} \dot{x}_1 &= p_1 f(x_2(t) - x_1(t)) \\ \dot{x}_2 &= -f(x_2(t) - x_1(t)) - x_3(t) \\ \dot{x}_3 &= p_2 x_2(t) \end{cases} \quad (1.13)$$

avec $x = [x_1 \ x_2 \ x_3]^T \in \mathbb{R}^3$ est le vecteur d'état. La fonction non linéaire f est définie comme suit :

$$f(x) = -ax(t) + \frac{1}{2}(a + b)(|x + 1| - |x - 1|) \quad (1.14)$$

où a , b , p_1 et p_2 sont les paramètres de contrôle du système. Pour illustrer le scénario de quasi-périodicité vers le chaos, on fixe les paramètres a , b et p_2 à $a = 0.07$, $b = 0.1$, $p_2 = 1$ et on fait varier le paramètre p_1 .

Comme nous pouvons le voir sur la figure 1.9, au fur et à mesure que le paramètre de bifurcation p_1 croît, les bifurcations de Hopf et de Tore apparaissent et disparaissent

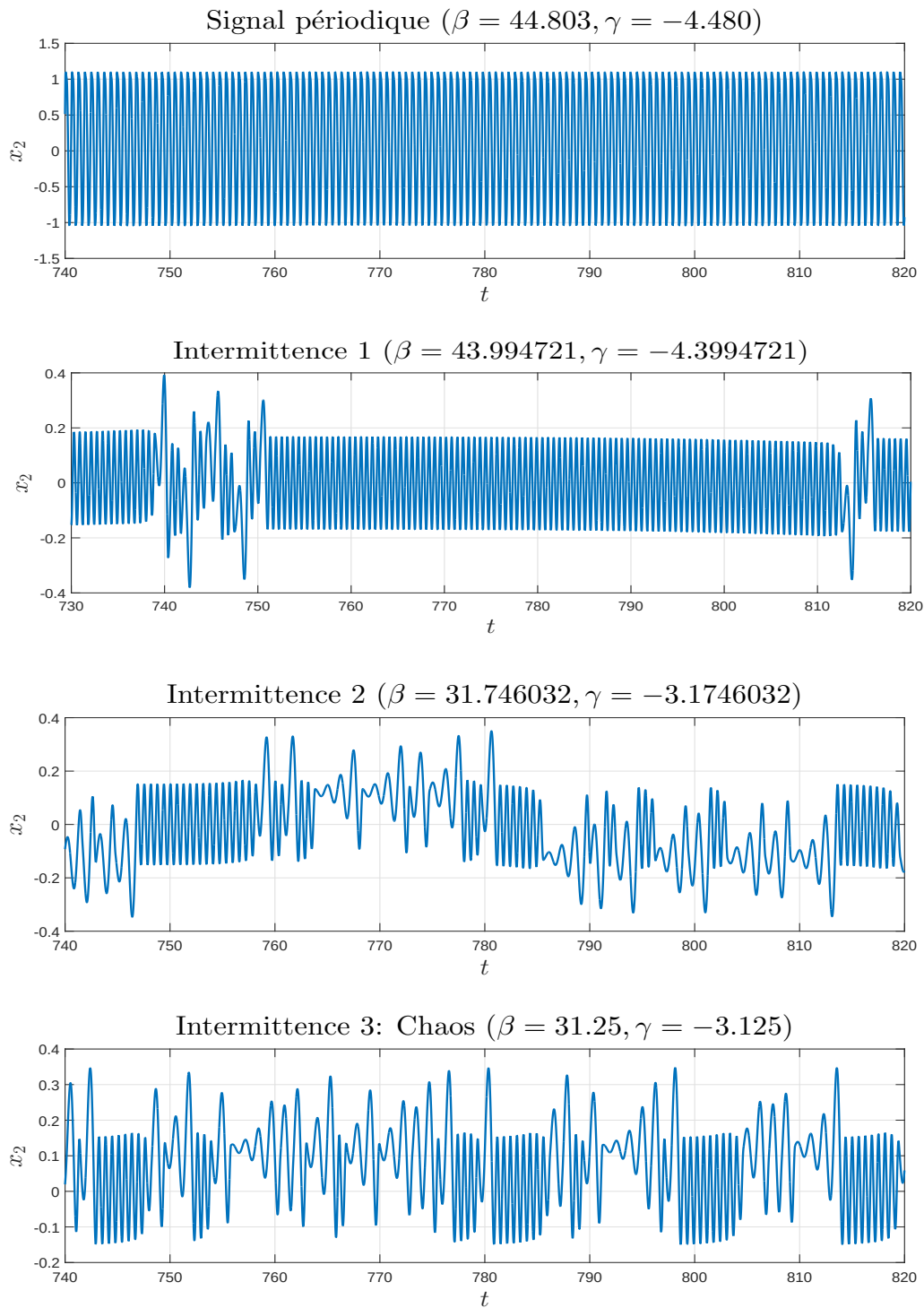


FIGURE 1.8 – Intermittences vers le chaos dans le circuit de Chua

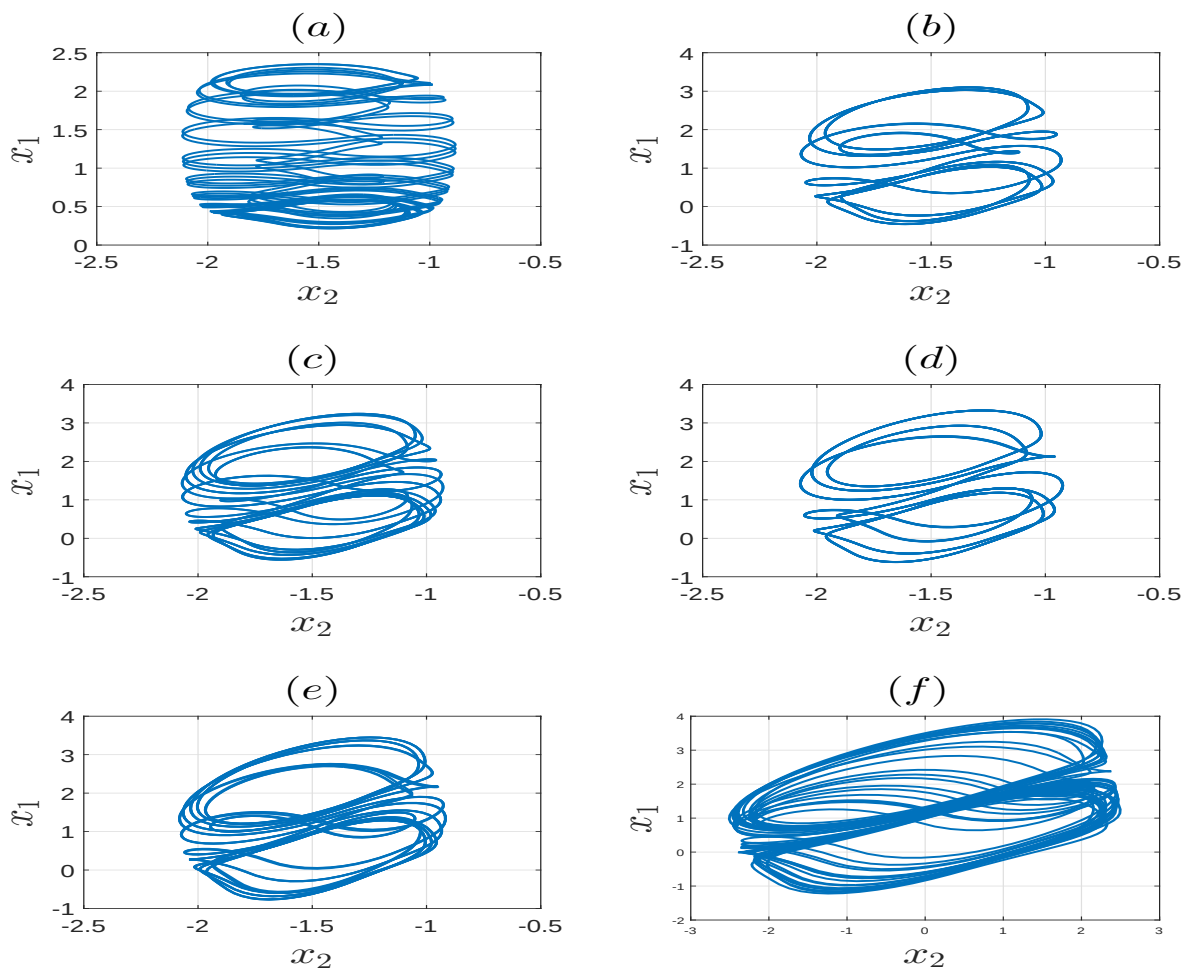


FIGURE 1.9 – Route vers le chaos par quasi-périodicité dans un circuit électrique, (a) : $p_1 = 2$, (b) : $p_1 = 8$, (c) : $p_1 = 8.8$, (d) : $p_1 = 9.6$, (e) : $p_1 = 10.8$, (f) : $p_1 = 15$

alternativement. Si on continue à augmenter la valeur de p_1 , le tore n'apparaît plus et le chaos peut survenir par doublements ou ajout de périodes [86].

1.3.3.3 Doublement de périodes

Cette route vers le chaos est aussi appelée route de Feigenbaum [61]. Dans ce scénario, un point d'équilibre se déstabilise par une bifurcation d'Andronov-Hopf donnant naissance à un cycle limite de période T . En continuant à varier le paramètre de bifurcation, le cycle limite subit une succession de bifurcations doublant la période jusqu'à l'apparition d'un attracteur chaotique étrange.

La figure 1.10 illustre ce scénario vers le chaos dans le système de Lorenz 1.6 présenté

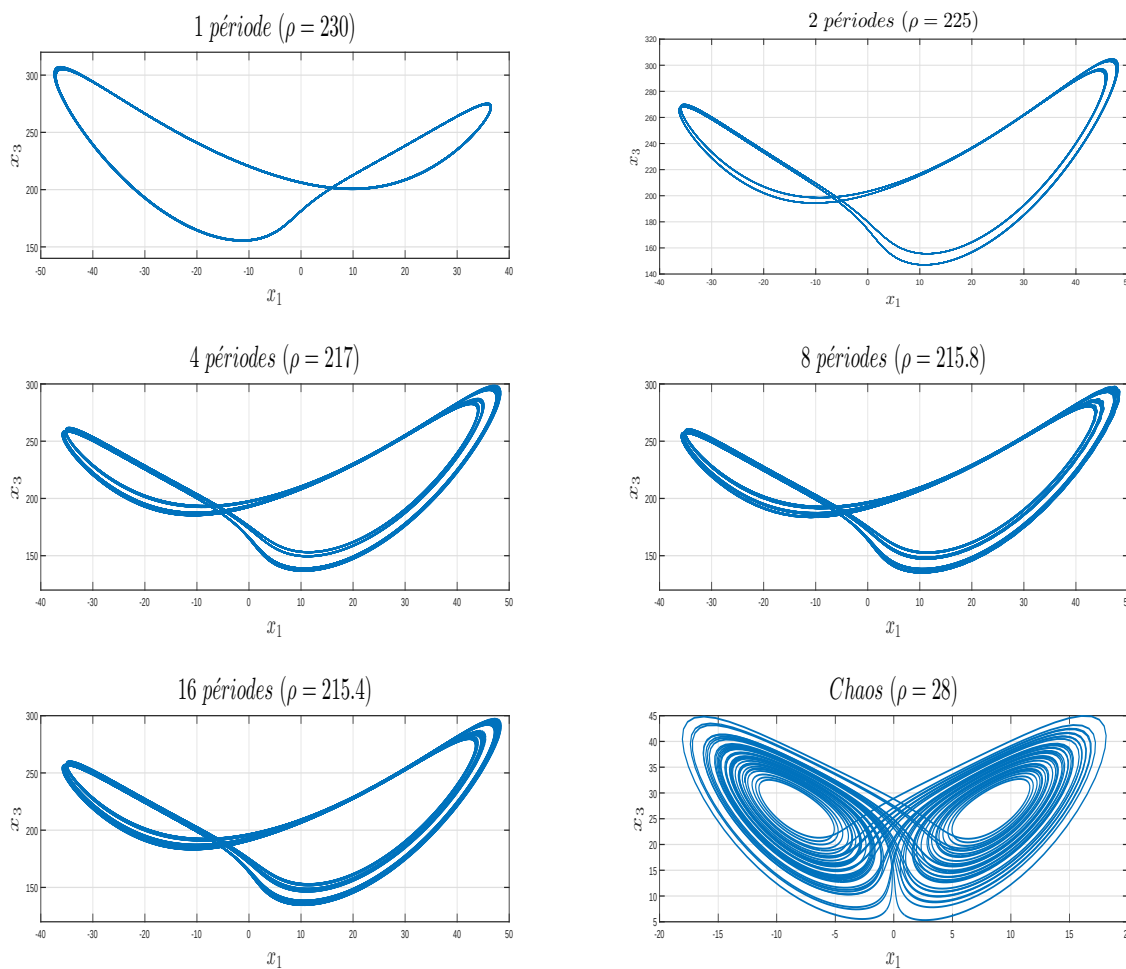


FIGURE 1.10 – Route vers le chaos par doublements de périodes dans le système de Lorenz

antérieurement. Les paramètres σ et β sont fixés à $\sigma = 10$ et $\beta = \frac{8}{3}$. En variant le paramètre ρ , nous pouvons observer une succession de doublements de périodes menant au chaos.

1.4 Analyse de la complexité des systèmes chaotiques

L'analyse de la complexité est l'une des méthodes utilisées pour caractériser les dynamiques des systèmes chaotiques. La complexité d'un système chaotique qualifie le degré de ressemblance de la séquence chaotique à une séquence aléatoire en utilisant un algorithme de corrélation. Plus la complexité est élevée, plus la séquence chaotique ressemble à un signal aléatoire. Dans notre travail de thèse, deux algorithmes sont utilisés pour quantifier

la complexité des séquences chaotiques : l'algorithme de l'entropie spectrale SE [87] et l'algorithme C_0 [88].

1.4.1 Complexité par l'algorithme de l'entropie spectrale

L'entropie spectrale reflète le désordre dans le domaine de la transformation de Fourier. Une grande valeur de l'entropie spectrale implique une complexité élevée d'une séquence temporelle. Considérons une série temporelle $x(n), n = 1, 2, \dots, N-1$ de longueur N . Posons $\tilde{x}(n) = x(n) - \bar{x}$ avec $\bar{x}$ est la moyenne de la série temporelle. La Transformée de Fourier Discrète (TFD) de cette série est calculée comme suit [89] :

$$X(k) = \sum_{n=0}^{N-1} \tilde{x}(n) e^{-j2\pi nkN/N} \quad (1.15)$$

où $k = 1, 2, \dots, N-1$ et j est le nombre imaginaire. Notons par $|X(k)|^2$ le spectre de puissance discret de la $k^{ième}$ fréquence. La probabilité de cette fréquence est alors définie par :

$$P_k = \frac{|X(k)|^2}{\sum_{k=0}^{N/2-1} |X(k)|^2} \quad (1.16)$$

L'entropie normalisée est alors calculée comme suit :

$$SE = \frac{\sum_{k=0}^{N/2-1} |P_k \ln(P_k)|}{\ln(N/2)} \quad (1.17)$$

1.4.2 Complexité par l'algorithme C_0

Le principe de l'algorithme C_0 est de décomposer la séquence analysée en composantes régulières et irrégulières et de mesurer la proportion des composantes irrégulières de la séquence [89]. Cette méthode est aussi basée sur le calcul de la TFD. La valeur du carré moyen de la transformée de Fourier discrète $X(k)$, de la séquence $x(n)$, est calculée comme suit

$$G_N = (1/N) \sum_{k=0}^{N-1} |X(k)|^2 \quad (1.18)$$

Soit le signal $\tilde{X}(k)$ défini comme suit :

$$\tilde{X}(k) = \begin{cases} X(k) & \text{si } |X(k)|^2 > rG_N \\ 0 & \text{si } |X(k)|^2 \leq rG_N \end{cases} \quad (1.19)$$

avec $r(r > 0)$ est un facteur de tolérance à choisir selon l'application. La transformée de Fourier inverse de $\tilde{X}(k)$ est

$$\tilde{x}(n) = (1/N) \sum_{k=0}^{N-1} \tilde{X}(k) e^{j2\pi nk/N} \quad (1.20)$$

où $n = 0, 1, 2, \dots, N-1$.

La complexité C_0 est définie comme suit :

$$C_0(r, n) = \frac{\sum_{n=0}^{N-1} |x(n) - \tilde{x}(n)|^2}{\sum_{n=0}^{N-1} |x(n)|^2} \quad (1.21)$$

1.5 Test 0 – 1 des systèmes chaotiques

Le test binaire 0 – 1 a été développé en 2004 par Gottwald et Melbourne [90] pour distinguer entre les dynamiques régulières et les dynamiques chaotiques dans un système déterministe. Le principe du test consiste à construire un processus aléatoire à partir d'un ensemble de données. Le test est décrit comme suit :

Considérons un ensemble discret de données noté $\phi(n)$, $n = 1, 2, 3, \dots$. On définit à partir de cette séquence deux fonctions réelles $p(n)$ et $s(n)$ définies comme suit :

$$p(n) = \sum_{j=1}^n \phi(j) \cos(\theta(j)), \quad n = 1, 2, 3, \dots \quad (1.22)$$

$$s(n) = \sum_{j=1}^n \phi(j) \sin(\theta(j)), \quad n = 1, 2, 3, \dots \quad (1.23)$$

avec

$$\theta(j) = jc + \sum_{j=1}^n \phi(j), \quad j = 1, 2, 3, \dots, n. \quad (1.24)$$

$c \in \mathbb{R}_+$ est une constante à choisir aléatoirement. Ensuite et sur la base de $p(n)$ (ou bien $s(n)$) on définit le déplacement quadratique moyen

$$M(n) = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{j=1}^N [p(j+n) - p(j)]^2, \quad n = 1, 2, 3, \dots \quad (1.25)$$

$M(n)$ peut être borné ou linéairement croissant dans le temps. En particulier, si le comportement de $p(n)$ ($s(n)$ évolue de manière similaire) est Brownien (non borné) alors $M(n)$ croît linéairement dans le temps et on peut conclure que la séquence analysée est chaotique. Dans le cas contraire, c'est à dire que le comportement de $p(n)$ est borné, alors $M(n)$ sera aussi borné et la séquence considérée n'est pas chaotique. Pour conclure sur l'évolution de $M(n)$ et par conséquent, sur celle de la séquence, il est nécessaire de calculer le taux de croissance asymptotique suivant [91] :

$$K = \lim_{n \rightarrow \infty} \frac{\log M(n)}{\log n} \quad (1.26)$$

Si la valeur de K est proche de 0 alors la séquence ϕ est classifiée comme régulière (périodique ou quasi-périodique). Par contre, si la valeur de K est très proche de 1 alors l'évolution de ϕ est classée comme chaotique.

Le test 0 – 1 présente plusieurs avantages comme son application facile et ne nécessitant aucune reconstruction de l'espace de phase ou connaissance des équations à l'origine de la séquence. En outre, ce test permet une analyse visuelle à partir du plan de phase des trajectoires des fonctions p et s .

Afin d'illustrer ce dernier point, considérons de nouveau la fonction logistique définie dans l'équation (1.5). Nous avons appliqué le test 0 – 1 décrit ci-dessus pour différentes valeurs du paramètre de bifurcation r . La figure (1.11) montre les plans de phases $p - s$ obtenus pour les valeurs $r = 2$, $r = 3.55$ et $r = 4$. Pour les valeurs $r = 2$ et $r = 3.55$ les trajectoires de $p(n)$ et $s(n)$ sont bornées. L'évolution de la fonction logistique est donc régulière pour ces valeurs du paramètres de bifurcation. Pour la valeur $r = 4$, on peut constater que l'évolution des trajectoires $p(n)$ et $s(n)$ sont différentes et ressemblent à un mouvement Brownien. Les valeurs du taux K proches de 0 pour les valeurs $r = 2$ et

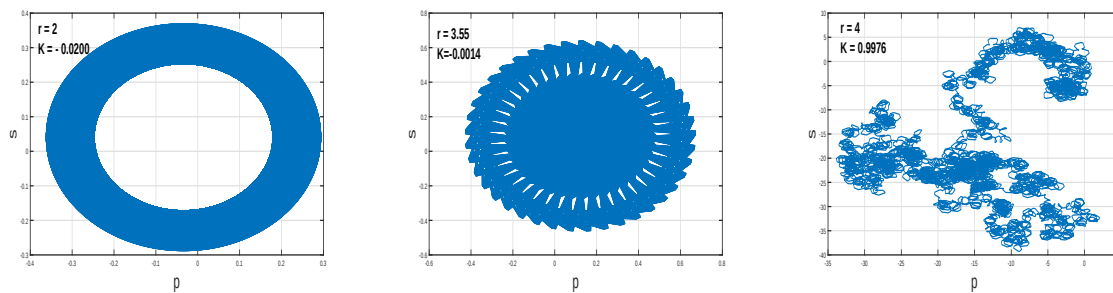


FIGURE 1.11 – Application du test 0 – 1 sur la fonction logistique : Plans de phases $p - s$ pour différentes valeurs de r

$r = 3.55$ et très proche de 1 pour $r = 4$ confirment cette analyse visuelle.

Avant de présenter quelques systèmes chaotiques d'ordre fractionnaire évoluant en temps continu et discrets, nous avons jugé nécessaire de présenter, dans la partie qui suit, et de manière synthétique et unifiée, les éléments de base de la théorie du calcul fractionnaire et des systèmes à dérivées d'ordre non entier sur lesquels s'appuient nos travaux décrits dans les chapitres 3 et 4.

1.6 Concepts de base et définitions dans le calcul fractionnaire

Au cours des dernières décennies, les systèmes chaotiques d'ordres fractionnaires (non entiers) ont suscité beaucoup d'intérêt de la communauté de recherche. Le calcul fractionnaire qui a été considéré comme l'extension du calcul d'ordre entier à un calcul d'ordre non-entier, est entré en image dans le 17^{ième} siècle. En raison de l'indisponibilité des techniques de résolution, le calcul fractionnaire n'a pas été exploré pendant près de trois cents ans. L'origine du calcul fractionnaire remonte à Leibniz qui proposa, dans sa lettre au Marquis de l'Hospital en 1695, de généraliser sa formule pour la $n^{\text{ième}}$ dérivée en introduisant la notation $d^{\frac{1}{2}}h$ [92]. Leibniz mentionna aussi les dérivées "d'ordres généraux" dans une autre lettre à Bernoulli. Euler aborda la question pour la deuxième fois en 1730 et introduisit, dans son article [93], la célèbre fonction Gamma, que nous verrons plus tard. En 1822, et grâce à sa transformée, Fourier obtint une autre définition de dérivée d'ordre réel

[94, 95]. Le calcul fractionnaire a été utilisé par Abel en 1823 pour résoudre le problème de tautochrone généralisé [96]. Liouville, fut le premier à étudier le calcul fractionnaire plus en détail [97]. Huit travaux de ce chercheur ont vu le jour entre 1832 et 1837. En 1847, Riemann proposa une définition d'intégrale fractionnaire [98]. A partir de 1867, Grünwald [99] et Letnikov [100] ont développé, indépendamment, une dérivée fractionnaire comme limite de différences finies, et ce inversement à l'approche de Riemann-Liouville, qui est donné par une intégrale. Letnikov a montré que sa définition coïncide avec les versions formulées par Liouville, notamment en ce qui concerne les valeurs de l'ordre, et celles fournies par Riemann, sous une pratique interprétation de la différence d'ordre dite non-entière. Hadamard publia, en 1892, un article où la dérivation d'ordre non entier d'une fonction analytique doit être faite en termes de sa série Taylor. Une étape importante dans l'application concrète des dérivées d'ordre fractionnaire a été le calcul opérationnel fourni par Heaviside, en 1892, dans le cadre de la résolution l'équation de la chaleur unidimensionnelle.

A partir de 1900, le calcul fractionnaire connut un développement rapide et afin de formuler des problèmes particuliers, d'autres définitions ont été proposées. Nous pouvons mentionner, par exemple, Weyl [102] qui a introduit une intégrale fractionnaire afin de contourner un problème impliquant les fonctions périodiques. En outre, Riesz [103] a prouvé le théorème de la valeur moyenne pour les intégrales fractionnaires et a introduit une autre formulation qui est reliée à la transformée de Fourier. En 1927, Marchaud a introduit une nouvelle définition pour les dérivées d'ordre non entier. L'avantage de cette définition est qu'elle est moins restrictive quand à la régularité de la fonction. En 1967, Caputo proposa sa définition de la dérivée d'ordre fractionnaire qui est plus restrictive que celle de Riemann-Liouville mais aussi mieux appropriée pour les problèmes impliquant des équations différentielles avec valeurs initiales [104].

En 1970 et dans leur article, Oldham et Spanier [105] abordèrent le problème du flux de chaleur à la surface d'un conducteur et ont réussi à démontrer que lors du phénomène de diffusion, le flux est proportionnel à la dérivée $\frac{1}{2}$ du paramètre physique que ce soit la température, la concentration d'espèces chimiques ou le potentiel électrique. Cette équation

tion est considérée comme un grand pas dans l'histoire du calcul fractionnaire puisqu'elle est exploitée hors du champ des mathématiques. Grâce à tous les travaux cités ci-dessus et aux contributions fournies, les applications du calcul fractionnaire ont été considérées dans différentes disciplines telles que l'automatique [106], la thermique [107], l'électricité [108], la physique [109], l'ingénierie [110] et la théorie du chaos, notamment la transmission sécurisée de données à base de systèmes chaotiques [111].

Dans ce qui suit, nous donnerons les définitions élémentaires et notions de base relatives au calcul fractionnaire. Ces dernières nous seront utiles pour présenter notre contribution dans les chapitres ultérieurs.

1.6.1 Les systèmes dynamiques d'ordre fractionnaire continus

Dans cette partie, les définitions fondamentales du calcul fractionnaire en temps continu seront données.

1.6.1.1 Opérateur de dérivation d'ordre fractionnaire

Le terme calcul fractionnaire décrit la théorie des intégrales et dérivées d'ordre arbitraire ce qui généralise et unifie les notions de dérivées et les intégrales d'ordre entier. L'opérateur proposé par Davis appelé opérateur de dérivation fractionnaire est noté par ${}_aD_t^\alpha$ et défini comme suit [112, 113]

$${}_aD_t^\alpha = \begin{cases} \frac{d^\alpha}{dt^\alpha}, & \alpha > 0 \\ 1, & \alpha = 0 \\ \int_a^t (d\tau)^\alpha, & \alpha < 0 \end{cases} \quad (1.27)$$

avec $\alpha \in \mathbb{R}$ est l'ordre de dérivation et a, t sont les limites de l'opération. A partir de l'équation (1.27), la notation englobe les définitions des opérateurs de dérivation et d'intégration. En effet, pour des valeurs positives de l'ordre ($\alpha > 0$), on effectue une opération de dérivation fractionnaire. Dans le cas où ($\alpha < 0$), on effectue une opération

d'intégration. C'est pour cette raison que l'opérateur est souvent appelé opérateur intégral-différentiel.

1.6.1.2 Fonctions spécifiques dans le calcul fractionnaire

Avant de fournir quelques définitions et notions de base dans le domaine du calcul fractionnaire, il est nécessaire de présenter les fonctions Gamma et Mittag-Leffler qui jouent un rôle très important dans la théorie du calcul fractionnaire.

A) La fonction Gamma

L'une des fonctions de base dans le calcul fractionnaire est la fonction Gamma $\Gamma(\cdot)$ qui généralise la factorielle $n!$ et permet à n de prendre des valeurs non entières et même complexes. Cette fonction joue un rôle important dans le calcul fractionnaire [114]. Elle est définie par l'intégrale suivante :

$$\Gamma(v) = \int_0^{\infty} t^{v-1} e^{-t} dt \quad (1.28)$$

avec $\Gamma(1) = 1$ et $\Gamma(0_+) = +\infty$

La fonction $\Gamma(v)$ est une fonction monotone et strictement décroissante pour $0 < v \leq 1$. Une propriété importante de cette fonction est la relation de récurrence suivante obtenue par l'intégration par partie de (1.28) [115].

$$\Gamma(v+1) = v\Gamma(v) \quad (1.29)$$

B) La fonction de Mittag-Leffler

La généralisation de la fonction exponentielle e^v à un seul paramètre au cas du calcul fractionnaire est donnée par la fonction de Mittag-Leffler définie comme suit [116] :

$$E_{\alpha}(v) = \sum_{k=0}^{\infty} \frac{v^k}{\Gamma(\alpha k + 1)}, \quad (v \in \mathbb{C}, \alpha > 0) \quad (1.30)$$

La fonction de Mittag-Leffler à 2 paramètres a été introduite par Agarwal [117] et

elle est définie par le développement en série suivant [118] :

$$E_{\alpha,\beta}(v) = \sum_{k=0}^{\infty} \frac{v^k}{\Gamma(\alpha k + \beta)}, \quad (v \in \mathbb{C}, \alpha > 0, \beta > 0) \quad (1.31)$$

Pour $\alpha = 1$ et $\beta = 1$, on aura [119] :

$$E_{1,1}(v) = \sum_{k=0}^{\infty} \frac{v^k}{\Gamma(k+1)} = \sum_{k=0}^{\infty} \frac{v^k}{k!} = e^v \quad (1.32)$$

Ainsi, la fonction de Mittag-Leffler joue le même rôle que la fonction exponentielle, dans le cas des équations différentielles d'ordre fractionnaire.

1.6.1.3 Définitions des dérivées et intégrales d'ordre fractionnaire

Différentes définitions de l'intégration et dérivation d'ordre fractionnaire ont été proposées durant le développement de la théorie du calcul fractionnaire. Certaines sont directement généralisées à partir du cas entier. Dans ce qui suit, nous présenterons les définitions les plus utilisées par la communauté scientifique.

1) La définition de Riemann-Liouville

La dérivée d'ordre fractionnaire au sens de Riemann-Liouville est la définition la plus répandue et connue [97, 98]. Elle est basée sur la primitive $n^{ième}$ d'une fonction f .

Considérons la formule de Cauchy pour l'intégration

$$\begin{aligned} {}_a I_t^n f(x) &= \int_a^t d\tau_1 \int_a^{\tau_1} d\tau_2 \cdots \int_a^{\tau_{n-1}} f(\tau_n) d\tau_n \\ &= \frac{1}{(n-1)!} \int_a^t f(t-\tau) d\tau \end{aligned} \quad (1.33)$$

où a , t sont les limites de l'intégrale $f(\tau)$. L'équation (1.34) peut-être généralisée pour $n \in \mathbb{R}$. Dans ce cas, nous obtenons la formule de Riemann-Liouville pour l'intégrale fractionnaire :

$${}_a^R I_t^\alpha f(t) = \frac{1}{\Gamma(\alpha)} \int_a^t f(t-\tau)^{\alpha-1} f(\tau) d\tau \quad (1.34)$$

Où $\alpha \in \mathbb{R}^+$ est l'ordre d'intégration de la fonction $f(t)$

Définition 1 *L'opérateur intégral-différentiel fractionnaire de Riemann-Liouville est défini comme suit [97, 98]*

$${}_a^R D_t^\alpha f(t) = \frac{1}{\Gamma(m - \alpha)} \frac{d^m}{dt^m} \int_a^t \frac{f(\tau)}{(t - \tau)^{\alpha - m + 1}} d\tau \quad (1.35)$$

où $\alpha \in \mathbb{R}$ est l'ordre fractionnaire. Pour $\alpha > 0, m - 1 < \alpha \leq m, m \in \mathbb{N}$ et pour $\alpha \leq 0, m = 0$ [120].

La transformée de Laplace de l'intégral-différentiation d'ordre fractionnaire de Riemann-Liouville est donnée comme suit [121] :

$$L[{}_0^R D_t^\alpha f(t)] = \begin{cases} p^\alpha F(p), & \alpha < 0 \\ p^\alpha F(p) - \sum_{k=0}^{n-1} p^k ({}_0^R D_t^{\alpha-k-1} f(0)), & \alpha > 0 \end{cases} \quad (1.36)$$

Avec $n - 1 < \alpha \leq n$ et $n \in \mathbb{N}$.

A partir de l'équation précédente, nous pouvons constater que la transformée de Laplace de la définition de Riemann-Liouville traite et implique les dérivées d'ordre fractionnaire des conditions initiales.

2) La définition de Caputo

L'ordre non-entier des conditions initiales implique le problème d'utilisation de la définition de Riemann-Liouville dans les applications réelles. En fait, malgré que les problèmes de conditions initiales peuvent être résolus mathématiquement, leurs solutions sont pratiquement sans utilité puisque l'interprétation physique de tels types de conditions initiales est non connue. Pour éventuellement pallier à cette situation, Caputo a proposé une nouvelle définition de la dérivée fractionnaire qui incorpore les conditions initiales de la fonction à traiter ainsi que ses dérivées entières [122]. Cette nouvelle définition a la forme suivante :

Définition 2 *L'opération d'intégré-différentiation d'ordre fractionnaire de Caputo est formulée comme suit :*

$${}_a^C D_t^\alpha f(t) = \frac{1}{\Gamma(m - \alpha)} \int_a^t \frac{f^{(m)}(\tau)}{(t - \tau)^{\alpha - m + 1}} d\tau \quad (1.37)$$

où $\alpha \in \mathbb{R}$ est l'ordre fractionnaire. Pour $\alpha > 0, m - 1 < \alpha \leq m, m \in \mathbb{N}$ pour $\alpha \leq 0, m = 0$.

Cette définition est plus restrictive que celle de Riemann-Liouville du fait qu'elle requiert l'intégrabilité absolue de la dérivée d'ordre m de la fonction $f(t)$. En général, les deux définitions sont non équivalentes excepté le cas où elles s'annulent à $t = 0^+$ pour la fonction $f(t)$ et ses $m - 1$ premières dérivées. Ceci peut-être traduit par les deux relations suivantes existant entre les deux définitions [123]

$${}_a^R D_t^\alpha f(t) = {}_a^C D_t^\alpha f(t) + \sum_{k=0}^{m-1} \frac{t_k - \alpha}{\Gamma(k - \alpha + 1)} f^{(k)}(0^+) \quad (1.38)$$

$${}_a^R D_t^\alpha f(t) (f(t) - \sum_{k=0}^{m-1} f^{(k)}(0^+) \frac{t^k}{k!}) = {}_a^C D_t^\alpha f(t) \quad (1.39)$$

La transformée de Laplace de l'opération intégré-différentiel d'ordre fractionnaire au sens de Caputo est donnée comme suit :

$$L[{}_0^C D_t^\alpha f(t)] = \begin{cases} p^\alpha F(p), & \alpha < 0 \\ p^\alpha F(p) - \sum_{k=0}^{n-1} p^{\alpha-k-1} f^{(k)}(0) & \alpha > 0 \end{cases} \quad (1.40)$$

avec $n - 1 < \alpha \leq n$.

La transformée de Laplace de la forme de Caputo implique la valeur de $f(t)$ et ses dérivées à la borne d'intégration $t = 0$ pour lesquelles une certaine interprétation physique existe. Par conséquent, la formule de Caputo est très utile pour la résolution de problèmes appliqués conduisant à une équation différentielle fractionnaire linéaire.

3) La définition de Grünwald-Letnikov

Une approche différente pour le calcul de dérivées d'ordre fractionnaire est la formule proposée par Grünwald et Letnikov. Cette définition consiste à la généralisation de l'équation aux différences pour le cas d'ordre fractionnaire [99].

Considérons une fonction continue $y = f(t)$. La dérivée d'ordre 1 est décrite par la formule suivante :

$$f'(t) = \frac{df}{dt} = \lim_{h \rightarrow 0} \frac{f(t-h) - f(t)}{h} \quad (1.41)$$

La dérivée d'ordre 2 de la fonction $f(t)$ peut-être écrite comme suit :

$$f''(t) = \frac{d^2f}{dt^2} = \lim_{h \rightarrow 0} \frac{f'(t-h) - f'(t)}{h} = \lim_{h \rightarrow 0} \frac{(t-2h) - 2f(t-h) + f(t)}{h^2} \quad (1.42)$$

Nous pouvons alors déduire la dérivée d'ordre n qui est donnée par

$$f^n(t) = \frac{d^n f}{dt^n} = \lim_{h \rightarrow 0} \frac{1}{h^n} \sum_{r=0}^n (-1)^r \binom{n}{r} f(t-rh) \quad (1.43)$$

Le terme $\binom{n}{r}$ peut-être calculé à partir de la relation :

$$\binom{n}{r} = \begin{cases} 1 & \text{pour } r = 0 \\ \frac{n(n-1)\dots(n-r+1)}{r!} & \text{pour } r > 0 \end{cases} \quad (1.44)$$

La généralisation de l'équation (1.44) au cas fractionnaire est l'objet de la définition de Grünwald-Letnikov suivante.

Définition 3 *La définition de Grünwald Letnikov pour l'intégro-différentiation d'ordre fractionnaire est formulée comme suit [99] :*

$$f^\alpha(t) = \frac{d^\alpha}{dt^\alpha} f = \lim_{h \rightarrow 0} \frac{1}{h^\alpha} \sum_{r=0}^{\alpha} (-1)^r \binom{\alpha}{r} f(t-rh) \quad (1.45)$$

où $\alpha \in \mathbb{R}$ est l'ordre fractionnaire

Cette définition sera utilisée ultérieurement dans l'étude des systèmes discrets d'ordre fractionnaire.

1.6.1.4 Fonction de transfert d'ordre fractionnaire

L'équation différentielle d'un système dynamique linéaire monovarié et continu d'ordre fractionnaire est écrite comme suit :

$$a_n D^{\alpha_n} y(t) + a_{n-1} D^{\alpha_{n-1}} y(t) + \dots + a_0 D^{\alpha_0} y(t) = b_m D^{\beta_m} u(t) + b_{m-1} D^{\beta_{m-1}} u(t) + \dots + b_0 D^{\beta_0} u(t) \quad (1.46)$$

où $\alpha_n, \dots, \alpha_0 \in \mathbb{R}$ et $\beta_n, \dots, \beta_0 \in \mathbb{R}$.

Si tous les ordres du système sont multiples d'un ordre de base α , autrement dit $\alpha_k, \beta_k = k\alpha, k \in \mathbb{R}^+$, le système est dit commensurable.

En appliquant la transformée de Laplace à l'équation (1.46) et considérant les conditions initiales nulles, la représentation entrée-sortie du système d'ordre fractionnaire peut-être obtenue comme suit [124]

$$G(p) = \frac{Y(p)}{U(p)} = \frac{b_m p^{\beta_m} + b_{m-1} p^{\beta_{m-1}} + \dots + b_0 p^{\beta_0}}{a_n p^{\alpha_n} + a_{n-1} p^{\alpha_{n-1}} + \dots + a_0 p^{\alpha_0}} \quad (1.47)$$

où $U(p), Y(p)$ sont les transformées de Laplace des signaux d'entrée et de sortie, respectivement, en supposant les conditions initiales nulles : $u(0) = 0, y(0) = 0$ et $m, n \in \mathbb{N}_+$. Dans le cas d'un système commensurable, la fonction de transfert continue est donnée par :

$$G(p) = \frac{\sum_{k=0}^m b_k (p^\alpha)^k}{\sum_{k=0}^n a_k (p^\alpha)^k} \quad (1.48)$$

1.6.1.5 Représentation d'état des systèmes d'ordre fractionnaire continus

Un système continu linéaire invariant dans le temps d'ordre fractionnaire peut-être représenté par le modèle d'état suivant [125] :

$$\begin{cases} D^\alpha x(t) &= Ax(t) + Bu(t) \\ y &= Cx(t) \end{cases} \quad (1.49)$$

Où $x \in \mathbb{R}^n, u \in \mathbb{R}^m, y \in \mathbb{R}^p$ sont respectivement les vecteurs d'état, d'entrées et de sorties du système. $\alpha = [\alpha_1, \alpha_2, \dots, \alpha_n]^T$ sont les ordres de dérivation non entiers et $A \in \mathbb{R}^{n \times n}$, $B \in \mathbb{R}^{n \times m}$, $C \in \mathbb{R}^{p \times n}$. m est le nombre d'entrées du système, p est le nombre de sorties et n est le nombre d'états.

Si $\alpha_1 = \alpha_2 = \dots = \alpha_n$, alors le système (1.49) est dit commensurable. Dans le cas contraire, on dit qu'il est non commensurable.

Dans le cas non linéaire, un système continu d'ordre fractionnaire peut être représenté dans le cas général comme suit :

$$\begin{cases} D^{\alpha_i} x_i(t) &= f_i(x_1(t), x_2(t), \dots, x_n(t), t) \\ x_i(0) &= c_i \quad i = 1, 2, \dots, n, \end{cases} \quad (1.50)$$

où c_i sont les conditions initiales.

La représentation vectorielle de (1.50) est :

$$D^\alpha x(t) = f(x(t), t) \quad (1.51)$$

où $\alpha = [\alpha_1, \alpha_2, \dots, \alpha_n]^T$ et $x \in \mathbb{R}^n$.

1.6.2 Les systèmes dynamiques discrets d'ordre fractionnaire

Le calcul fractionnaire discret est toujours en phase de développement et reste un sujet de recherche ouvert dans le domaine de mathématiques [30]. Dans cette partie de notre thèse, nous donnerons quelques notions et remarques indispensables pour l'analyse des

systèmes chaotiques discrets d'ordres fractionnaires.

1.6.2.1 Les différences d'ordre fractionnaire

Dans cette section, nous présenterons trois définitions de différences d'ordre fractionnaire qui sont la différence au sens de Caputo, la différence au sens de Riemann-Liouville et la différence au sens de Grünwald-Letnikov.

Soit l'ensemble $\mathbb{N}_a$ défini par $\mathbb{N}_a = \{a, a+1, \dots\}$.

La fonction fractionnaire t^α , $t \in \mathbb{R} \setminus \mathbb{Z}_-$, est définie par l'équation [126] :

$$t^\alpha = \frac{\Gamma(t+1)}{\Gamma(t+1-\alpha)} \quad (1.52)$$

où $\mathbb{Z}_- = -1, -2, \dots$ et Γ est la fonction d'Euler Gamma.

A) Différence de Caputo d'ordre fractionnaire

La première définition de différence d'ordre fractionnaire que nous présenterons est celle de Caputo. Elle est donnée comme suit :

Définition 4 [127]

soit $\alpha > 0$ et $m-1 < \alpha < m$. m est un entier positif tel que $m = \lceil \alpha \rceil$ où $\lceil \alpha \rceil$ désigne la partie entière supérieure de α .

La différence d'ordre α selon Caputo est définie comme suit :

$$\begin{aligned} ({}_a\Delta_C^\alpha f)(t) &= {}_a\Delta^{\alpha-m}(\Delta^m f)(t) \\ &= \frac{1}{\Gamma(m-\alpha)} \sum_{s=a}^{t-(m-\alpha)} (t-s-1)^{m-\alpha-1} (\Delta^m f)(s), \quad t \in \mathbb{N}_{a+m-\alpha} \end{aligned} \quad (1.53)$$

avec $t \in \mathbb{N}_{a+(m-\alpha)}$, $\alpha \in (0, 1]$ et $f : \mathbb{N}_a \rightarrow \mathbb{R}$.

Remarque 1 Si $0 < \alpha < 1$, alors $m = 1$ et la différence (1.53) peut-être réécrite comme suit [128] :

$$\begin{aligned}
({}_a\Delta_C^\alpha f)(t) &= ({}_a\Delta^{\alpha-1}(\Delta f(t))) \\
&= \frac{1}{\Gamma(1-\alpha)} \sum_{s=a}^{t-(1-\alpha)} (t-s-1)^{-\alpha} (\Delta f)(s), \quad t \in \mathbb{N}_{a+1-\alpha}
\end{aligned} \tag{1.54}$$

avec $\Delta f(s) = f(s+1) - f(s)$ est la différence classique.

Théoreme 2 [129] Pour l'équation aux différences fractionnaire suivante :

$$\begin{cases}
({}_{\alpha-1}\Delta_C^\alpha x(t) = f(t, x(t+\alpha-1))), & t \in \mathbb{N}_0 \\
x(\alpha-1) = x_0, & x_0 \in \mathbb{R}^n
\end{cases} \tag{1.55}$$

la solution discrète intégrale équivalente peut-être obtenue comme suit

$$x(t) = x_0 + \sum_{s=0}^{(t-\alpha)} \frac{(t-s-1)^{\alpha-1}}{\Gamma(\alpha)} f(s, x(s+\alpha-1)) \tag{1.56}$$

où $t \in \mathbb{N}_\alpha = \alpha, \alpha+1, \dots$ et $x \in \mathbb{R}^n$ est le vecteur d'état, n étant la dimension du système discret.

B) Différence de Riemann-Liouville d'ordre fractionnaire

La différence d'ordre fractionnaire au sens de Riemann-Liouville est formulée comme suit :

Définition 5 [130] La différence d'ordre fractionnaire α , au sens de Riemann-Liouville, de la fonction $f : \mathbb{N}_\alpha \rightarrow \mathbb{R}$ est définie comme suit :

$${}_a\Delta_{RL}^\alpha f(t) = {}_a\Delta^m (\Delta^{-(m-\alpha)} f)(t). \tag{1.57}$$

Remarque 3 Si $0 < \alpha < 1$, alors $m = 1$, l'équation (1.57) peut-être réécrite sous forme [131]

$${}_a\Delta_{RL}^\alpha f(t) = {}_a\Delta (\Delta^{-(1-\alpha)} f)(t), \quad t \in \mathbb{N}_{a+(1-\alpha)}. \tag{1.58}$$

Remarque 4 (a) Pour $\alpha = 1$, La relation suivante est vérifiée

$$({}_a\Delta_C^1 f)(t) = ({}_a\Delta_{RL}^1 f)(t) = \Delta(f)(t). \quad (1.59)$$

(b) Il a été démontré que pour toute fonction $f : \mathbb{N}_a \rightarrow \mathbb{R}$, La relation suivante, entre l'opérateur de différence de Riemann-Liouville et celui de Caputo, est vraie [132].

$${}_a\Delta_{RL}^\alpha f(t) = {}_a\Delta_C^\alpha f(t) + \frac{(t-a)^{(-\alpha)}}{\Gamma(1-\alpha)} f(a). \quad (1.60)$$

Théoreme 5 [133] Soit $f : \mathbb{N}_0 \times \mathbb{R}^n \rightarrow \mathbb{R}^n$ et $\alpha \in (0, 1]$

Le système d'équations aux différences d'ordre fractionnaire suivant :

$$\begin{cases} ({}_{\alpha-1}\Delta_{RL}^\alpha x)(t) &= f(t, x(t+\alpha-1)), & t \in \mathbb{N}_0 \\ x(\alpha-1) &= x_0, & x_0 \in \mathbb{R}^n \end{cases} \quad (1.61)$$

admet une solution unique donnée par le formule récurrente

$$x(t) = \frac{t^{(\alpha-1)}}{\Gamma(\alpha)} x_0 + \sum_{s=0}^{(t-\alpha)} \frac{(t-s-1)^{\alpha-1}}{\Gamma(\alpha)} f(s, x(s+\alpha-1)) \quad (1.62)$$

avec $t \in \mathbb{N}_{\alpha-1}$

C) Différence de Grünwald-Letnikov d'ordre fractionnaire

Considérons la différence d'ordre 1 suivante :

$$\Delta x(k) = x(k) - x(k-1) \quad (1.63)$$

La différence d'ordre 2 est présentée alors comme suit :

$$\Delta^2 x(k) = x(k) - 2x(k-1) + x(k-2) \quad (1.64)$$

La différence d'ordre entier m peut-être alors calculée à partir de la relation suivante

[130] :

$$\Delta^m x(k) = \sum_{j=0}^m (-1)^j \binom{m}{j} x(k-j) \quad (1.65)$$

En utilisant la relation (1.65), la différence de Grünwald-Letnikov d'ordre fractionnaire est définie ci-dessous [134] :

$$\Delta^\alpha x(k) = \sum_{j=0}^k (-1)^j \binom{\alpha}{j} x(k-j) \quad (1.66)$$

où $\alpha \in \mathbb{R}$ est l'ordre fractionnaire.

Dans la suite de cette thèse, nous nous baserons sur cette dernière définition pour modéliser un système chaotique discret d'ordre fractionnaire. Pour ce faire, considérons le système discret d'ordre entier suivant :

$$x(k+1) = f(x(k)) \quad (1.67)$$

où f est une fonction non linéaire.

La différence d'ordre 1 pour ce système discret est donnée par

$$\Delta^1 x(k+1) = x(k+1) - x(k) = f(x(k)) - x(k) \quad (1.68)$$

A partir de l'équation (1.68), nous définissons la différence d'ordre α comme suit :

$$\Delta^\alpha x(k+1) = f(x(k)) - x(k) \quad (1.69)$$

D'autre part, et à partir de l'équation (1.66), nous pouvons déduire que

$$\begin{aligned} \Delta^\alpha x(k+1) &= x(k+1) - \alpha x(k) \\ &+ \sum_{j=2}^{k+1} (-1)^j \binom{\alpha}{j} x(k-j+1) \end{aligned} \quad (1.70)$$

Pour simplifier la dernière équation, introduisons le changement de variable suivant

$p = j - 1$. L'équation (1.70) devient alors :

$$\begin{aligned} \Delta^\alpha x(k+1) &= x(k+1) - \alpha x(k) \\ &+ \sum_{p=1}^k (-1)^{p+1} \binom{\alpha}{p+1} x(k-p) \end{aligned} \quad (1.71)$$

Définissons le paramètre $C_p = (-1)^{p+1} \binom{\alpha}{p+1}$.

En remplaçant l'équation (1.71) dans (1.69), nous obtenons l'équation qui suit :

$$x(k+1) = f(x(k)) + (\alpha - 1)x(k) - \sum_{p=1}^k C_p x(k-p) \quad (1.72)$$

Remarque 6 On peut noter que si on pose $\alpha = 1$ dans l'équation (1.72), tous les coefficients $C_p, p = 1, 2, \dots, k$ s'annuleront. On peut considérer, par conséquent, qu'un système d'ordre entier est un cas particulier des systèmes d'ordre fractionnaire.

Remarque 7 Dans les applications réelles et pour diverses raisons telles les nombre de calculs et l'espace nécessaire importants pour chaque itération, on ne peut pas sauvegarder tous les états des systèmes discrets d'ordre fractionnaire [135]. Pour résoudre ce problème, on a souvent recours à une troncature finie pour l'approximation d'un système discret d'ordre fractionnaire. La longueur de cette troncature, que nous notons L , représente la taille de la mémoire considérée du système et elle est choisie de façon appropriée au problème à résoudre.

En appliquant cette limitation dans notre cas, nous obtenons l'approximation suivante.

$$x(k+1) = f(x(k)) + (\alpha - 1)x(k) - \sum_{p=1}^L C_p x(k-p) \quad (1.73)$$

Remarque 8 La figure 1.12 illustre les valeurs des coefficients C_p pour différentes valeurs de l'ordre de dérivation α et pour une mémoire de longueur $L = 20$. Les tracés obtenus

montrent que quelque soit l'ordre de dérivation, la valeur du coefficient C_p décroît et tend vers 0 à chaque fois que la valeur de p augmente.

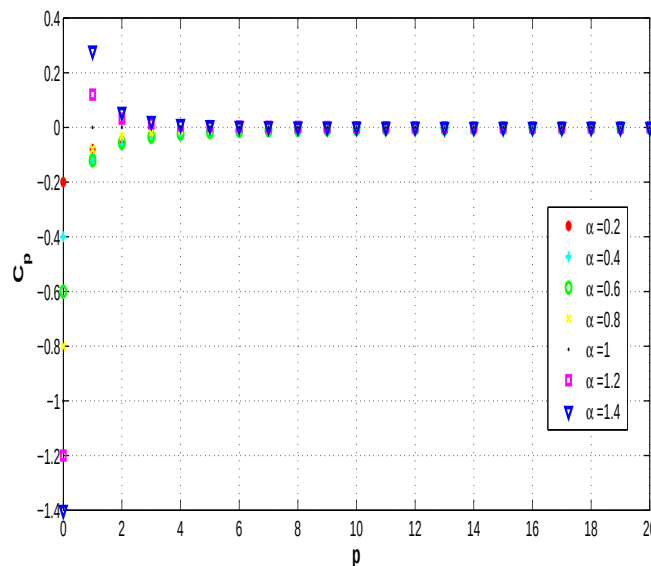


FIGURE 1.12 – Valeurs des coefficients C_p pour différents ordres fractionnaires

Remarque 9 L'approximation formulée par l'équation (1.73) s'applique uniquement au cas commensurable puisque l'ordre de dérivation α est le même pour toutes les variables d'état.

Pour traiter le cas contraire, c'est à dire le cas non commensurable, il est primordial de considérer tout les ordres de dérivation $\alpha_1, \alpha_2, \dots, \alpha_n$ respectifs aux états $x_1, x_2, \dots, x_n$ [136].

1.6.2.2 Fonction de transfert des systèmes discrets d'ordre fractionnaire

Dans le cas des systèmes discrets linéaires (ou systèmes équivalents discrets des systèmes continus) d'ordre fractionnaire on parle d'équation aux différences d'ordre fractionnaire. Cette dernière se présente sous la forme suivante :

$$\begin{aligned}
 a_n \Delta^{\alpha_n} y(t) + a_{n-1} \Delta^{\alpha_{n-1}} y(t) + \dots + a_0 \Delta^{\alpha_0} y(t) \\
 = b_m \Delta^{\beta_m} u(t) + b_{m-1} \Delta^{\beta_{m-1}} u(t) + \dots + b_0 \Delta^{\beta_0} u(t)
 \end{aligned}
 \tag{1.74}$$

où $a_n, a_{n-1}, \dots, a_0 \in \mathbb{R}$ et $b_m, b_{m-1}, \dots, b_0 \in \mathbb{R}$. $\alpha_i \in \mathbb{R}_+, i = 1, 2, \dots, n$ et $\beta_j \in \mathbb{R}_+, j = 1, 2, \dots, m$ sont les ordres de différences fractionnaires. Δ^{α_i} et Δ^{β_j} sont les opérateurs de différences d'ordre $\alpha_i, i = 1, 2, \dots, n$ et $\beta_j, j = 1, 2, \dots, m$ respectivement. $u(t)$ est l'entrée du système et $y(t)$ désigne sa sortie. En appliquant la transformée en Z à l'équation (1.74), la représentation Entrée-Sortie du système discret d'ordre fractionnaire est donnée par la fonction de transfert suivante [123] :

$$G(z) = \frac{b_m(\omega(z^{-1}))^{\beta_m} + b_{m-1}(\omega(z^{-1}))^{\beta_{m-1}} + \dots + b_0(\omega(z^{-1}))^{\beta_0}}{a_n(\omega(z^{-1}))^{\alpha_n} + a_{n-1}(\omega(z^{-1}))^{\alpha_{n-1}} + \dots + a_0(\omega(z^{-1}))^{\alpha_0}} \quad (1.75)$$

avec $\omega(z^{-1})$ est la transformée en Z de l'opérateur Δ^1 , ou, en d'autres termes, l'équivalent de l'opérateur de Laplace p en temps discret.

1.6.2.3 Représentation d'état des systèmes d'ordre fractionnaire discrets

La représentation d'état des systèmes discrets d'ordre fractionnaire linéaires a été introduite par Dzieliński et Sierociuk [137]. Leur définition contient trois équations essentielles pour calculer :

- la différence d'ordre fractionnaire de la variable d'état.
- La prochaine valeur de la variable d'état.
- la sortie du système.

La représentation d'état des systèmes discrets non linéaire d'ordre fractionnaire est définie par le système d'équations suivant :

$$\begin{cases} \Delta^\alpha x(k+1) &= f(x(k), u(k)) \\ x(k+1) &= \Delta^\alpha x(k+1) - \sum_{p=1}^L C_p x(k-p) \\ y(k) &= h(x(k)) \end{cases} \quad (1.76)$$

avec $x \in \mathbb{R}^n$ est le vecteur d'état, n étant le nombre d'états du système.

$\alpha \in \mathbb{R}$ est l'ordre de dérivation du système, f et h sont des fonctions non linéaires.

Un système linéaire d'ordre fractionnaire, en représentation d'état, est donc défini par [138] :

$$\begin{cases} \Delta^\alpha x(k+1) = Ax(k) + Bu(k) \\ x(k+1) = \Delta^\alpha x(k+1) - \sum_{p=1}^L C_p x(k-p) \\ y(k) = Cx(k) + Du(t) \end{cases} \quad (1.77)$$

avec $x \in \mathbb{R}^n$ est le vecteur d'état, $A \in \mathbb{R}^{n \times n}$, $B \in \mathbb{R}^{n \times m}$, $C \in \mathbb{R}^{p \times n}$, $D \in \mathbb{R}^{p \times m}$, n étant le nombre d'états du système, m le nombre d'entrées, p le nombre de sorties et $\alpha \in \mathbb{R}$ l'ordre de dérivation du système.

1.7 Les systèmes chaotiques d'ordre fractionnaire

Au cours des dernière décades, il a été constaté que les systèmes d'ordre fractionnaire peuvent présenter un comportement chaotique. En outre, il a été aussi démontré que l'ordre des systèmes chaotiques continus d'ordre fractionnaire peut-être inférieur à 3 alors que ça ne peut pas arriver dans le cas de systèmes d'ordre entier selon le théorème de Poincaré-Bendixon [114]. Dans la partie qui suit, nous présenterons quelques systèmes chaotiques d'ordre fractionnaire évoluant en temps continus et discrets.

1.7.1 Systèmes chaotiques d'ordre fractionnaire continus

Nous développerons, dans cette partie, deux exemples de systèmes chaotiques continus d'ordre fractionnaire. Il s'agit des systèmes de Rössler et de Chen d'ordre fractionnaire.

Exemple 1 : le système chaotique de Rössler d'ordre fractionnaire

Le système de Rössler est un système tridimensionnel qui a été proposé en 1976 par Otto Rössler. Plus tard, les équations de ce système sont avérées utiles pour modéliser l'équilibre dans les réactions chimiques [16]. Les équations du système de Rössler sont données comme suit [139]

$$\begin{cases} \dot{x}_1 &= -(x_2(t) + x_3(t)) \\ \dot{x}_2 &= x_1(t) + ax_2(t) \\ \dot{x}_3 &= b + x_3(t)(x_1(t) - c) \end{cases} \quad (1.78)$$

où x_1, x_2 et x_3 sont les états du système. Pour les valeurs $a = 0.2$, $b = 0.2$ et $c = 5.7$, le système (1.78) présente un comportement chaotique.

La généralisation du système de Rössler au cas fractionnaire est représentée comme suit [140] :

$$\begin{cases} D^{\alpha_{11}}x_1 &= -(x_2(t) + x_3(t)) \\ D^{\alpha_{12}}x_2 &= x_1(t) + ax_2(t) \\ D^{\alpha_{13}}x_3 &= b + x_3(t)(x_1(t) - c) \end{cases} \quad (1.79)$$

avec $0 < \alpha_{11} \leq 1$, $0 < \alpha_{12} \leq 1$ et $0 < \alpha_{13} \leq 1$ sont les ordres de dérivation fractionnaires des états x_1, x_2 et x_3 respectivement.

La figure 1.13 présente l'attracteur étrange obtenu pour les valeurs des paramètres $a = 0.5$, $b = 0.2$ et $c = 10$ et pour les valeurs des ordres de dérivations fractionnaires $\alpha_{11} = 0.9$, $\alpha_{12} = 0.85$, $\alpha_{13} = 0.95$ [16]. Les conditions initiales considérées sont $(x_1(0), x_2(0), x_3(0)) = (0.5, 1.5, 0.1)$. L'évolution chaotique des états x_1, x_2 et x_3 est illustrée sur la figure 1.14.

Exemple 2 : le système chaotique de Chen d'ordre fractionnaire

Le deuxième exemple que nous verrons est le système chaotique de Chen proposé en 1999.

Ce système est décrit par les équations suivantes [141] :

$$\begin{cases} \dot{x}_1 &= \bar{a}(x_2(t) - x_1(t)) \\ \dot{x}_2 &= (\bar{c} - \bar{a})x_1(t) - x_1(t)x_3(t) + \bar{c}x_2(t) \\ \dot{x}_3 &= x_1(t)x_2(t) - \bar{b}x_3(t) \end{cases} \quad (1.80)$$

avec x_1, x_2 et x_3 sont les états du système et $\bar{a}$, $\bar{b}$ et $\bar{c}$ les paramètres de contrôle. Pour les valeurs $\bar{a} = 35$, $\bar{b} = 3$ et $\bar{c} = 28$, le système (1.80) présente un comportement chaotique.

Les équations du système de Chen d'ordre fractionnaire sont données comme suit

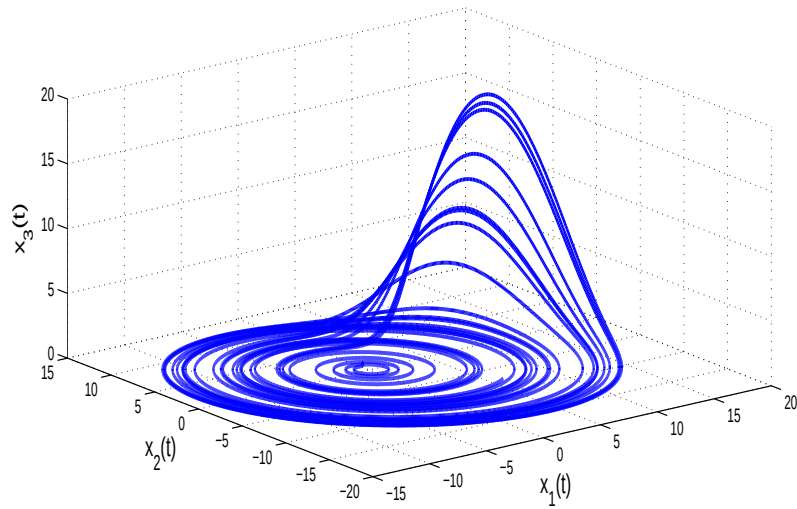


FIGURE 1.13 – Attracteur étrange de Rössler d'ordre fractionnaire avec $a = 0.5$, $b = 0.2$, $c = 10$ et $\alpha_{11} = 0.9$, $\alpha_{12} = 0.85$ et $\alpha_{13} = 0.95$

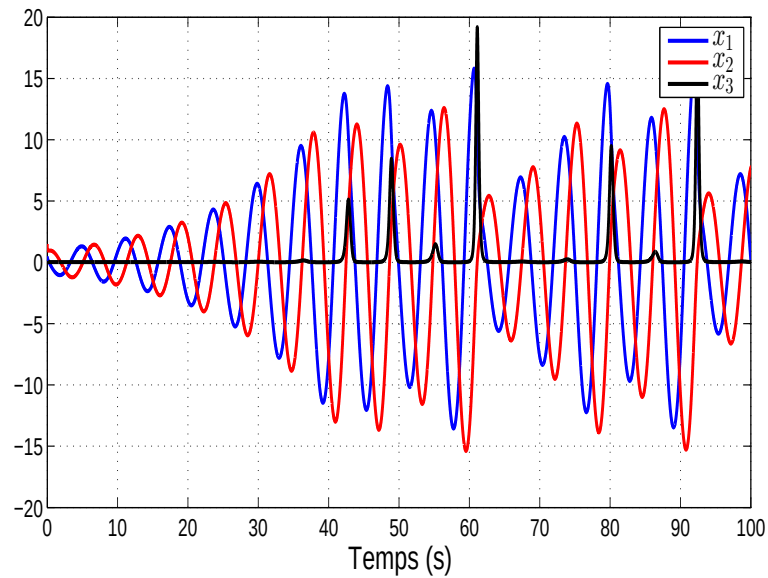


FIGURE 1.14 – Evolution chaotique des états x_1 , x_2 et x_3 du système de Rössler d'ordre fractionnaire avec $a = 0.5$, $b = 0.2$, $c = 10$ et $\alpha_{11} = 0.9$, $\alpha_{12} = 0.85$ et $\alpha_{13} = 0.95$

[142] :

$$\begin{cases} D^{\alpha_{21}} x_1 &= \bar{a}(x_2(t) - x_1(t)) \\ D^{\alpha_{22}} x_2 &= (\bar{c} - \bar{a})x_1(t) - x_1(t)x_3(t) + \bar{c}x_2(t) \\ D^{\alpha_{23}} x_3 &= x_1(t)x_2(t) - \bar{b}x_3(t) \end{cases} \quad (1.81)$$

avec α_{21} , α_{22} et α_{23} sont les ordres de dérivation des états x_1, x_2 et x_3 respectivement tels que $0 < \alpha_{21}, \alpha_{22}, \alpha_{23} \leq 1$. Pour les mêmes valeurs des paramètres $\bar{a}$, $\bar{b}$ et $\bar{c}$, et pour les valeurs $\alpha_{21} = \alpha_{22} = \alpha_{23} = 0.95$, le système (1.81) évolue en régime chaotique [16].

La figure 1.15 montre l'attracteur étrange obtenu en plan de phase en choisissant les conditions initiales suivantes $(x_1(0), x_2(0), x_3(0)) = (-9, -15, 14)$.

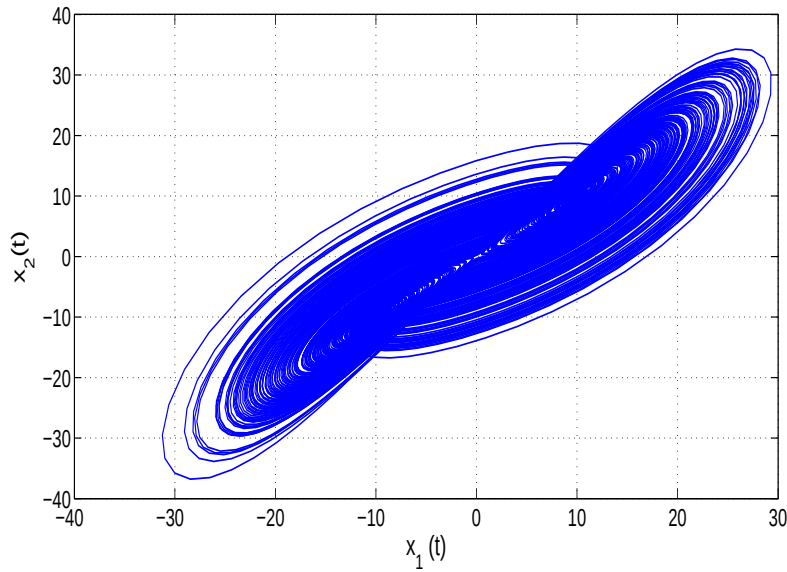


FIGURE 1.15 – Attracteur étrange de Chen d'ordre fractionnaire avec $\bar{a} = 35$, $\bar{b} = 3$, $\bar{c} = 28$ et $\alpha_{21} = \alpha_{22} = \alpha_{23} = 0.95$

La figure 1.16 présente l'évolution chaotique des états x_1 , x_2 et x_3 du système de Chen d'ordre fractionnaire.

1.7.2 Systèmes chaotiques d'ordre fractionnaire discrets

Comme nous l'avons mentionné dans l'introduction de cette thèse, notre contribution se porte sur les systèmes chaotiques d'ordre fractionnaire discrets. Dans cette partie, nous verrons comme exemples deux systèmes chaotiques discrets : la fonction logistique et le système de Lozi d'ordre fractionnaire.

Exemple 1 : La fonction logistique d'ordre fractionnaire

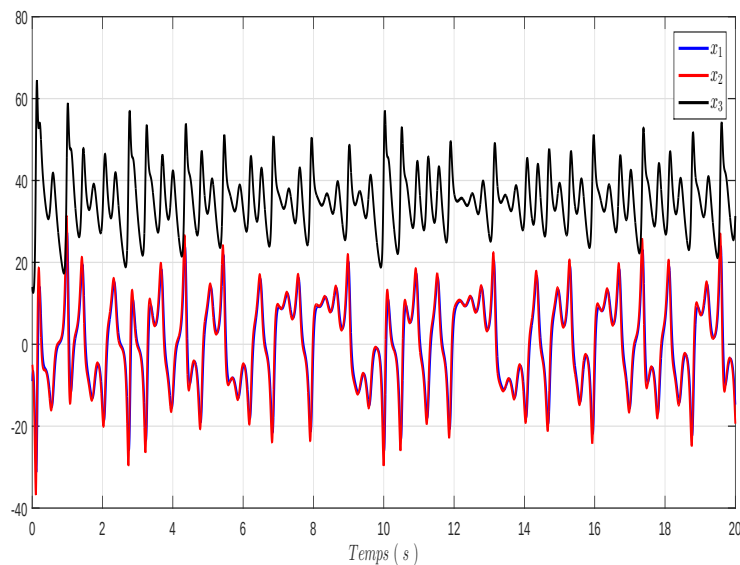


FIGURE 1.16 – Evolution chaotique des états x_1 , x_2 et x_3 du système de Chen d'ordre fractionnaire avec $\bar{a} = 35$, $\bar{b} = 3$, $\bar{c} = 28$ et $\alpha_{21} = \alpha_{22} = \alpha_{23} = 0.95$

Considérons, de nouveau, la fonction logistique définie par l'équation (1.5).

En utilisant l'approximation de Grünwald-Letnikov (1.73), la fonction logistique d'ordre fractionnaire est définie comme suit :

$$x(k+1) = rx(k)(1-x(k)) + (\alpha-1)x(k) - \sum_{p=1}^L C_p x(k-p) \quad (1.82)$$

avec α est l'ordre de dérivation fractionnaire et $C_{p1} = (-1)^{p+1} \binom{\alpha_1}{p+1}$.

L désigne la taille de la mémoire.

Pour les valeurs de $r = 4$, $\alpha = 0.96$, $L = 20$ et $x(0) = 0.3$, la fonction logistique d'ordre non entier (1.82) présente un comportement chaotique. L'évolution chaotique du système (1.82) est illustrée sur la figure 1.17. La figure 1.18 illustre l'attracteur chaotique obtenu dans le plan de phase des états $x(k)$ et $x(k-1)$.

Exemple 2 : Le système de Lozi d'ordre fractionnaire

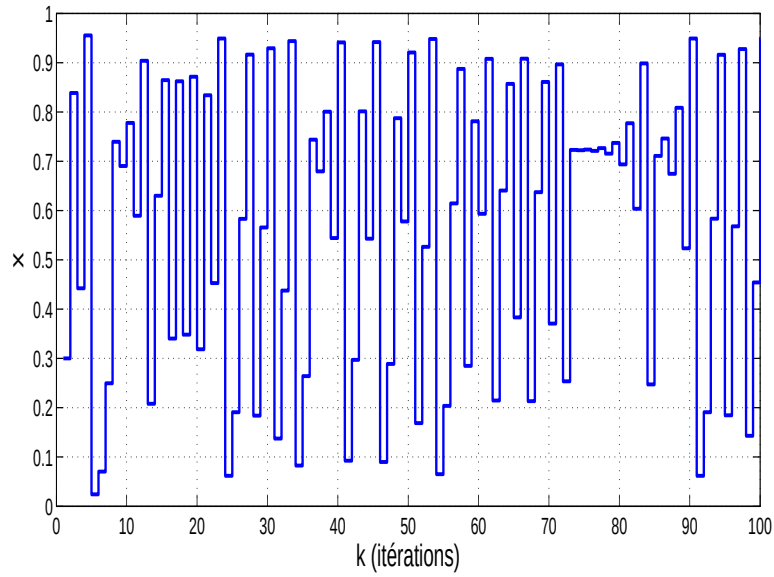


FIGURE 1.17 – Evolution chaotique de la fonction logistique d'ordre fractionnaire pour $r = 4$, $\alpha = 0.96$ et $L = 20$

Le système de Lozi d'ordre entier est un système discret à deux dimensions [143]. Ses équations sont données par :

$$\begin{cases} x_1(k+1) &= 1 - a |x_1(k)| + bx_2(k) \\ x_2(k+1) &= x_1(k) \end{cases} \quad (1.83)$$

où $[x_1 \ x_2]^T \in \mathbb{R}^2$ est le vecteur d'état et a, b sont deux paramètres constants. Ils satisfont les conditions $0 < b < 1$ et $1 + b < a < 2 - \frac{b}{2}$. Nous choisissons $a = 1.7$ et $b = 0.5$ de telle manière à ce que le système présente une évolution chaotique.

Le système discret de Lozi d'ordre fractionnaire est obtenu en utilisant l'approximation de Grünwald-Letnikov présentée précédemment dans ce chapitre. Le modèle obtenu est décrit par le système suivant.

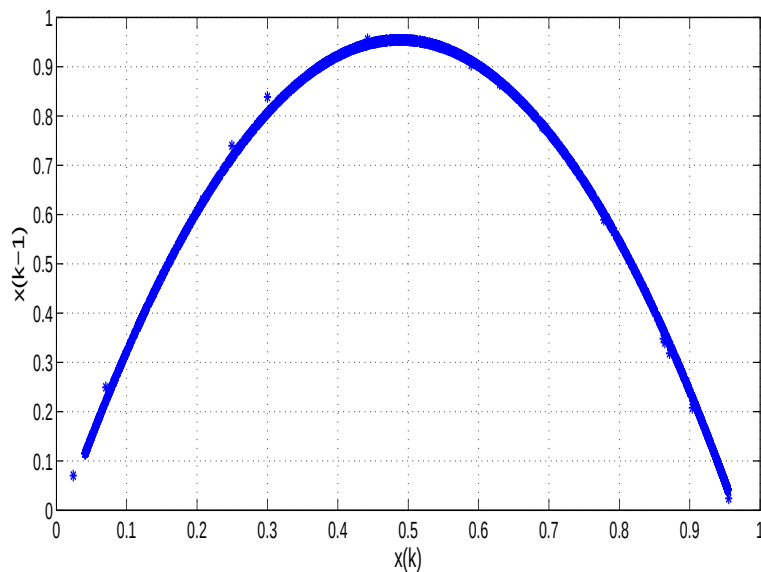


FIGURE 1.18 – Attracteur étrange de la fonction logistique d'ordre fractionnaire pour $r = 4$, $\alpha = 0.96$ et $L = 20$ en plan de phase $(x(k) - x(k - 1))$

$$\left\{ \begin{array}{l} x_1(k+1) = 1 - a |x_1(k)| + bx_2(k) + (\alpha_1 - 1)x_1(k) \\ \quad - \sum_{p=1}^L C_{p1} x_1(k-p) \\ x_2(k+1) = x_1(k) + (\alpha_2 - 1)x_2(k) \\ \quad - \sum_{p=1}^L C_{p2} x_2(k-p) \end{array} \right. \quad (1.84)$$

avec $0 \leq \alpha_1 \leq 1$, $0 \leq \alpha_2 \leq 1$ sont les ordres de dérivation et les coefficients C_p sont définis comme suit :

$$C_{p1} = (-1)^{p+1} \binom{\alpha_1}{p+1}, \quad C_{p2} = (-1)^{p+1} \binom{\alpha_2}{p+1}.$$

Comme nous l'avons introduit lors de la définition de la dérivée fractionnaire selon Grünwald-Letnikov, L dénote la taille de la mémoire du système.

Les figures 1.19 et 1.20 illustrent, respectivement, l'attracteur étrange, obtenu en plan de phase des états x_1 and x_2 , du système de Lozi d'ordre fractionnaire et les évolutions temporelles de ces deux états. Les ordres de dérivation sont pris comme suit : $\alpha_1 = \alpha_2 = 0.95$. Les conditions initiales choisies sont $x_1(0) = 0.1$ et $x_2(0) = 0.2$.

Le système de Lozi d'ordre fractionnaire sera pris comme exemple tout au long des

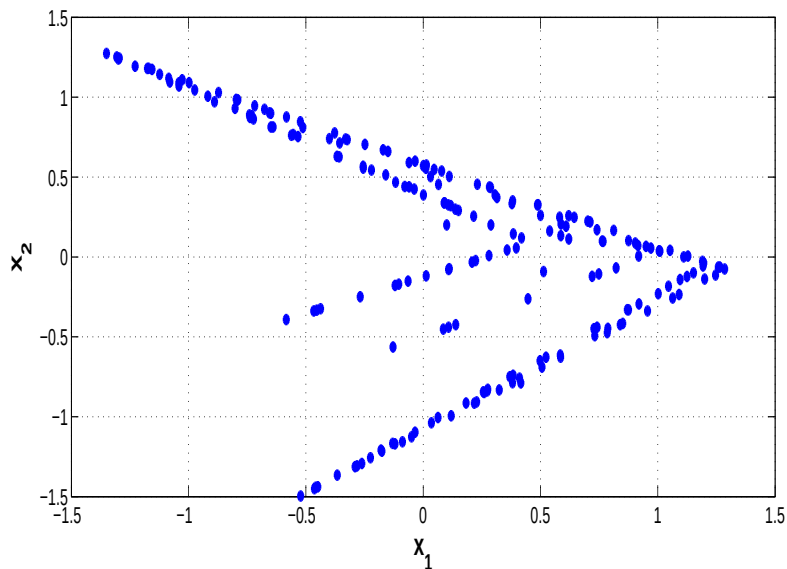


FIGURE 1.19 – Attracteur étrange du système de Lozi d'ordre fractionnaire avec $a = 1.7, b = 0.5, \alpha_1 = \alpha_2 = 0.95$ et $L = 10$

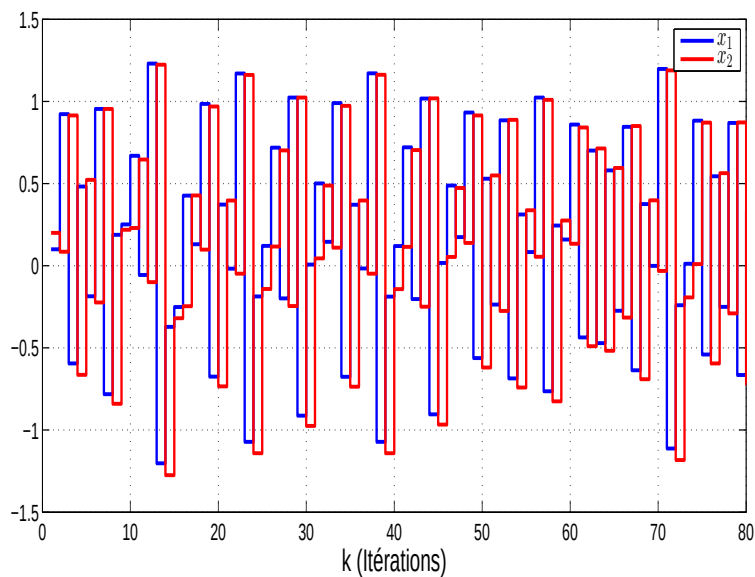


FIGURE 1.20 – Evolution chaotique des états x_1 et x_2 du système de Lozi d'ordre fractionnaire avec $a = 1.7, b = 0.5$ et $\alpha_1 = \alpha_2 = 0.95$

chapitres qui suivent. Une étude plus approfondie et une analyse pertinente de ses dynamiques seront établies dans le troisième chapitre de cette thèse.

1.8 Conclusion

Dans ce chapitre, nous avons fourni les notions de bases et les outils mathématiques nécessaires pour étudier et appliquer les systèmes chaotiques d'ordre fractionnaire. En premier lieu, nous avons présenté un état de l'art sur la théorie du chaos et sur les propriétés essentielles des systèmes chaotiques. La théorie de la dérivation non entière a été introduite juste après et ce, à partir de quelques rappels sur les fonctions de base comme les fonctions de Gamma Euler et de Mittag-Leffler. Nous avons, ensuite, présenté les différentes définitions et propriétés de la dérivée fractionnaire en temps continu d'abord puis en temps discret.

Nous avons clos le chapitre par quelques exemples de systèmes chaotiques d'ordre fractionnaire continus et discrets en précisant pour chaque exemple, ses caractéristiques telles les équations dynamiques, l'attracteur étrange et l'aspect aléatoire des évolutions chaotiques.

Afin d'utiliser les systèmes chaotiques, qu'ils soient d'ordre entier ou d'ordre fractionnaire, dans la transmission de données, il est nécessaire de les synchroniser. Pour cette raison, et dans le chapitre qui suit, nous développerons en détails, le principe de synchronisation des systèmes chaotiques et les méthodes proposées pour sa réalisation.

Chapitre 2

Synchronisation des systèmes chaotiques d'ordre entier

2.1 Introduction

Le terme synchronisation vient du grec : *syn* qui signifie avec et *chronos* qui est le temps ce qui donne "a lieu au même temps". Le phénomène de synchronisation se manifeste donc lorsque deux systèmes évoluent d'une manière identique en fonction de temps.

La synchronisation est un processus omniprésent dans la vie courante et joue un rôle important dans différents contextes [144] tels la bioluminescence des lucioles [145], les horloges génétiques [146], les communications synchrones [147], la synchronisation des signaux audio et vidéo, etc. A première vue, et tenant compte de leur sensibilité aux conditions initiales, parler de synchronisation pour des systèmes chaotiques semble surprenant, et on peut penser que le chaos est incontrôlable. Cependant et depuis les célèbres travaux de Pecora et Carroll [21], montrant que les systèmes chaotiques peuvent être complètement synchronisés, la synchronisation des systèmes chaotiques et hyper-chaotiques a suscité un grand intérêt de la communauté scientifique. En effet, durant les deux dernières décennies, on retrouve la synchronisation du chaos dans différents domaines comme la physique [148] , la chimie [149], la communication sécurisée [150], la robotique [151], etc. Dans ce chapitre, nous développerons plus en détails le principe de synchronisation

des systèmes chaotiques et nous présenterons les différents types et différentes méthodes de synchronisation. Nous nous focaliserons par la suite sur la synchronisation des systèmes chaotiques à base d'observateurs impulsifs, appelée également synchronisation impulsive, qui est la méthode adoptée dans notre cas et donnerons quelques exemples et résultats dans le cas de systèmes chaotiques d'ordre entier continus et discrets. Nous terminerons ce chapitre par quelques remarques et une conclusion.

2.2 Synchronisation des systèmes chaotiques d'ordre entier

Dans cette partie, nous développerons davantage le principe de synchronisation des systèmes chaotiques et développerons les différents régimes de synchronisation existants et les méthodes proposées. Avant cela, nous présenterons un bref historique sur la synchronisation chaotique ainsi que les premiers travaux de recherche qui y ont été consacrés.

2.2.1 Historique

L'histoire de synchronisation remonte au dix-septième siècle. Le chercheur hollandais Christian Huygens a été le premier qui a observé et décrit le phénomène de synchronisation en 1658 [152]. Le scientifique a, en effet, constaté que deux de ses horloges à balancier, placées côte à côte, se synchronisaient parfaitement, en d'autres termes convergeaient rapidement vers un mouvement identique en phase et en fréquence même en présence de perturbations [153]. Le chercheur conclut alors l'existence d'un mouvement synchrone qu'il qualifia de *sympathie entre les deux horloges*. En 1870, et environ deux siècles plus tard, le physicien anglais Lord Rayleigh constata la possibilité des tubes sonore à vibrer à l'unisson. Lors des années 1920, V. Appleton et B. Van der Pol étudièrent le phénomène de synchronisation dans des générateurs de triode sous l'influence de faibles signaux de synchronisation. Cette étude a reçu une attention considérable due à son importance physique et signification pratique pour les communications radio [154]. En 1940, le chercheur V. Adler décrit le phénomène de verrouillage qui est un concept clé dans la synchronisation

des oscillateurs périodiques.

La synchronisation des systèmes chaotiques vit le jour dans les travaux de Fujisaka et Yamada en 1983 [155]. Les chercheurs ont ouvert la voie avec leurs études pionnières sur la synchronisation du chaos en utilisant une approche locale. Par la suite, Afraimovich et son équipe de recherche ont développé les concepts importants liés à la synchronisation chaotique [156]. En 1990, L. Pecora et T. Carroll démontrèrent théoriquement et expérimentalement la possibilité de synchronisation identique entre deux circuits chaotiques couplés, l'un appelé *Maître* et l'autre est dit *Esclave* [21]. Une autre approche de synchronisation chaotique a été proposée par Rulkov [24]. Le schéma de synchronisation considère aussi une paire de systèmes configurés en maître-esclave, excepté que cette fois le couplage n'est pas limité aux systèmes identiques. Grâce à ces derniers travaux, le problème de synchronisation des systèmes chaotiques a été de plus en plus étudié. Plusieurs idées et approches ont été proposées pour synchroniser les systèmes chaotiques et les appliquer dans divers domaines d'ingénierie comme la transmission sécurisée.

Dans ce qui suit, nous développerons, plus en détails, la notion de synchronisation chaotique et présenterons les différents régimes de synchronisation existants.

2.2.2 Principe de synchronisation des systèmes chaotiques

La configuration Maître-Esclave est l'une des configurations les plus populaires de la synchronisation de systèmes chaotiques. Dans un schéma maître-esclave, un système dynamique dit esclave suit le rythme et l'évolution imposés par un autre système dynamique dit système maître. On dit, alors, qu'un système esclave défini, dans le cas continu, par le système différentiel

$$\dot{x}_s(t) = f_s(x_s(t)), \quad x_s \in \mathbb{R}^n \quad (2.1)$$

et, dans le cas discret, par l'équation aux différences :

$$x_s(k+1) = f_s(x_s(k)), \quad x_s(k) \in \mathbb{R}^n \quad (2.2)$$

se synchronise avec un système maître donné, en temps continu, par le système d'équations différentielles :

$$\dot{x}_m(t) = f_m(x_m(t)), \quad x_m(t) \in \mathbb{R}^n \quad (2.3)$$

et, en temps discret, par l'équation aux différences :

$$x_m(k+1) = f_m(x_m(k)), \quad x_m(k) \in \mathbb{R}^n \quad (2.4)$$

si, pour toute paire de conditions initiales $(x_m(0), x_s(0)) \in \mathbb{R}^n \times \mathbb{R}^n$, on a :

$$\lim_{(t,k) \rightarrow +\infty} \|x_s - x_m\| = 0 \quad (2.5)$$

où $\|\cdot\|$ est la norme euclidienne.

2.2.3 Types de synchronisation

Différents types de synchronisations ont été introduits suite à la découverte innovatrice de Pecora et Carroll. Ces types sont la synchronisation par répartition du système, la synchronisation généralisée, la synchronisation décalée, la synchronisation projective, la synchronisation Q-S et la synchronisation de phase. Dans cette section, nous définirons et donnerons le principe de chaque type de synchronisation.

2.2.3.1 Synchronisation par répartition du système

Appelée aussi synchronisation de Pecora et Carroll, cette méthode consiste à décomposer d'une manière appropriée un système chaotique donné par les équations

$$\begin{cases} \dot{x} &= f(x), & x \in \mathbb{R}^n \\ y &= h(x) \end{cases} \quad (2.6)$$

en deux sous-systèmes

$$\dot{x}_1 = f_1(x_1, x_2) \quad (2.7)$$

et

$$\dot{x}_2 = f_2(x_2, x_1) \quad (2.8)$$

avec $x = [x_1^T \ x_2^T]$

de telle sorte que les exposants de Lyapunov conditionnels du système (2.8) soient négatifs [157]. La figure (2.1) illustre le principe de synchronisation par répartition du système.

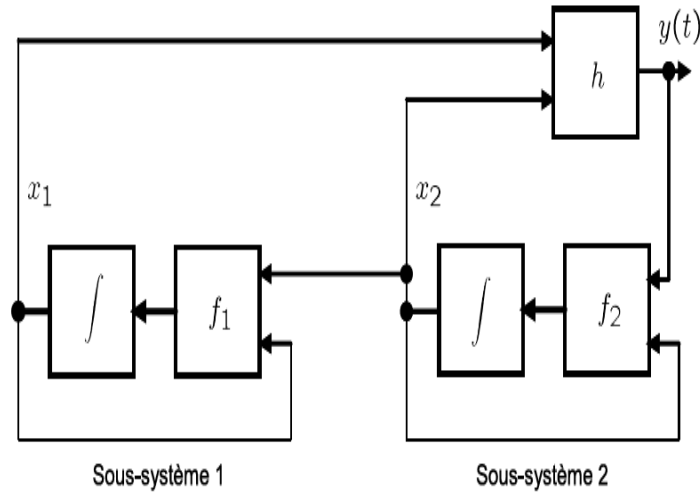


FIGURE 2.1 – Principe de synchronisation par répartition du système

2.2.3.2 Synchronisation généralisée

Cette méthode de synchronisation a été introduite par Rulkov [24] comme une généralisation de l'idée de synchronisation. On dit que les deux systèmes (2.1) et (2.3) sont synchronisés au sens généralisé, s'il existe une fonction $\Psi : \mathbb{R}^n \rightarrow \mathbb{R}^n$ telle que toutes les trajectoires des systèmes maître et esclave, avec les conditions initiales $x_s(0)$ et $x_m(0)$;

vérifient :

$$\lim_{(t,k) \rightarrow +\infty} \|x_s - \Psi(x_m)\| = 0 \quad (2.9)$$

2.2.3.3 Synchronisation projective

La synchronisation projective est une autre forme spéciale de la synchronisation généralisée. On dit qu'une synchronisation projective a lieu, si chaque état x_{si} , $i = 1, 2, \dots, n$ du système chaotique esclave se synchronise avec un multiple de l'état x_{mi} , $i = 1, 2, \dots, n$ du système chaotique maître. Cette synchronisation peut-être formulée comme suit [22] :

$$\exists a_i \neq 0, \quad \lim_{(t,k) \rightarrow +\infty} |x_{si} - a_i x_{mi}| = 0, \quad \forall (x_m(0), x_s(0)) \quad i = 1, 2, \dots, n. \quad (2.10)$$

2.2.3.4 Synchronisation retardée

Dans les méthodes de synchronisation que nous avons présentées jusqu'ici, l'interaction entre les systèmes est instantanée. Toutefois, deux systèmes dynamiques chaotiques non identiques peuvent exposer un phénomène de synchronisation dans lequel les états des deux systèmes deviennent synchronisés, mais avec un décalage dans le temps. Cette synchronisation est alors qualifiée de synchronisation retardée ou décalée ou même anticipée [23]. On dit alors qu'il y a une synchronisation retardée entre deux systèmes maître et esclave représentés respectivement par les équations (2.3) et (2.1), si la relation suivante est vérifiée.

$$\lim_{t \rightarrow +\infty} \|x_s(t) - x_m(t - \tau)\| = 0 \quad (2.11)$$

où τ est un retard positif très petit.

Dans le cas discret, une synchronisation retardée entre les deux systèmes chaotiques discrets maître et esclave représentés par (2.4) et (2.2) respectivement a lieu si

$$\lim_{k \rightarrow +\infty} \|x_s(k) - x_m(k - \tau)\| = 0 \quad (2.12)$$

2.2.3.5 Synchronisation $Q - S$

La synchronisation de type Q-S est considérée comme une généralisation de tous les types de synchronisations précédentes [158]. On dit qu'un système maître x_m de dimension n et un système esclave x_s de dimension m sont en synchronisation $Q - S$ dans la dimension d , s'il existe deux fonctions $Q : \mathbb{R}^n \rightarrow \mathbb{R}^d$ et $S : \mathbb{R}^m \rightarrow \mathbb{R}^d$ telles que

$$\lim_{(t,k) \rightarrow +\infty} \|Q(x_m) - S(x_s)\| = 0 \quad (2.13)$$

2.2.3.6 Synchronisation de phase

On peut définir la synchronisation de phase en se basant sur la théorie classique linéaire des vibrations.

Considérons deux oscillateurs couplés de phases Φ_1 et Φ_2 . Il a été démontré que la synchronisation de phase entre ces deux oscillateurs a lieu lorsque l'inégalité suivante est satisfaite [159].

$$|n\Phi_1 - m\Phi_2| < c \quad \forall n, m \in \mathbb{Z}. \quad (2.14)$$

où c est une constante.

La relation (2.14) n'impose aucune condition sur les amplitudes des oscillations.

2.2.4 Techniques et stratégies de synchronisation

La théorie de commande des systèmes a joué un rôle important dans le développement des méthodes modernes de synchronisation. Diverses méthodes, basées sur la conception de différentes lois de commande, ont été largement rapportées dans la littérature. Nous présenterons dans cette partie, les méthodes de synchronisation souvent utilisées dans le contexte de synchronisation.

2.2.4.1 Synchronisation avec commande par rétroaction

Cette approche est considérée comme l'une des méthodes efficaces pour la synchronisation des systèmes chaotiques. En effet, la technique de commande par retour par rétroaction a attiré l'intérêt de nombreux chercheurs et plusieurs commandes par retour linéaire ou non linéaire ont été appliquées pour la synchronisation du chaos [160].

Dans l'objectif de développer cette méthode, nous considérons le cas simple d'un retour linéaire.

Soit le système chaotique maître défini par

$$\dot{x}_m = Ax_m + f(x_m) \quad (2.15)$$

où $x_m \in \mathbb{R}^n$ est le vecteur d'état, $A \in \mathbb{R}^{n \times n}$ est la matrice d'état et $f(\cdot)$ une fonction non linéaire.

En appliquant la commande par retour, le système esclave est formulé comme suit [160] :

$$\dot{x}_s = Ax_s + f(x_s) + u(t) \quad (2.16)$$

où $x_s \in \mathbb{R}^n$ est le vecteur d'état et $u(t)$ est la loi de commande définie par

$$u(t) = K(x_s - x_m) \quad (2.17)$$

où $K \in \mathbb{R}^{n \times n}$ est une matrice constante appelée matrice de gains de retour ou matrice de couplage.

A partir de (2.15), (2.16) et (2.17), on peut déduire le système d'erreur suivant :

$$\dot{e} = (A - K)e + f(x_m) - f(x_s) = (A - K)e + f(x_m) - f(x_m - e) \quad (2.18)$$

avec $e = x_m - x_s = [e_1, e_2, \dots, e_n]^T$ est le vecteur d'erreurs.

Le problème de synchronisation revient donc à concevoir la loi de commande K de telle sorte que le système d'erreur (2.18) vérifie la stabilité asymptotique uniforme et converge vers 0.

2.2.4.2 Synchronisation par backstepping

La synchronisation par backstepping est une approche de conception systématique. C'est une procédure récursive qui combine de manière efficace le choix de la fonction de Lyapunov avec la sélection du contrôleur [161]. Cette méthode présente plusieurs avantages comme le fait qu'elle puisse être appliquée à différents systèmes chaotiques, la simplicité de son implémentation et la possibilité de réaliser la synchronisation avec un seul contrôleur. Afin d'illustrer le principe de cette technique, considérons le système maître défini sous la forme suivante :

$$\begin{cases} \dot{x}_{m1} &= f_1(x_{m1}, x_{m2}) \\ \dot{x}_{m2} &= f_2(x_{m1}, x_{m2}, x_{m3}) \\ &\vdots \\ \dot{x}_{mn} &= f_n(x_{m1}, x_{m2}, \dots, x_{mn}) + f_{n+1}(t) \end{cases} \quad (2.19)$$

avec $x_m = [x_{m1}, x_{m2}, \dots, x_{mn}]^T \in \mathbb{R}^n$ est le vecteur d'état, f_1 est une fonction linéaire et $f_i (i = 2, 3, \dots, n+1)$ sont des fonctions non linéaires. Quand il s'agit de systèmes comme ceux de Lorenz, Rössler ou Chua, $f_{n+1}(t) = 0$.

Le système esclave couplé avec le système (2.19) est défini par le système suivant [162] :

$$\begin{cases} \dot{x}_{s1} &= f_1(x_{s1}, x_{s2}) \\ \dot{x}_{s2} &= f_2(x_{s1}, x_{s2}, x_{s3}) \\ &\vdots \\ \dot{x}_{sn} &= f_n(x_{s1}, x_{s2}, \dots, x_{sn}) + f'_{n+1}(t) + u \end{cases} \quad (2.20)$$

avec $x_s = [x_{s1}, x_{s2}, \dots, x_{sn}]^T \in \mathbb{R}^n$ est le vecteur d'état, $f'_{n+1}(t)$ est une fonction qui possède des caractéristiques similaires à $f_{n+1}(t)$ et u est un contrôleur qui doit être choisi adéquatement afin d'obtenir la synchronisation entre les systèmes (2.19) et (2.20).

Les erreurs de synchronisation sont définies comme suit

$$\begin{cases} e_1 = x_{s1} - x_{m1} \\ e_2 = x_{s2} - x_{m2} \\ \vdots \\ e_n = x_{sn} - x_{mn} \end{cases} \quad (2.21)$$

A partir de (2.21), nous avons

$$\begin{cases} x_{s1} = e_1 + x_{m1} \\ x_{s2} = e_2 + x_{m2} \\ \vdots \\ x_{sn} = e_n + x_{mn} \end{cases} \quad (2.22)$$

En soustrayant (2.19) de (2.20) et en tenant compte de (2.21) et (2.22), le système d'erreur peut être représenté comme suit :

$$\begin{cases} \dot{e}_1 = g_1(e_1, e_2) \\ \dot{e}_2 = g_2(x_{m1}, x_{m2}, x_{m3}, e_1, e_2, e_3) \\ \vdots \\ \dot{e}_n = g_n(x_{m1}, x_{m2}, \dots, x_{mn}, e_1, e_2, \dots, e_n) + f'_{n+1}(t) - f_{n+1}(t) + u \end{cases} \quad (2.23)$$

où $e = [e_1, e_2, \dots, e_n]^T \in \mathbb{R}^n$ est le vecteur d'erreur, g_1 est une fonction linéaire et $g_i (i = 1, 2, \dots, n)$ sont des fonctions non linéaires.

Pour utiliser l'algorithme du backstepping, le système d'erreur doit être décomposé en sous-systèmes $e_1, (e_1, e_2), (e_1, e_2, e_3), \dots, (e_1, e_2, e_3, \dots, e_n)$.

L'algorithme récursif de backstepping consiste alors à définir pour chaque sous-système une fonction de Lyapunov positive V telle que :

$$\dot{V}_j(e_j, u_j, \varrho_j) < 0 \quad (2.24)$$

où j est l'ordre du sous-système, V_j est la fonction de Lyapunov définie pour le sous-

système d'ordre j et u_j, ϱ_j sont la loi de commande et le contrôleur dit virtuel du sous système j .

2.2.4.3 Synchronisation par contrôle actif

Cette méthode, proposée par Bai et Lonngren, a montré son efficacité pour la synchronisation des systèmes chaotiques identiques et non identiques. Elle offre une simplicité d'implémentation remarquable [153].

Pour comprendre son principe, considérons comme système maître, le système non linéaire suivant :

$$\dot{x}_m = Ax_m + g(x_m) \quad (2.25)$$

où $x_m \in \mathbb{R}^n$ est le vecteur d'état, $A \in \mathbb{R}^{n \times n}$ est une matrice constante et $g(x_m)$ est une fonction non linéaire.

Le système esclave est défini par [163] :

$$\dot{x}_s = Bx_s + f(x_s) + \phi(t) \quad (2.26)$$

avec $x_s \in \mathbb{R}^n$ est le vecteur d'état, $B \in \mathbb{R}^{n \times n}$ est une matrice constante, $f(x_s)$ est une fonction non linéaire et $\phi(t)$ est une fonction de contrôle actif.

L'erreur de synchronisation est définie par $e = x_s - x_m$; les dynamiques de l'erreur sont données par l'équation :

$$\dot{e} = \dot{x}_s - \dot{x}_m = Ce + G(x_m, x_s) + \phi(t) \quad (2.27)$$

où $C = \bar{B} - \bar{A}$ représente les parties communes des matrices des systèmes maître et esclave. Les parties non communes sont regroupées dans la fonction $G(x_m, x_s)$ définie comme suit.

$$G(x, y) = f(x_s) - g(x_m) + (B - \bar{B})x_s - (A - \bar{A})x_m \quad (2.28)$$

Un contrôleur approprié $\phi(t)$ doit faire converger les erreurs de synchronisation vers 0. Il doit éliminer les termes non linéaires et les parties non communes et contenir une autre part pour assurer la stabilité. Le contrôleur $\phi(t)$ peut alors être défini par :

$$\phi(t) = -G(x_m, x_s) + u(t) \quad (2.29)$$

où $u(t) = -Ke$ est un contrôleur linéaire et $K \in \mathbb{R}^{n \times n}$ est une matrice de gains.

En remplaçant le contrôleur $\phi(t)$ par sa valeur dans l'équation (2.27), on obtient

$$\dot{e} = Ce + u(t) \quad (2.30)$$

En remplaçant $u(t) = -Ke$ dans l'équation (2.30), la dynamique de l'erreur sera définie par

$$\dot{e} = (C - K)e \quad (2.31)$$

Si les valeurs propres λ_i , $i = 1, 2, \dots, n$ de la matrice $C - K$ sont négatives ($\lambda_i < 0$), les erreurs de synchronisation convergent exponentiellement vers 0, autrement dit, les systèmes maître et esclave se synchronisent exponentiellement.

2.2.4.4 Synchronisation par commande adaptative

Récemment, de nouveaux résultats expérimentaux ont démontré que la synchronisation du chaos peut être accomplie en utilisant des contrôleurs très simples et relatifs au système chaotique utilisé. Pour cette raison, de nombreuses études théoriques sur le contrôle et synchronisation du chaos avec des lois de commande adaptées ont été effectuées et plusieurs schémas de synchronisation par contrôleurs adaptatifs ont vu le jour.

Pour développer le principe de synchronisation par contrôle adaptatif, nous nous baserons sur les travaux de R.W. Guo [164] où un contrôleur adaptatif simple mais robuste a été proposé pour la synchronisation des systèmes chaotiques et hyperchaotiques. La méthode proposée par l'auteur a été également utilisée plus tard pour synchroniser des

systèmes chaotiques incertains [165] ou avec des paramètres inconnus [166].

Considérons le système maître suivant :

$$\dot{x}_m = f(x_m) \quad (2.32)$$

où $x_m = (x_{m1}, x_{m2}, \dots, x_{mn})^T \in \mathbb{R}^n$ est le vecteur d'état, $f(x_m) = (f_1(x_m), f_2(x_m), \dots, f_n(x_m))^T : \mathbb{R}^n \rightarrow \mathbb{R}^n$ est un champs de vecteur non linéaire.

Sans perte de généralités, on suppose que $\Omega \subset \mathbb{R}^n$ est un ensemble borné et globalement attractif de l'espace de phase. Pour la fonction vectorielle $f(x_m)$, on suppose qu'elle vérifie la condition donnée dans l'hypothèse suivante.

Hypothèse 1 $\forall x_m = (x_{m1}, x_{m2}, \dots, x_{mn})^T \in \Omega$ et $\forall x_s = (x_{s1}, x_{s2}, \dots, x_{sn})^T \in \Omega$, $\exists l > 0$ tel que

$$|f_i(x_m) - f_i(x_s)| \leq l |x_m - x_s|_\infty, \quad i = 1, 2, \dots, n \quad (2.33)$$

où $|x_m - x_s|_\infty$ est la norme ∞ de $x_m - x_s$ telle que $|x_m - x_s|_\infty = \max_j |x_{mj} - x_{sj}|$, $j = 1, 2, \dots, n$.

Le système chaotique esclave est donné par :

$$\dot{x}_s = f(x_s) + k_1(x_s - x_m) = f(x_s) + k_1 e \quad (2.34)$$

où $x_s = (x_{s1}, x_{s2}, \dots, x_{sn})^T \in \mathbb{R}^n$ est le vecteur d'état, $f(x_s) = (f_1(x_s), f_2(x_s), \dots, f_n(x_s))^T : \mathbb{R}^n \rightarrow \mathbb{R}^n$ est un champs de vecteur non linéaire. $e = (e_1, e_2, \dots, e_n)$ est le vecteur d'erreur tel que $e_i = x_{si} - x_{mi}$, $i = 1, 2, \dots, n$.

Contrairement à la commande par retour définie précédemment, le gain de commande k_1 est dûment adapté selon la loi suivante :

$$\dot{k}_1 = -\gamma \sum_{i=1}^n e_i^2 \quad (2.35)$$

où γ est une constante positive arbitraire.

2.2.4.5 Synchronisation par la commande H_∞

Dans les systèmes physiques réels, on est souvent confronté à des incertitudes de modèle, des perturbations, des bruits et à un manque d'informations statistiques sur les signaux. Dans le cas de la synchronisation des systèmes chaotiques, ces perturbations et incertitudes sont aussi nuisibles. Réduire leurs effets sur la synchronisation représente un défi majeur [167]. Ceci a mené plusieurs chercheurs, dans le domaine, à s'intéresser à la commande H_∞ avec la conviction qu'elle est plus robuste et moins sensible aux perturbations et aux incertitudes des modèles.

2.2.4.6 Synchronisation par commande floue

Au cours des dernières années, beaucoup de recherches sur la synchronisation des systèmes chaotiques basée sur les modèles flous de Takagi-Sugeno (T-S) ont été menées. En effet, les modèles flous décrits par des règles SI-ALORS peuvent être utilisés aussi bien pour la modélisation des systèmes chaotiques que pour leur synchronisation. Cette dernière est réalisée suivant les étapes suivantes [168] :

1. *Description des systèmes chaotiques maître et esclave par modèles flous*
2. *Calcul de la loi de commande floue*
3. *Vérification du comportement chaotique par calcul d'exposants de Lyapunov.*

Une autre méthode de synchronisation intéressante qui continue à gagner du terrain ces dernières années et que nous avons utilisée dans notre travail est la méthode basée sur l'utilisation d'observateurs d'état. Dans ce qui suit, nous développerons en détail cette méthode de synchronisation.

2.2.4.7 Synchronisation à base d'observateurs

En 1997, Nijmeijer et Mareels [25] ont démontré que la synchronisation des systèmes chaotique peut être ramené à un problème d'estimation d'état où le système esclave est conçu à base d'un estimateur d'état, dit aussi observateur, pour le système chaotique maître. Un observateur est un capteur logiciel qui permet de fournir une estimation des variables d'états non mesurées d'un système. En termes plus précis, c'est un système dynamique qui utilise les mesures disponibles (entrées et sortie) pour fournir une estimation des variables d'états qui ne peuvent pas être mesurées directement : soit parce qu'ils sont inaccessibles, soit par économie. La figure 2.2 illustre le principe de synchronisation à base d'observateurs.

Depuis ce constat, les observateurs non linéaires jouent un rôle fondamental dans le dé-

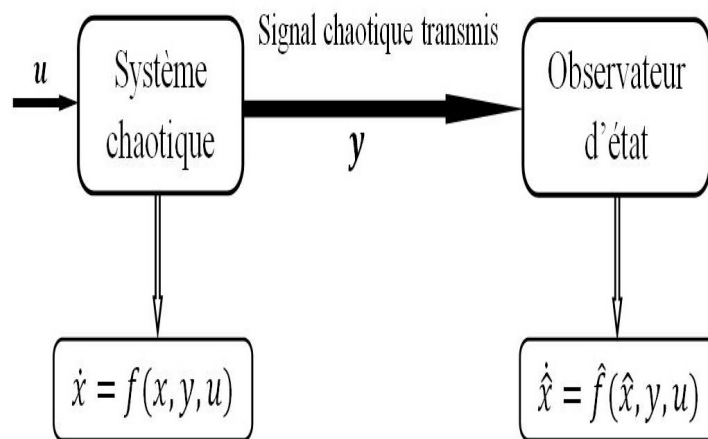


FIGURE 2.2 – Principe de synchronisation à base d'observateurs

veloppement des méthodes de synchronisation des systèmes chaotiques et ses applications dans la transmission sécurisée d'informations. Avant de développer en détails le principe de synchronisation à base d'observateurs, il est nécessaire de fournir quelques concepts de base sur les observateurs d'état.

2.3 Notions de base sur les observateurs d'états

Nous rappellerons dans cette partie de notre thèse, quelques concepts et notions de bases sur les observateurs non linéaires et sur la propriété d'observabilité.

2.3.1 Principe d'un observateur

Soit le système dynamique non linéaire suivant :

$$\begin{cases} \dot{\xi}_x &= f(x, u, t) \\ y &= h(x, u, t), \end{cases} \quad (2.36)$$

avec

$$\xi_x = \begin{cases} \dot{x}(t), t \in \mathbb{R}_+ & \text{Dans le cas continu} \\ x(t+1), t \in \mathbb{N} & \text{Dans le cas discret} \end{cases} \quad (2.37)$$

où $x \in \mathbb{R}^n$ est le vecteur d'état, $u \in \mathbb{R}^m$ est le vecteur d'entrées et $y \in \mathbb{R}^p$ est le vecteur de sorties mesurées. Les fonctions f et h sont supposées de classes C^∞ .

Définition 6 *Un observateur pour le système (2.36) est un système dynamique auxiliaire qui a comme entrées, les entrées/sorties de (2.36) et comme sorties, les états estimés $\hat{x}$. Un tel système peut-être représenté de façon générale comme suit*

$$\begin{cases} \dot{\xi}_z &= F(z, u, y) \\ \hat{x}(t) &= H(z, u, y) \end{cases} \quad (2.38)$$

où $z \in \mathbb{R}^{\tilde{n}}$, $\tilde{n} \leq n$ et $\hat{x} \in \mathbb{R}^n$. F et H sont deux fonctions à concevoir telles que le système (2.38) vérifie les deux conditions suivantes [169] :

$$(i) \quad \hat{x}(0) = x(0) \longrightarrow \hat{x}(t) = x(t), \forall t \geq 0.$$

$$(ii) \quad \|\hat{x}(t) - x(t)\| \longrightarrow 0 \text{ quand } t \longrightarrow +\infty.$$

La condition (i) signifie que si l'observateur (2.38) et le système (2.36) possèdent tous les deux le même état initial, alors l'état estimé de (2.38) devrait être égal à l'état réel de (2.36) à tout instant t [170].

La condition (ii) signifie que $\hat{x}(t)$ converge asymptotiquement vers $x(t)$. On dit alors que le système (2.38) est un observateur asymptotique.

Si la condition (ii) est satisfaite $\forall x(t), \hat{x}(t)$, l'observateur (2.38) est dit global.

Si la condition (ii) est vérifiée avec une convergence exponentielle, autrement dit $\|\hat{x}(t) - x(t)\|$ tend exponentiellement vers 0, alors l'observateur est dit exponentiel.

Si la condition (ii) est vérifiée avec une vitesse de convergence réglable, alors l'observateur est dit réglable.

2.3.2 Observabilité des systèmes non linéaires

Avant d'entamer la conception d'un observateur pour un système dynamique, il est important et nécessaire de vérifier son observabilité, c'est à dire s'assurer que l'état peut-être estimé à partir des informations sur l'entrée et la sortie. Dans le cas de systèmes non linéaires, la définition est liée aux entrées et aux conditions initiales. Dans cette partie, nous présenterons quelques définitions et notions sur l'observabilité des systèmes non linéaires dans les cas continus et discrets [169], [45, 46].

Définition 7 : Indiscernabilité

Soient x_0 et $\hat{x}_0$ deux conditions initiales différentes du système (2.36). Soient $X_u(t, x_0)$ et $X_u(t, \hat{x}_0)$ les solutions de l'équation d'état du système (2.36) par rapport aux conditions initiales x_0 et $\hat{x}_0$ respectivement.

On dit que les états $(x_0, \hat{x}_0)$ sont indiscernables (ou indistinguables) si

$$\forall u \in \mathbb{R}^m, \forall t \geq 0, h(X_u(t, x_0)) = h(X_u(t, \hat{x}_0)).$$

Dans le cas contraire, on dit que x_0 et $\hat{x}_0$ sont discernables.

Définition 8 : Observabilité

Le système (2.36) est dit observable en x_0 si x_0 est discernable (distinguable) de tout $x \in \mathbb{R}^n$. En outre, le système (2.36) est dit observable si $\forall x_0 \in \mathbb{R}^n$, le système, x_0 est distinguable.

Cette définition est assez globale et même très générale pour une utilisation pratique surtout lorsqu'on s'intéresse uniquement à distinguer les états dans un certain voisinage. On parle dans ce cas d'une observabilité faible.

Un système non linéaire est faiblement observable en x_0 s'il existe un voisinage W de x_0 de telle sorte que l'ensemble des états dans W qui sont indiscernables de x_0 contient seulement x_0 .

Un système non linéaire est faiblement observable s'il est faiblement observable pour tout $x \in \mathbb{R}^n$. Cette définition ne prend pas en compte les cas où les trajectoires doivent aller au delà de W avant de distinguer entre deux états en W . Dans ce cas une observabilité locale doit être définie.

Ainsi, un système non linéaire défini par (2.36) est localement faiblement observable s'il existe un voisinage W de x , tel que pour tout voisinage V contenu dans W , il n'y a pas d'états indiscernables de x dans V . Cette notion d'observabilité locale, qui signifie qu'on peut distinguer chaque état de son voisin sans "aller trop loin", est très intéressante en pratique. De plus, elle présente l'avantage de caractérisation de condition au sens du rang. Cette dernière est basée sur le concept d'espace d'observabilité qui correspond à l'espace de tous les états observables.

Définition 9 : *Espace d'observabilité*

L'espace d'observabilité du système (2.36) est défini comme le plus petit sous-espace vectoriel $\mathcal{O}(h)$, de fonctions de classe C^∞ , contenant les sorties de h et invariant sous l'action de la dérivée de Lie le long de $f(u) := f(., u)$ pour tout $u \in \mathbb{R}^m$ (à savoir que pour tout $\varphi \in \mathcal{O}(h)$, $L_{f_u}\varphi \in \mathcal{O}(h)$, avec $L_{f_u}\varphi(x) = \frac{\partial \varphi}{\partial x} f(x, u)$).

Définition 10 : *Condition de rang pour l'observabilité*

On dit que le système (2.36) satisfait la condition du rang pour l'observabilité, si la condition suivante est satisfaite. $\forall x, \dim d\mathcal{O}(h)|_x = n$ avec $\dim d\mathcal{O}(h)|_x$ est l'ensemble de $d\varphi(x)$ avec $\varphi \in \mathcal{O}(h)$.

Cette condition nous mène au théorème qui suit :

Théoreme 10 [169]

- *Un système non linéaire défini par (2.36) satisfaisant la condition de rang d'observabilité en x_0 est localement faiblement observable en x_0 .*
- *Un système non linéaire défini par (2.36) satisfaisant la condition de rang d'observabilité est localement faiblement observable.*
- *Inversement, un système défini par (2.36) localement faiblement observable satisfait la condition de rang génériquement.*

Pour les systèmes en général, la condition de rang n'est pas suffisante pour la possible conception d'un observateur. Cela est dû au fait que l'observabilité dépend des entrées du système et il est indispensable de vérifier s'il existe parmi elles des entrées qui pourraient affecter l'observabilité du système. On parle alors d'observabilité uniforme.

Définition 11 (*Entrées universelles*) : Soient x_0 et $\dot{x}_0$ deux conditions initiales du système (2.36). Soient $X_u(t, x_0)$ et $X_u(t, \dot{x}_0)$ les solutions de l'équation d'état du système (2.36) par rapport aux conditions initiales x_0 et $\dot{x}_0$ respectivement.

L'entrée u est dite universelle si :

$$\forall x_0 \neq \dot{x}_0, \exists \tau > 0 \text{ tel que}$$

$$h(X_u(\tau, x_0)) \neq h(X_u(\tau, \dot{x}_0))$$

Remarque 11 *Une entrée qui n'est pas universelle est dite singulière.*

Définition 12 : *Observabilité uniforme*

Un système est uniformément observable si toutes ses entrées sont universelles.

2.3.2.1 Les différents types d'observateurs non linéaires

Contrairement aux systèmes linéaires, la conception d'observateurs pour systèmes non linéaires est plus délicate et il n'existe pas, à ce jour, une méthode universelle pour la

synthèse d'observateurs non linéaires. Les méthodes existantes sont soit une généralisation des méthodes dédiées aux cas linéaires soit des techniques spécifiques. Dans ce qui suit, nous citerons quelques approches souvent adoptées pour la synthèse d'observateurs non linéaires.

- Méthodes de transformation non linéaire : Cette technique consiste à transformer, à l'aide d'un changement de coordonnées, un système non linéaire en un système linéaire [171].
- Observateurs étendus : Dans cette approche, le calcul du gain de l'observateur se fait à partir du modèle linéarisé autour d'un point de fonctionnement.
- Observateurs à grand gain : Comme son nom l'indique, le choix du gain de l'observateur dans ce cas est suffisamment grand pour compenser la non-linéarité du système. Cette méthode utilise un retour de sortie linéaire [172].
- Observateurs de Luenberger généralisés : Cette approche consiste à ajouter à l'observateur de Luenberger, un deuxième retour de sortie linéaire dans la partie non linéaire du système [173].
- Observateurs à base de la théorie de contraction : Dans ce type d'observateurs, la théorie de contraction est utilisée comme outil d'analyse de la convergence. Cette approche mène à des conditions de synthèse différentes de celles obtenues par les approches précédentes [174].

Dans le cas de systèmes chaotiques, plusieurs observateurs ont été proposés. Nous pouvons citer, comme exemples, l'observateur adaptatif pour l'estimation des états et des paramètres du système dynamique [175], l'observateur dead-beat pour les systèmes chaotiques discrets [176], l'observateur retardé étape par étape, l'observateur à mode glissant basé sur la théorie des systèmes à structure variable [177] et l'observateur impulsif que nous utiliserons dans notre travail de thèse et dont nous donnerons plus de détails dans la partie qui suit.

2.4 Synchronisation des systèmes chaotiques d'ordre entier à base d'observateurs impulsifs

Dans les schémas de synchronisation que nous venons de voir jusqu'ici, un ou plusieurs états du système dynamique chaotique est transmis de manière durable afin de réaliser la synchronisation avec le système chaotique esclave. Dans le but de réduire la redondance du signal transmis, c'est-à-dire , envoyer le signal de synchronisation partiellement, la synchronisation à base d'observateurs impulsif appelée aussi synchronisation impulsive a été proposée. La figure 2.3 décrit le principe de synchronisation par observateur impulsif. Un ou plusieurs états du système chaotique maître seront envoyés dans le canal de transmission aux instants d'arrivées des impulsions de commande [178]. Il s'agit, en d'autres termes, d'envoyer le ou les signaux chaotiques échantillonnés, par un train d'impulsion, du système maître vers le système esclave [179].

Dans cette approche, le problème de synchronisation de systèmes chaotiques devient

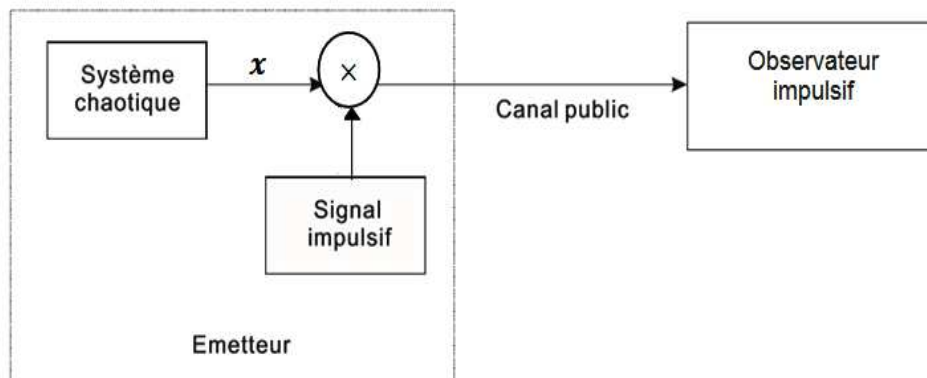


FIGURE 2.3 – Principe de la méthode de synchronisation par observateur impulsif

alors celui de stabiliser des systèmes différentiels dits impulsifs [180]. Ces derniers sont largement étudiés et plusieurs travaux ont été proposés dans la littérature.

Dans ce qui suit, et afin de mieux illustrer le principe de synchronisation impulsive en

temps continu et discret, nous donnerons, dans chaque cas, quelques notions de bases et définitions sur les systèmes impulsifs et présenterons, en outre, quelques résultats théoriques obtenus lors de l'étude de leur stabilité.

2.4.1 Synchronisation impulsive des systèmes chaotiques continus

Dans cette partie, nous présenterons d'abord la théorie des équations différentielles impulsives développée dans [180]. Les chercheurs et auteurs Yang et Chua ont utilisé cette théorie pour étudier la stabilité asymptotique de la synchronisation impulsive de deux systèmes chaotiques continus identiques [181]. Nous illustrerons, dans ce qui suit, le principe de la synchronisation impulsive développée par les auteurs et les résultats de son application sur le système chaotique de Lorenz.

2.4.1.1 Notions de base sur les systèmes différentiels impulsifs

Considérons le système non linéaire suivant :

$$\dot{x} = f(t, x) \quad (2.39)$$

où $f : \mathbb{R}_+ \times \mathbb{R}^n \rightarrow \mathbb{R}^n$ est une fonction continue et $x \in \mathbb{R}^n$ est le vecteur d'état.

Soit τ_i un ensemble d'instants discrets vérifiant la relation.

$$0 \leq t_0 < \tau_1 < \tau_2 < \dots < \tau_i < \tau_{i+1} < \dots, \lim_{i \rightarrow \infty} \tau_i = \infty.$$

Le saut $U(i, x)$ dans les variables d'état, à l'instant τ_i , est défini comme suit :

$$U(i, x) = \Delta x|_{t=\tau_i} \equiv x(\tau_i^+) - x(\tau_i^-) \quad (2.40)$$

avec $x(\tau_i^+) = \lim_{t \rightarrow \tau_i^+} x(t)$, $x(\tau_i^-) = \lim_{t \rightarrow \tau_i^-} x(t)$. En général, et afin simplifier les calculs, on suppose que $x(\tau_i^-) = x(\tau_i)$.

A partir des définitions ci-dessus, un système d'équations différentielles impulsives est décrit par [181] :

$$\begin{cases} \dot{x} &= f(t, x) & , t \neq \tau_i \\ \Delta x &= U(i, x) & , t = \tau_i \\ x(t_0) &= 0 & t_0 = 0, i = 1, 2, \dots \end{cases} \quad (2.41)$$

Afin d'étudier la stabilité du système (2.41), plusieurs approches ont été proposées comme l'approche par système de comparaison, l'approche de type Lyapunov, l'approche par deux mesures,...etc. Nous supposons, dans ce qui suit, que $f(t, 0) = 0$ et $U(i, 0) = 0$ et rappellerons quelques définitions et résultats utiles pour l'étude de la stabilité.

Définition 13 soit $V : \mathbb{R}_+ \times \mathbb{R}^n \rightarrow \mathbb{R}_+$. On dit que V appartient à la classe Σ si

1. V est continue dans $(\tau_{i-1}, \tau_i] \times \mathbb{R}^n$ et pour chaque $x \in \mathbb{R}^n$, $i = 1, 2, \dots$,
 $\lim_{(t,y) \rightarrow (\tau_i^+, x)} V(t, y) = V(\tau_i^+, x)$ existe.
2. V est localement Lipschitzienne en x .

Définition 14 Pour $(t, x) \in (\tau_{i-1}, \tau_i] \times \mathbb{R}^n$, la dérivée supérieure à droite de Dini de la fonction $V \in \Sigma$ est définie par

$$D^+V(t, x) \equiv \lim_{h \rightarrow 0^+} \sup \frac{1}{h} [V(t+h, x+hf(t, x)) - V(t, x)] \quad (2.42)$$

Pour déduire les conditions de stabilité du système (2.41), nous introduisons l'approche par système de comparaison de Yang [182]. L'idée consiste à proposer un système de comparaison de telle sorte que sa stabilité implique la stabilité du système considéré. Toutefois, il n'est pas toujours évident et facile de trouver un système de comparaison approprié au système impulsif considéré. Dans ce qui suit, nous développerons le système de comparaison proposé dans [182] ainsi que les résultats obtenus.

Définition 15 [182]

soit $V \in \Sigma$ et supposons que

$$\begin{aligned} D^+V(t, x) &\leq g[t, V(t, x)], & t \neq \tau_i, \\ V(t, x + U(i, x)) &\leq \Psi_i[V(t, x)], & t = \tau_i, \end{aligned}$$

où $g : \mathbb{R}_+ \times \mathbb{R}_+ \rightarrow \mathbb{R}$ est continue et $g(t, 0) = 0$, $\Psi_i : \mathbb{R}_+ \rightarrow \mathbb{R}_+$ est non décroissante. Alors, le système

$$\begin{cases} \dot{\omega} &= g(t, x) & , t \neq \tau_i \\ \omega(\tau_i^+) &= \Psi(\omega(\tau_i)) & , t = \tau_i \\ \omega(t_0) &= \omega_0, \end{cases} \quad (2.43)$$

est appelé système de comparaison du système (2.41).

Définition 16

$$S_\rho = \{x \in \mathbb{R}^n, \|x\| < \rho\}, \quad (2.44)$$

où $\|\cdot\|$ est la norme Euclidienne dans $\mathbb{R}^n$.

Définition 17 Une fonction α est dite appartenir à la classe Γ si $\alpha \in C[\mathbb{R}_+, \mathbb{R}_+]$, $\alpha(0) = 0$ et $\alpha(x)$ est strictement croissante en x .

Théoreme 12 [181]

Si les trois conditions suivantes sont satisfaites :

1. $V : \mathbb{R}_+ \times S_\rho \rightarrow \mathbb{R}_+$, $\rho > 0$, $V \in \Sigma$, $D^+V(t, x) \leq g[t, V(t, x)]$, $t \neq \tau_i$.
2. Il existe un $\rho_0 > 0$ tel que $x \in S_{\rho_0}$ implique que $x + U(i, x) \in S_{\rho_0}$, $\forall i$ et $V[t, x + U(i, x)] \leq \Psi_i[V(t, x)]$, $t = \tau_i$, $x \in S_{\rho_0}$.
3. $\beta(\|x\|) \leq V(t, x) \leq \alpha(\|x\|)$ sur $\mathbb{R}_+ \times S_\rho$, où $\alpha(\cdot), \beta(\cdot) \in \Gamma$.

Alors, les propriétés de stabilité de la solution triviale du système de comparaison (2.43) impliquent celles de la stabilité du système (2.41).

Le théorème ci-dessus joue un rôle important pour l'étude de la convergence du système (2.41). En effet, on peut énoncer quelques conditions suffisantes pour la stabilité d'un système impulsif complexe à partir de son simple système de comparaison. Le théorème suivant développe les résultats de la stabilité asymptotique basés sur le théorème ci-dessus [181].

Théoreme 13 Soit $g(t, \omega) = \dot{\lambda}(t)\omega$, $\lambda \in C^1[\mathbb{R}_+, \mathbb{R}_+]$, $\Psi_i(\omega) = d_i(\omega)$, $d_i \geq 0$, $i = 1, 2, \dots$. L'origine du système (2.41) est asymptotiquement stable si les conditions suivantes sont vérifiées.

1. $\exists \gamma, \gamma > 1$ telle que :

$$\lambda(\tau_{i+1}) + \ln(\gamma d_i) \leq \lambda(\tau_i) \quad (2.45)$$

2. $\dot{\lambda}(t) \geq 0$;

2.4.1.2 Synchronisation impulsive de deux systèmes chaotiques de Lorenz

Les théorèmes énoncés seront appliqués au système chaotique de Lorenz que nous avons présenté dans le chapitre précédent. Le modèle d'état du système de Lorenz est donné comme suit.

$$\dot{x} = Ax(t) + \psi(x(t)), \quad (2.46)$$

où $x = [x_1, x_2, x_3]^T$ est le vecteur d'état et

$$A = \begin{pmatrix} -\sigma & \sigma & 0 \\ r & -1 & 0 \\ 0 & 0 & -b \end{pmatrix} \text{ et } \psi = \begin{pmatrix} 0 \\ -x_1 x_3 \\ x_1 x_2 \end{pmatrix}$$

où σ , r et b sont les paramètres du système.

Dans le schéma de synchronisation, le système esclave est un observateur qui a pour variables d'état $\hat{x} = [\hat{x}_1, \hat{x}_2, \hat{x}_3]^T$. Dans un premier temps, il est défini par :

$$\dot{\hat{x}} = A\hat{x}(t) + \psi(\hat{x}(t)), \quad (2.47)$$

Aux instants discrets $\tau_i, i = 1, 2, \dots$, les variables d'état du système (2.46) sont transmises au système esclave. Les variables d'état de ce dernier sont sujettes à de soudains changements à ces instants. Alors, le système esclave peut-être décrit par l'observateur impulsif suivant, régi par des équations différentielles impulsives [183].

$$\begin{cases} \dot{\hat{x}}(t) &= A\hat{x}(t) + \psi(\hat{x}(t)), & t \neq \tau_i, \\ \Delta\hat{x}|_{t=\tau_i} &= -Be, & t = \tau_i, i = 1, 2, \dots, \end{cases} \quad (2.48)$$

où $e = (e_1, e_2, e_3)^T = (x_1 - \hat{x}_1, x_2 - \hat{x}_2, x_3 - \hat{x}_3)^T$ sont les erreurs de synchronisation et B est une matrice 3×3 . Le système d'erreur de synchronisation impulsive est, alors, donné par

$$\begin{cases} \dot{e}(t) &= Ae(t) + \phi(x(t), \hat{x}(t)), & t \neq \tau_i, \\ \Delta e|_{t=\tau_i} &= Be, & i = 1, 2, \dots, \end{cases} \quad (2.49)$$

$$\text{avec } \phi(x, \hat{x}) = \psi(x) - \psi(\hat{x}) = \begin{pmatrix} 0 \\ -(x_1x_3 - \hat{x}_1\hat{x}_3) \\ x_1x_2 - \hat{x}_1\hat{x}_2 \end{pmatrix},$$

Hypothèse 2 *Comme les signaux signaux chaotiques sont bornés, on suppose que $|x_3(t)| \leq M_3$, $|x_2(t)| \leq M_2$. Soit $M = \max(M_2, M_3)$.*

A partir de cette hypothèse et afin de démontrer la convergence du système d'erreurs de synchronisation impulsive, Dans [183], les auteurs ont énoncé le théorème suivant :

Théoreme 14 [183] *Soit d_1 la plus grande valeur propre de $(I_n + B^T)(I_n + B)$ où B est Hermitienne. Soient ρ le rayon spectral de la matrice $I_n + B$ tel que $\rho \leq 1$ et q la plus grande valeur propre de $(A + A^T)$. Supposons que les impulsions sont équidistantes avec un intervalle δ .*

Si

$$0 \leq (q + 2M) \leq -\frac{1}{\delta} \ln(\zeta d_1), \quad \zeta > 1, \quad (2.50)$$

alors la synchronisation impulsive entre deux systèmes de Lorenz identique est asymptotiquement stable.

Lors des simulations numériques sous Matlab/Simulink, les paramètres du système de Lorenz sont choisis de telle sorte que le système évolue dans un régime chaotique a savoir :

$\sigma = 10, r = 28$ et $b = \frac{8}{3}$. Les états chaotiques x_2 et x_3 évoluent dans les intervalles $[-24.75, 27.68]$ et $[0, 48.36]$ respectivement. Nous pouvons alors choisir $M = 50$. La matrice B doit être Hermitienne, et doit satisfaire la condition : $\rho(I_n + B) \leq 1$ du théorème. Dans notre cas, elle est choisie comme suit :

$$B = \begin{pmatrix} 0 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \quad (2.51)$$

En outre, nous avons

$$A = \begin{pmatrix} -10 & 10 & 0 \\ 28 & -1 & 0 \\ 0 & 0 & -\frac{8}{3} \end{pmatrix}$$

ce qui implique que

$$A + A^T = \begin{pmatrix} -20 & 38 & 0 \\ 38 & -2 & 0 \\ 0 & 0 & -\frac{16}{3} \end{pmatrix} \quad (2.52)$$

A partir de (2.51) et (2.52), et après calculs numériques, on obtient $d_1 = 1, q = 28.0512$ donc $q + 2M > 0$.

On peut, alors, déduire la condition suivante sur la période δ des impulsions τ_i :

$$0 \leq \delta \leq \frac{\ln(\zeta d_1)}{q + 2M}, \quad \zeta > 1. \quad (2.53)$$

En prenant $\zeta = 10$, nous obtenons la condition $0 \leq \delta \leq 0.0295$.

La figure 2.4 montre l'estimation des états x_1 , x_2 et x_3 du système de Lorenz par l'observateur impulsif avec $\delta = 0.02$. Comme nous pouvons le voir, les états sont reconstruits après un très court régime transitoire.

Les erreurs de synchronisation impulsive convergentes affichées sur la figure 2.5 confirment l'estimation réussie des états et la stabilité de la synchronisation impulsive. Au fur et à

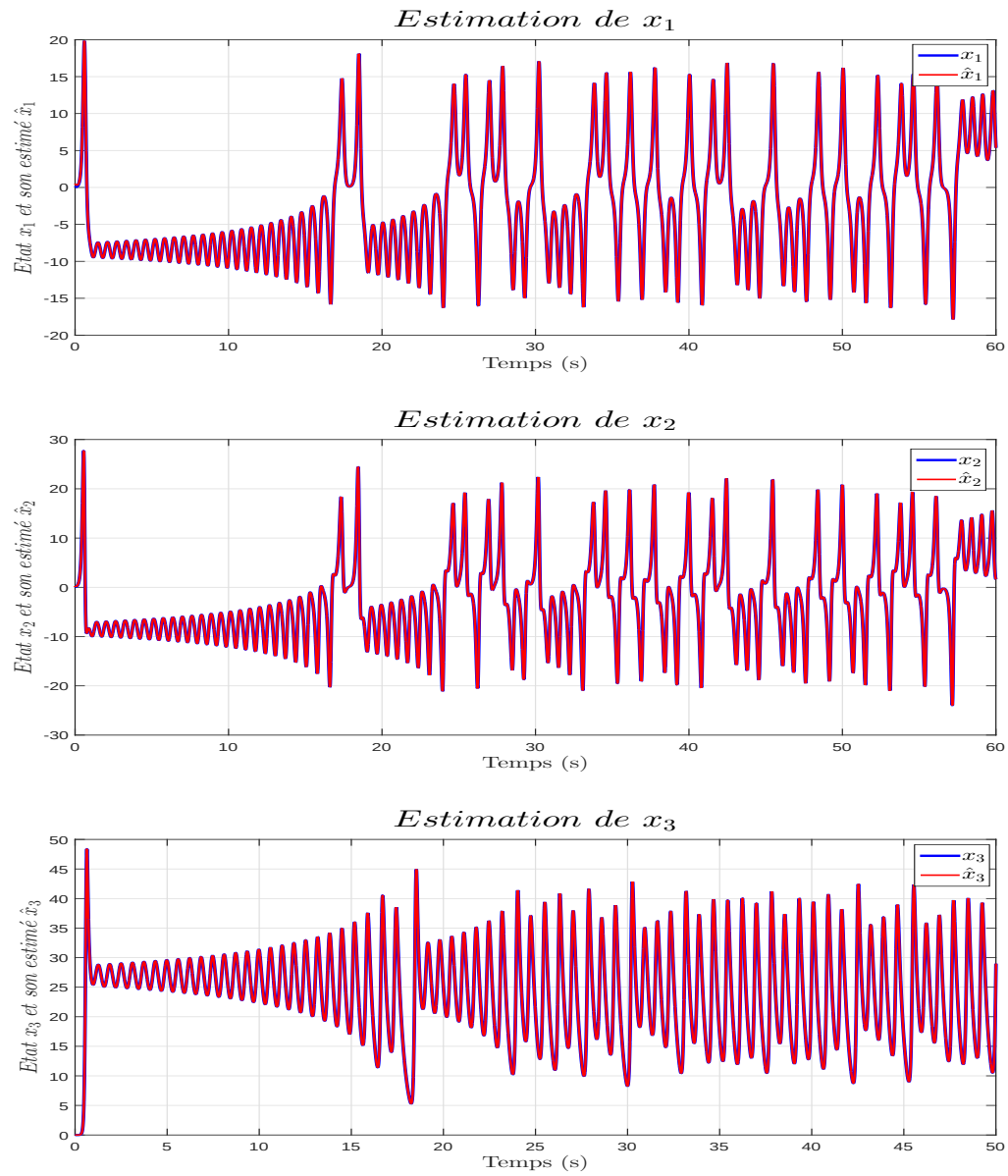


FIGURE 2.4 – Estimation des états du système de Lorenz par l'observateur impulsif

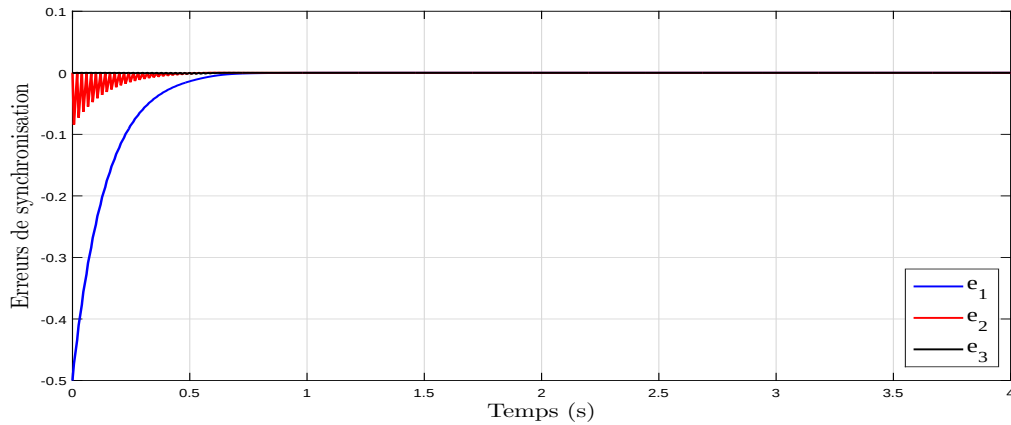


FIGURE 2.5 – Erreurs de synchronisation impulsive entre deux systèmes chaotiques de Lorenz

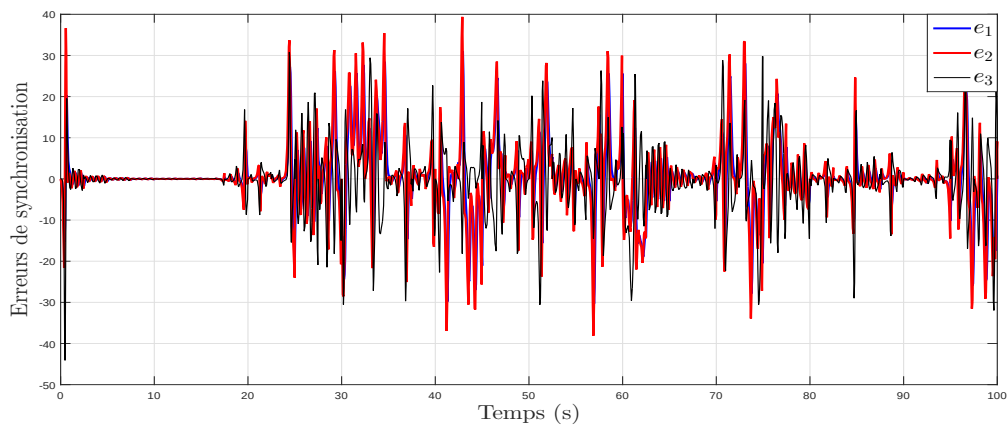


FIGURE 2.6 – Erreurs de synchronisation impulsive avec $\delta = 2.5$ entre deux systèmes chaotiques de Lorenz

mesure que nous nous éloignons de la valeur limite de δ , le régime transitoire augmente peu à peu et à partir d'une certaine valeur, nous perdons la stabilité du système d'erreur. Ainsi pour la même valeur de ζ et pour $\delta = 2.5$ les erreurs de synchronisation sont instables. La figure (2.6) illustre les erreurs de synchronisation obtenues.

2.4.2 Synchronisation impulsive des systèmes chaotiques discrets

Dans cette partie, nous développerons l'approche de synchronisation impulsive dans le cas de systèmes discrets. Le principe de synchronisation reste le même que pour le cas des

systèmes continus. Dans ce qui suit, nous présenterons quelques concepts et notations qui seront utilisés pour établir la synchronisation impulsive des systèmes chaotiques discrets puis nous illustrerons les résultats, théoriques et de simulation, obtenus.

2.4.2.1 Préliminaires sur les systèmes impulsifs discrets

Considérons le système chaotique discret suivant :

$$x(k+1) = Ax(k) + \Phi(x(k)) \quad (2.54)$$

où $x \in \mathbb{R}^n$ est le vecteur d'état, $A \in \mathbb{R}^{n \times n}$ et $\phi : \mathbb{R}^n \rightarrow \mathbb{R}^n$ est une fonction non linéaire. Nous définissons k_i comme l'ensemble des instants discrets auxquels arrivent les impulsions de synchronisation. Ils sont choisis comme suit : $0 < 1 = k_1 < k_2 < \dots < k_i < \dots$ et $\lim_{i \rightarrow \infty} k_i = \infty$. En outre, nous définissons k_i^- et k_i^+ comme les instants juste avant et juste après l'arrivée de l'impulsion k_i , nous pouvons reformuler cette définition comme suit :

$$k_i^+ = \lim_{\epsilon \rightarrow 0} k_i + \epsilon, \quad \epsilon > 0 \quad (2.55)$$

$$k_i^- = \lim_{\epsilon \rightarrow 0} k_i - \epsilon, \quad \epsilon > 0 \quad (2.56)$$

L'observateur impulsif et système esclave de (2.54) est alors défini comme suit [184] :

$$\begin{cases} \hat{x}(k+1) = A\hat{x}(k) + \phi(\hat{x}(k)) & \text{pour } k \neq k_i \\ \hat{x}(k_i^+) = \hat{x}(k_i) - B(k_i)e(k_i) & \text{pour } k = k_i, i = 1, 2, \dots \end{cases} \quad (2.57)$$

où $\hat{x} \in \mathbb{R}^n$ est le vecteur d'état estimé, Φ est une fonction non linéaire Lipschitzienne qui satisfait la relation suivante

$$\| \phi(x(k)) - \phi(\hat{x}(k)) \| < l \| x(k) - \hat{x}(k) \| \quad (2.58)$$

$B(k_i)$ est une séquence de matrices symétriques de dimension $n \times n$. Les éléments de la matrice $B(k_i)$ représentent les sauts des variables d'état $x_1, x_2, \dots, x_n$ à l'arrivée de

l'impulsion k_i . Ils peuvent être considérés comme des gains de corrections apportées au système à l'instant k_i [185].

le terme $\hat{x}(k_i^-)$ est défini comme suit :

$$\hat{x}(k_i^-) = \hat{x}(k_i) \quad (2.59)$$

$e(k)$ est l'erreur de synchronisation définie par

$$e(k) = x(k) - \hat{x}(k) \quad (2.60)$$

Nous introduisons deux autres erreurs liées à l'instant k_i qui sont : $e(k_i^-)$ et $e(k_i^+)$. Elles sont définies comme suit :

$$e(k_i^-) = x(k_i) - \hat{x}(k_i^-) = e(k_i) \quad (2.61)$$

$$e(k_i^+) = x(k_i) - \hat{x}(k_i^+) \quad (2.62)$$

La synchronisation impulsive entre les systèmes (2.54) et (2.57) dépend directement de la stabilité asymptotique du système d'erreur de synchronisation défini comme suit :

$$\left\{ \begin{array}{ll} e(k+1) = Ae(k) + \varphi(x(k)) - \varphi(\hat{x}(k)) & \text{pour } k \neq k_i \\ \Delta e(k) = e(k_i^+) - e(k_i^-) & \\ = B(k_i)e(k_i^-) = B(k_i)e(k) & \\ & \text{pour } k = k_i \\ & i = 1, 2, \dots \end{array} \right. \quad (2.63)$$

La synchronisation impulsive consiste à trouver les matrices de correction $B(k_i)$ et la distance entre les impulsions δ de telle sorte que le système d'erreur vérifie la stabilité asymptotique pour toute condition initiale $e(0)$.

Les conditions de stabilité asymptotique du système (2.63) sont énoncées dans le théorème qui suit :

Théoreme 15 [186]

Soit $d(k_i)$ la plus grande valeur propre de $(I_n + B(k_i))^T(I_n + B(k_i))$ où I_n est la matrice d'identité de dimension $n \times n$ et q la plus grande valeur propre de $A^T A$.

Le système (2.63) est asymptotiquement stable si les conditions suivantes sont vérifiées :

1. $\sup_i (\sqrt{q} + L)^{2(k_{i+1} - k_i)} = \epsilon_0 < +\infty$.

2. Il existe deux entiers finis $m_0 > 0$ et $r > 1$ tels que :

$$0 \leq 2(k_{m_0(n+1)+1} - k_{m_0 n+1} \ln(\sqrt{q} + L) \leq \ln(r d_{k_{m_0(n+1)}} \cdots d_{k_{m_0 n+1}}) ; n = 0, 1, 2, 3, \dots$$

2.4.2.2 Synchronisation impulsive de deux systèmes chaotiques discrets de Lozi

Nous appliquerons dans ce qui suit la méthode de synchronisation impulsive sur le système chaotique discret de Lozi.

Considérons le système chaotique discret de Lozi présenté lors du chapitre précédent et donné par (1.83). Le système (1.83) peut être réécrit sous la représentation d'état suivante :

$$x(k+1) = Ax(k) + \phi(x(k)) \quad (2.64)$$

Avec $A = \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix}$ et $\phi = \begin{pmatrix} 1 - a |x_1(k)| \\ 0 \end{pmatrix}$

L'observateur impulsif du système(2.64) est alors donné comme suit

$$\begin{cases} \hat{x}(k+1) &= A\hat{x}(k) + \phi(\hat{x}) & k \neq k_i \\ \hat{x}(k_i^+) &= \hat{x}(k_i) - B(k_i)e(k_i) & k = k_i \quad i = 1, 2, \dots \end{cases} \quad (2.65)$$

où $\hat{x} = [\hat{x}_1 \hat{x}_2]^T$ est le vecteur d'états estimés et $\phi(\hat{x}) = \begin{pmatrix} 1 - a |\hat{x}_1(k)| \\ 0 \end{pmatrix}$

$B(k_i)$ sont des matrices diagonales contenant les gains de contrôle appliqués aux instants k_i .

A partir de (2.64) et (2.65), le système d'erreur de synchronisation obtenu est décrit par

le système d'équations suivant :

$$\begin{cases} e(k+1) = Ae(k) + \Gamma(x(k), \hat{x}) & k \neq k_i \\ e(k_i^+) = e(k_i) + B(k_i)e(k_i) & k = k_i \quad i = 1, 2, \dots \end{cases} \quad (2.66)$$

avec $\Gamma(x(k), \hat{x}) = \phi(x(k)) - \phi(\hat{x}(k))$.

Nous utiliserons le théorème suivant afin de garantir la synchronisation impulsive.

Théoreme 16 [186] *Soit d la plus grande valeur propre de $(I_2 + B)^T(I_2 + B)$ où B est une matrice symétrique de dimension 2×2 et I_2 est la matrice identité de dimension 2×2 .*

Supposons que les instants discrets k_i sont équidistantes et notons par δ la distance entre deux instants successifs.

S'il existe une constante $r > 1$ telle que :

$$0 \leq \ln(1 + a) \leq -\frac{1}{2\delta} \ln(rd) \quad (2.67)$$

alors le système d'erreur (2.66) est asymptotiquement stable et les deux systèmes (2.64) et (2.65) sont impulsivement synchronisés.

Lors des simulations sous Matlab, la matrice de gains $B(k_i)$ est choisie constante et diagonale.

Pour les valeurs de $B = \begin{pmatrix} -0.95 & 0 \\ 0 & -0.95 \end{pmatrix}$ et $\delta = 3$, le système d'erreur satisfait les conditions du théorème 16. Le système est par conséquent asymptotiquement stable et la synchronisation impulsive entre les systèmes (2.64) et (2.65) est bien établie. Les figures 2.7 et 2.8 montrent, respectivement, la synchronisation des états x_1 et x_2 . Les conditions initiales sont $(x_1, x_2) = (0.1, 0.2)$ pour le système maître (2.64) et $(\hat{x}_1, \hat{x}_2) = (3, 2)$ pour le système esclave donné par l'observateur impulsif (2.65).

Les erreurs de synchronisation e_1 et e_2 sont respectivement illustrées sur les figures 2.9 et 2.10. A partir de ces figures, on peut constater que la synchronisation impulsive est établie et que les états ont été correctement estimés après un court régime transitoire.

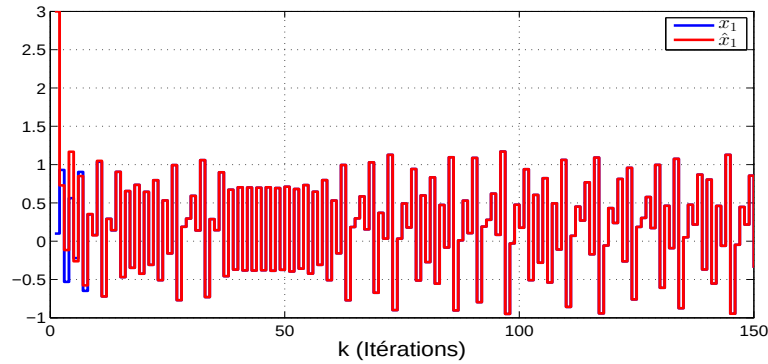


FIGURE 2.7 – Etats synchronisés x_1 et $\hat{x}_1$ du système de Lozi d'ordre entier

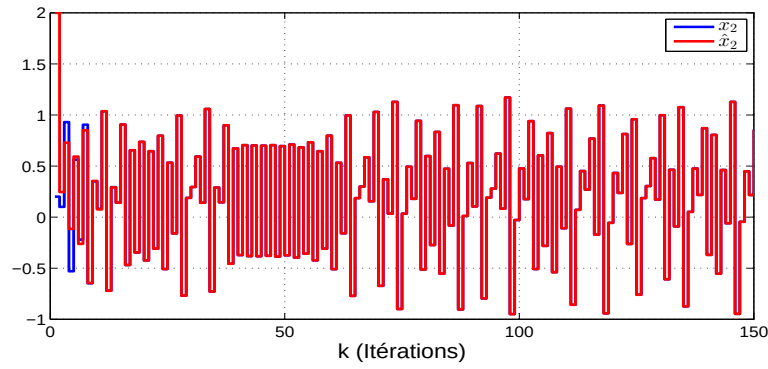


FIGURE 2.8 – Etats synchronisés x_2 et $\hat{x}_2$ du système de Lozi d'ordre entier

2.5 Conclusion

Dans ce chapitre consacré à la synchronisation des systèmes chaotiques d'ordre entier, nous avons présenté les différentes méthodes existantes pour la synchronisation de systèmes chaotiques d'ordre entier. Parmi les méthodes proposées, celle de la synchronisation impulsive, qui est une approche à base d'observateurs de type impulsifs, offre plusieurs avantages. En effet, cette méthode évite la redondance du signal transmis et permet ainsi son application pour la transmission sécurisée de données. Nous avons donc rappelé des notions de base sur les systèmes impulsifs et développé les conditions suffisantes de synchronisation dans les cas des systèmes continus et discrets. Un exemple d'application est choisi pour chaque cas, pour illustrer les résultats théoriques. Dans le chapitre suivant, nous présenterons les techniques de synchronisation développées pour le cas des systèmes chaotiques d'ordre fractionnaire et apporterons notre contribution qui

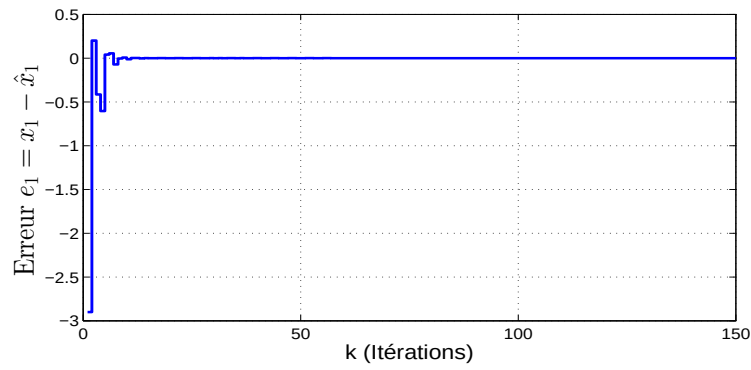


FIGURE 2.9 – Erreur de synchronisation impulsive $e_1 = x_1 - \hat{x}_1$ entre deux systèmes chaotiques de Lozi

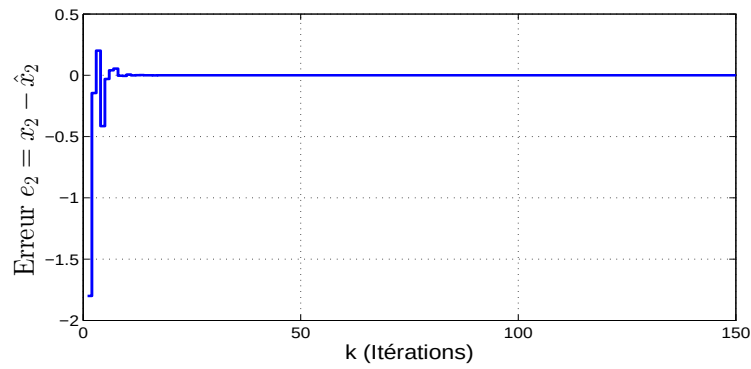


FIGURE 2.10 – Erreur de synchronisation $e_2 = x_2 - \hat{x}_2$ entre deux systèmes chaotiques de Lozi

consiste à généraliser la synchronisation impulsive au cas des systèmes chaotiques discrets d'ordre fractionnaire.

Chapitre 3

Synchronisation impulsive des systèmes chaotiques discrets d'ordre fractionnaire

3.1 Introduction

Récemment, l'étude et la commande des systèmes chaotiques d'ordre fractionnaire est devenu un domaine de recherche bien connu avec un grand nombre de travaux de recherche et de résultats. Durant les dix dernières années, les études entreprises ont montré que les systèmes chaotiques d'ordre fractionnaire peuvent aussi être synchronisés [187]. Ainsi, plusieurs stratégies de commande ont été proposées et employées pour la modélisation, la stabilisation et la synchronisation des systèmes chaotiques d'ordre fractionnaire. Plusieurs types de synchronisation déjà établis pour le cas des systèmes chaotiques d'ordre entier, ont été généralisés pour le cas des systèmes d'ordre fractionnaire. En effet, tout comme la synchronisation complète, la synchronisation généralisée [188], projective [189], retardée [190] et de phase ont été établies avec succès entre les systèmes chaotiques d'ordre fractionnaire. En outre, il a été constaté que la valeur de l'ordre fractionnaire peut affecter le processus de synchronisation [191, 192]. Toutefois, les études et recherches sur la synchronisation des systèmes chaotiques d'ordre fractionnaire discrets sont très limitées comparant à celles effectuées dans le cas continu. En effet, très peu d'approches ont été proposées pour synchroniser les systèmes chaotiques discrets d'ordre fractionnaire. D'autres

méthodes de synchronisation, notamment la synchronisation impulsive n'ont pas encore été envisagées ou étudiées, à notre connaissance, dans le cas fractionnaire discret.

Dans ce chapitre, nous proposons un schéma de synchronisation impulsif pour les systèmes chaotiques discrets d'ordre fractionnaire. Nous développerons dans un premier temps les résultats théoriques obtenus, puis nous présenterons les résultats d'application du schéma de synchronisation sur un exemple de systèmes chaotiques discrets d'ordre fractionnaire.

3.2 Méthodes de synchronisation des systèmes chaotiques d'ordre fractionnaire : État de l'art

Plusieurs techniques ont été utilisées afin d'atteindre les différents régimes de synchronisation entre systèmes chaotiques d'ordre fractionnaire. Les méthodes les plus répandues sont les méthodes de contrôle actif, de commande adaptative, de commande par retour, la commande par backstepping et la méthode de synchronisation à base d'observateurs. Les principes de ces méthodes restent similaires à ceux définis dans le cas de systèmes chaotiques d'ordre entier. Pour cette raison, nous nous limiterons, dans cette section, à citer quelques exemples de travaux effectués dans ce contexte pour chaque approche.

3.2.1 Synchronisation par contrôle actif

La méthode de contrôle actif présentée dans le chapitre précédent fait partie des techniques les plus utilisées pour synchroniser les systèmes chaotiques d'ordre fractionnaire identiques et non identiques. Nous pouvons citer, comme exemple, l'article de Bhalekar *et al.* [193] où les auteurs ont appliqué les résultats de Matignon [194] concernant les conditions de stabilité pour choisir les lois de commande. De plus, le théorème de la valeur finale de la transformée de Laplace a été utilisé par He et Luo [195] pour la synchronisation de deux systèmes de Duffing d'ordre fractionnaire par contrôle actif. D'autre part, Singh *et al.* ont utilisé, dans leur article [196] la méthode de contrôle actif pour synchroniser les

systèmes de Chen et Qi d'ordre fractionnaire.

3.2.2 Commande par rétroaction

Cette approche a été largement exploitée pour synchroniser les systèmes chaotiques d'ordre fractionnaire évoluant aussi bien en temps continu qu'en temps discret.

Pour le cas de systèmes continus, Song *et al.* se sont basés sur la théorie de stabilité de Lyapunov des systèmes d'ordre fractionnaire pour calculer les lois de commande et synchroniser deux systèmes chaotiques de Q_i d'ordre fractionnaire [197]. Dans le cas de systèmes discrets fractionnaire, Wu et Baleanu [198] ont proposé un schéma de synchronisation de la fonction logistique d'ordre fractionnaire en utilisant deux types de retours d'état : un retour linéaire et un retour non linéaire. La méthode de commande par retour a été également appliquée par Xin pour la synchronisation de deux systèmes chaotiques discrets d'ordre fractionnaire présentant une non linéarité cubique [199]. Une commande par retour non linéaire a été aussi appliquée à la synchronisation de la fonction logistique d'ordre fractionnaire dans [200].

3.2.3 Synchronisation par la commande backstepping

Une autre méthode de commande puissante, pour la synchronisation des systèmes chaotiques d'ordre fractionnaire, est la méthode par backstepping. Dans leur contribution Shukla et Sharma ont appliqué une extension de la stabilité de Lyapunov et la stabilité de Mittag-Leffler pour la synthèse d'une commande par backstepping et la synchronisation d'une classe de systèmes chaotiques d'ordre fractionnaire [201]. Dans son article [202], U. E. Vincent a établi une analyse comparative entre la méthode du contrôle actif et la méthode par backstepping. L'auteur est arrivé à la conclusion que les deux méthodes présentent d'excellentes performances mais la complexité des contrôleurs actifs suggère que le contrôleur de backstepping serait plus approprié pour une réalisation pratique.

3.2.4 Synchronisation par la commande adaptative

Dans le but de synchroniser des systèmes chaotiques d'ordre fractionnaire, Hosseinia *et al.* [203] ont proposé une nouvelle idée de contrôleur fractionnaire adaptatif. Le contrôleur est de type PID. Ses coefficients K_p , K_I et K_D seront mis à jour selon un mécanisme basé sur le gradient. Le contrôleur synthétisé a été appliqué pour la synchronisation de deux gyroscopes chaotiques incertains *gyro*.

En outre, et en se basant sur la théorie de stabilité de Lyapunov et les techniques de la commande adaptative, Zhang a proposé dans son article une approche de commande adaptative pour synchroniser une classe de systèmes chaotiques d'ordre fractionnaire incommensurables. L'approche proposée par les auteurs est générale et peut synchroniser plusieurs types de systèmes chaotiques connus [204]. Des méthodes de commande par retour adaptatives ont été aussi proposées, par C. Li et Y. Tong [205] pour réaliser la synchronisation impulsive des systèmes chaotiques d'ordre fractionnaire.

3.2.5 Synchronisation à base d'observateurs

Grâce aux résultats de synchronisation à base d'observateurs, obtenus pour le cas de systèmes entiers, et aux nombreux travaux et théories élaborées dans le cas de systèmes dynamiques d'ordre fractionnaire, plusieurs observateurs ont été proposés pour l'estimation des états de systèmes chaotiques d'ordre fractionnaire. Les observateurs d'ordre fractionnaire jouent un rôle important dans les systèmes de communications sécurisées. Nous citerons ci-dessous quelques exemples d'observateurs proposés pour la synchronisation des systèmes chaotiques d'ordre fractionnaire.

3.2.5.1 Observateurs à modes glissants

Ce types d'observateurs est basé sur la théorie des systèmes à structures variables. Le choix de cet observateur est justifié par le fait que la commande à mode glissant est très efficace pour faire face aux incertitudes du système et aux perturbations externes. Ce type d'observateurs a été utilisé dans de nombreux schémas de synchronisation des systèmes

chaotiques fractionnaire continus [206], [207] et discrets [208].

3.2.5.2 Observateurs à grand gain

Cet observateur est très populaire et a été intensément utilisé pour l'estimation des systèmes non linéaires d'ordre entier. Il présente plusieurs avantages comme la convergence globale ou semi globale indépendante des conditions initiales pour un grand nombre de systèmes non linéaires. De plus, il offre une robustesse remarquable vis à vis des incertitudes et perturbations externes. Il a été généralisé pour la première fois aux cas de systèmes d'ordre fractionnaire par Bettayeb *et al.* dans [209]. Les auteurs de la contribution ont appliqué une chaîne d'observateurs à grand gain d'ordre fractionnaire mis en cascade pour la synchronisation de systèmes chaotiques d'Arneodo d'ordre fractionnaire.

3.2.5.3 Filtre de Kalman étendus

Ce type d'observateurs est largement utilisé pour la synchronisation des systèmes chaotiques d'ordre fractionnaire. En effet, plusieurs travaux de recherches, comme celui décrit dans [210], ont démontré que le filtre de Kalman étendu peut synchroniser différents systèmes chaotiques en vue de leur application dans les schémas de communications sécurisées.

3.2.5.4 Observateurs impulsifs

Ce type d'observateur a le même principe que celui présenté dans le cas de système entier, à savoir l'estimation des états d'un système par envoi des signaux de synchronisation à des instants précis. De nombreux travaux portent sur la synthèse d'observateurs impulsifs de systèmes chaotiques continus d'ordre fractionnaire. Nous en parlerons dans la suite de ce chapitre. Toutefois la synthèse d'observateurs impulsifs n'a pas été abordée dans le cas de systèmes chaotiques discrets d'ordre fractionnaire.

3.2.5.5 Observateurs retardés étape par étape

Ce type d'observateurs est essentiellement développé pour le cas de systèmes discrets. Il a été généralisé au cas de systèmes d'ordre fractionnaire dans [211] et appliqué ensuite à la transmission d'images.

L'observabilité des systèmes dynamiques d'ordre fractionnaire a été vastement étudiée ces dernières années et d'intéressants résultats ont été obtenus dans les cas de systèmes linéaires et non linéaires. L'annexe A a été consacrée à présenter les résultats les plus souvent cités et utilisés pour l'étude de l'observabilité des systèmes dynamiques d'ordre fractionnaire.

3.3 Synchronisation des systèmes chaotiques d'ordre fractionnaire à base d'observateurs impulsifs

Nous consacrerons cette section, de notre manuscrit de thèse, à présenter les différentes approches de synchronisation impulsive appliquées aux systèmes chaotiques continus d'ordre fractionnaire d'une part, et à présenter notre contribution pour la synchronisation des systèmes chaotiques discrets d'ordre fractionnaire d'une autre part.

3.3.1 Synchronisation impulsive des systèmes chaotiques continus d'ordre fractionnaire

Plusieurs approches ont été proposées et utilisées dans l'objectif de synchronisation des systèmes chaotiques continus d'ordre fractionnaire. On peut toutefois les classer, selon leurs principes, en trois catégories comme suit :

- Les approches basées sur l'application directe des résultats de synchronisation impulsive obtenus dans le cas de systèmes chaotiques d'ordre entier
- Les approches de synchronisation impulsive modifiées

- Les approches de synchronisation impulsive par l'étude de stabilité des systèmes différentiels impulsifs d'ordre fractionnaire

Nous développerons, plus en détails, le principe de chacune de ces catégories dans la suite de cette section

3.3.1.1 Synchronisation impulsive par application directe des résultats obtenus dans le cas de systèmes d'ordre entier

La première approche qui a été utilisée pour la synchronisation impulsive des systèmes chaotiques d'ordre fractionnaire consistait à appliquer directement les résultats théoriques obtenus dans le cas de systèmes impulsifs d'ordre entier. Nous pouvons citer comme exemple le travail de Xing-Yuan [212]. En effet, l'auteur a proposé dans un premier temps une condition pour la synchronisation impulsive de deux systèmes hyperchaotiques.

Le système maître présente la structure suivante :

$$\dot{x} = Ax(t) + \Phi(x(t)), \quad (3.1)$$

avec $x = [x_1, x_2, \dots, x_n]^T$ est le vecteur d'état, Ax représente la partie linéaire du système et $\Phi(x)$ représente la partie non linéaire.

Le système esclave proposé est un observateur impulsif défini par

$$\begin{cases} \dot{\hat{x}} &= A\hat{x}(t) + \Phi(\hat{x}(t)), & t \neq t_k \\ \Delta\hat{x} &= B_k e(t_k), & t = t_k, k = 1, 2, \dots \\ \hat{x}(t_0^+) &= \hat{x}_0 \end{cases} \quad (3.2)$$

où $\hat{x} = [x_1, x_2, \dots, x_n]^T$ est le vecteur d'états estimés, $\Delta\hat{x} = \hat{x}(t_k^+) - \hat{x}(t_k^-)$ et B_k est la matrice de gains de contrôle et définissant le saut sur les variables d'état à l'instant t_k .

Afin d'établir la synchronisation impulsive entre les systèmes (3.1) et (3.2), la stabilité du système d'erreur de synchronisation a été étudiée. Les résultats obtenus ont montré que la période τ , des instants auxquels surviennent les sauts sur les états de l'observateur, doit satisfaire la condition suivante :

$$\gamma\beta e^{2(\lambda+M)\tau} \leq 1, \quad (3.3)$$

avec $\gamma > 1$ est une constante, λ est la plus grande valeur propre de $0.5(A^T + A)$, β est la plus grande valeur propre de $(I + B_k)^T(I + B_k)$, $k = 1, 2, \dots$ et M est une constante positive telle que :

$$|x_j(t)| \leq M \text{ et } |\hat{x}_j(t)| \leq M, j = 1, 2, \dots, n$$

.

Ce résultat a été ensuite directement appliqué sur les systèmes d'ordre fractionnaire puisqu'un système d'ordre entier est considéré comme un cas particulier de systèmes d'ordre fractionnaire. En faisant varier l'ordre de dérivation α , les utilisateurs de cette approche observent les résultats de simulation et choisissent, au final, l'ordre qui garantit une synchronisation plus rapide. Bien que cette méthode est simple, elle manque toutefois de bases théoriques et la synchronisation n'est pas toujours préservée dans le cas de systèmes d'ordre fractionnaire.

3.3.1.2 Synchronisation impulsive modifiée des systèmes chaotiques d'ordre fractionnaire

Une approche de synchronisation impulsive modifiée a été proposée par d'autres chercheurs tels Fu *et al.* [213] ainsi que Ma *et al.* [214]. Nous décrivons, dans ce qui suit, le principe du schéma de synchronisation modifiée. Pour cela, nous considérons comme exemple le schéma de Fu *et al.*

Soit le système maître d'ordre fractionnaire suivant

$$D^\alpha x = Ax(t) + \varphi(x(t)), \quad (3.4)$$

avec $x = [x_1, x_2, \dots, x_n]^T$ est le vecteur d'état, $0 \leq \alpha \leq 1$ est l'ordre de dérivation, $A \in \mathbb{R}^{n \times n}$ est la matrice d'état du système et $\varphi(x(t))$ est une fonction non linéaire.

L'approche de synchronisation impulsive modifiée consiste à concevoir un système

esclave approprié de sorte à obtenir un système d'erreur d'ordre entier et ramener l'étude de la stabilité de la synchronisation à l'étude classique de la stabilité d'un système d'erreur impulsif d'ordre entier.

L'observateur impulsif d'ordre fractionnaire proposé est alors donné par le système

$$\begin{cases} \dot{\hat{x}} &= A\hat{x}(t) + \varphi(\hat{x}(t)) + \eta(x(t)), & t \neq t_k \\ \Delta\hat{x} &= B_k e(t_k), & t = t_k, \quad k = 1, 2, \dots \end{cases} \quad (3.5)$$

avec $\hat{x} = [\hat{x}_1, \hat{x}_2, \dots, \hat{x}_n]^T$ est le vecteur d'états estimés, B_k est la matrice de gains de contrôle et $\eta(x(t)) = \dot{x}(t) - D^\alpha(x(t))$. Les termes $\dot{x}(t)$ et $D^\alpha(x(t))$ peuvent être obtenus à partir du système maître (3.4) et des solutions numériques des équations $\dot{x}(t)$ et $D^\alpha(x(t))$. Ainsi, et à partir des équations (3.4) et (3.5), le nouveau système d'erreur obtenu a la structure suivante [213] :

$$\begin{cases} \dot{e}(t) &= Ae(t) + \psi(x(t), \hat{x}(t)), & t \neq t_k \\ \Delta e(t_k) &= B_k e(t_k), & t = t_k, k = 1, 2, \dots \end{cases} \quad (3.6)$$

où $e = [e_1, e_2, \dots, e_n]^T$ est le vecteur d'erreur et $\psi(x(t), \hat{x}(t)) = \varphi(x(t)) - \varphi(\hat{x}(t))$.

L'étude de la stabilité de la synchronisation impulsive entre le système d'ordre fractionnaire (3.4) et le système esclave proposé (3.5) revient alors à étudier la stabilité asymptotique du système d'erreur d'ordre entier (3.6).

3.3.1.3 Synchronisation impulsive à base de l'étude de la stabilité de systèmes différentiels impulsifs d'ordre fractionnaire

La troisième approche de synchronisation impulsive des systèmes chaotiques continus d'ordre fractionnaire est celle proposée par Liu et qui consiste à étudier la stabilité des systèmes impulsifs d'ordre fractionnaire en utilisant l'inégalité de Gronwall-Bellman [215]. Cette méthode appropriée pour le cas $0 < \alpha < 1$ est plus générale que les deux approches développées ci-dessus. Avant de présenter le schéma de synchronisation impulsive, nous introduirons d'abord quelques définition et lemmes sur la stabilité des systèmes impulsifs d'ordre fractionnaire.

A) Systèmes impulsifs d'ordre fractionnaire

Dans cette partie, nous présenterons quelques résultats théoriques sur la stabilité des systèmes d'équations différentielles impulsives d'ordre fractionnaire. Considérons le système différentiel d'ordre fractionnaire suivant :

$$\begin{cases} \frac{d^\alpha x(t)}{dt^\alpha} = f(x(t)), \\ x(t_0) = x_0, \end{cases} \quad (3.7)$$

où $x \in \mathbb{R}^n$ est le vecteur d'état du système, $f \in \mathbb{R}^n$ est un vecteur de fonctions continues et différentiables. $\frac{d^\alpha x(t)}{dt^\alpha}$ dénote la dérivée d'ordre non entier α tel que $0 < \alpha < 1$. Parmi les définitions de la dérivée fractionnaire présentées dans le premier chapitre, c'est la définition de Caputo suivante qui est utilisée pour l'étude des systèmes impulsifs continus d'ordre fractionnaire.

$$\frac{d^\alpha x(t)}{dt^\alpha} = \frac{1}{\Gamma(1-\alpha)} \int_{t_0}^t (t-\tau)^{-\alpha} x'(\tau) d\tau \quad (3.8)$$

avec $\Gamma(\cdot)$ est la fonction Gamma Euler, telle que

$$\Gamma(1-\alpha) = \int_0^\infty e^{-t} t^{-\alpha} dt, \quad (3.9)$$

Soit un ensemble d'instants discrets t_k tels que $0 < t_1 < t_2 < \dots < t_k < \dots$, $\lim_{k \rightarrow \infty} t_k = \infty$.

Le système impulsif d'ordre fractionnaire est alors donné par

$$\begin{cases} \frac{d^\alpha x(t)}{dt^\alpha} = f(x(t)), & t \neq t_k \\ \Delta x(t_k) = U(k, x), & t = t_k, \\ x(t_0^+) = x_0, \end{cases} \quad (3.10)$$

Définition 18 [215]

– La solution triviale du système (3.7) est dite stable, si $\forall \varepsilon > 0$, il existe $\delta_0(\varepsilon, t_0) >$

0, tel que chaque solution $x(t)$ du système (3.7) satisfaisant $\|x(t_0)\| < \delta_0(\varepsilon, t_0)$, satisfait $\|x(t)\| < \varepsilon$ pour tout $t \geq t_0$.

- La solution triviale du système (3.7) est dite asymptotiquement stable, si en plus d'être stable, $\|x(t)\| \rightarrow 0$ quand $t \rightarrow \infty$.

Lemme 1 [215] Le système (3.7) est équivalent à l'équation intégrale suivante :

$$x(t) = x_0 + \frac{1}{\Gamma(q)} \int_{t_0}^t (t-s)^{q-1} f(x) ds, \quad (3.11)$$

où $0 < t_0 < t \leq b$, et b est une constante positive. Ainsi, toute solution de l'équation (3.11) est aussi une solution du système (3.7) et vice versa.

Lemme 2 : Inégalité de Gronwall-Bellman

Soit $u(t)$ et $v(t)$ deux fonctions continues non négatives sur un intervalle $t_0 \leq t \leq b$. De plus, soit la fonction $h(t)$ positive, continue et monotone non décroissante sur $t_0 \leq t \leq b$ et vérifiant la relation

$$u(t) \leq h(t) + \int_{t_0}^t u(s)v(s)ds, \quad (3.12)$$

alors

$$u(t) \leq h(t) \exp \int_{t_0}^t v(s)ds, \quad t_0 \leq t \leq b. \quad (3.13)$$

En s'inspirant du principe des systèmes de comparaison des système impulsifs d'ordre entier, les théorèmes suivants sont présentés pour étudier la stabilité du système impulsif d'ordre fractionnaire (3.10).

Théoreme 17 [215]

Supposons que

(a) $|f(x(t))| \leq g(t, |x|), t \neq t_k, (t, x) \in \mathbb{R}^+ \times S(\rho)$, où $g \in C(\mathbb{R}_+ \times \mathbb{R}_+, R)$ avec $g(t, 0) = 0$, $S(\rho) = \{x \in \mathbb{R}^n, \|x\| < \rho\}$;

(b) $|x + U(k, x)| \leq \psi_k(|x|)$, $t = t_k$, avec $\psi_k : [0, \rho_0) \rightarrow [0, \rho)$, $\psi_k(0) = 0$ et $\psi_k(u)$ est strictement croissante en u .

Alors, la stabilité asymptotique de la solution triviale $w = 0$ du système

$$\begin{cases} \frac{d^\alpha w(t)}{dt^\alpha} = g(w(t)), & t \neq t_k \\ w(t_k^+) = \psi_k(w(t_k)), & t = t_k, \\ w(t_0^+) = w_0 \geq 0, \end{cases} \quad (3.14)$$

implique la stabilité asymptotique de la solution triviale $x = 0$ du système (3.10).

Théoreme 18 Soit $g(w) = \lambda w$, $\lambda > 0$, $\psi_k(w) = d_k w$, $d_k \geq 0$ pour tout k et $w(t_0^+) = w_0 \geq 0$, alors la solution triviale $w = 0$ du système

$$\begin{cases} \frac{d^\alpha w(t)}{dt^\alpha} = \lambda w, & t \neq t_k \\ w(t_k^+) = d_k w, & t = t_k, \\ w(t_0^+) = w_0 \geq 0, \end{cases} \quad (3.15)$$

est asymptotiquement stable si la condition suivante est vérifiée

$$\gamma d_k E_\alpha(\lambda \tau_k^\alpha) < 1 \quad (3.16)$$

avec $\gamma > 1$, $\tau_k = t_{k+1} - t_k$, $k = 1, 2, \dots$. $E_\alpha(\cdot)$ est la fonction de Mittag-Leffler, définie dans le premier chapitre de cette thèse.

B) Synchronisation impulsive des systèmes chaotiques continus d'ordre fractionnaire

Afin d'établir la synchronisation impulsive, un observateur impulsif d'ordre fractionnaire a été proposé au système (3.7). La dynamique de l'observateur est définie par

le système d'équations suivant

$$\begin{cases} \frac{d^\alpha \hat{x}(t)}{dt^\alpha} = f(\hat{x}(t)), & t \neq t_k \\ \Delta \hat{x} = U(k, e) = B_k(\hat{x} - x), & t = t_k, \\ \hat{x}(t_0^+) = \hat{x}_0, \end{cases} \quad (3.17)$$

où $\hat{x} \in \mathbb{R}^n$ est le vecteur d'état de l'observateur, $\Delta \hat{x}(t_k) = \hat{x}(t_k^+) - \hat{x}(t_k^-)$, $\hat{x}(t_k^+) = \lim_{t \rightarrow t_k^+} \hat{x}(t)$, $\hat{x}(t_k^-) = \lim_{t \rightarrow t_k^-} \hat{x}(t)$ et U est la loi de commande qui définit le saut dans la variable d'état à l'instant t_k . On suppose que $\hat{x}(t_k^-) = \hat{x}(t_k)$.

Soit le vecteur d'erreur $e = [e_1, e_2, \dots, e_n]^T = [x_1 - \hat{x}_1, x_2 - \hat{x}_2, \dots, x_n - \hat{x}_n]^T$.

Alors, à partir de (3.7) et (3.17), le système dynamique d'erreur de synchronisation est donné par

$$\begin{cases} \frac{d^\alpha e(t)}{dt^\alpha} = f(\hat{x}(t)) - f(x(t)), & t \neq t_k \\ \Delta e(t_k) = U(k, e) = B_k e, & t = t_k, \\ e(t_0^+) = e_0, \end{cases} \quad (3.18)$$

L'objectif est donc de déterminer la matrice de gains de contrôle B_k et la distance τ_k entre deux instants discrets successifs t_{k+1} et t_k garantissant la stabilité asymptotique du système (3.18) et donc la synchronisation des systèmes (3.7) et (3.17).

On peut formuler ceci mathématiquement comme suit :

$$\lim_{t \rightarrow \infty} \|e(t)\| = \lim_{t \rightarrow \infty} \|\hat{x}(t) - x(t)\| = 0$$

.

Théoreme 19 [215] : Supposons que $f(x)$ satisfait l'inégalité $\|f(x) - f(\hat{x})\| \leq l\|x(t) - \hat{x}(t)\|$ où l est une constante positive.

S'il existe un nombre positif $\gamma > 1$ tel que la condition suivante est vérifiée

$$\gamma |\beta_k| E_\alpha(l\tau_k^\alpha) < 1, \quad (3.19)$$

avec β_k^2 est la plus grande valeur propre de la matrice $(I_n + B_k)^T(I_n + B_k)$, $\tau_k =$

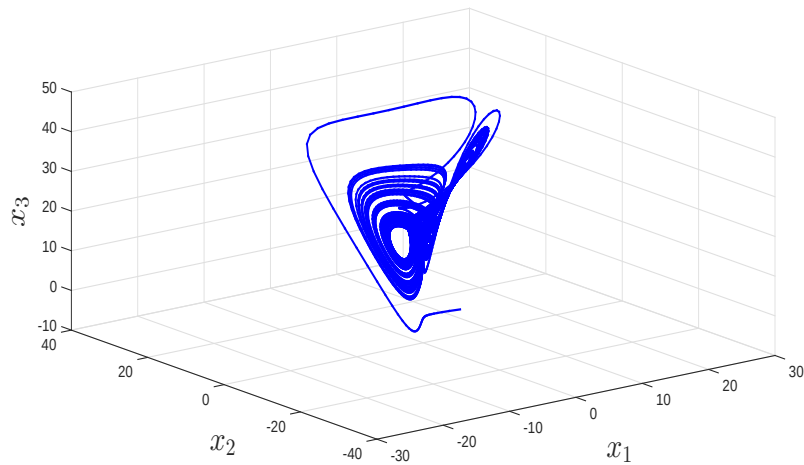


FIGURE 3.1 – Attracteur étrange du système chaotique de Lü d'ordre fractionnaire avec $\alpha = 0.95$

$t_{k+1} - t_k, k = 1, 2, \dots$ et $E_\alpha(v) = \sum_{k=0}^{\infty} \frac{v^k}{\Gamma(\alpha k + 1)}$ est la fonction de Mittag-Leffler alors la synchronisation impulsive entre les systèmes (3.7) et (3.17) est obtenue.

C) Exemple : Application au système chaotique de Lü d'ordre fractionnaire

Afin de vérifier la validité du théorème précédent, nous l'avons appliqué sur le système chaotique de Lü d'ordre fractionnaire. Ce dernier est défini par le système d'équations différentielles d'ordre fractionnaire suivant :

$$\begin{cases} \frac{d^\alpha x_1(t)}{dt^\alpha} = 36(x_2 - x_1) \\ \frac{d^\alpha x_2(t)}{dt^\alpha} = 20x_2 - x_1x_3 \\ \frac{d^\alpha x_3(t)}{dt^\alpha} = -3x_3 + x_1x_2 \end{cases} \quad (3.20)$$

Le système de Lü d'ordre fractionnaire (3.20) présente un comportement chaotique pour $\alpha > 0.9156$. La figure 3.1 illustre l'attracteur étrange obtenu en plan de phase quand $q = 0.95$. La matrice de gains de contrôle est choisie comme suit :

$$B_k = \begin{pmatrix} -0.9 & 0 & 0 \\ 0 & -0.9 & 0 \\ 0 & 0 & -0.9 \end{pmatrix}$$

Ainsi, on peut déduire par calculs simples que $\beta_k = 0.1$. A partir de l'équation (3.19), la région de stabilité est fixé comme $0 \leq \tau \leq 0.0027$. Les valeurs initiales considérées lors des simulations sont $(x_1(0), x_2(0), x_3(0)) = (5, -1, -3)$ pour le système maître et $(\hat{x}_1(0), \hat{x}_2(0), \hat{x}_3(0)) = (2, 4, 1)$ pour l'observateur impulsif d'ordre fractionnaire.

La figure 3.2 illustre l'estimation des états x_1 , x_2 et x_3 du système de Lü d'ordre fractionnaire par l'observateur impulsif fractionnaire pour une période d'impulsions choisie égale à $\tau = 0.002$ s.

Pour la même valeur de τ , les erreurs de synchronisation e_1, e_2 et e_3 sont affichées sur la figure 3.3. Comme on peut le constater, elles convergent toutes vers 0 après un court régime transitoire d'environ 1 s.

3.3.2 Synchronisation impulsive des systèmes chaotiques discrets d'ordre fractionnaire

Afin de représenter un système chaotique discret d'ordre fractionnaire, nous utiliserons le modèle (1.73) obtenu lors du premier chapitre et calculé à partir de la définition de Grünwald-Letnikov. Un système chaotique discret d'ordre fractionnaire commensurable (l'ordre de dérivation est le même pour tout les états) est alors donné par la représentation d'état suivante.

$$x(k+1) = Ax(k) + \varphi(x(k)) - \sum_{p=1}^L C_p x(k-p) \quad (3.21)$$

Pour un système non commensurable, c'est à dire les ordres de dérivation des états sont différents, nous pouvons réécrire le système en tenant compte des différents ordres de dérivations $\alpha_1, \alpha_2, \dots, \alpha_n$ des états $x_1, x_2, \dots, x_n$ respectivement. Nous obtenons alors le modèle suivant [216] :

$$x(k+1) = Ax(k) + \varphi(x(k)) - \sum_{p=1}^L A_d(p)x(k-p) \quad (3.22)$$

où la matrice $A \in \mathbb{R}^{n \times n}$ décrit la partie linéaire non retardée du système et $\varphi(x(k))$

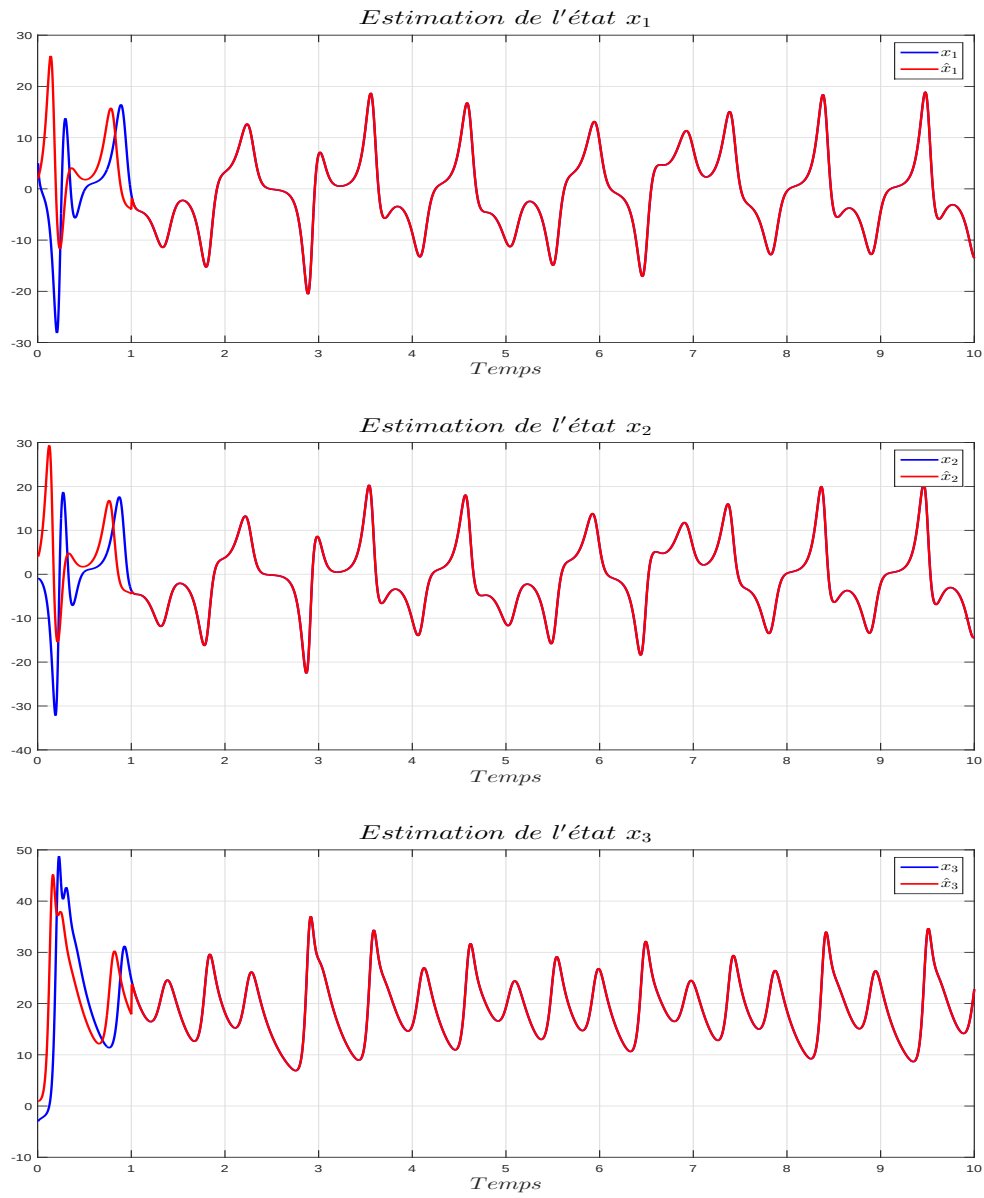


FIGURE 3.2 – Estimation des états du système de Lü d'ordre fractionnaire par l'observateur impulsif

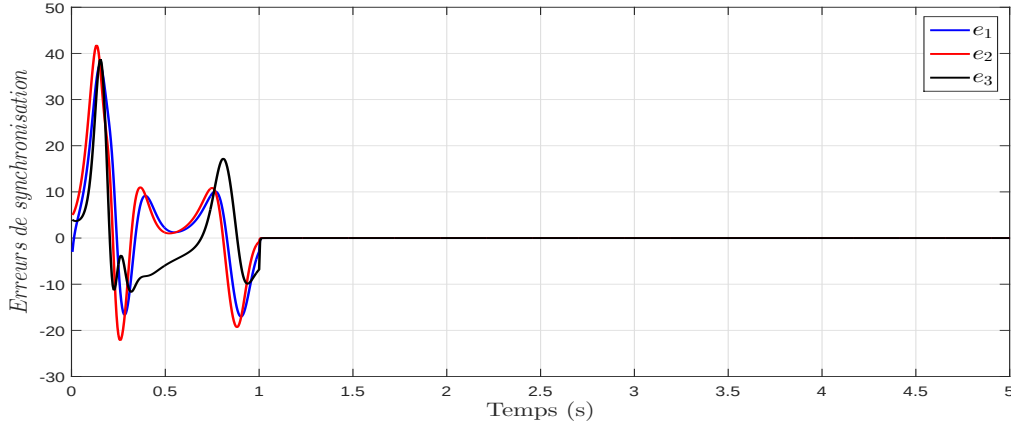


FIGURE 3.3 – Erreurs de synchronisation impulsive pour le système de Lü d'ordre fractionnaire

est une fonction non linéaire lipschitzienne.

Les matrices $A_d(p)$ sont des matrices symétriques contenant les coefficients $C_{p1}, C_{p2}, \dots, C_{pn}$ relatifs aux ordres de dérivation non entiers $\alpha_1, \alpha_2, \dots, \alpha_n$. Elles sont, donc, données comme suit :

$$A_d(p) = \begin{pmatrix} C_{p1} & 0 & \dots & 0 \\ 0 & C_{p2} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & C_{pn} \end{pmatrix} \quad (3.23)$$

L'observateur impulsif d'ordre fractionnaire pour le système (3.22) est donné par le système suivant.

$$\begin{cases} \hat{x}(k+1) = A\hat{x}(k) + \varphi(\hat{x}(k)) \\ \quad - \sum_{p=1}^L A_d(p)\hat{x}(k-p), & k \neq k_i \\ \hat{x}(k_i^+) = \hat{x}(k_i) - B(k_i)e(k_i), & k = k_i, \\ \quad i = 1, 2, \dots \end{cases} \quad (3.24)$$

où $\hat{x} \in \mathbb{R}^n$ est le vecteur d'état estimé. $k_i, i = 1, 2, \dots$ dénote l'ensemble des instants discrets auxquels les variables d'état de l'observateur subissent des sauts dans leurs trajectoires. Les nouvelles valeurs de ces variables d'états sont calculées à partir des valeurs

des erreurs $e(k_i)$ et des matrices $B(k_i) \in \mathbb{R}^{n \times n}$. Les instants $k_i, i = 1, 2, \dots$ sont supposés équadistants et la distance entre deux instants discrets k_i et $k_{i+1}, i = 1, 2, \dots$ est notée δ .

Le système d'erreur de synchronisation entre les systèmes (3.22) et (3.24) est défini comme suit

$$\left\{ \begin{array}{lcl} e(k+1) & = & Ae(k) + \tilde{\varphi}(x(k), \hat{x}(k)) \\ & - & \sum_{p=1}^L A_d(p)e(k-p), \\ & & k \neq k_i \\ \Delta e(k) & = & B(k_i)e(k_i), \\ & & k = k_i, i = 1, 2, \dots \end{array} \right. \quad (3.25)$$

avec $\tilde{\varphi}(x(k), \hat{x}(k)) = \varphi(x(k)) - \varphi(\hat{x}(k))$.

Nous pouvons constater à partir de (3.25), que la structure du système d'erreur contient des termes retardés. Alors, et pour étudier la stabilité du système d'erreur et la synchronisation impulsive entre les systèmes (3.22) et (3.24), nous nous sommes inspirés des travaux et résultats obtenus par Liu et Marquez [217] lors de l'étude de la synchronisation impulsive dans un réseau de systèmes chaotiques discrets à retards.

Le théorème suivant fournit des conditions suffisantes pour la stabilité du système d'erreur.

Théoreme 20 [218] *Soit λ la valeur singulière de A et γ la valeur singulière de la matrice A_α définie comme suit :*

$$A_\alpha = \begin{pmatrix} \frac{\alpha_1 * (\alpha_1 - 1)}{2} & 0 & \dots & 0 \\ 0 & \frac{\alpha_2 * (\alpha_2 - 1)}{2} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \frac{\alpha_n * (\alpha_n - 1)}{2} \end{pmatrix}$$

où $\alpha_1, \alpha_2, \dots, \alpha_n$ sont respectivement les ordres de dérivation fractionnaires des états $x_1, x_2, \dots, x_n$.

Si la condition de Lipschitz suivante est vérifiée,

$$\| \varphi(x(k)) - \varphi(\hat{x}(k)) \| < l \| x(k) - \hat{x}(k) \| \text{ où } l \text{ est la constante de Lipschitz.}$$

et s'il existe deux constantes positives $q \leq 1$ et C définie comme suit :

$$C = \lambda + l + L \frac{\gamma}{q}$$

et vérifiant la condition suivante

$$\lim_{k \rightarrow \infty} C^k \| I_n + B(k_i) \|^i = 0$$

Alors le système d'erreur (3.25) est asymptotiquement stable et la synchronisation impulsive est établie entre les systèmes (3.22) et (3.24).

Démonstration 1 [218]

– Pour $k \in \mathbb{N}$, considérons la fonction de Lyapunov suivante :

$$V(e(k)) = \| e(k) \| \quad (3.26)$$

$$\begin{aligned} V(e(k+1)) &= \| e(k+1) \| \\ &\leq \| A \| \| e(k) \| + \| \tilde{\varphi}(x(k), \hat{x}(k)) \| \end{aligned}$$

Alors nous avons :

$$\begin{aligned} &+ \sum_{p=1}^L \| A_d(p) \| \| e(k-p) \| \\ &\leq (\lambda + l) \| e(k) \| \\ &+ \| A_\alpha \| \sum_{p=1}^L \| e(k-p) \| \end{aligned}$$

Compte tenu de la remarque 8 concernant la convergence des coefficients C_p et donnée dans le premier chapitre, nous pouvons déduire que

$$\begin{aligned} V(e(k+1)) &\leq (\lambda + l)V(e(k)) \\ &+ \gamma \sum_{p=1}^L V(e(k-p)) \end{aligned} \quad (3.27)$$

Si pour tout $p \in \mathbb{N}$, $qV(e(k-p)) \leq V(e(k))$, alors en sommant les termes à retards $V(e(k-p))$ de 1 jusqu'à la taille de la mémoire L , nous obtenons la relation suivante.

$$q \sum_{p=1}^L V(e(k-p)) \leq LV(e(k)) \quad (3.28)$$

Si on multiplie la dernière inégalité (3.28) par la constante γ , nous obtenons

$$\gamma \sum_{p=1}^L V(e(k-p)) \leq \frac{L\gamma}{q} V(e(k)) \quad (3.29)$$

A partir de (3.29), l'inégalité (3.27) peut être réécrite comme suit :

$$V(e(k+1)) \leq (\lambda + l + \frac{L\gamma}{q}) V(e(k)) \quad (3.30)$$

ce qui nous mène à

$$V(e(k)) \leq (\lambda + l + L\frac{\gamma}{q}) V(e(k-1)) \quad (3.31)$$

– Lorsque $k = k_i$ nous avons

$$\begin{aligned} V(e(k_i^+)) &= \| I_n + B(k_i) \| \| e(k_i) \| \\ &= \| I_n + B(k_i) \| V(e(k_i)) \end{aligned} \quad (3.32)$$

En combinant les inégalités (3.31) et (3.32) et après plusieurs itérations successives, nous pouvons déduire que

$$\left\{ \begin{array}{ll} V(e(k)) \leq C^k \| I_n + B(k_i) \|^{i-1} V(e(0)) & k_i < k < k_{i+1} \\ V(e(k_i^+)) \leq C^k \| I_n + B(k_i) \|^i V(e(0)) & k = k_i \\ & k = 1, 2, \dots, i = 1, 2, \dots \end{array} \right. \quad (3.33)$$

avec

$$C = \lambda + l + L\frac{\gamma}{q} \quad (3.34)$$

A partir de (3.33), nous pouvons constater que si la relation

$$\lim_{k \rightarrow \infty} C^k \| I_n + B(k_i) \|^i = 0 \quad (3.35)$$

est vérifiée, alors le système d'erreur de synchronisation (3.25) est asymptotique-

ment stable pour toute condition initiale $e(0)$, et que la synchronisation impulsive est établie entre les systèmes (3.22) et (3.24).

3.4 Synchronisation impulsive de deux systèmes chaotiques de Lozi d'ordre fractionnaire

Dans cette partie, et afin de valider les résultats théoriques développés dans la section précédente, nous proposerons un observateur impulsif d'ordre fractionnaire pour le système chaotique de Lozi d'ordre non entier.

Pour cela, considérons de nouveau le système de Lozi discret d'ordre fractionnaire introduit dans le premier chapitre et donné par la représentation d'état suivante :

$$\begin{cases} x(k+1) &= Ax(k) + \varphi(x(k)) \\ &- \sum_{p=1}^L A_d(p)x(k-p) \\ y(k) &= h(x(k)) \end{cases} \quad (3.36)$$

avec $x = [x_1 \ x_2]^T \in \mathbb{R}^2$ est le vecteur d'état. $y(k)$ est le vecteur de sortie et $h(\cdot)$ est une fonction non linéaire. Les matrices $A \in \mathbb{R}^{2 \times 2}$, $A_d \in \mathbb{R}^{2 \times 2}$ et le vecteur $\varphi(x(k))$ sont définis comme suit :

$$A = \begin{pmatrix} \alpha_1 - 1 & b \\ 1 & \alpha_2 - 1 \end{pmatrix}, A_d(p) = \begin{pmatrix} C_{p1} & 0 \\ 0 & C_{p2} \end{pmatrix}, \varphi(x(k)) = \begin{pmatrix} 1 - a |x_1(k)| \\ 0 \end{pmatrix}$$

Les coefficients C_{p1} et C_{p2} sont calculés comme suit : $C_{p1} = (-1)^{p+1} \begin{pmatrix} \alpha_1 \\ p+1 \end{pmatrix}$, $C_{p2} = (-1)^{p+1} \begin{pmatrix} \alpha_2 \\ p+1 \end{pmatrix}$

avec α_1 et α_2 sont, respectivement, les ordres de dérivation fractionnaires des états x_1 et x_2 .

Avant de développer la structure de l'observateur impulsif d'ordre fractionnaire au sys-

tème (3.36), nous allons d'abord analyser dans la section qui suit les dynamiques et la complexité du système de Lozi d'ordre fractionnaire.

3.4.1 Analyse des dynamiques du système de Lozi d'ordre fractionnaire

Dans cette partie, nous appliquerons les méthodes d'analyses des dynamiques non linéaires présentées dans le premier chapitre pour étudier les caractéristiques du système de Lozi d'ordre fractionnaire. Cette analyse nous permettra, en effet, de définir les valeurs des paramètres de bifurcation du système et les ordres de différence fractionnaires pour lesquelles le système présente un comportement chaotique.

3.4.1.1 Analyse de Bifurcations

En fixant la valeur du paramètre de bifurcation à $b = 0.5$ et les ordres de dérivation à $\alpha_1 = \alpha_2 = 0.95$, et en faisant varier le paramètre a de 0 à 1.8 avec un pas de 0.0025, nous obtenons le diagramme de bifurcation illustré sur la figure 3.4. Comme nous pouvons le voir sur la figure, pour les valeurs de a inférieures à 1.5, les trajectoires du systèmes sont périodiques. Une séquence de doublements de périodes se produit pour les valeurs de a comprises entre $a = 0.5$ et 1.5. Pour les valeurs de a appartenant à l'intervalle $[1.5 - 1.8]$ le système évolue en régime chaotique. Afin d'observer l'effet de l'ordre de dérivation non entier sur l'évolution des états du système de Lozi d'ordre fractionnaire, nous fixons les valeurs des paramètres a et b et l'un des ordre de dérivation et faisons varier l'autre ordre. La figure 3.5 présente un autre type de diagrammes de bifurcations obtenu pour les valeurs fixes $a = 1.7$, $b = 0.5$ et $\alpha_2 = 0.95$ et pour les valeurs de α_1 variant de 0 et 1. A partir de la figure, nous pouvons constater que le système exhibe un comportement chaotique pour les valeurs de α comprises entre 0.4 et 1.

3.4.1.2 Analyse spectrale

Comme nous l'avons introduit dans le premier chapitre, un signal chaotique est riche en fréquence et son spectre est étalé et semblable à celui d'un bruit blanc. Une analyse

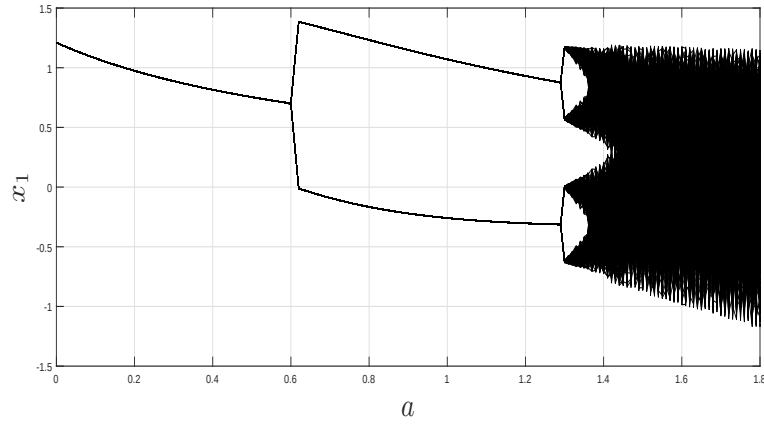


FIGURE 3.4 – Diagramme de bifurcation du système de Lozi pour différentes valeurs de a (Cas commensurable)

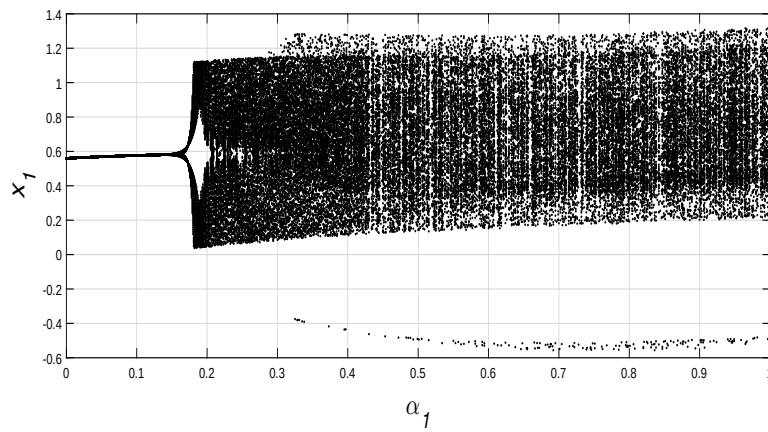


FIGURE 3.5 – Diagramme de bifurcation du système de Lozi d'ordre fractionnaire pour différentes valeurs de α_1

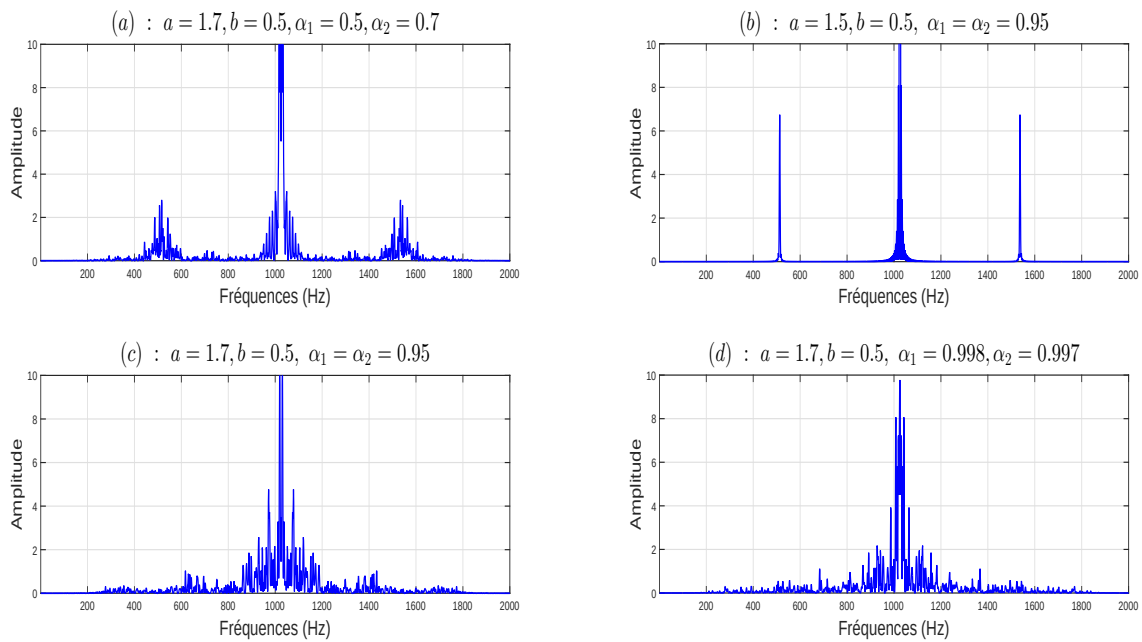


FIGURE 3.6 – Spectres de fréquences du signal x_1 du système de Lozi d'ordre fractionnaire pour différentes valeurs des paramètres a et b et des ordres α_1 et α_2

spectrale peut alors nous fournir des informations sur un signal dans le domaine fréquentiel. A partir de cette analyse, on peut observer si un signal est chaotique ou non. Dans le cas d'un signal périodique, le spectre est discret tandis que pour un signal chaotique, le spectre est continu. Le spectre de fréquence des signaux x_1 et x_2 du système de Lozi d'ordre fractionnaire a été établi pour différentes valeurs des paramètres a et b et pour différentes valeurs des ordres de différences α_1 et α_2 . Les figures 3.6 et 3.7 illustrent respectivement les spectres des signaux x_1 et x_2 obtenus en variant les paramètres de bifurcation et les ordres α_1 et α_2 .

En observant les spectres obtenus, on peut remarquer que dans les tracés (a) et (b) sur chaque figure, les spectres sont discrets. On peut déduire alors que l'évolution du système de Lozi d'ordre fractionnaire est périodique ou quasi-périodique pour les valeurs considérées. D'une autre part, et pour les valeurs $a = 1.7$ et $b = 0.5$, et pour des valeurs des ordres de différence proches de 1, les spectres des signaux x_1 et x_2 sont continus (riches en fréquences). Nous pouvons alors conclure que le système de Lozi d'ordre fractionnaire évolue en régime chaotique pour ces valeurs.

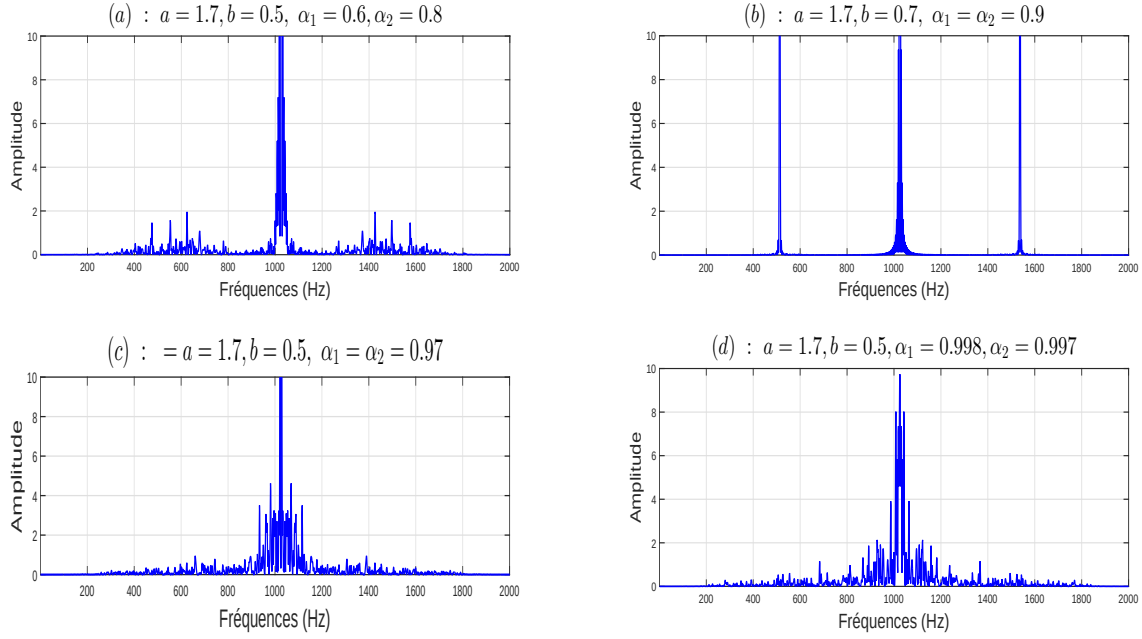


FIGURE 3.7 – Spectres de fréquences du signal x_2 du système de Lozi d'ordre fractionnaire pour différentes valeurs des paramètres a et b et des ordres α_1 et α_2

3.4.1.3 Analyse de la complexité des états du système de Lozi d'ordre fractionnaire

Dans cette section, nous fournirons les résultats d'application des algorithmes de calcul de complexité SE et C_0 , introduits dans le premier chapitre, sur les séquences chaotiques x_1 et x_2 , de longueur fixée à $N = 5000$, du système de Lozi d'ordre fractionnaire. Nous considérons les cas de systèmes commensurable et non commensurable.

A) Cas commensurable

La complexité des séquences x_1 et x_2 du système de Lozi d'ordre fractionnaire (3.36) a été en premier lieu mesurée dans le cas commensurable. Les ordres de différences α_1 et α_2 associés aux états x_1 et x_2 sont alors choisis égaux soit $\alpha_1 = \alpha_2 = \alpha$. La complexité a été évaluée en utilisant les algorithmes de l'entropie spectrale (SE) et C_0 .

Nous commencerons d'abord par les résultats de l'algorithme SE . Les deux courbes (a) et (b) de la figure 3.8 illustrent la complexité SE de la séquence x_1 pour différentes valeurs

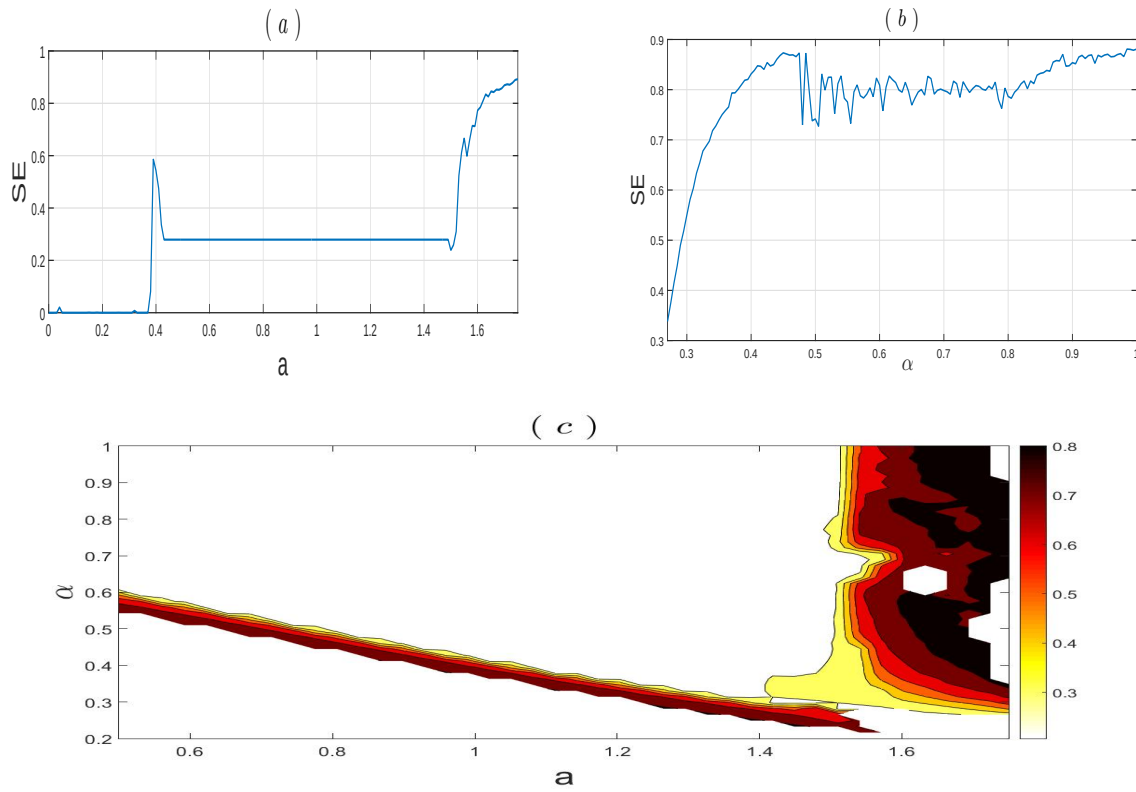


FIGURE 3.8 – Complexité SE du signal chaotique x_1 du système de Lozi d'ordre fractionnaire dans le cas commensurable. (a) : Valeurs de SE en fonction du paramètre a , (b) : Valeurs de SE en fonction de l'ordre α , (c) : Plan $(a - \alpha)$

du paramètre a en fixant $\alpha_1 = 0.95$ d'une part puis pour différentes valeurs de l'ordre α en fixant $a = 1.7$. La complexité dans le plan $(a - \alpha)$ est obtenue en variant le paramètre a , de 0 à 1.75, et l'ordre α , de 0 à 1, à la fois. Le résultat obtenu est affiché sur le graphique (c).

On peut constater que la complexité est maximale pour les valeurs de a allant de 1.6 à 1.75 et pour les valeurs de α comprises dans l'intervalle $[0.4 - 1]$. On peut en outre constater que ces résultats coïncident avec ceux de l'analyse de bifurcation obtenus précédemment.

La complexité C_0 a été aussi mesurée pour les deux signaux x_1 et x_2 . La valeur du facteur de tolérance r a été fixée à $r = 15$. De manière similaire au calcul de la complexité SE . La complexité C_0 a été calculée pour toutes les valeurs du paramètre a dans l'intervalle $[0 - 1.8]$ puis pour toutes les valeurs de α comprises entre 0 et 1. A partir des tracés (a) et (b) de la figure 3.9, on peut conclure que la complexité C_0 est particulièrement élevée

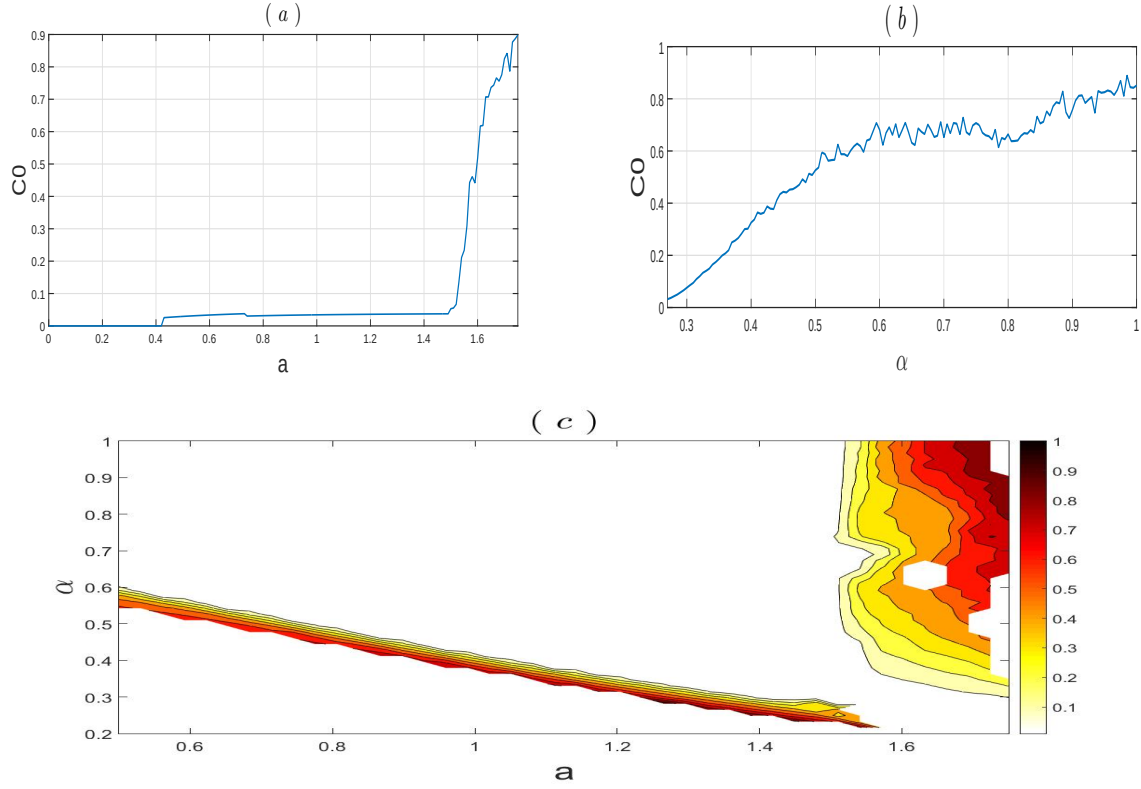


FIGURE 3.9 – Complexité C_0 du signal chaotique x_1 du système de Lozi d'ordre fractionnaire dans le cas commensurable. (a) : Valeurs de C_0 en fonction du paramètre a , (b) : Valeurs de C_0 en fonction de l'ordre α , (c) : Plan $(a - \alpha)$

pour les valeurs de a allant de 1.7 à 1.75 et pour les valeurs de α appartenant à l'intervalle $[0.9 - 1]$. Cette région de complexité élevée est aussi illustrée sur le plan $(a - \alpha)$ affiché sur la sous-figure (c).

B) Cas non commensurable

Dans cette partie, nous allons étudier la complexité du système de Lozi d'ordre fractionnaire dans le cas non commensurable c'est à dire que les ordres de différences fractionnaires associés aux états x_1 et x_2 sont différents. La figure 3.10 illustre les résultats de la complexité en utilisant l'algorithme SE . La courbe (a) illustre la variation de la complexité en fonction du paramètre a . Les ordres de dérivations sont arbitrairement choisis égaux à $\alpha_2 = 0.997$ et $\alpha_1 = 0.9$. Le tracé (b) illustre les valeur de la complexité SE en fixant les paramètres de bifurcation $a = 1.7$ et $b = 0.5$ ainsi que la valeur de l'ordre $\alpha_2 = 0.997$

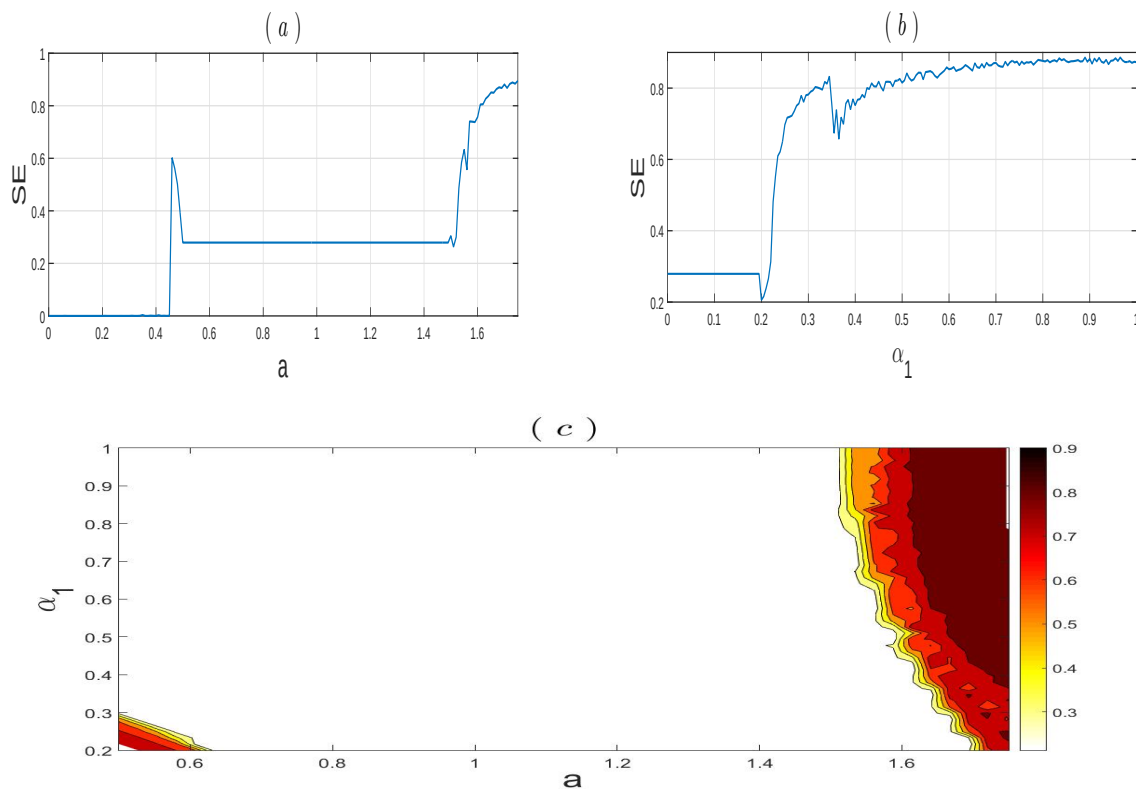


FIGURE 3.10 – Complexité SE du signal chaotique x_2 du système de Lozi d'ordre fractionnaire dans le cas non commensurable (a) : Valeurs de SE en fonction du paramètre a , (b) : Valeurs de SE en fonction de l'ordre α_1 , (c) : Plan $(a - \alpha_1)$

et en variant α_1 de 0 à 1. Les valeurs de la complexité SE en variant simultanément les valeurs de a et α_1 sont données sur le plan $a - \alpha_1$. La région la plus sombre indiquant une haute complexité est située dans l'intervalle $[1.6 - 1.75]$ des valeurs de a et dans l'intervalle $[0.4 - 1]$ des valeurs de α_1 .

La même stratégie a été utilisée pour évaluer la complexité C_0 . Les résultats de l'application de l'algorithme C_0 dans le cas non commensurable sont affichés sur la figure 3.11. Comme on peut le voir sur les trois tracés (a), (b) et (c), la complexité C_0 maximale est atteinte pour les valeurs de a allant de 1.7 à 1.8 et pour les valeurs de α_1 comprises entre 0.6 et 1.

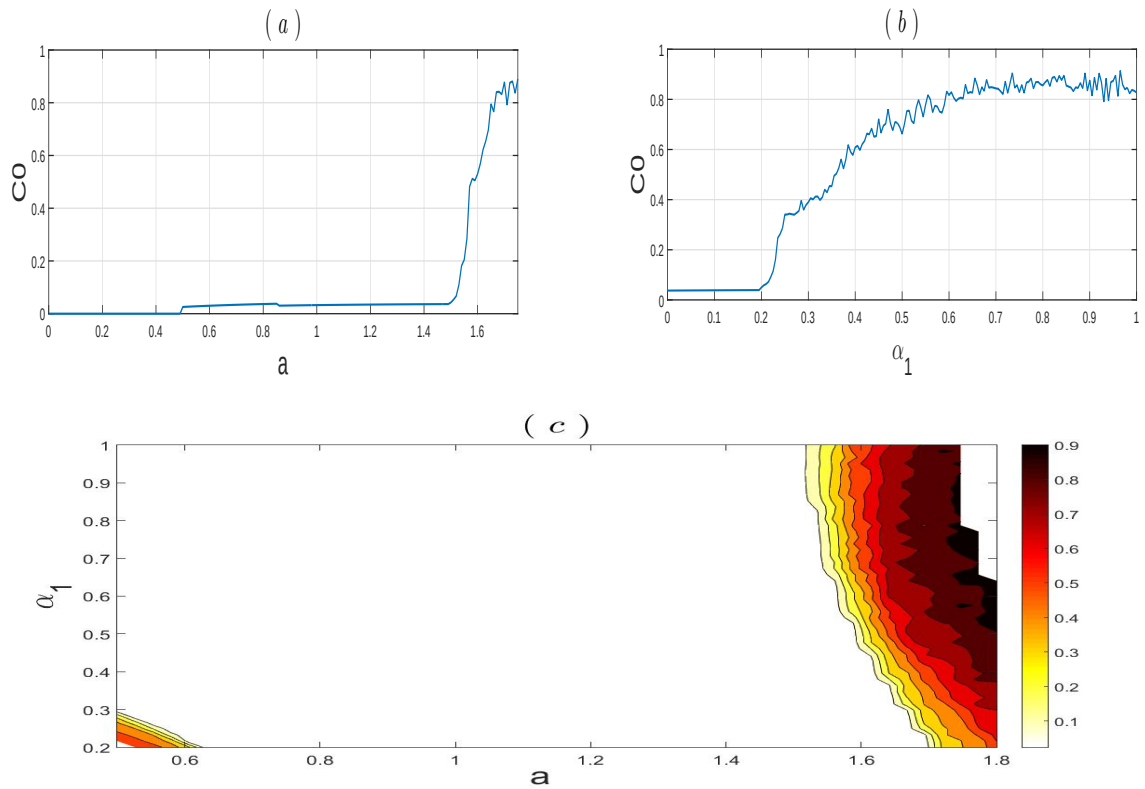


FIGURE 3.11 – Complexité C_0 du signal chaotique x_2 du système de Lozi d'ordre fractionnaire dans le cas non commensurable. (a) : Valeurs de C_0 en fonction du paramètre a , (b) : Valeurs de C_0 en fonction de l'ordre α_1 , (c) : Plan $(a - \alpha_1)$

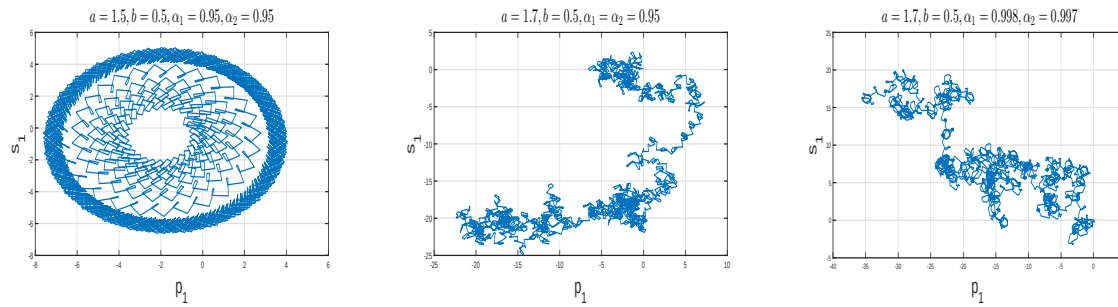


FIGURE 3.12 – Résultats d'application du test 0 – 1 sur la séquence x_1 du système de Lozi d'ordre fractionnaire : Plans de phases $p - s$ pour différentes valeurs des paramètres et des ordres fractionnaires

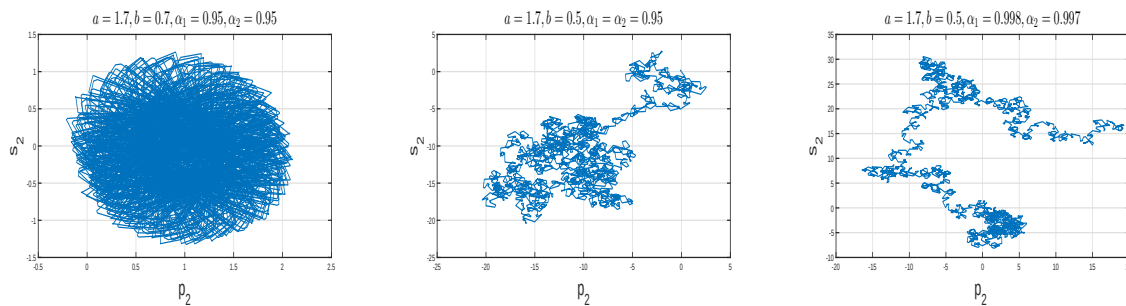


FIGURE 3.13 – Résultats d'application du test 0 – 1 sur la séquence x_2 du système de Lozi d'ordre fractionnaire : Plans de phases $p - s$ pour différentes valeurs des paramètres et des ordres fractionnaires

3.4.1.4 Application du test 0 – 1

Cette partie sera consacrée à présenter les résultats de l'application du test 0 – 1 sur les séquences x_1 et x_2 du système de Lozi d'ordre fractionnaire. La taille de la mémoire a été fixée à $L = 10$ et les conditions initiales sont choisies égales à $(x_1(0), x_2(0)) = (0.1, 0.2)$. La figure 3.12 illustre les résultats obtenus sur les plans de phase ($p - s$) associés à la séquence x_1 pour différentes valeurs des paramètres a et b et des ordres de différences fractionnaires α_1 et α_2 . Les résultats de l'application du test sur la séquence x_2 sont illustrés sur la figure 3.13.

On peut constater à partir de ces résultats graphiques que dans le cas commensurable pour les valeurs des ordres $\alpha_1 = \alpha_2 = 0.95$ et en fixant les valeurs de paramètres $a = 1.7$ et $b = 0.5$, le système de Lozi d'ordre fractionnaire présente un comportement chaotique. En effet, les trajectoires obtenues en plans de phase des signaux p et s ne sont pas bornées. Des résultats similaires sont obtenus sur les deux séquences x_1 et x_2 pour le cas non

Valeurs des paramètres				K_1	K_2	Dynamique
a	b	α_1	α_2			
1.7	0.5	0.95	0.95	0.9974	0.9983	Chaotique
1.5	0.5	0.95	0.95	0.0016	0.0037	Non chaotique
1.7	0.7	0.95	0.95	0.0055	0.0089	Non chaotique
1.7	0.5	0.998	0.997	0.9981	0.9978	Chaotique

TABLE 3.1 – Résultats du test 0 – 1

commensurable avec les valeurs des ordres $\alpha_1 = 0.998$ et $\alpha_2 = 0.997$. Cependant et en modifiant l'un des paramètres de bifurcation (a ou b), nous obtenons des trajectoires bornées sur les plan de phase $p-s$ correspondants aux états x_1 et x_2 . Ce résultat confirme les résultats d'analyse des bifurcations concernant la dynamique régulière (périodique ou quasi périodique) du système de Lozi d'ordre fractionnaire pour ces nouvelles valeurs des paramètres.

Afin de confirmer ces résultats, le tableau 3.1 donne les valeurs calculées des taux de déplacement K_1 et K_2 correspondant, respectivement, aux états x_1 et x_2 du système de Lozi d'ordre fractionnaire pour différentes valeurs des paramètres a et b et des ordres α_1 et α_2 .

3.4.1.5 Exposants de Lyapunov

Le calcul des exposants de Lyapunov est l'un des critères les plus importants pour caractériser les dynamiques d'un système qu'il soit d'ordre entier ou d'ordre fractionnaire. Le tableau 3.2 illustre les valeurs de l'exposant de Lyapunov maximal λ_{max} pour différentes valeurs des ordres de dérivations α_1 et α_2 et des paramètres a et b . Dans le cas d'une évolution chaotique, la valeur de λ_{max} est positive. Dans le cas d'un comportement non chaotique la valeur de λ_{max} est négative et est très proche de 0.

Valeurs des paramètres				$\lambda_{\max}$	Dynamique
a	b	α_1	α_2		
1.2	0.5	0.95	0.95	-0.0021	Non Chaotique
1.7	0.5	0.95	0.95	0.4367	Chaotique
1	0.45	0.9	0.9	-0.0267	Non chaotique
1.7	0.5	0.998	0.997	0.3861	Chaotique
1.7	0.5	0.85	0.85	0.5255	Chaotique

TABLE 3.2 – Valeurs de l'exposant de Lyapunov maximal obtenues pour le système de Lozi d'ordre fractionnaire pour différents paramètres et ordre fractionnaire

3.4.2 Structure de l'observateur impulsif d'ordre fractionnaire

L'observateur impulsif d'ordre fractionnaire pour le système (3.36) est donné par le système suivant :

$$\begin{cases} \hat{x}(k+1) = A\hat{x}(k) + \varphi(\hat{x}(k)) \\ \quad - \sum_{p=1}^L A_d(p)\hat{x}(k-p) & k \neq k_i \\ \hat{x}(k_i^+) = \hat{x}(k_i) - B(k_i)e(k_i) & k = k_i \end{cases} \quad (3.37)$$

avec $\hat{x} = [\hat{x}_1 \ \hat{x}_2]^T \in \mathbb{R}^2$ est le vecteur d'états estimés, $k_i, i = 1, 2, \dots$ est l'ensemble des instants discrets auxquels les variables d'état de l'observateur subissent des sauts dans leurs trajectoires. Les matrices $B(k_i) \in \mathbb{R}^{2 \times 2}$ sont symétriques et contiennent les gains de contrôle permettant la synchronisation impulsive.

Le système d'erreur obtenu entre les systèmes (3.36) et (3.37) est donné par le système d'états suivant :

$$\begin{cases} e(k+1) = Ae(k) + \tilde{\varphi}(x(k), \hat{x}(k)) \\ \quad - \sum_{p=1}^L A_d(p)e(k-p), & k \neq k_i \\ \Delta e(k_i) = B(k_i)e(k_i), & k = k_i \end{cases} \quad (3.38)$$

où $e = [e_1 \ e_2]^T \in \mathbb{R}^2$ est le vecteur d'erreur.

Le vecteur $\tilde{\varphi}(x(k), \hat{x}(k))$ est défini comme suit.

$$\begin{aligned} \tilde{\varphi}(x(k), \hat{x}(k)) &= \begin{pmatrix} 1 - a |x_1(k)| - 1 + a |\hat{x}_1(k)| \\ 0 \end{pmatrix} \\ &= \begin{pmatrix} -a(|x_1(k)| - |\hat{x}_1(k)|) \\ 0 \end{pmatrix} \end{aligned}$$

A partir de la première composante du vecteur $\tilde{\varphi}(x(k), \hat{x}(k))$, il est facile de déduire que la constante de Lipschitz l n'est autre que le paramètre du système de Lozi a .

3.4.3 Résultats de simulations

Dans cette partie, nous fournirons les résultats de synchronisation impulsive simulée sous Matlab. Afin de satisfaire les conditions du théorème 20, la distance δ entre deux instants k_i et k_{i+1} , $i = 1, 2, \dots$, les ordres de dérivations fractionnaires et la matrice de gains de correction sont, dans un premier temps, choisis comme suit :

$$\delta = 3, \alpha_1 = \alpha_2 = 0.95, B = \begin{pmatrix} b_1 & 0 \\ 0 & b_2 \end{pmatrix} = \begin{pmatrix} -0.98 & 0 \\ 0 & -0.98 \end{pmatrix}$$

la taille de la mémoire L est choisie égale à $L = 10$.

Pour ces valeurs des paramètres, nous obtenons les résultats numériques suivants :

$\lambda = \|A\| = 1.0099$, $\gamma = \|A_\alpha\| = 5.64 \cdot 10^{-4}$, $q = 0.0369$. Les figures 3.14 et 3.15 illustrent respectivement la synchronisation des états x_1 , $\hat{x}_1$ et x_2 , $\hat{x}_2$ pour les conditions initiales $(x_1(0), x_2(0)) = (0.1, 0.2)$ pour le système maître et $(\hat{x}_1(0), \hat{x}_2(0)) = (3, 2)$ pour le l'observateur impulsif. Nous pouvons constater que les états se synchronisent bien après un court nombre d'itérations. Les courbes d'erreurs de synchronisation illustrées sur la figure 3.16 montrent que les erreurs convergent après un court régime transitoire et confirment les résultats théoriques obtenus.

Pour vérifier la stabilité de la synchronisation dans le cas non commensurable, nous avons modifié les ordres de différence fractionnaire en choisissant les valeurs $\alpha_1 = 0.998$ et $\alpha_2 = 0.997$. Les autres paramètres et les conditions initiales sont les même que pour le cas commensurable. Les figures 3.17 et 3.18 présentent l'estimation des états x_1 et x_2 pour les nouvelles valeurs des ordres α_1 et α_2 . A partir des deux figures, on peut constater

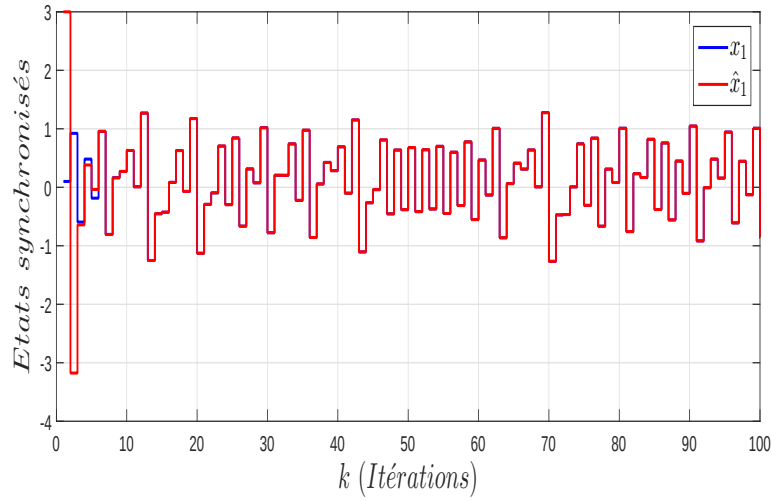


FIGURE 3.14 – États synchronisés x_1 et $\hat{x}_1$ du système de Lozi d'ordre fractionnaire et de l'observateur impulsif d'ordre fractionnaire

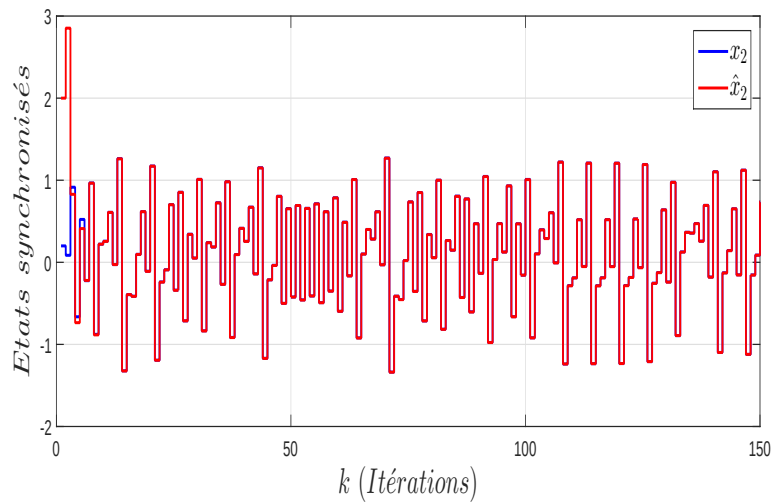


FIGURE 3.15 – États synchronisés x_2 et $\hat{x}_2$ du système de Lozi d'ordre fractionnaire et de l'observateur impulsif d'ordre fractionnaire

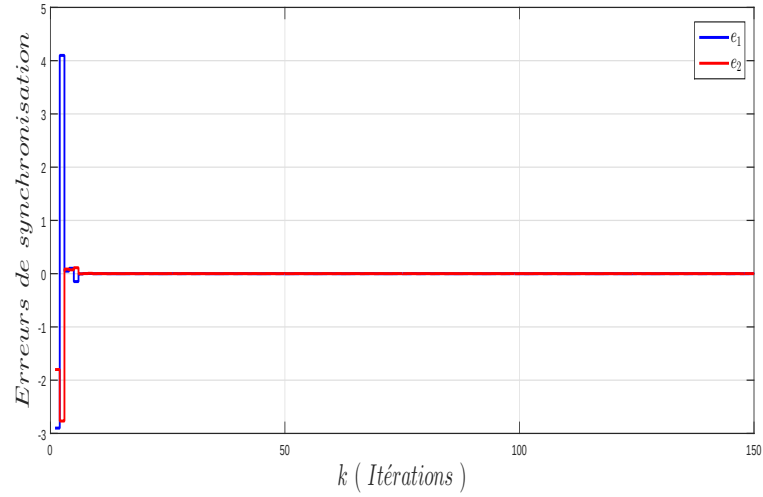


FIGURE 3.16 – Erreurs de Synchronisation impulsive entre le système de Lozi d'ordre fractionnaire et l'observateur impulsif d'ordre fractionnaire

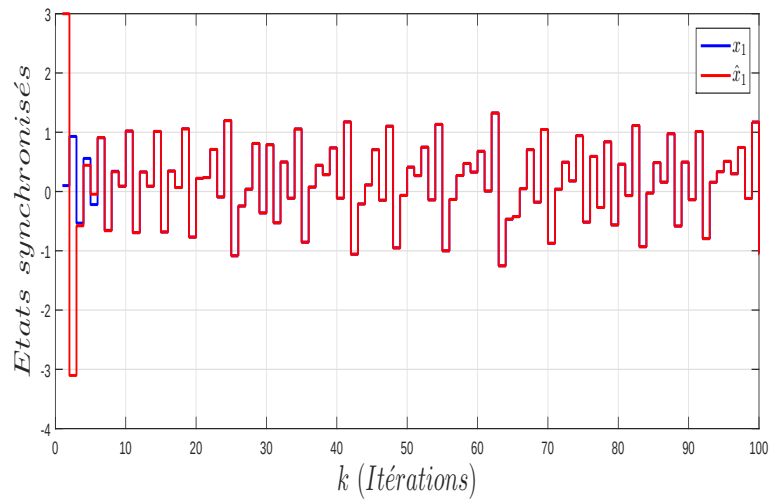


FIGURE 3.17 – Estimation de l'état x_1 du système de Lozi par l'observateur impulsif dans le cas non commensurable

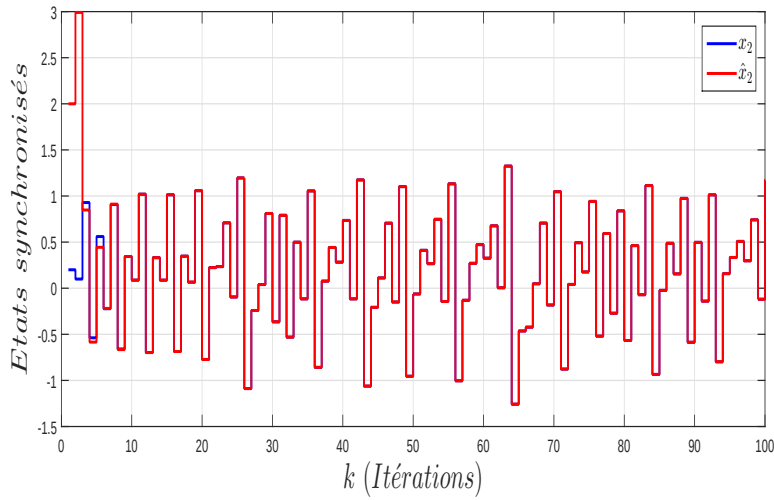


FIGURE 3.18 – Estimation de l'état x_2 du système de Lozi par l'observateur impulsif dans le cas non commensurable

que la synchronisation a toujours lieu même lorsque les valeurs des ordres fractionnaires de différences des états ne sont pas égales. Les évolutions des erreurs de synchronisation $e_1 = x_1 - \hat{x}_1$ et $e_2 = x_2 - \hat{x}_2$ sont affichées sur la figure 3.19. Comme nous pouvons le voir, les erreurs de synchronisation finissent par converger après un court régime transitoire.

Comme nous l'avons introduit et illustré lors du premier chapitre, les systèmes chaotiques sont très sensibles aux conditions initiales. Toutefois, le processus de synchronisation ne doit pas être affecté par cette caractéristique. Afin de vérifier ceci et d'observer l'effet de variations des conditions initiales, nous avons choisi des valeurs initiales largement différentes des états de l'observateur impulsif fractionnaire.

Les figures 3.20 et 3.21 montrent les résultats de synchronisation pour les valeurs initiales $(x_1(0), \hat{x}_1(0)) = (0.1, -17)$. Comme nous pouvons le voir, malgré le large écart sur la valeur initiale de l'état $\hat{x}_1(0)$, la synchronisation impulsive est bien établie. L'erreur de synchronisation affichée sur la figure 3.22 confirme le résultat précédent puisqu'elle converge après quelques itérations transitoires.

De même que pour l'état $\hat{x}_1$, nous pouvons conclure que le changement de la valeur initiale de l'état $\hat{x}_2$ n'affectera pas le processus de synchronisation. En effet, et à partir des figures

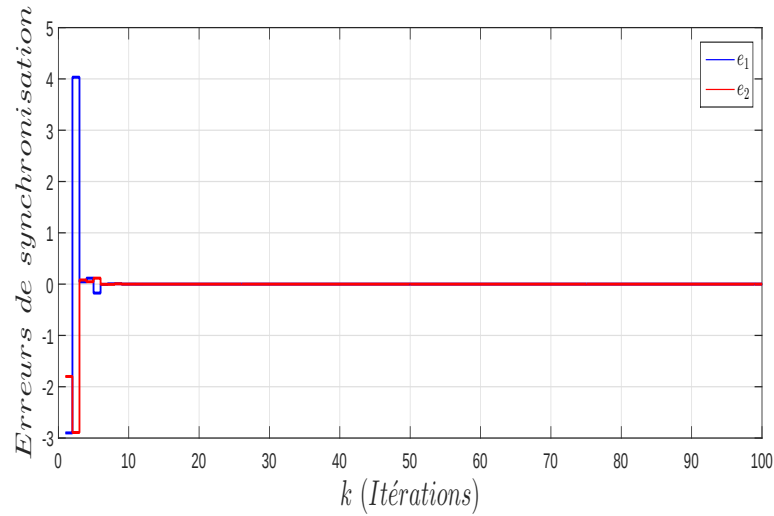
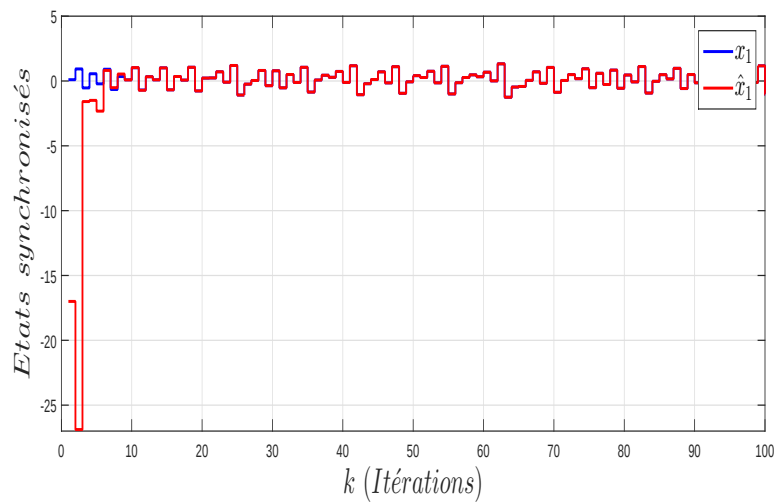


FIGURE 3.19 – Erreurs de synchronisation dans le cas non commensurable


FIGURE 3.20 – États synchronisés x_1 et $\hat{x}_1$ pour $\hat{x}_1(0) = -17$

3.23, 3.24 et 3.25, nous pouvons affirmer que la synchronisation impulsive a lieu même pour les valeurs $(x_2(0), \hat{x}_2(0)) = (0.2, 8)$.

3.4.4 Résultats expérimentaux

Dans cette partie, nous développerons l'implémentation de la synchronisation impulsive entre le système de Lozi d'ordre fractionnaire (3.36) et son observateur impulsif (3.37) sur cartes à microcontrôleurs de type Arduino-Mega.

La carte Arduino-Mega utilisée est illustrée sur la figure 3.26. C'est une carte à micro-

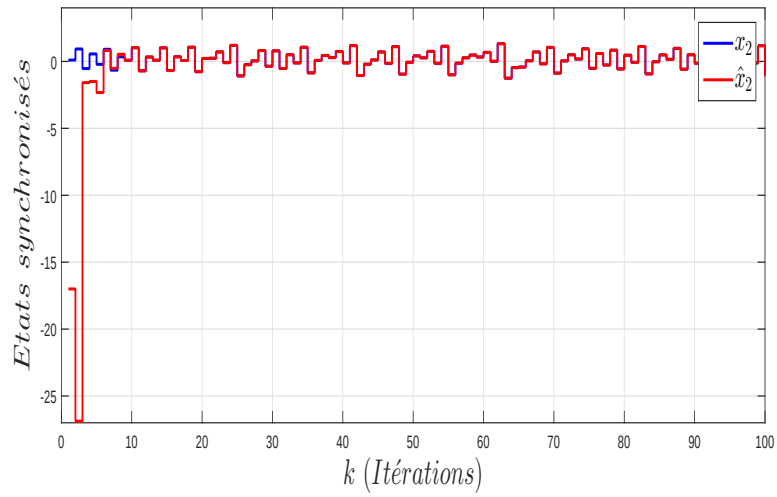


FIGURE 3.21 – États synchronisés x_2 et $\hat{x}_2$ pour $\hat{x}_1(0) = -17$

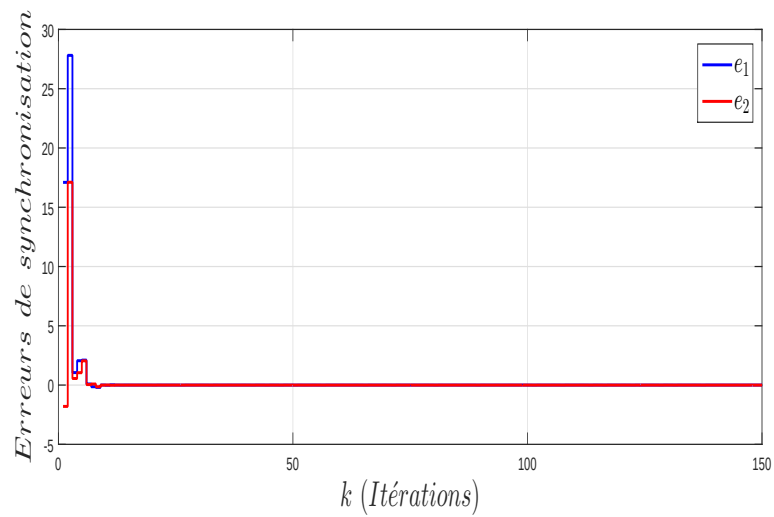


FIGURE 3.22 – Erreurs de synchronisation pour $\hat{x}_1(0) = -17$

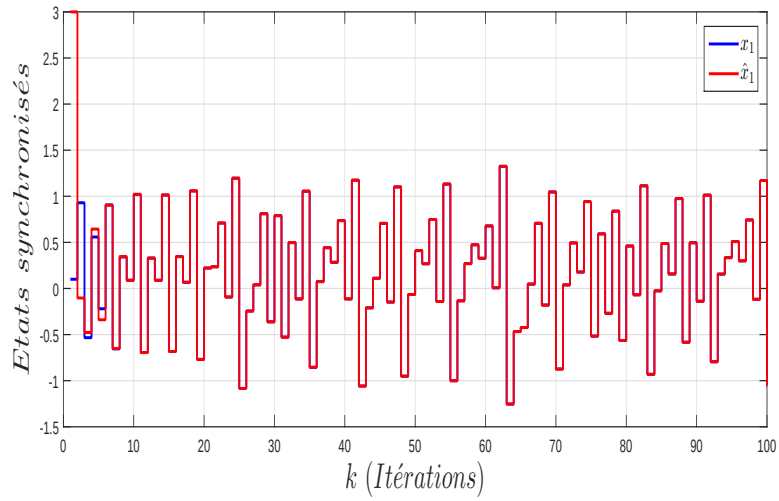


FIGURE 3.23 – États synchronisés x_1 et $\hat{x}_1$ pour $\hat{x}_2(0) = 8$

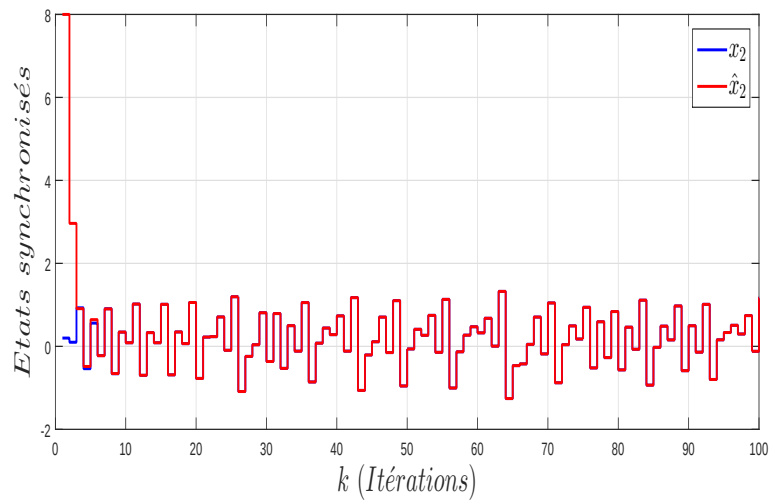
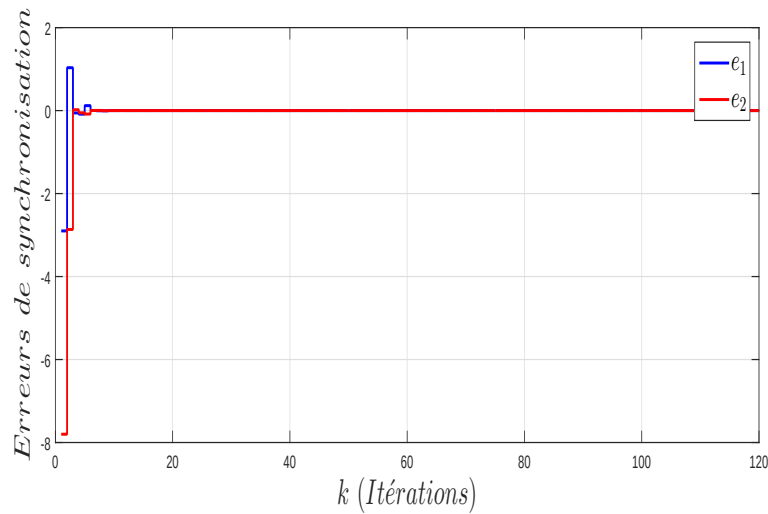


FIGURE 3.24 – États synchronisés x_2 et $\hat{x}_2$ pour $\hat{x}_2(0) = 8$

FIGURE 3.25 – Erreurs de synchronisation pour $\hat{x}_2(0) = 8$

contrôleur avec Hardware et Software open source. Il existe une large gamme de micro-contrôleurs avec différentes caractéristiques sur le marché. Toutefois, ils partagent tous la même propriété qui est la facilité de leur programmation [185]. En outre, les cartes Arduino fournissent un environnement de développement libre pour aider l'utilisateur à éditer, compiler puis charger les codes dans la carte.

Le composant de base de la carte Arduino Mega est le contrôleur de type Atmel ATmega328. Ce dernier fonctionne avec une fréquence de 16 Mhz et une mémoire limitée qui consiste en 32 kilobytes de sauvegarde et 2 kilobytes de RAM [219].

De plus, la carte Arduino Mega est équipée de 54 entrées/sorties, 16 entrées analogiques, 4 ports UART, un port USB, une tête ICSP et un bouton reset [220].

Dans notre cas, nous avons utilisé deux cartes Arduino-Mega. A l'aide d'un câble USB, nous avons chargé le code du système Lozi maître d'ordre fractionnaire dans la première carte, et le code de l'observateur impulsif d'ordre fractionnaire dans l'autre carte. la connexion entre les deux cartes est réalisée par un câble reliant le port TX de la première carte Arduino (système Maître de Lozi) au port RX de la deuxième carte (Observateur impulsif d'ordre fractionnaire). Les données sont codées sur 8 bits et transmises en série. Les codes du système de Lozi d'ordre fractionnaire et de l'observateur impulsif ont été programmés avec un langage similaire au langage C. Les deux algorithmes sont donnés dans les figures 3.27 et 3.28.

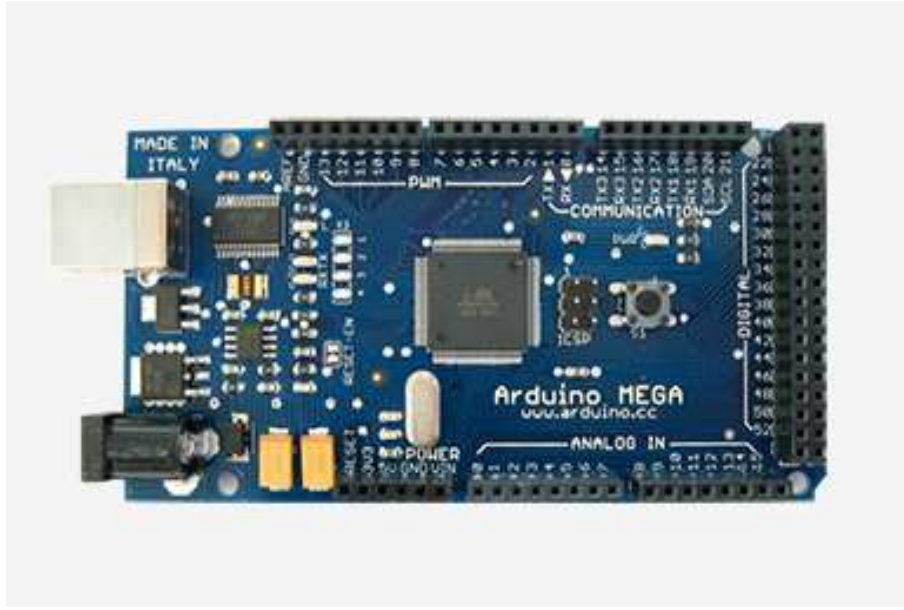


FIGURE 3.26 – Carte à microcontrôleur Arduino-Mega

Dans l'objectif de visualiser les résultats d'exécution des deux codes, nous avons utilisé deux ordinateurs individuels munis chacun d'une interface graphique écrite en Java. Les processus de connexion des deux cartes et de visualisation des résultats sont illustrés sur la figure 3.29.

Nous présenterons dans ce qui suit, les résultats expérimentaux de la synchronisation entre le système de Lozi d'ordre fractionnaire et son observateur impulsif. Nous commençons par la figure 3.30 qui illustre l'attracteur chaotique de Lozi présenté précédemment dans le chapitre 1.

Les états x_1 et x_2 du système de Lozi d'ordre fractionnaire (3.36) sont affichés dans la figure 3.31, le signal supérieur représente l'évolution chaotique de l'état x_1 et le signal en-dessous montre l'évolution chaotique de l'état x_2 .

La reconstruction des états du système de Lozi d'ordre fractionnaire par l'observateur impulsif a été effectuée avec succès en utilisant les cartes Arduino comme nous pouvons le voir dans la figure 3.32. Cinq signaux y sont affichés : Les deux signaux supérieurs représentent les états x_1 et $\hat{x}_1$, les deux évolutions qui suivent sont celles de x_2 et $\hat{x}_2$ et le dernier signal montre les impulsions de commande utilisées.

Chacun des plans de phases des états $x_1 - \hat{x}_1$ et $x_2 - \hat{x}_2$, donnés par les figures 3.33 et

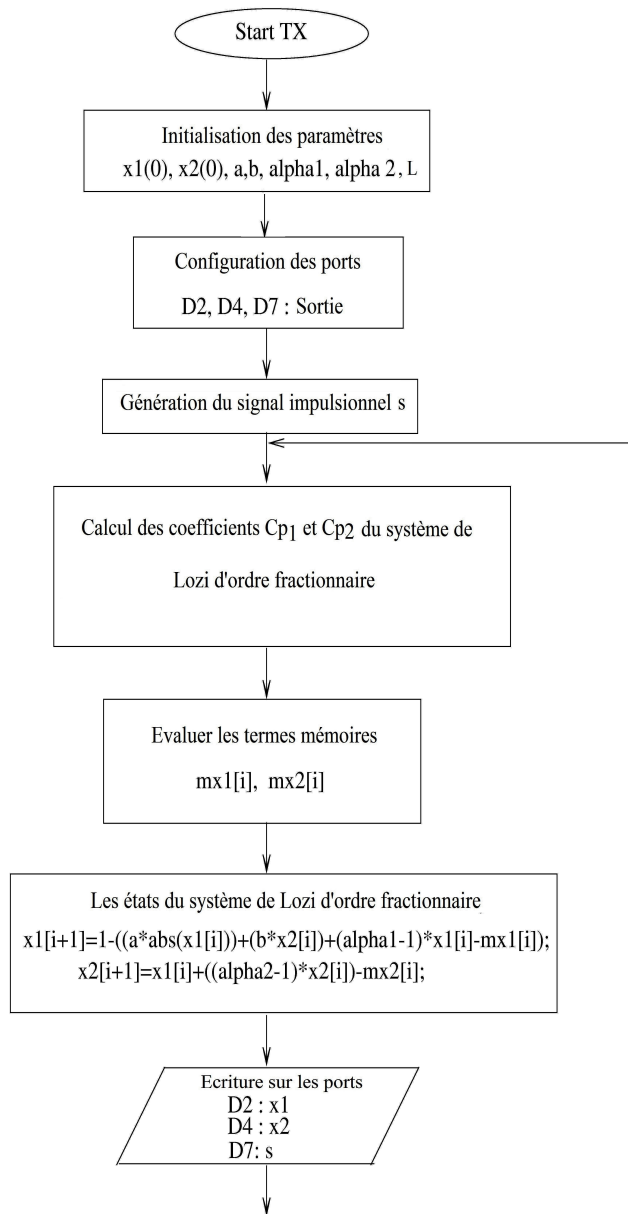


FIGURE 3.27 – Code du système de Lozi d'ordre fractionnaire

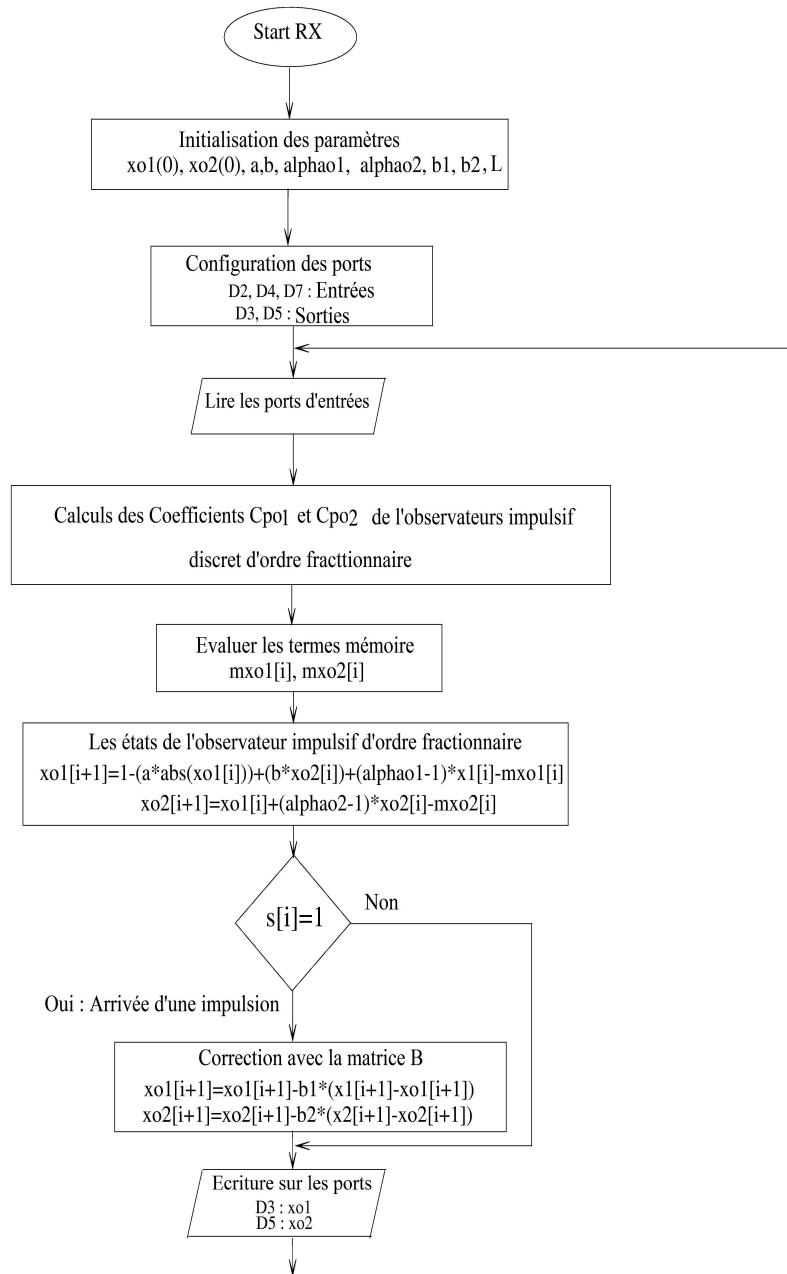


FIGURE 3.28 – Code de l'observateur impulsif d'ordre fractionnaire

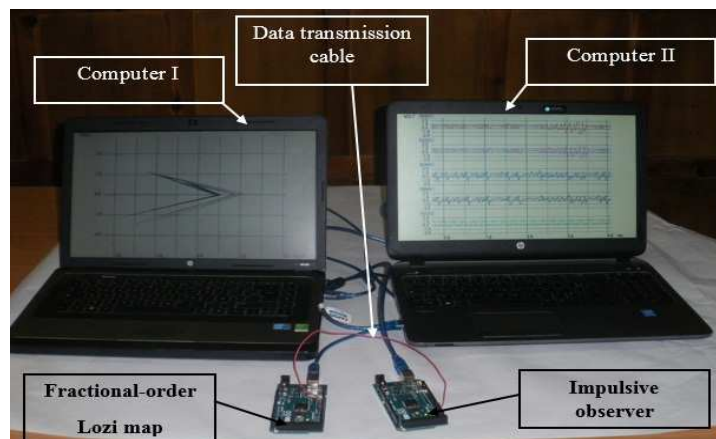


FIGURE 3.29 – Implémentation de la synchronisation impulsive sur cartes Arduino-Mega

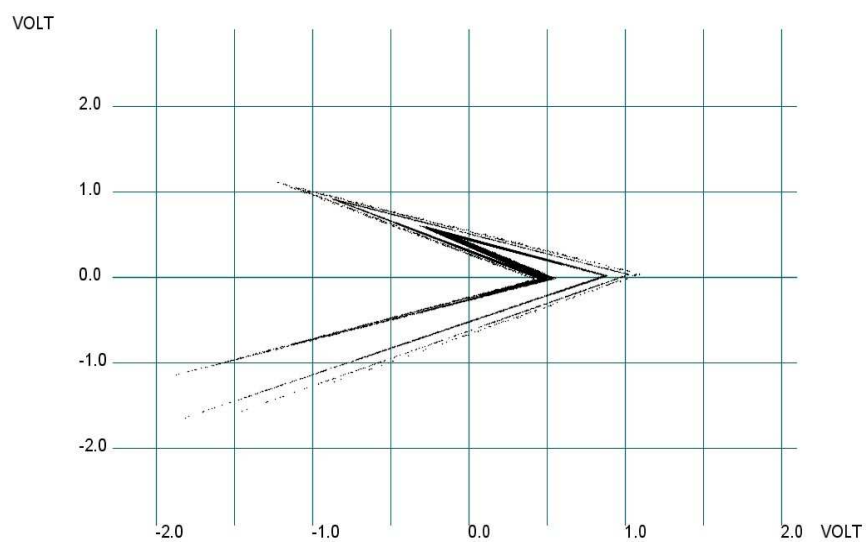


FIGURE 3.30 – Attracteur étrange du système de Lozi d'ordre fractionnaire en utilisant la carte Arduino-Mega (x_1 en abscisse et x_2 en ordonnée)

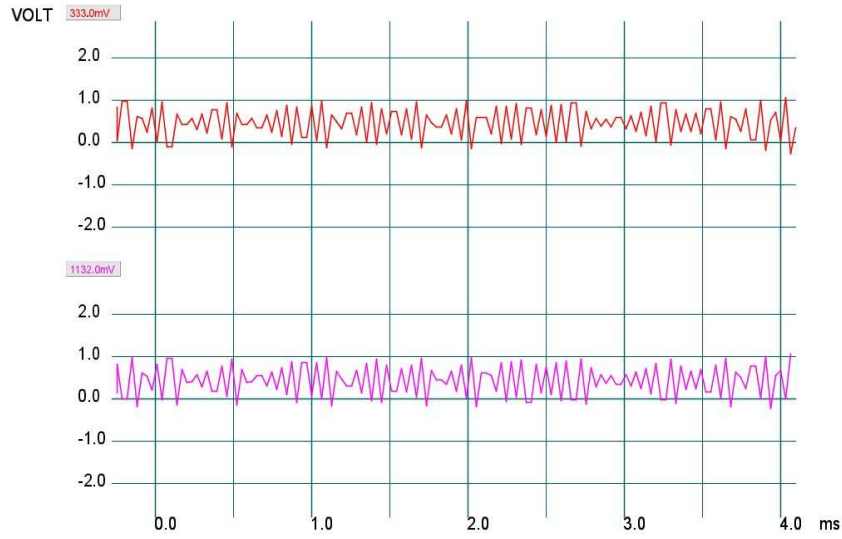


FIGURE 3.31 – Etats x_1 (signal supérieur) et x_2 (signal inférieur) du système de Lozi d'ordre fractionnaire

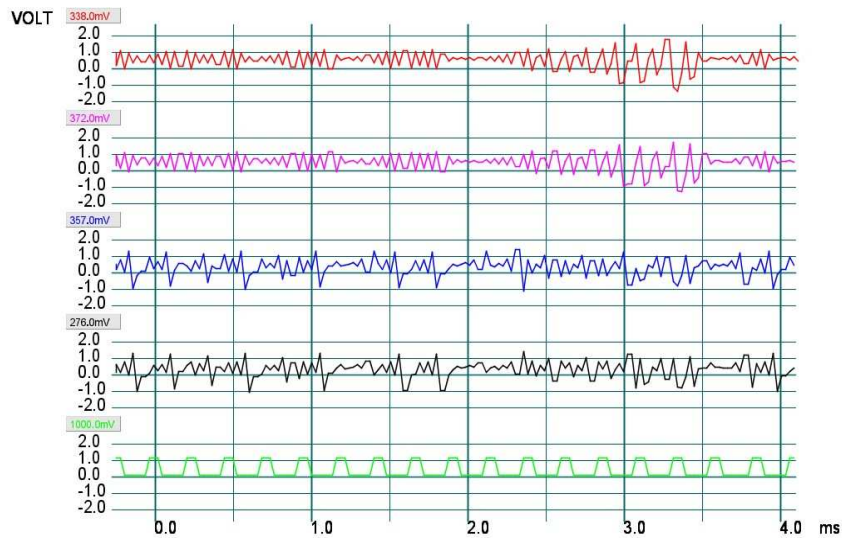


FIGURE 3.32 – Résultats de la synchronisation impulsive : (du haut vers le bas) : état x_1 , état estimé $\hat{x}_1$, état x_2 , état estimé $\hat{x}_2$ et les impulsions de contrôle

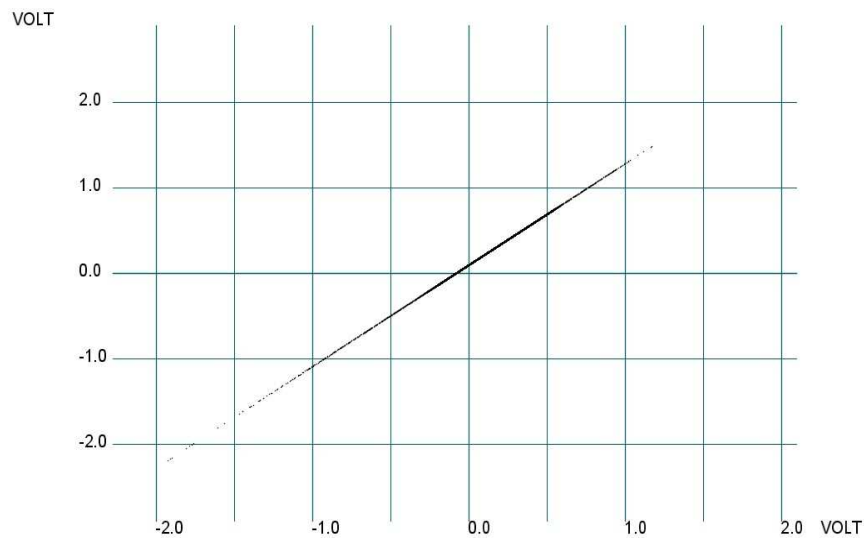


FIGURE 3.33 – Plan de phase des états synchronisés x_1 (en abscisse) et $\hat{x}_1$ (en ordonnée) obtenus par la carte Arduino-Mega

3.34, montre une ligne droite. Cela signifie que les états sont bien synchronisés.

3.5 Conclusion

Dans ce chapitre, nous avons étudié la possibilité de synchronisation des systèmes chaotiques discrets d'ordre fractionnaire en utilisant un observateur impulsif.

Nous avons d'abord présenté un bref état de l'art sur les méthodes de synchronisation proposées pour le cas des systèmes chaotiques d'ordre fractionnaire. Parmi ces méthodes, on retrouve la méthode de synchronisation impulsive. Toutefois, cette méthode a été étudiée uniquement dans le cas des systèmes d'ordre non entier continu et n'a pas été traitée dans le cas discret. Nous avons, pour cette raison, proposé un observateur discret de type impulsif d'ordre fractionnaire et avons défini des conditions suffisantes pour stabiliser le système d'erreur de synchronisation.

Le reste du chapitre a été consacré à l'application des résultats théoriques que nous avons obtenus pour le cas du système de Lozi d'ordre fractionnaire. Nous avons, en effet, présenté quelques résultats de la synchronisation impulsive simulée sous Matlab et constaté l'établissement de celle-ci et la reconstruction réussie des états du système de lozi d'ordre fractionnaire par l'observateur impulsif. Ces derniers résultats ont été validés par ceux de

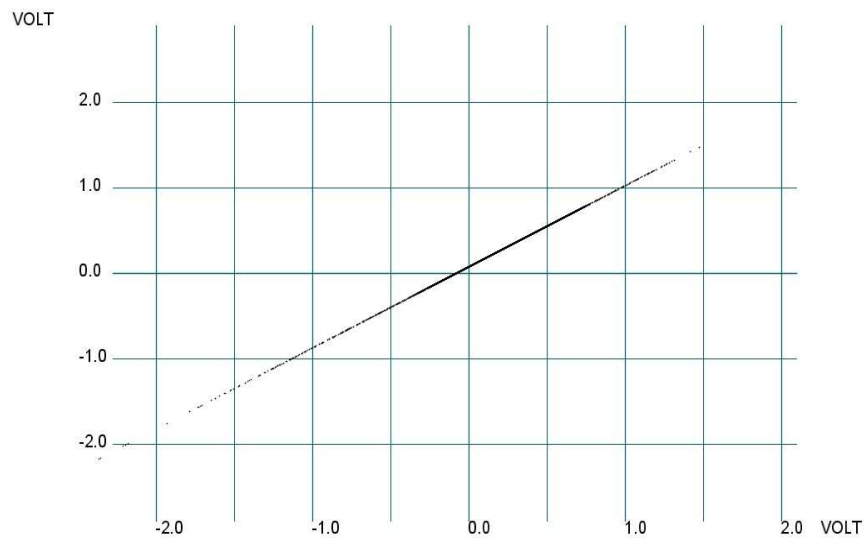


FIGURE 3.34 – Plan de phase des états x_2 (en abscisse) et $\hat{x}_2$ (en ordonnée) obtenus par la carte Arduino-Mega

l'implémentation du schéma de la synchronisation impulsive sur des cartes Arduino.

Afin d'illustrer l'efficacité de la méthode de synchronisation impulsive dans le cas de systèmes chaotiques discrets d'ordre fractionnaire, nous avons utilisé notre exemple de synchronisation impulsive dans un schéma de transmission sécurisée d'images couleur. La structure du système de communication sécurisée et les résultats obtenus feront l'objet du chapitre suivant.

Chapitre 4

Application de la synchronisation impulsive des systèmes chaotiques discrets d'ordre fractionnaire à la transmission sécurisée de données

4.1 Introduction

Au cours des dernières années, avec l'avènement des applications web et des sites de réseaux sociaux, la sécurité de l'information est devenue un défi majeur. En effet lors de la transmission, la confidentialité des données peut être compromise par un tiers [221]. Parmi les fichiers multimédias, les images et vidéos sont celles qui sont les plus recherchées, partagées et téléchargées. Cela les rend plus vulnérables à toutes sortes d'attaques et d'intrusions. En outre, et contrairement aux messages textes, les données images présentent des caractéristiques propres telles qu'une importante capacité , une redondance et une corrélation élevée entre ses pixels constitutifs [222]. La sécurité est l'un des objectifs majeur à atteindre lors de leur transmission sur le réseau et la cryptographie est la manière conventionnelle pour y arriver [223].

Le principe de la cryptographie, est de rendre l'information à transmettre illisible par

cryptage afin que seules les personnes autorisées puissent correctement récupérer l'information. Cette technique peut être appliquée aussi bien aux données simples que complexes telles les images et vidéos en utilisant différentes méthodes de chiffrement.

Récemment, le chiffrement d'images a suscité un intérêt croissant dû au fait que la plupart d'image comme les images militaires, les desseins d'architecture et les images médicales doivent être confidentielles entre l'expéditeur et le destinataire [224]. Plusieurs algorithmes de cryptage ont été proposés dans la littérature sur la base de différents principes . Parmi eux, les algorithmes de cryptage basés sur la théorie du chaos sont considérés comme très intéressants pour les applications pratiques car ils offrent une excellente combinaison de vitesse, sécurité, sensibilité et complexité [225].

Actuellement, et suite aux nombreux travaux et études fructueux sur les systèmes dynamique d'ordre fractionnaire, de nombreux chercheurs dans le domaine du cryptage à base du chaos, ont inclus les systèmes chaotiques d'ordre fractionnaire dans leurs schémas de transmission. En effet, et pour de nombreuses raisons, l'application des systèmes chaotiques d'ordre fractionnaire est plus intéressante que celle des systèmes chaotiques d'ordre entier dans les communications sécurisées [226]. Parmi ces raisons, on peut citer la complexité des dynamiques des systèmes chaotiques d'ordre fractionnaire et l'utilisation des ordres de dérivation comme clés secrètes de cryptage outre les paramètres de contrôle. Pour les raisons citées ci-dessus, nous avons utilisé le schéma de synchronisation des systèmes chaotiques discrets d'ordre fractionnaire à base d'observateur impulsif, présenté dans le chapitre précédent, pour la transmission d'images couleurs.

Après une introduction à la cryptographie, nous développerons les raisons d'utiliser les systèmes chaotiques d'ordre entier et fractionnaire pour le cryptage de données et présenterons un états de l'art des différents algorithmes et schémas proposés dans ce domaine. Nous décrirons ensuite le système de transmission proposé et illustrerons les résultats obtenus.

4.1.1 Introduction à la cryptographie

Comme nous l'avons mentionné dans l'introduction, la cryptographie est l'art et la science de sécurisation de l'information [227]. Elle est réalisée à travers deux procédures : le cryptage et le décryptage. Le cryptage est la modification du message de telle sorte que son contenu ne peut être reconstruit que par un légal récepteur tandis que le décryptage est la reconstruction du message original à partir du message crypté.

En utilisant la cryptographie pour la transmission de l'information, plusieurs objectifs sont atteints. Ces objectifs sont principalement comme suit [228] :

- la confidentialité : Aucun individu, hormis les personnes autorisées, ne peut comprendre le message transmis.
- L'authentification : Il s'agit de confirmer et tester l'identité d'une entité, en s'assurant que l'entité communicante est celle qu'elle prétend être.
- Intégrité : Assurer que le message reçu n'a été modifié d'aucune façon de sa forme originale.
- Non répudiation : C'est un mécanisme pour prouver que l'expéditeur a réellement envoyé le message, de sorte que le destinataire ne peut pas prétendre que le message n'a pas été envoyé.
- Contrôle d'accès : C'est un processus qui empêche l'utilisation non autorisée des ressources, c'est à dire, contrôler qui peut avoir accès aux ressources, quand il peut y avoir accès, sous quelle restrictions et conditions l'accès peut être accordé et enfin quel est le niveau d'autorisation d'un accès donné.
- Signature : C'est une méthode pour lier une information à une entité.

- Autorisation : Le propriétaire donne l'autorité à quelqu'un de faire quelque chose en son nom.

Les systèmes cryptographiques peuvent être classifiés selon plusieurs critères. Si on considère, par exemple, la manière de traiter les données, on distingue deux types de chiffrement : le *chiffrement par flot ou par flux* [229] (dit aussi *chiffrement en continu*) et le *chiffrement par bloc* [4]. La première classe consiste à traiter les données de longueur quelconque sans avoir à les découper. Ce chiffrement se présente souvent sous la forme d'un générateur de nombres pseudo-aléatoires avec lesquels on opère un XOR ou autre opération avec les bits provenant des données. Les chiffrements de données par flot les plus connus sont RC4, E0... etc. Le chiffrement par bloc, par contre, traite les données du texte clair (message original) par blocs, de taille généralement fixe. Des exemples de ce type de chiffrement sont les chiffrements DES [230], IDEA [231], BlowFish [232] et AES [233]. D'autre part, les algorithmes de cryptage sont aussi classés en algorithmes *symétriques* (également dits à *clé secrète*) et *asymétriques* (à *clés publique et privée*). Lors du cryptage symétrique, la même clé est utilisée pour le cryptage et le décryptage alors que les algorithmes asymétriques utilisent des clés différentes pour le cryptage et le décryptage. Un exemple de ce dernier type d'algorithmes est l'algorithme RSA [234].

4.2 Le chaos en cryptographie

La cryptographie à base de systèmes chaotiques consiste à utiliser la théorie du chaos dans les systèmes de transmission sécurisée de données. L'idée de l'utilisation de la théorie du chaos dans le cryptage semble avoir été posée il y a plus d'un demi-siècle, par Claude E. Shannon [235]. L'application du chaos en cryptographie a été une grande contribution pour améliorer la sécurité des données. Dans ce qui suit, nous développerons, plus en détail, l'histoire et les raisons de l'utilisation de la théorie du chaos en cryptographie.

4.2.1 Relation entre les systèmes chaotiques et les systèmes cryptographiques

Dans cette partie, nous présenterons, en détails, les motivations derrière l'utilisation des systèmes chaotiques en cryptographie. Il s'agit, en effet, de faire le lien entre les propriétés essentielles d'un système chaotique, citées auparavant, et les propriétés requises d'un système cryptographique [236].

- a) Un bon système cryptographique doit avant tout vérifier deux propriétés essentielles : la confusion et la diffusion.
 - La confusion est une propriété qui fait qu'il est difficile de faire le lien entre le texte en clair et le texte chiffré. Dans un système cryptographique, la confusion a lieu lorsque la règle de cryptage combinée avec la clé secrète rendent le processus de trouver l'algorithme liant les deux, très complexe. Cette propriété équivaut à l'ergodicité des systèmes chaotiques. Cette dernière propriété fait référence à une mesure statistique qui donne en moyenne le même résultat à travers le temps et à travers l'espace de l'attracteur chaotique. C'est cette propriété d'ergodicité qui assure que chaque intervalle de l'attracteur chaotique dans un système chaotique sera parcouru aussi continûment que le nombre d'itérations d'une condition initiale tend vers l'infini [237].
 - La diffusion signifie qu'un système cryptographique doit être sensible par rapport aux clés secrètes ainsi que par rapport au texte en clair. Ceci signifie qu'un petit changement dans la clé donnera lieu à un texte chiffré complètement différent. De même, un très léger changement au niveau du texte clair doit générer un texte chiffré totalement différent. Cette propriété coïncide avec la sensibilité aux conditions initiales et par rapport aux paramètres de contrôle (paramètres de bifurcation) des systèmes chaotiques.
- b) Comme nous l'avons expliqué, dans le premier chapitre, les signaux chaotiques présentent une allure qui semble aléatoire bien qu'ils soient déterministes. Cette carac-

Propriété chaotique	Propriété cryptographique	Description
Ergodicité	Confusion	La sortie a la même distribution à travers le temps et à travers l'espace de phase pour chaque entrée
Sensibilité aux conditions initiales	Diffusion	De petites variations sur l'entrée causent de grands changements sur la sortie
Dynamiques déterministes	Allure pseudo-aléatoire déterministe	Un processus déterministe peut engendrer un comportement pseudo-aléatoire
Complexité de la structure	Complexité de l'algorithme de cryptage	Un simple processus peut avoir une grande complexité

TABLE 4.1 – Comparaison entre les propriétés des systèmes chaotiques et les propriétés des systèmes cryptographiques

téristique permet à la fois d'utiliser le signal chaotique pour masquer l'information utile ou message (texte en clair) et de pouvoir la récupérer à la fin de la réception.

- c) La complexité de la structure des systèmes chaotiques est liée à la complexité de l'algorithme de cryptage où un simple algorithme peut produire des sorties complexes.

Le tableau (4.1) dresse une comparaison récapitulative entre les propriétés des systèmes chaotiques et les propriétés requises des systèmes cryptographiques [237].

4.2.2 Techniques de cryptage à base de systèmes chaotiques

Au cours des deux dernières décennies, de nombreux travaux ont été publiés sur la cryptographie basée sur le chaos. Plusieurs algorithmes de cryptage utilisant les systèmes chaotiques ont été proposés. Les schéma de chiffrement à base de systèmes chaotiques peuvent être classés en deux catégories : Les systèmes cryptographiques numériques et les systèmes cryptographiques analogiques. La première classe est destinée aux systèmes évoluant en temps discret alors que la deuxième classe concerne les systèmes chaotiques

évoluant aussi bien en temps continu qu'en temps discret et est basée sur la synchronisation du chaos [238]. Nous décrirons, dans ce qui suit, le principe, les approches et les schémas proposés dans chacune de ces classes.

4.2.2.1 Les systèmes cryptographiques numériques

Le premier travail publié sur le chiffrement à base de systèmes dynamique a été réalisé par Wolfram en 1985 ; il consiste en un algorithme de chiffrement de flux basé sur l'automatisation cellulaire [239]. Deux ans plus tard, un autre système cryptographique, à clé publique, similaire a été proposé par Guan [240]. En 1989, Matthews a publié le premier algorithme de chiffrement par flux, à base du chaos, qui a attiré l'attention de nombreux chercheurs [241]. A partir de là, et entre 1989 et 1992, plusieurs schémas de cryptage, exploitant la théorie chaos, ont vu le jour. A titre d'exemples, nous pouvons citer les travaux de Habutsu, Forré, Bersteinet et Erdmann [242]. Cependant, des études effectuées par Wheeler et Biham [243, 244] ont montré qu'une grande partie de ces systèmes souffrent de problèmes. Par conséquent, lors des cinq ans qui ont suivi, très peu d'algorithmes de cryptage basés sur le chaos ont été développés. C'est à partir de 1997, qu'un nombre considérable d'algorithmes cryptographiques basés sur le chaos ont été proposés. Les approches les plus utilisées sont le chiffrement par blocs, le chiffrement par générateurs chaotiques de nombres aléatoire et le chiffrement par fonctions de hachage [245].

a) Chiffrement par bloc

Le chiffrement par bloc comme nous l'avons présenté précédemment consiste en une transformation de blocs de bits du texte clair en blocs de même taille de bits du texte chiffré en utilisant une clé secrète. En 1991, Hubutsu proposa un nouveau schéma de cryptage à clé secrète en itérant une forme généralisée de l'application Tente chaotique. L'inconvénient de ce schéma était la taille du texte chiffré qui était plus large que celle du texte en clair. Plusieurs versions modifiées de l'algorithme de

Habutsu ont été proposées afin d'améliorer sa sécurité. En 1998, Baptisa proposa son schéma de chiffrement appliqué à la fonction logistique. Cet algorithme de cryptage a fait l'objet de plusieurs études et recherches [246] qui ont d'ailleurs souligné quelques inconvénients du schéma. A partir de 2001, plusieurs chercheurs ont proposés des algorithmes de chiffrement par bloc mais ces derniers ont été sujets à de nombreuses attaques et ont été cassés.

En 2009, Yang [247] a proposé un nouveau chiffrement par blocs basé sur la fonction logistique chaotique avec retour de sortie. Il a utilisé le retour de sortie pour assurer une meilleure sécurité que les autres schémas de cryptage déjà proposés. En 2011, un groupe de recherche mexicain a proposé un nouvel algorithme de chiffrement par bloc basé sur l'application Tente chaotique [248]. L'application chaotique Tente a été choisie pour générer une séquence de bits car elle n'a pas d'ilots de stabilité telles que dans une application logistique.

b) Chiffrement avec fonctions de hachage

Les fonctions de hachage sont très utilisées en informatique et en cryptographie. Une fonction de hachage prend en entrée un message de taille quelconque, applique une série de transformations et réduit ces données. On obtient à la sortie une chaîne de caractères hexadécimaux, le condensé qui résume en quelque sorte le fichier. Cette sortie a une taille fixe qui varie selon les algorithmes (128 bits pour MD5 et 160 bits pour SHA-1)[242].

Concevoir une fonction de hachage sécurisée basée sur les systèmes chaotiques a attiré davantage l'intérêt de la communauté scientifique grâce à ses caractéristiques qui répondent aux exigences de la fonction de hachage cryptographique. Wong a été le premier à combiner les systèmes chaotiques et la fonction de hachage dans un algorithme de cryptage [249]. Le schéma de chiffrement proposé utilise une table de correspondance dynamique au lieu d'une table statique. Toutefois, le schéma s'est avéré, plus tard, non sécurisé et inefficace. En 2005, une fonction de hachage basée sur une application Tente chaotique a été proposée dans [250] ; les messages d'entrée sont traités arbitrairement pour produire des valeurs de hachage de deux fois la

longueur du bloc de message d'entrée. Plusieurs analyses de sécurité statistiques ont été appliquées, et ont montré que le schéma de hachage proposé est assez fort contre tous les types d'attaques et est plus efficace que le schéma de hachage de Wang. Plusieurs autres schémas de cryptage ont été proposés par la suite. Par exemple, Xiao présenta une nouvelle fonction de hachage à base d'une application chaotique unidimensionnelle et avec des paramètres changeables [251]. Dans le même contexte, J. Zhang *et al.* développèrent en 2007 une fonction de hachage à base d'un filtre digital non linéaire [252]. Les auteurs décrivent leur algorithme comme étant facile à implémenter matériellement et aussi de manière logicielle et présentant de bonnes propriétés cryptographiques.

c) Chiffrement par générateurs chaotiques de séquences pseudo-aléatoires

Une autre idée intéressante pour utiliser les systèmes chaotiques en cryptographie est de les utiliser en tant que générateurs de séquences pseudo-aléatoires. En effet, comme les systèmes chaotiques génèrent des résultats imprévisibles, de nombreux chercheurs ont été tentés par leur utilisation comme générateurs de nombres pseudo-aléatoires [253]. Les résultats des générateurs de nombres pseudo-aléatoires (PRNGs) sont principalement utilisés dans les algorithmes de chiffrement par flot en tant que clés, auxquelles on applique XOR avec du texte en clair, afin de générer le texte chiffré.

Les cellules automatisées introduites au préalable dans cet état de l'art, ont été utilisées pour générer des séquences pseudo-aléatoires. Le message chiffré est alors obtenu par l'application d'un XOR entre les bits du message original et ceux des nombres générés.

En outres, Shujuna proposa, en 2001, un générateur de séquence binaire pseudo-aléatoire basé sur les systèmes chaotiques couplés [254]. L'utilisation de deux systèmes chaotiques différents, au lieu d'un seul, est dans le but de fournir une plus grande sécurité, selon les auteurs. Dans la même année, une autre nouvelle approche de chiffrement par flux basée sur une application logistique a été proposée [255]. Le

nouveau schéma utilise deux ou plusieurs systèmes chaotiques pour générer des séquences pseudo-aléatoires. Les auteurs ont utilisé deux trajectoires proches de la fonction logistique pour générer la séquence pseudo-aléatoire. Le texte en clair a été chiffré par la séquence générée avec l'opérateur XOR pour donner le texte chiffré. Le chercheur Skrobek a toutefois souligné, en 2007, les inconvénients de cet algorithme et montré comment le casser [256]. D'autres schémas ont été proposés plus tard. Le principe reste le même toutefois, les nouveaux algorithmes diffèrent de ceux que nous venons de décrire par le nombre de systèmes chaotiques utilisés pour la génération des nombres pseudo-aléatoires [257], par les éléments ajoutés comme les filtres numériques [258] ou par les opérations effectuées comme les permutations [259] pour renforcer leur sécurité.

4.2.2.2 Systèmes cryptographiques analogiques

Les systèmes de communication développés à base de la synchronisation des systèmes chaotiques peuvent être classés, selon l'algorithme de cryptage utilisé, en quatre sous-catégories : Le cryptage par addition [260], le cryptage par commutation [261], le cryptage par modulation [262] et le cryptage par inclusion.

Bien que plusieurs algorithmes de cryptage, utilisant les systèmes chaotiques synchronisés, ont été développés, la majorité d'entre eux sont les résultats de modifications ou de généralisation des quatre schémas de bases cités. Pour cette raison, nous définirons en détail, dans ce qui suit, chacun de ces schémas.

a) Cryptage par addition

La première et plus simple approche de cryptage de données, à base de la synchronisation des systèmes chaotiques, est l'approche par addition. Le principe de cette méthode consiste à additionner le signal message $m(t)$ à un signal $x(t)$ généré par un système chaotique pour former un signal crypté $s(t) = m(t) + x(t)$. Une fois la synchronisation établie entre l'émetteur et le récepteur, une estimation de $x(t)$ peut être obtenue au niveau du récepteur et sera donc soustraite de $s(t)$ pour récupérer le message. La figure 4.1 illustre le principe de cryptage par addition.

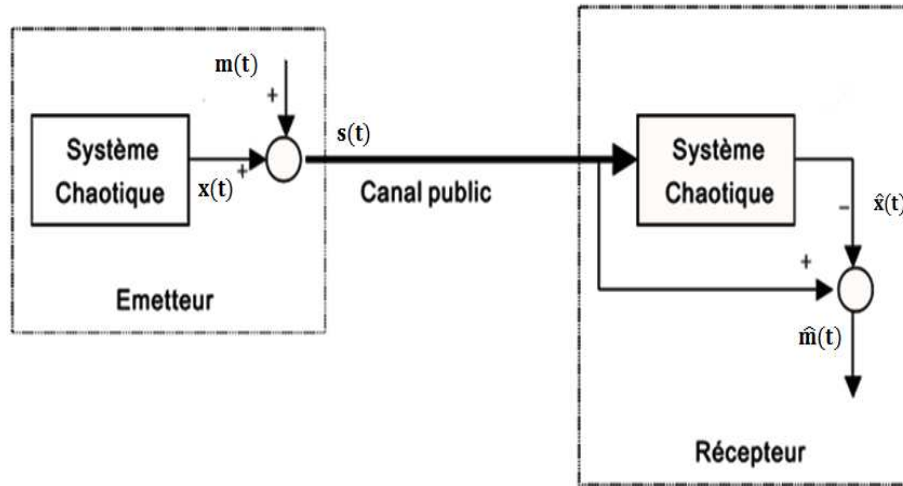


FIGURE 4.1 – Principe du cryptage par addition

Dans le but d'éviter l'effet négatif du signal message sur le processus de synchronisation, l'amplitude du signal message doit être très inférieure à celle de la porteuse chaotique $x(t)$. En effet, si le message perturbe le signal porteuse, la synchronisation ne sera pas établie correctement et par conséquent, le signal $m(t)$, récupéré à la fin de réception, sera différent du message original. L'inconvénient du cryptage par addition est la sécurité médiocre face aux diverses attaques. En effet, un intrus peut toujours obtenir quelques informations à partir du signal $s(t)$ [263].

b) Cryptage par commutation chaotique

Ce schéma de transmission est principalement destiné à la transmission de signaux numériques. Au niveau de l'émetteur, deux systèmes chaotiques différents sont utilisés pour les bits à 0 et à 1, respectivement, du signal message. Ainsi, le système chaotique utilisé est commuté de temps en temps par le signal message. Au niveau du récepteur, seulement un des systèmes chaotiques est requis et les bits du message

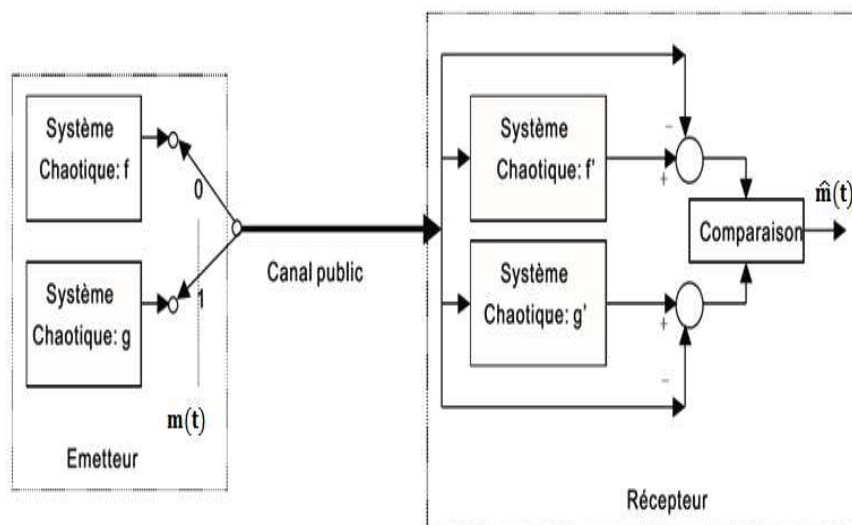


FIGURE 4.2 – Principe du cryptage par commutation

peuvent être récupérés selon que le système esclave se synchronise ou non avec le système maître.

La figure 4.2 illustre le principe de cryptage par la méthode de commutation. Pour assurer la synchronisation entre les systèmes maître et esclave, le temps de transmission de chaque bit du signal message doit être assez long. Par conséquent, le temps de transmission dans un schéma de cryptage par commutation est généralement plus lent que celui du cryptage par addition. En outre, le cryptage par commutation tel qu'il est présenté ci-dessus n'est pas sécurisé face à plusieurs types d'attaques [263]. Afin d'améliorer la sécurité de transmission, plusieurs modifications ont été apportées au schéma de commutation ces dernières années.

D'autre part, l'avantage principal de la commutation chaotique est que le signal message peut-être correctement récupéré même dans le cas où le taux signal utile sur bruit est très faible.

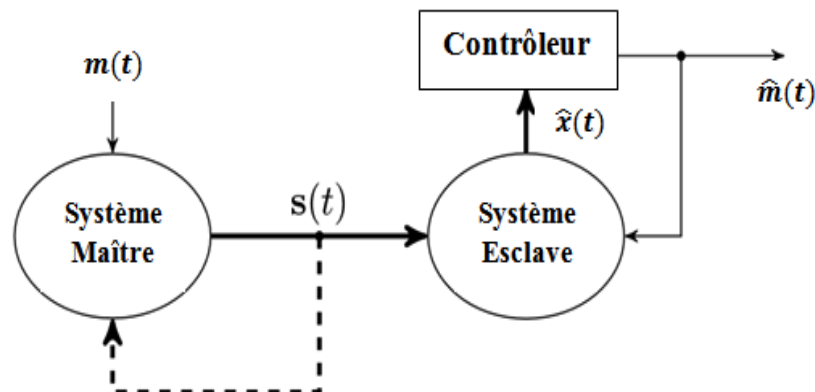


FIGURE 4.3 – Principe du cryptage par modulation chaotique

c) Cryptage par modulation chaotique

Dans un schéma de chiffrement par modulation chaotique, le message m est introduit dans le système maître de telle manière que ses dynamiques sont changées continuellement par le signal message. Dans ce cas, un contrôleur adaptatif est généralement utilisé avec le système esclave, au niveau du récepteur, afin de faire converger asymptotiquement sa sortie $\hat{m}$ vers m . La figure 4.3 illustre la structure de base d'un système de cryptage par modulation chaotique. Il est à noter que dans certains schémas, il peut ne pas y avoir de retour de $s(t)$ vers le système maître.

Il existe deux types de modulation chaotique : la modulation paramétrique [264] et la modulation directe [265]. Dans le premier type, le signal message m module les valeurs de l'un ou plusieurs paramètres de contrôle du système chaotique de l'émetteur. Dans le cas de modulation directe, le message m est injecté dans une ou plusieurs variables du système maître sans pour autant changer la valeur d'aucun paramètre de contrôle [263]. Comparé au schéma de cryptage par commutation, qui est destiné seulement à la transmission d'un signal numérique, les schémas basés sur la modulation chaotique présentent plus de performances. En effet, la technique de modulation chaotique peut même être utilisée pour la transmission de plusieurs

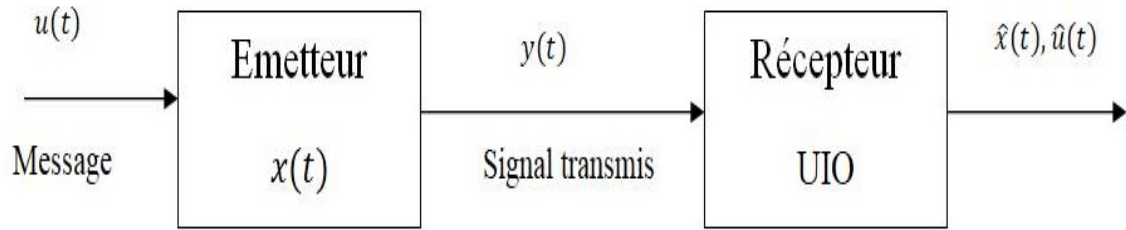


FIGURE 4.4 – Cryptage par inclusion et décryptage par Observateur à entrées inconnues

messages à la fois. L'une des manières de le faire consiste à moduler n paramètres de contrôle du système maître avec n signaux messages respectivement.

L'inconvénient majeur de la transmission par modulation chaotique est que le contrôleur adaptatif dépend de la structure des systèmes maître et esclave. Ce qui implique que plusieurs contrôleurs doivent être développés pour différents systèmes maîtres. En outre, le contrôleur peut même ne pas exister dans certains cas.

d) Cryptage par Inclusion

La technique de cryptage par inclusion consiste à injecter le message dans la dynamique de l'émetteur [266]. La restauration de l'information est effectuée par deux techniques. L'une repose sur les observateurs à entrée inconnue. L'autre technique est basée sur l'inversion du système émetteur. Le décryptage du message crypté par inclusion en utilisant un observateur à entrée inconnue UIO (Unknown Input Observer), est illustré sur la figure 4.4. Dans ce type de schéma, il est nécessaire de reconstruire l'état $x(t)$ du système émetteur et également l'entrée inconnue $u(t)$ qui est le message [26].

Le principe de décryptage par l'inversion du système émetteur et illustré sur la figure 4.5 consiste à concevoir le récepteur du message en inversant le modèle de l'émetteur.

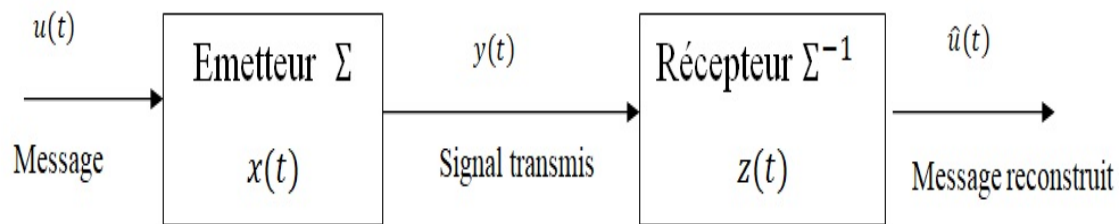


FIGURE 4.5 – Cryptage par inclusion et décryptage par Inversion du modèle de l'émetteur

4.2.3 Schémas de transmission de données à base de systèmes chaotiques d'ordre fractionnaire

Afin de renforcer les systèmes de transmissions à base de systèmes chaotiques et d'améliorer leurs sécurité, une nouvelle idée commence à prendre de l'ampleur ces dernières années et à attirer plus d'attention. Elle consiste à utiliser les systèmes chaotiques d'ordre fractionnaire dans les algorithmes de chiffrement. En effet, il s'est avéré que les systèmes de transmission à base de systèmes chaotiques fractionnaires sont plus sécurisés et robuste que les algorithmes de chiffrement classiques ou ceux basés sur les systèmes chaotiques d'ordre entier. Les principaux avantages de cette nouvelle technique de chiffrement est la complexité élevée apportée à l'algorithme de chiffrement et l'augmentation du nombre de clés secrètes.

Dans son travail séminal, B. Kiani et *al.* ont proposé une technique de communication basée sur les systèmes chaotiques d'ordre fractionnaire et sur l'utilisation d'un estimateur d'états d'ordre fractionnaire de type filtre de Kalman étendu [210]. Sheu et *al.* de leurs côté ont proposée une version modifiée d'un schéma de transmission à deux canaux, à base de la théorie du chaos, en utilisant les systèmes chaotiques d'ordre fractionnaire [267]. En outre, dans [268], le système chaotique de Chen d'ordre fractionnaire a été inclus dans un schéma de transmission afin d'élargir l'espace de clés et ainsi améliorer le niveau de sécurité. Muthukumar *et al.* ont étudié la synchronisation multi-échelle dans le système chaotique d'ordre fractionnaire King Cobra et la commande par mode glissant des systèmes chaotiques d'ordre fractionnaire pour le chiffrement d'images [269]. Les sys-

tèmes hyperchaotiques ont aussi été utilisés pour la transmission d'informations secrètes. Un schéma de chiffrement d'images couleur a d'ailleurs été proposé par Huang *et al.* en appliquant les systèmes hyperchaotiques d'ordre fractionnaire [270]. Un autre algorithme de cryptage utilisant le système hyperchaotique de Lorenz d'ordre fractionnaire a été présenté par Zhen *et al.* dans leur article [271].

L'application des systèmes chaotiques d'ordre fractionnaire en communication sécurisées n'est pas limitée au cas de systèmes continus. En fait, plusieurs systèmes chaotiques discrets d'ordre fractionnaire ont servi à la génération de séquences chaotiques et au chiffrement de données. A titre d'exemple, la fonction logistique retardée a été utilisée par Zhen *et al.* dans un nouvel algorithme de cryptage d'images [18]. En outre, et dans leur travail, Liu *et al.* ont introduit un nouveau système chaotique d'ordre fractionnaire à deux dimensions, à base de différences d'ordre fractionnaire, et l'ont appliqué pour le chiffrement d'images [272].

Par ailleurs, plusieurs travaux ont été effectués au sein de notre laboratoire L2CSP dans le cadre de la transmission sécurisée de données à base de systèmes chaotiques en général et des systèmes chaotiques d'ordre fractionnaire en particulier. Concernant cette dernière thématique, nous pouvons citer, entre autres, le schéma de transmission de données proposé par Hamiche *et al.* et basé sur les systèmes chaotiques discrets d'ordre fractionnaire [273]. Un autre système de transmission a été présenté par Djennoune *et al.* dans [274]. Les auteurs y ont appliqué la synchronisation du système chaotique d'ordre fractionnaire de Chua, via un observateur à modes glissants, dans un système de communication de données. De plus, et dans leur article [211], les auteurs ont proposé un nouveau schéma de transmission d'images à base du système chaotique de Hénon modifié d'ordre fractionnaire et d'un observateur retardé étape par étape d'ordre fractionnaire. Deux méthodes de synchronisation à base de systèmes chaotiques discrets d'ordre fractionnaire ont été présentées et appliquées pour la transmission d'images dans [19]. De même, un autre système de transmission hybride, à base de deux méthodes de synchronisation de systèmes chaotiques d'ordre fractionnaire et de deux types d'observateurs, a été proposé et développé dans [275].

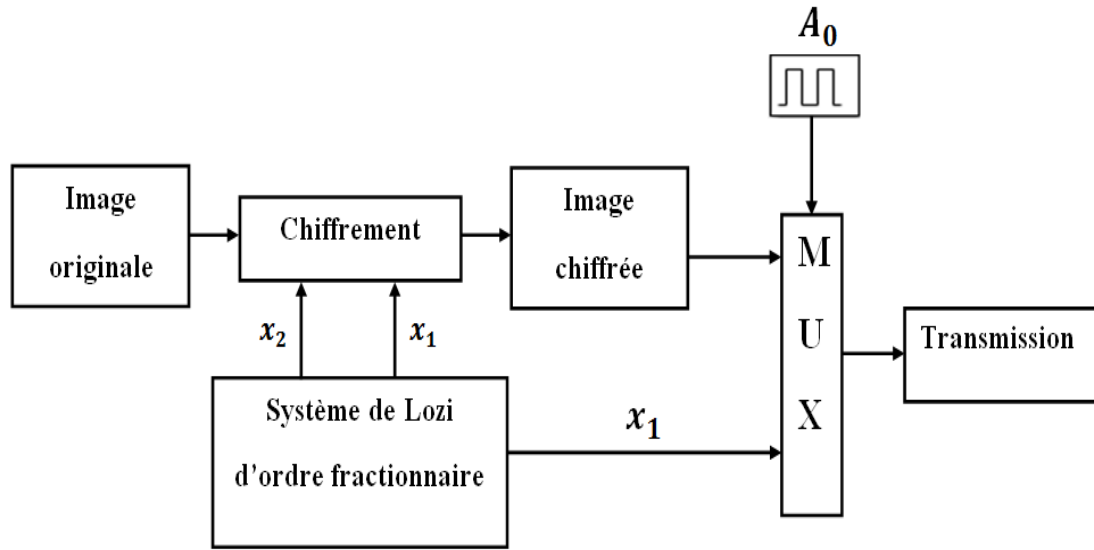


FIGURE 4.6 – Diagramme bloc de l'émetteur du schéma de transmission proposé

4.3 Transmission d'images à base de la synchronisation impulsive des systèmes chaotiques discrets d'ordre fractionnaire

Dans cette partie, nous décrirons en détail le système de transmission d'images couleur proposé à base de la synchronisation impulsive des systèmes chaotiques discrets d'ordre fractionnaire. Ce dernier est composé d'un émetteur, d'un récepteur et d'un seul canal de transmission. Les figures 4.6 et 4.7 présentent respectivement les diagrammes bloc de l'émetteur et du récepteur du système de transmission proposé.

Nous développerons dans la suite de cette section, et dans l'ordre, le rôle que joue chaque élément de ces deux blocs.

4.3.1 Structure de l'émetteur

L'émetteur est constitué de trois sous-blocs fonctionnels : Un générateur chaotique d'ordre fractionnaire, un algorithme de cryptage et un multiplexeur pour une utilisation appropriée du canal de transmission.

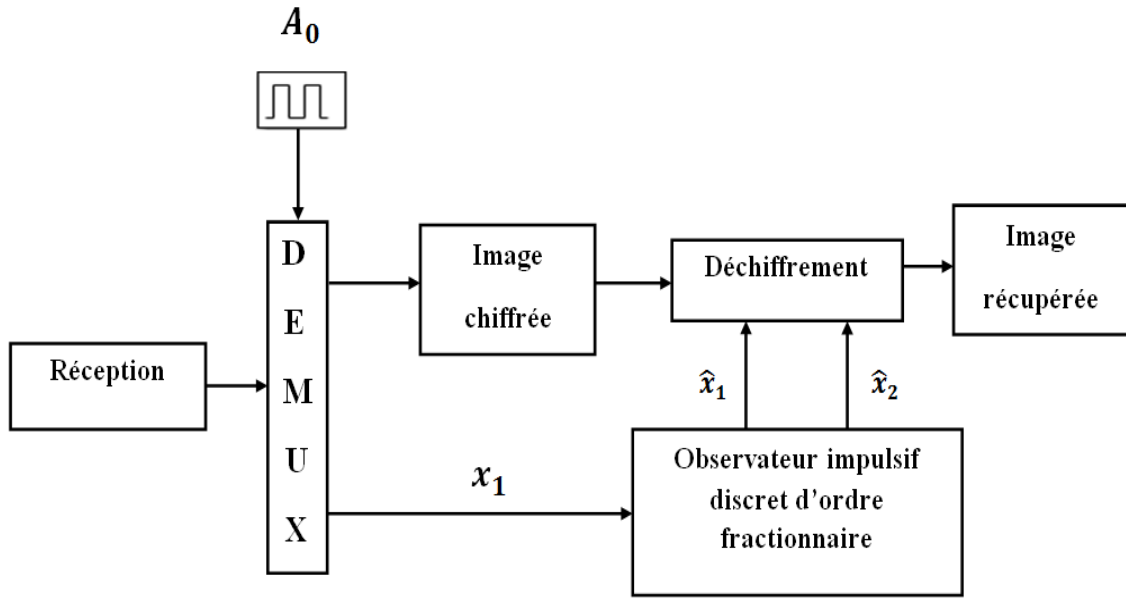


FIGURE 4.7 – Diagramme bloc du récepteur du schéma de transmission proposé

4.3.1.1 Le générateur chaotique d'ordre fractionnaire

Le générateur de séquences chaotiques que nous avons choisi, est le système de Lozi d'ordre fractionnaire maître donné par sa représentation d'état (3.36) dans le troisième chapitre. Dans notre application, seul l'état x_1 sera envoyé comme signal de synchronisation à l'arrivée des instants k_i . La sortie y du système sera alors

$$y(k) = \begin{cases} x_1(k) & \text{si } k = k_i \\ 0 & \text{si } k \neq k_i \end{cases} \quad (4.1)$$

4.3.1.2 L'algorithme de chiffrement

Les étapes effectuées pour chiffrer l'image originale sont décrites comme suit :

- *Etape 1* : L'image couleur originale est représentée par une matrice $I_{M \times N \times P}$ où M est le nombre de lignes, N est le nombre de colonnes et P est le nombre de composantes couleurs. Dans le cas d'une image à niveaux de gris, $P = 1$. Dans le cas d'une image couleur, $P = 3$. Les pixels de l'image sont ensuite rangés, en ordre, de la gauche vers la droite, du haut vers le bas, de la composante rouge R vers la composante verte G , pour une image couleur, pour former un ensemble de

valeurs décimales $V = \{V_{1,1,1}, \dots, V_{M,N,1}, V_{1,1,2}, \dots, V_{M,N,2}, V_{1,1,3}, \dots, V_{M,N,3}\}$ correspondant à l'image I .

- *Etape 2* : Deux séquences chaotiques $Z_1(i)$, $i = 1, 2, \dots, M \times N \times P$ et $Z_2(i)$, $i = 1, 2, \dots, M \times N \times P$ sont générées à partir de deux fonctions non linéaires f_1 et f_2 ayant comme variables d'entrées, les états x_1 et x_2 du système de Lozi d'ordre fractionnaire (3.36). Dans notre cas, les deux séquences sont définies comme suit :

$$Z_1(i) = f_1(x_1, x_2) = \frac{1}{3}(-4x_1(i) - 2x_2(i) + x_1(i)x_2(i)) \quad (4.2)$$

$$Z_2(i) = f_2(x_1, x_2) = \frac{1}{2}(4x_1(i) - 2x_2(i) - x_1(i)x_2(i)) \quad (4.3)$$

- *Etape 3* : Pré-traitement des séquences Z_1 et Z_2 et génération de deux nouvelles séquences entières positives Z'_1 et Z'_2 [276].
- *Etape 4* : Conversion des séquences V , Z'_1 et Z'_2 en séquences binaires V_B , Z'_{1B} et Z'_{2B} dont chaque élément est codé sur 8 bits.
- *Etape 5* génération d'un ensemble chiffré binaire BI de taille $M \times N \times P$ tel que

$$BI = Z'_{1B} \oplus (Z'_{2B} \oplus V_B)$$

Remarque 21 la séquence BI obtenue est une matrice binaire de $M \times N \times P$ lignes et 8 colonnes.

- *Etape 6* : Retourner les éléments de la matrice BI de gauche à droite et du haut vers le bas et génération d'une nouvelle matrice BI_F .
- *Etape 7* : Transformation de la séquence BI_F en une séquence décimale $E = E_1, E_2, \dots, E_{M \times N \times P}$ qui constitue, une fois, les éléments arrangés, l'image couleur chiffrée I_C .

Remarque 22 Les séquences Z_1 et Z_2 sont obtenues par simulation du système de

Lozi d'ordre fractionnaire (3.36) pour un nombre d'itérations j supérieur à $M \times N \times P$. En supposant que la synchronisation a lieu à l'instant $k = k_s$, il est important de considérer seulement les valeurs obtenues à partir de l'instant $k \geq k_s$ afin de dépasser le régime transitoire situé avant la convergence des erreurs de synchronisation. Dans le cas contraire, l'image ne sera pas correctement récupérée au niveau du récepteur.

4.3.1.3 Le multiplexeur

Comme nous l'avons introduit lors du chapitre précédent, la synchronisation impulsive présente l'avantage d'appliquer les signaux de synchronisation à des instants discrets $k_i \in k$. On peut alors, exploiter l'absence de ces signaux sur le canal pour envoyer d'autres données ou informations et éviter d'utiliser un canal supplémentaire.

Afin d'établir la synchronisation impulsive, des échantillons de x_1 sont envoyés, aux instants $k = k_i$, vers le récepteur. En dehors de ces instants, la séquence E correspondant à l'image chiffrée I_C est transmise sur le même canal. Le rôle du multiplexeur MUX est donc d'ordonnancer l'envoi des deux signaux x_1 et E

La sortie du multiplexeur MUX , qu'on notera S peut alors être exprimée comme suit :

$$S(k) = x_1(k)A_0(k) + E(k)(1 - A_0(k)) \quad (4.4)$$

où A_0 est l'entrée d'adresse du multiplexeur définie comme suit

$$A_0(k) = \begin{cases} 1 & \text{si } k = k_i \\ 0 & \text{si } k \neq k_i \end{cases} \quad i = 1, 2, \dots \quad (4.5)$$

4.3.2 Structure du récepteur

Tout comme l'émetteur, le bloc récepteur comprend trois éléments : Un démultiplexeur noté $DEMUX$, un observateur impulsif d'ordre fractionnaire afin d'estimer les états du système chaotique d'ordre fractionnaire de Lozi maître et un bloc de décryptage pour déchiffrer l'image originale envoyée. Nous développerons ci-dessous, la structure de chaque élément.

4.3.2.1 Le démultiplexeur

Le démultiplexeur *DEMUX* a pour rôle d'envoyer sur l'une de ces deux sorties le signal S reçu à l'entrée du récepteur. Tout comme le multiplexeur, l'entrée d'adresse A_0 a pour rôle de séquencer l'envoi du signal S vers l'observateur impulsif d'ordre fractionnaire et vers le bloc de décryptage comme suit :

- Si $A_0(k) = 1$, alors $k = k_i$. Le signal $S(k)$ est un échantillon du signal de synchronisation $x_1(k)$ du système (3.36) et sera donc envoyé vers l'observateur impulsif discret.
- Si $A_0(k) = 0$, alors $k = k_i$. Le signal $S(k)$ est un élément de la séquence $E(k)$ correspondant aux pixels de l'image chiffrée I_c .

4.3.2.2 L'observateur impulsif discret d'ordre fractionnaire

Afin d'estimer les états x_1 et x_2 , nous avons utilisé l'observateur impulsif d'ordre fractionnaire (3.37) proposé dans le chapitre précédent.

Comme nous envoyons un seul signal de synchronisation, dans notre cas, la matrice de gains de contrôle B est choisie constante et égale à

$$B = \begin{pmatrix} b_1 & 0 \\ 0 & 0 \end{pmatrix}$$

où $0 < |b_1| < 1$ est un gain de contrôle constant.

4.3.2.3 L'algorithme de décryptage

Une fois les valeurs des états x_1 et x_2 sont correctement estimées, il est possible de récupérer l'image couleur envoyée. En effet, il suffit de réaliser les étapes inverses de celles effectuées lors de l'algorithme de cryptage en utilisant les états estimés.

4.3.3 Résultats de transmission

Dans cette partie du chapitre, nous présenterons les résultats de transmission d'images en utilisant le système de transmission proposé. Trois images test sont utilisées : L'image

Cameraman aux niveaux de gris de taille 225×225 , l'image Peppers.jpeg de taille $225 \times 225 \times 3$ et l'image Baboon.jpeg de taille $229 \times 220 \times 3$. Les trois images utilisées sont illustrées sur la figure 4.8.

Les simulations sont réalisées en utilisant le logiciel Matlab version 8.5.0. Les valeurs ini-



FIGURE 4.8 – Les images tests utilisées : *a* : Image Cameraman.jpg, *b* : Image Peppers.jpg, *c* : Image Baboon.jpg

tiales des états du système de Lozi d'ordre fractionnaire sont $(x_1(0), x_2(0)) = (0.8, -0.5)$. Les valeurs initiales de l'observateur impulsif d'ordre fractionnaire sont $(\hat{x}_1(0), \hat{x}_2(0)) = (1, -3)$. Dans notre schéma, nous avons considéré le cas de systèmes fractionnaire non commensurables, autrement dits, les ordres de dérivation α_1, α_2 des états x_1, x_2 , respectivement, sont différents. La taille L de la mémoire utilisée est $L = 200$. L'espace de clés secrètes que nous noterons K comprends les paramètres de bifurcation a et b et les ordres de dérivation fractionnaire α_1 et α_2 . Leurs valeurs sont choisies égales à : $a = 1.7, b = 0.5, \alpha_1 = 0.998, \alpha_2 = 0.997$.

Le gain de contrôle b_1 est choisi égal à $b_1 = -0.9998$ de sorte à ce que les conditions du théorème 20, énoncé lors du chapitre précédent, soient satisfaites et que les erreurs de synchronisation convergent vers 0. La stabilité de la synchronisation impulsive est par conséquent atteinte pour ces valeurs. La figure 4.9 montre la convergence des erreurs de synchronisation impulsive. La figure 4.10 illustre l'image Cameraman.jpeg originale (à gauche), l'image chiffrée obtenue après application de l'algorithme de cryptage (au milieu)

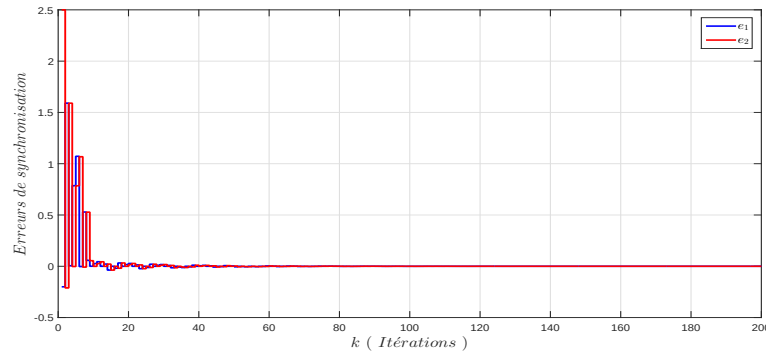


FIGURE 4.9 – Erreurs de synchronisation impulsive

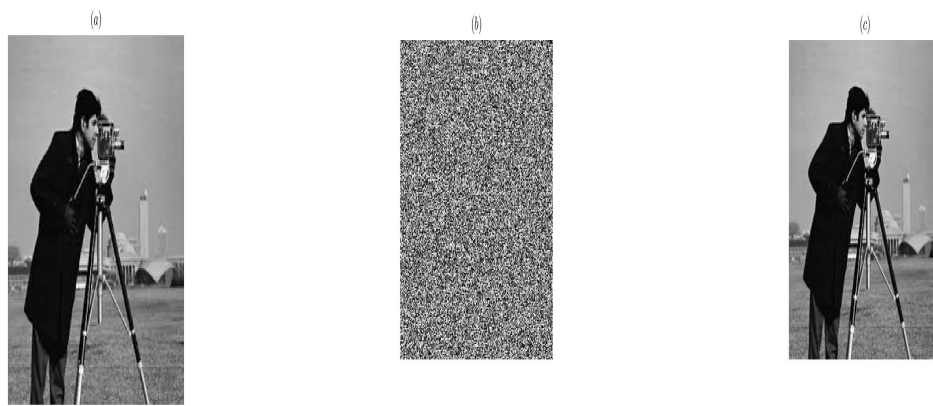


FIGURE 4.10 – Transmission de l'image Cameraman.jpg. (a) : Image originale , (b) : Image chiffrée, (c) : Image reçue

et l'image récupérée au niveau du récepteur (à droite).

La figure 4.11 illustre l'image Baboon.jpeg originale (à gauche), l'image chiffrée obtenue après application de l'algorithme de cryptage (au milieu) et l'image récupérée au niveau du récepteur (à droite).

De même, la figure 4.12 illustre l'image Peppers.jpeg originale (à gauche), l'image chiffrée obtenue après application de l'algorithme de cryptage (au milieu) et l'image récupérée au niveau du récepteur (à droite).

Les signaux S envoyés sur le canal en utilisant les différentes images tests sont illustrés sur les figures 4.13, 4.14 et 4.15.

La figure 4.16 illustre les plans de phase des images originales et reçues pour chaque

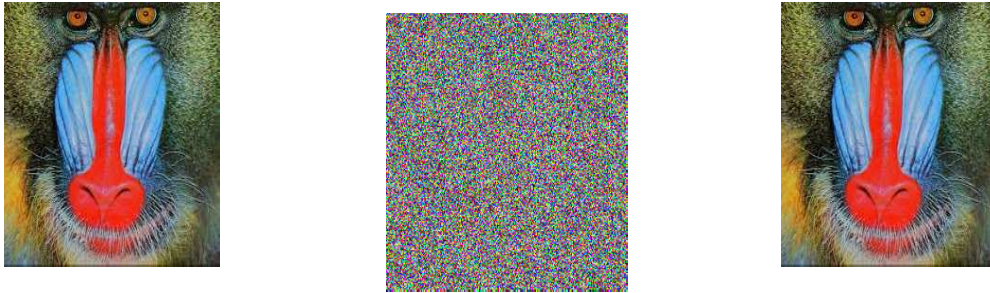


FIGURE 4.11 – Transmission de l'image Baboon.jpg. (a) : Image originale , (b) : Image chiffrée, (c) : Image reçue

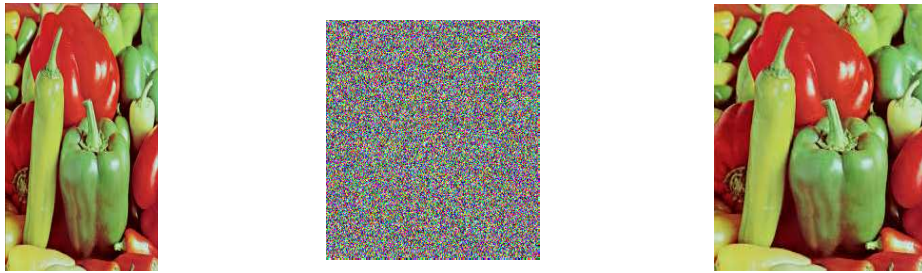


FIGURE 4.12 – Transmission de l'image Peppers.jpg. (a) : Image originale , (b) : Image chiffrée, (c) : Image reçue

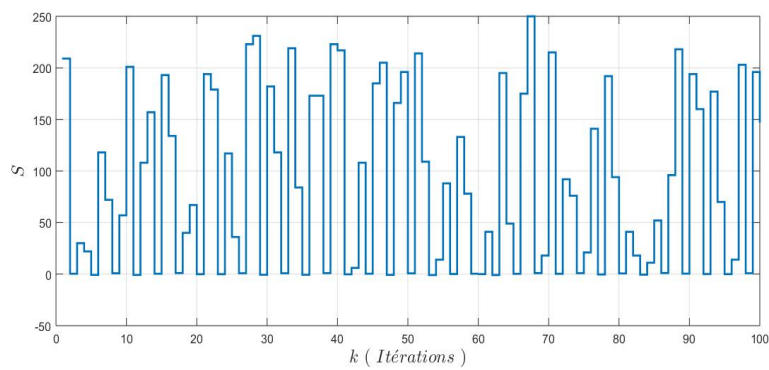


FIGURE 4.13 – Signal envoyé sur le canal lors de la transmission de l'image Cameraman

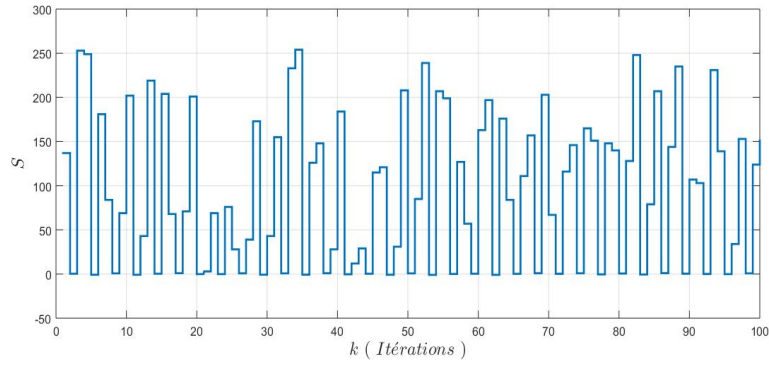


FIGURE 4.14 – Signal envoyé sur le canal lors de la transmission de l'image Peppers

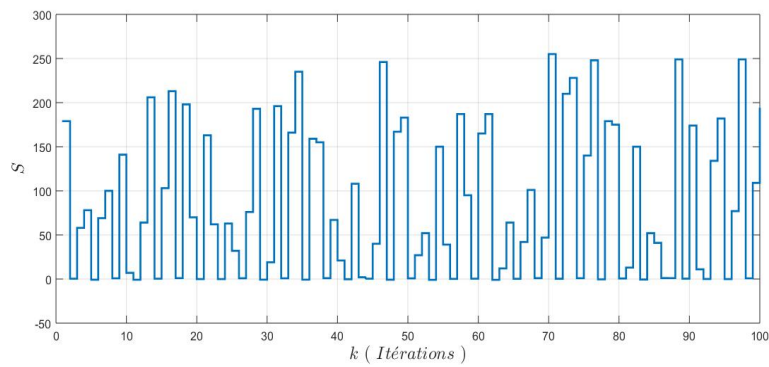


FIGURE 4.15 – Signal envoyé sur le canal lors de la transmission de l'image Baboon

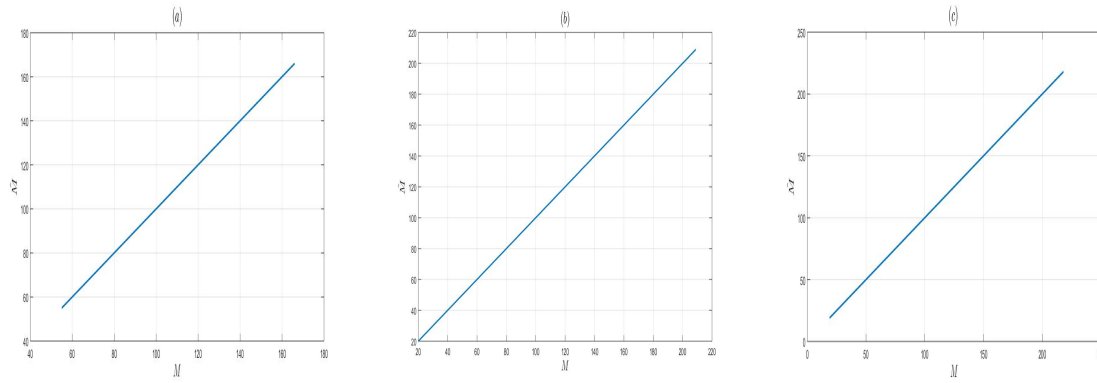


FIGURE 4.16 – Plans de phases des images originales et reçues. (a) : Image Cameraman, (b) : Image Pepper, (c) : Image Baboon

exemple considéré. Les droites obtenues confirment la récupération réussie des images test utilisées.

4.4 Conclusion

Dans ce chapitre, un nouveau schéma de transmission d'images couleur a été proposé. Après une introduction à la cryptographie en général, nous avons présenté les avantages d'utiliser le chaos pour sécuriser les communication de données. Nous avons ensuite présenté les différents algorithmes de cryptage à base des systèmes chaotiques d'ordres entier et fractionnaire. Juste après, nous avons proposé un schéma de transmission basé sur la synchronisation des systèmes chaotiques discrets d'ordre fractionnaire. De nombreuses étapes ont été effectuées pour chiffrer l'image originale avant son envoi sur le canal. Outre les paramètres du système chaotique utilisé, l'espace des clé comprend de nouvelles clés secrètes qui sont les ordres de différences fractionnaires des états du systèmes. Les valeurs des paramètres de bifurcation et des ordres de différences sont choisis sur la base des résultats d'analyse du système de Lozi d'ordre fractionnaire effectuée dans le troisième chapitre et de sorte à satisfaire les condition du théorème 20. Pour souligner l'apport de ces nouvelles clés ainsi que celui de l'observateur impulsif d'ordre fractionnaire utilisé pour synchroniser l'émetteur et le récepteur, nous avons soumis le système de transmission proposé à une analyse de robustesse et de sécurité. Cette dernière sera décrite dans le prochain chapitre.

Chapitre 5

Etude de la robustesse et analyse de la sécurité du schéma de transmission

5.1 Introduction

Dans le monde actuel des avancées technologiques dans les domaines du web, multimédias et réseaux sans fils, il y a une demande croissante pour le développement de méthodes de sécurité robustes et efficaces afin de protéger les données. Un algorithme de chiffrement robuste doit présenter des caractéristiques statistiques élevées, résister aux différentes éventuelles attaques et répondre à l'exigence classique de Shannon concernant les propriétés de confusion et de diffusions [277]. En effet, la combinaison de ces deux techniques fournit une qualité de cryptage, une robustesse et une sécurité très élevées [278]. Afin d'analyser la sécurité d'un système de transmission d'images quelconque, de nombreux tests doivent être effectués pour étudier les caractéristiques statistiques des images originale et chiffrée et afin de quantifier la sensibilité du schéma de cryptage aux variations des clés secrètes.

Lors du chapitre précédent, nous avons proposé un schéma de transmission à base de la conception d'un observateur impulsif pour le système de Lozi d'ordre fractionnaire. L'objectif de ce chapitre est l'étude de la robustesse du schéma de transmission développé en utilisant différents tests et en considérant plusieurs critères pour l'analyse de sa sécurité

vis à vis de différentes attaques et intrusions.

Ce chapitre est organisé comme suit, après une brève introduction à la cryptanalyse classique, et définition de quelques attaques connues, nous présenterons les différents critères considérés pour analyser la robustesse d'un système de transmission d'images face à ces attaques. Nous donnerons juste après, les résultats d'application de ces critères sur le système de transmission proposé dans le chapitre précédent afin de souligner ses avantages et de détecter d'éventuelles défaillances à surmonter à l'avenir. Le chapitre sera clos par une conclusion et quelques perspectives à envisager pour améliorer le schéma de communication proposé.

5.2 Introduction à la cryptanalyse

La cryptanalyse est le domaine englobant les différentes méthodes ayant pour objectif de compromettre l'algorithme de cryptage. Le terme *attaques* est souvent utilisé pour qualifier une tentative à briser l'algorithme de cryptage. [279]

Il existe plusieurs types d'attaques, les plus connues sont [280]

- Attaque à texte chiffré seul : Cette expression signifie que le cryptanalyste ou l'intrus dispose du texte chiffré (message crypté) et tentera de retrouver le message clair ou encore mieux, de déduire la clé lui permettant de déchiffrer d'autres messages chiffrés avec le même algorithme.
- Attaque à texte clair connu : Comme son nom l'indique, lors de cette attaque, le cryptanalyste a accès au texte chiffré ainsi qu'au texte clair, son objectif consiste alors à retrouver la ou les clés de chiffrement.
- Attaque à texte clair choisi : Dans ce type d'attaques, le cryptanalyste ne dispose pas que des messages clair et chiffré, mais de plus, il peut choisir les textes en clair qui lui fourniront plus d'informations sur la clé.
- Attaque à texte chiffré choisi : Le cryptanalyste, dans cette attaque, a le choix entre différents textes chiffrés. Il peut alors obtenir les textes en clair.
- Attaque différentielle : Lors de cette attaque, l'intrus étudie l'effet d'un système de

cryptage sur des textes en clair et utilise cette information afin de retrouver la ou les clés de chiffrement.

- Attaque à force brute : Dans ce type d'intrusions, le cryptanalyste mène une recherche exhaustive sur l'espace des clés secrètes. Toutefois, pour de larges espaces de clés, cette tentative aboutit à l'échec à moins que le cryptanalyste dispose d'informations supplémentaires sur la structure de l'espace des clés secrètes.

5.3 Analyse de la robustesse du schéma de transmission proposé

La mesure cruciale pour la qualité d'un système cryptographique, est sa capacité à résister aux tentatives d'une personne non autorisée ou d'un opposant pour acquérir des connaissances sur les informations non cryptées. Dans cette partie de thèse, nous présenterons les différents critères et tests appliqués dans l'objectif d'évaluer la robustesse et la sécurité d'un système de transmission.

5.3.1 Analyse statistique

Dans la littérature, il a été constaté que plusieurs algorithmes de chiffrement d'images existants, ont été brisés avec succès à l'aide d'une attaque statistique. Pour prouver la robustesse d'un schéma de transmission, une analyse statistique doit être effectuée afin de vérifier que les propriétés de confusion et diffusion résultent en une forte résistance aux attaques statistiques [281]. Cette analyse comprend l'étude de la distribution des pixels par analyse de l'histogramme, l'étude de la corrélation entre pixels adjacents et le calcul de l'entropie de l'image chiffrée. Nous développerons ci-dessous, le principe de chaque test.

5.3.1.1 Analyse de l'histogramme

L'une des attaques communes est celle basée sur l'analyse de l'histogramme de l'image cryptée. Un schéma de transmission d'image est considéré comme robuste face aux attaques statistiques, si l'histogramme de l'image crypté est uniformément distribué.

L'histogramme d'une image est un outil puissant dans le domaine de traitement d'images numériques. Il fait référence à un graphique montrant le nombre de pixels dans une image à différentes valeurs d'intensité trouvées [282]. Dans le cas d'images aux niveaux de gris, on retrouve 256 intensités différentes et donc l'histogramme affichera 256 nombres montrant la distribution des pixels sur ces valeurs de niveaux de gris. Dans le cas d'images couleur, il est nécessaire d'analyser les histogrammes des trois composantes Rouge (R), Verte (G) et Bleue (B). Pour un bon chiffrement, la distribution des échelles de gris dans l'image chiffrée devrait être assez uniforme et différente de l'histogramme de l'image originale pour qu'un adversaire ne puisse extraire aucune information de l'histogramme.

Bien que cette analyse visuelle est nécessaire, cependant, elle n'est pas suffisante. Pour confirmer l'uniformité de l'histogramme, le test de χ^2 représenté par l'équation qui suit, doit être appliqué.

$$\chi^2 = \sum_{i=2}^{Q-1} \frac{(O_i - e_i)^2}{e_i} \quad (5.1)$$

le terme Q dans l'équation (5.1) est le nombre de niveaux d'intensité de l'image (dans notre cas $Q = 256$). O_i est la fréquence d'occurrence observée de chaque niveau de couleur sur l'histogramme de l'image chiffrée et e_i est la fréquence d'occurrence prévue pour une distribution uniforme.

Dans un algorithme de cryptage sécurisé, la valeur expérimentale de χ^2 doit être inférieure à la valeur théorique pour un niveau de signifiante de 0.05 et qui est égale à $\chi_{0.05,255}^2 = 293$ [283].

5.3.1.2 Analyse de la corrélation entre pixels adjacents

L'analyse de la corrélation est l'une des méthodes régulières et standard pour mesurer la similarité entre l'image cryptée et l'image originale. En effet, il est bien connu que les pixels adjacents dans une image sont très redondants et corrélés, que ce soit horizontalement, verticalement ou dans la direction diagonale. Par conséquent, dans une image chiffrée, les pixels adjacents doivent avoir une redondance et corrélation aussi faibles que possible. Afin de tester la sécurité de l'image dans ce contexte, les premières N paires de

pixels adjacents horizontalement, verticalement et en diagonale sont sélectionnées dans l'image originale et dans l'image cryptée. Les équations suivantes sont utilisées pour calculer le coefficient de corrélation [284].

$$\rho_{xy} = \frac{cov(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (5.2)$$

avec

$$cov(x, y) = \frac{1}{N} \sum_{i=1}^N ([x_i - E(x)] [y_i - E(y)]) \quad (5.3)$$

$$D(x) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))^2 \quad (5.4)$$

$$E(x) = \frac{1}{N} \sum_{i=1}^N (x_i) \quad (5.5)$$

Dans les équations ci-dessus, x_i et y_i sont les valeurs de deux pixels adjacents dans l'image originale ou l'image chiffrée correspondante. Le résultat du calcul est une valeur réelle comprise dans l'intervalle $[0, 1]$. Si le coefficient de corrélation dans chaque direction est proche de 1, donc les pixels sont très corrélés. Dans le cas où ce coefficient est très petit et est proche de 0, alors les pixels adjacents sont faiblement corrélés [285].

5.3.1.3 Analyse de l'entropie

Les valeurs des pixels d'une image varient de 0 à 255. Dans un algorithme de chiffrement robuste, la probabilité d'occurrence de chaque pixel doit être la même (ou presque la même). Le comportement aléatoire d'une image chiffrée peut-être évaluée en utilisant l'information sur l'entropie définie par :

$$H(I_C) = \sum_{i=0}^{Q-1} Pro(c_i) \times \log_2 \frac{1}{Pro(c_i)} \quad (5.6)$$

où $H(I_C)$ est l'entropie de l'image chiffrée I_C , $Pro(c_i)$ est l'occurrence de chaque niveau d'intensité $i = 0, 1, 2, \dots, 255$). Dans le cas de probabilités d'occurrence égales,

$Pro(c_i) = \frac{1}{256}$, l'entropie est maximale, et on aura $H(I_C) = \sum_{i=0}^{255} \frac{1}{256} \times \log_2 256 = 8$ [287].

5.3.2 Analyse de sensibilité des clés secrètes

La sensibilité de la clé est extrêmement importante pour tout système de chiffrement. Un algorithme de cryptage a un niveau de sécurité élevé relativement à la sensibilité des clés secrètes, si un léger changement dans la clé secrète produit une image chiffrée complètement différente. Afin de vérifier cette sensibilité des clé secrète, Les étapes suivantes doivent être effectuées dans l'ordre [286] :

1. Une seule image claire I est utilisée lors du processus de cryptage.
2. Une seule clé secrète de l'espace de clé K est variée légèrement d'une valeur δ . Nous aurons ainsi deux ensembles de clés différents : $K_1 = K$ qui est l'ensemble de clés originales et K_2 qui est l'ensemble obtenu après la modification de l'une des clés secrètes.
3. L'image originale I est chiffrée avec l'ensemble de clés K_1 et génère une image chiffrée I_{C_1} . La même image originale est chiffrée avec l'ensemble de clés K_2 pour générer une image chiffrée I_{C_2} .
4. Deux paramètres de sécurité $NPCR$ et $UACI$ sont calculés pour les deux images chiffrées I_{C_1} et I_{C_2} pour évaluer la sensibilité de la clé variée.

Afin de tester l'influence d'un petit changement dans l'algorithme de cryptage sur l'image chiffrée, deux mesures communes sont souvent utilisées : Le NPCR (Number of Pixels Change Rate) et UACI (Unified Average Changing Intensity).

La valeur de NPCR donne le taux de pixels différents entre les deux images chiffrées obtenues avant et après modification sur l'un des paramètres de cryptage ou sur l'image originale.

La valeur de UACI représente la différence d'intensité moyenne entre les deux images chiffrées. Les formules utilisées pour calculer ces deux taux sont comme suit :

$$NPCR = \frac{\sum_{i,j} D(i,j,p)}{M \times N \times P} \times 100\% \quad (5.7)$$

$$UACI = \frac{1}{M \times N \times P} \left[\sum_{i,j,p} \frac{|I_{C_1}(i,j,p) - I_{C_2}(i,j,p)|}{255} \right] \times 100\% \quad (5.8)$$

avec M , N , P représentent respectivement la longueur et la hauteur et la profondeur des images chiffrées. Les éléments de la matrice D sont calculés comme suit [288]

$$D(i,j) = \begin{cases} 1 & \text{si } I_{C_1}(i,j,p) \neq I_{C_2}(i,j,p) \\ 0 & \text{si } I_{C_1}(i,j,p) = I_{C_2}(i,j,p) \end{cases} \quad (5.9)$$

Les valeurs optimales de ces taux sont $NPCR = 99.6094$ et $UACI = 33.4635$.

5.3.3 Analyse de l'espace de clés

La taille de l'espace de clés est le nombre total des différentes clés qui sont utilisées dans l'algorithme de cryptage. Un espace de clé doit être assez large pour résister aux attaques à force brute définies au début de ce chapitre. La taille minimale de l'espace des clés pour qu'un système de transmission à base de systèmes chaotiques puissent résister à ce type d'attaques est de 2^{100} [289].

5.3.4 Analyse de la qualité de cryptage

Une mesure très utile pour quantifier la qualité de cryptage est le calcul du PSNR (Peak Signal-to-Noise Ratio). Soient deux images I_1 et I_2 . Le PSNR est défini comme le rapport entre la plus grande valeur de la première image et la racine de l'erreur quadratique moyenne entre les deux images.

Le taux PSNR d'une image aux niveaux de gris ou d'une composante d'une image couleur peut-être alors déterminée à partir de l'équation suivante [290].

$$PSNR = 20 \log_{10} \left(\frac{\text{Max}(I_1(i,j))}{\sqrt{MSE}} \right) \quad (5.10)$$

avec $Max(I_1(i, j))$ est la valeur maximale de l'image I_1 et MSE est l'erreur quadratique moyenne obtenue comme suit :

$$MSE = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N |I_1(i, j) - I_2(i, j)|^2 \quad (5.11)$$

Dans le cas où l'image I_2 considérée est l'image décryptée, alors le taux PSNR doit être assez grand (≥ 30), Dans le cas où I_2 représente l'image chiffrée, le taux $PSNR$ doit être très petit.

5.3.5 Analyse de la rapidité

Outre l'analyse de sécurité, le temps d'exécution est un facteur important dans tout système de transmission. Le temps pris pour crypter les différentes images de tailles variées doit être aussi faible que possible.

5.3.6 Robustesse vis à vis du bruit

Généralement, l'addition d'un bruit à l'image est responsable de sa dégradation et sa distorsion [291]. L'image cryptée est aussi dégradée par l'ajout de bruit ce qui cause des difficultés à déchiffrer l'image. L'effet du bruit sur la qualité de l'image déchiffrée, peut être calculé à l'aide de la mesure du taux de $PSNR$ défini auparavant entre l'image originale et l'image déchiffrée.

5.4 Analyse de sécurité du système de transmission proposé

Dans cette section, nous présenterons les résultats d'application des tests précédents sur le schéma de transmission proposé à base de la synchronisation impulsive des systèmes chaotiques discrets d'ordre fractionnaire. Nous entamerons les résultats de notre analyse par l'étude de la distribution des pixels de l'image cryptée par comparaison des

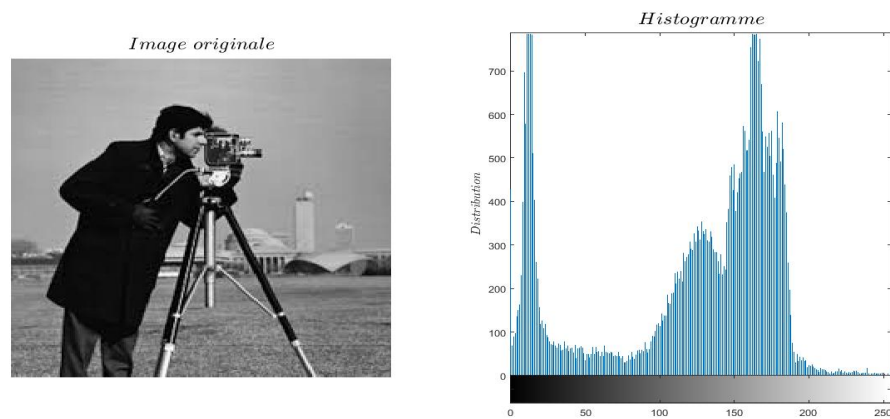


FIGURE 5.1 – Image Cameraman originale et son histogramme

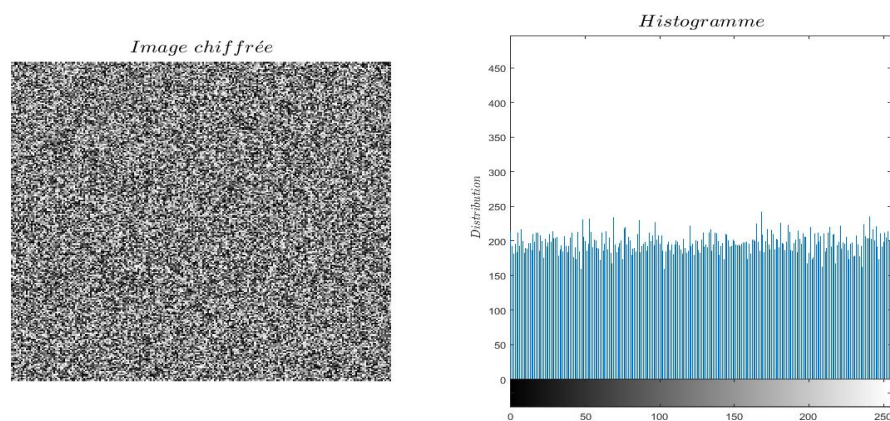


FIGURE 5.2 – Image Cameraman chiffrée et son histogramme

histogrammes des images chiffrée et originale.

5.4.1 Résultats de l'analyse de l'histogramme

Le figure 5.1 montre l'image test Cameraman et son histogramme. Le résultat du chiffrement de cette image ainsi que son histogramme sont affichés sur la figure 5.2.

De même que pour la première image test, les figures 5.3, 5.4, 5.5 et 5.6 illustrent les deux autre images couleurs Peppers et Baboon originale et après chiffrement ainsi que les histogrammes associés aux composantes R, G et B. Comme nous pouvons le constater sur ces figures, les histogrammes des images chiffrées sont uniformes et ne portent aucune ressemblance statistique avec les histogrammes des images originales.

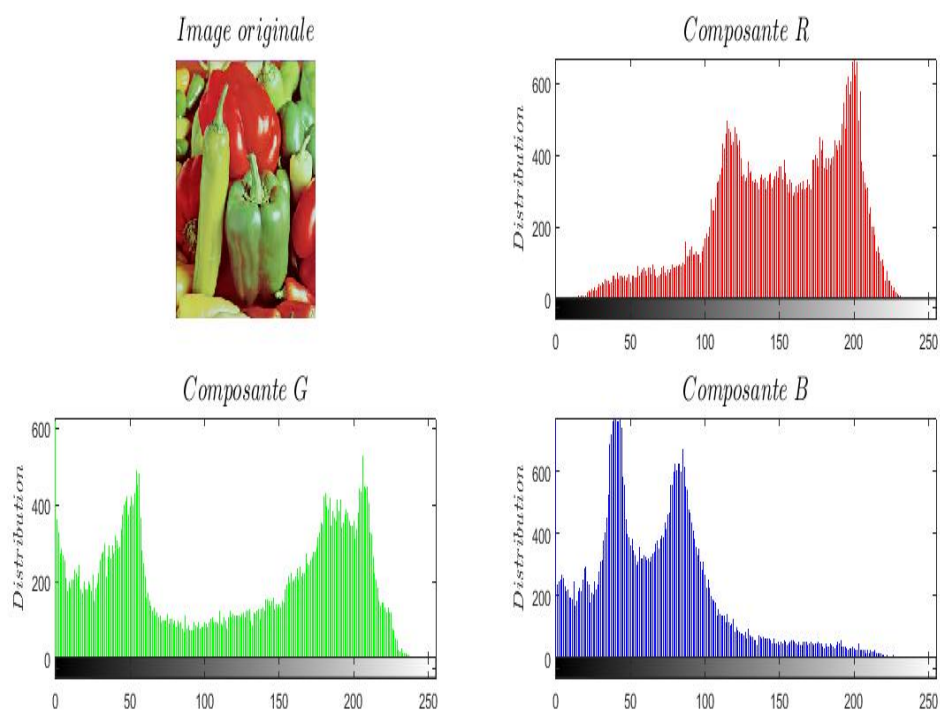


FIGURE 5.3 – Image Peppers originale et ses histogrammes

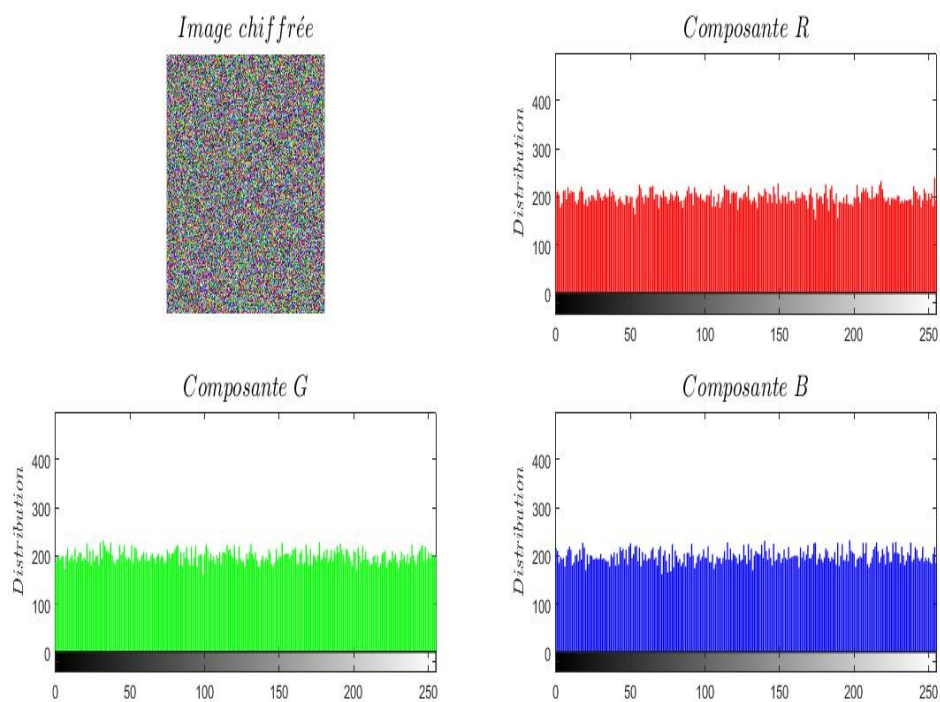


FIGURE 5.4 – Image Peppers chiffrée et ses histogrammes

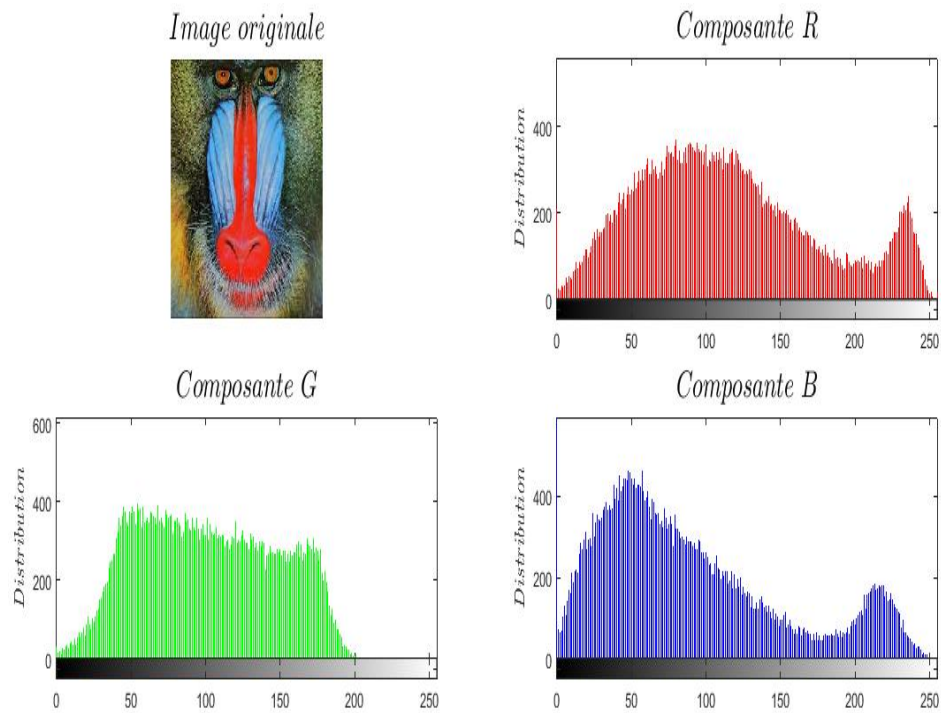


FIGURE 5.5 – Image Baboon originale et ses histogrammes

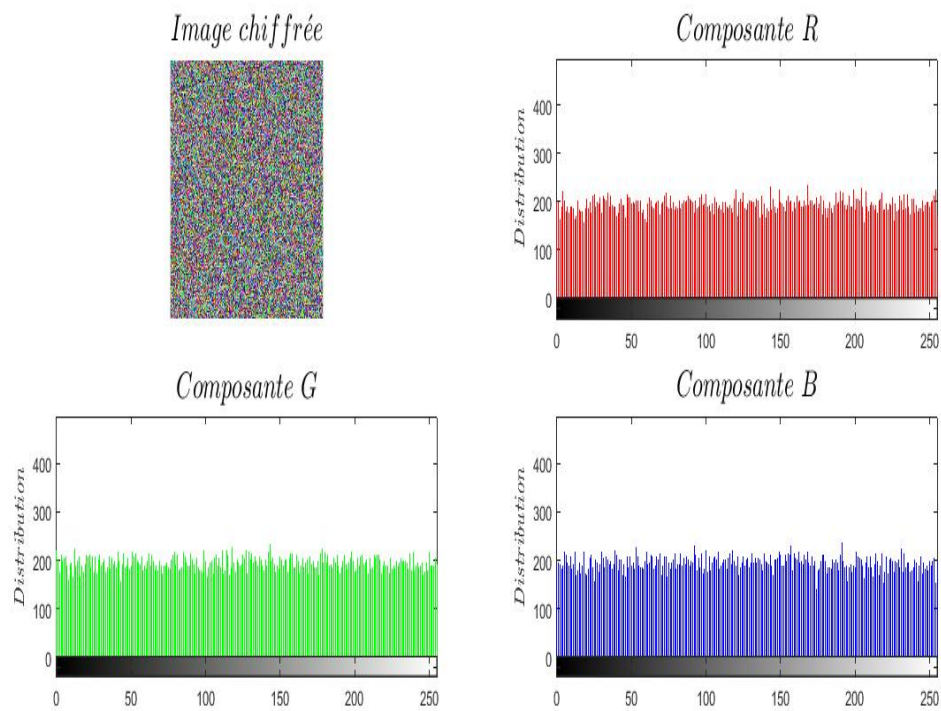


FIGURE 5.6 – Image Baboon chiffrée et ses histogrammes

Image	χ^2
Cameraman	284.97

TABLE 5.1 – Valeur de χ^2 obtenue pour l'image cameraman

Image	R	G	B
Peppers	246.92	259.55	251.89
Baboon	213.8725	217.6225	260.2655

TABLE 5.2 – Valeurs de χ^2 obtenues pour les images test Peppers.jpg et Baboon.jpg

Le test χ^2 a été appliqué sur les trois images test pour confirmer le résultat de comparaison visuelle des histogrammes. Les tableaux 5.1 et 5.2 montrent les résultats du test Chi-carré sur les images tests utilisées.

Comme nous pouvons le voir, les valeurs de χ^2 sont inférieures à la valeur théorique. Ceci confirme la distribution uniforme des pixels de l'image chiffrée.

5.4.2 Résultats de l'analyse de corrélation entre pixels adjacents

Afin de comparer la différence de corrélation entre pixels adjacents avant et après chiffrement de l'image, la figure 5.7 illustre la corrélation des pixels adjacents dans l'image Cameraman dans les directions horizontale, verticale et diagonale avant et après chiffrement. On peut constater que les pixels adjacents perdent en corrélation une fois l'image est chiffrée.

Les coefficients de corrélation dans notre cas, sont calculés en considérant les 3000 premières paires de pixels adjacents de l'image originale et de l'image chiffrée.

Les tableaux 5.3, 5.4 et 5.5 illustrent les coefficients de corrélation obtenus, avant et après chiffrement, pour les trois images tests en utilisant le système de transmission proposé. Ces résultats montrent que l'algorithme de cryptage utilisé supprime, avec succès, la corrélation entre les pixels adjacents dans les directions horizontale, verticale et diagonale.

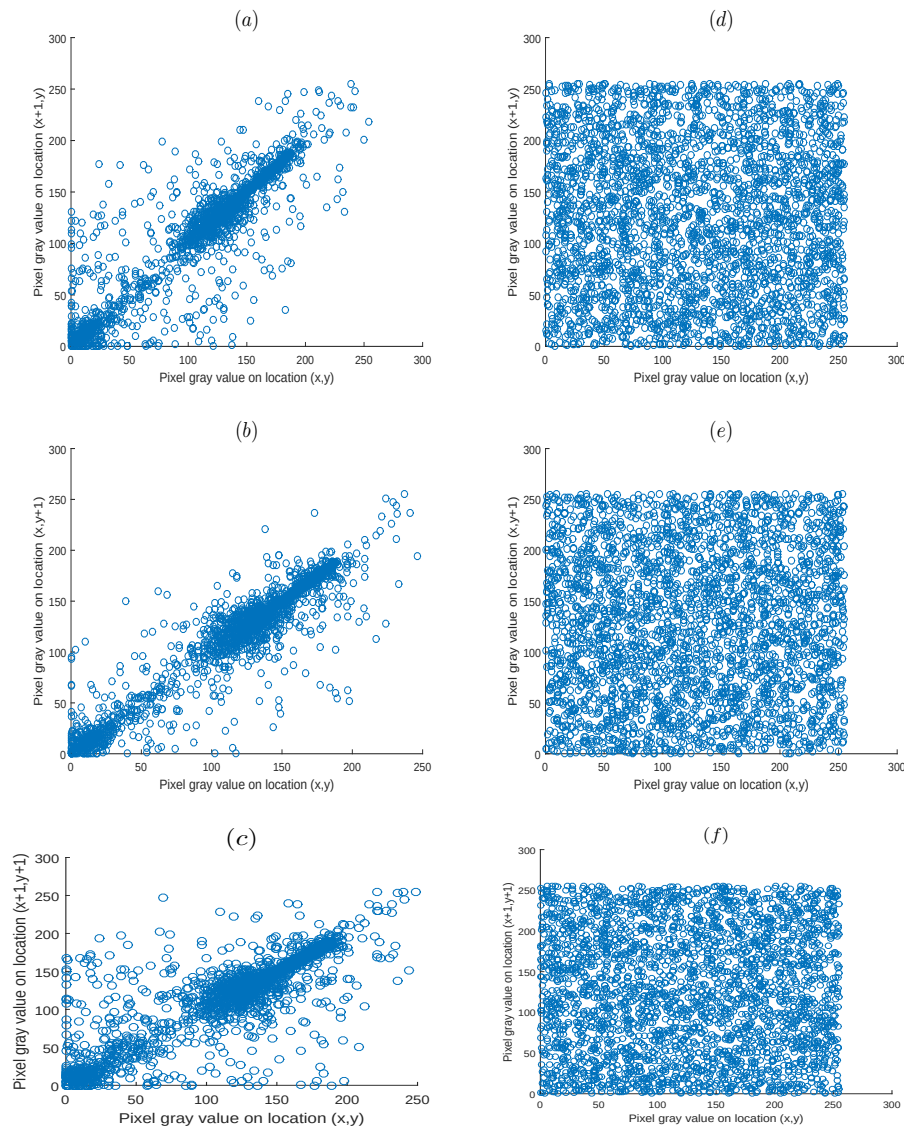


FIGURE 5.7 – Corrélation des pixels adjacents dans les images Cameraman originale et chiffrée dans les différentes directions

Direction	Image Claire	Image chiffrée
Horizontale	0.9326	-0.0090
Verticale	0.9664	-0.0093
Diagonale	0.9266	-0.0066

TABLE 5.3 – Les résultats de corrélation entre pixels adjacents en utilisant l'image Cameraman

Direction	Image originale			Image chiffrée		
	R	G	B	R	G	B
Horizontale	0.9466	0.96533	0.9422	0.0002	-0.0266	-0.0019
Verticale	0.9574	0.9736	0.9472	-0.0172	-0.0036	0.0145
Diagonale	0.9091	0.9417	0.8937	-0.0054	0.0284	0.0160

TABLE 5.4 – Résultats de corrélation entre pixels adjacents en utilisant l'image Peppers.jpg

Direction	Image originale			Image chiffrée		
	R	G	B	R	G	B
Horizontale	0.9204	0.8565	0.9187	0.0003	-0.0169	-0.0269
Verticale	0.8881	0.8025	0.8972	-0.0126	0.0331	0.0308
Diagonale	0.87348	0.7771	0.8725	0.0187	0.0066	-0.0197

TABLE 5.5 – Résultats de corrélation entre pixels adjacents en utilisant l'image Baboon.jpg

5.4.3 Résultats de l'analyse de l'entropie

Les valeurs de l'entropie, avant et après chiffrement, des images Cameraman, Baboon et Peppers sont données dans les tableaux 5.6 et 5.7.

Les valeurs de l'entropie obtenues après chiffrement de chaque image test sont très proches de la valeur théorique idéale qui est $H(I_C) = 8$. Ainsi, notre système de transmission peut résister aux différentes attaques à base de l'analyse de l'entropie.

5.4.4 Résultats d'analyses de la sensibilité vis à vis des clés secrètes

Dans notre cas, et afin de tester la sensibilité de l'algorithme aux variations des clés secrètes, des variations de $\delta = 10^{-15}$ à 10^{-16} ont été appliquées sur chaque clé secrète réelle. Ce test est appliqué sur les trois images tests et pour toutes les clés réelles de l'ensemble K . Les figures 5.8 et 5.9 illustrent, respectivement, l'effet d'une très petite variation de l'une des clés sur la transmission des images Cameraman et Peppers. Comme

	Image Claire	Image chiffrée
Cameraman	7.0939	7.9959

TABLE 5.6 – Les résultats d’entropie des images Cameraman originale et chiffrée

Image	Image originale			Image chiffrée		
	R	G	B	R	G	B
Peppers	7.3513	7.6165	7.1500	7.9965	7.9963	7.9964
Baboon	7.7840	7.4543	7.6669	7.9969	7.9969	7.9963

TABLE 5.7 – Valeur d’entropie en utilisant les images couleur

nous pouvons le voir à travers les résultats du décryptage, notre système est très sensible aux variations des clés secrètes.

Outre cette analyse visuelle, les tableaux 5.8, 5.9 et 5.10 illustrent, par les valeurs des paramètres *NPCR* et *UACI*, la sensibilité des clés réelles en utilisant les images Cameraman, Peppers et Baboon respectivement. Comme nous pouvons le constater à partir des résultats numériques affichés sur les trois tableaux, notre algorithme de cryptage présente une sensibilité élevée aux variations des clés et peut ainsi résister aux éventuelles attaques différentielles.

5.4.5 Résultats de l’analyse de l’espace des clés

A partir des résultats de l’analyse différentielle précédente, nous avons constaté une précision de 10^{-14} pour la clé a et une précision minimale de 10^{-15} pour les clés b , α_1 et

Paramètre modifié	Variation δ	<i>NPCR</i> (%)	<i>UACI</i> (%)
a	10^{-15}	99.4976	33.5289
b	10^{-16}	99.4844	33.4553
α_1	10^{-16}	99.4567	33.4647
α_2	10^{-16}	99.4923	33.5473

TABLE 5.8 – La sensibilité aux variations des clés en utilisant l’image Cameraman

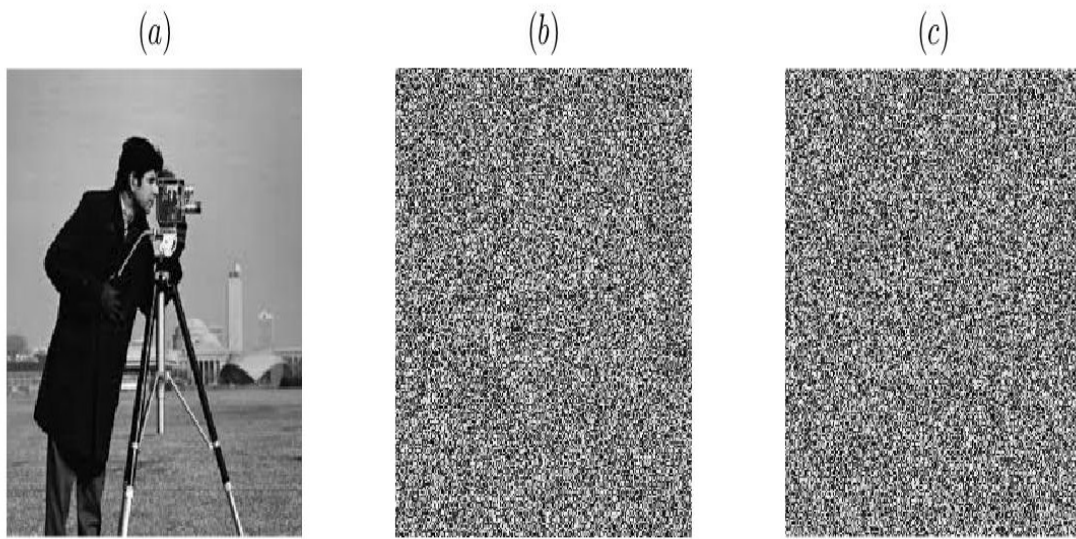


FIGURE 5.8 – Sensibilité aux variations des clés en utilisant l'image Cameraman. (a) : Image Cameraman originale, (b) : Image Cameraman chiffrée, (c) : Image Cameraman déchiffrée avec une variation 10^{-16} du paramètre b

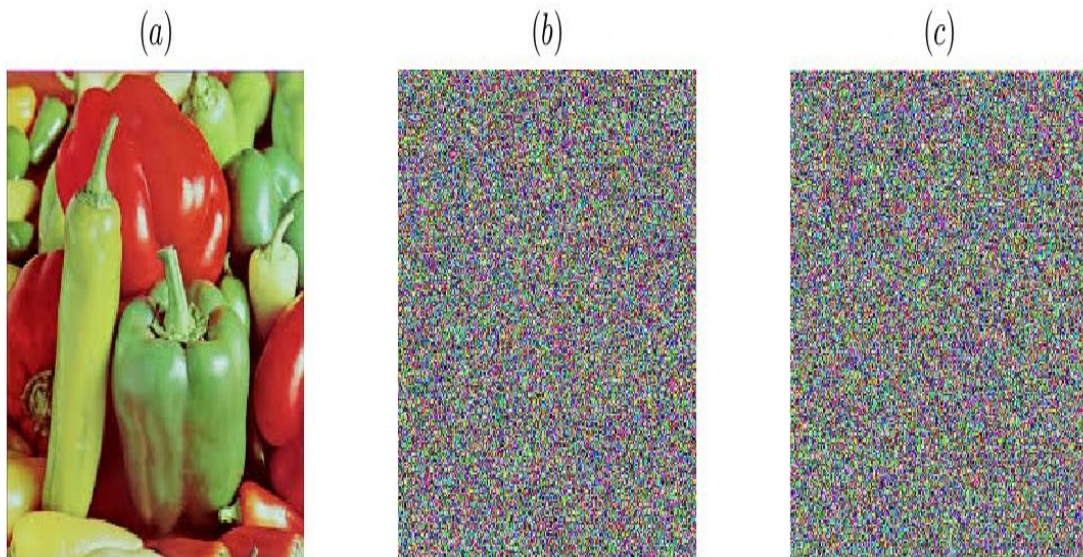


FIGURE 5.9 – Sensibilité aux variations des clés en utilisant l'image Peppers. (a) : Image Peppers originale, (b) : Image Peppers chiffrée, (c) : Image Peppers déchiffrée avec une variation 10^{-16} du paramètre α_1

Paramètre modifié	Variation δ	$NPCR(\%)$	$UACI(\%)$
a	10^{-15}	99.5667	33.4403
b	10^{-16}	99.5706	33.5112
α_1	10^{-16}	99.5522	33.3483
α_2	10^{-16}	99.5608	33.3442

TABLE 5.9 – La sensibilité aux variations des clés en utilisant l'image Peppers

Paramètre modifié	Variation δ	$NPCR(\%)$	$UACI(\%)$
a	10^{-15}	99.5818	33.3949
b	10^{-16}	99.5679	33.4193
α_1	10^{-16}	99.5633	33.3972
α_2	10^{-16}	99.5600	33.4129

TABLE 5.10 – La sensibilité aux variations des clés en utilisant l'image Baboon

α_2 . Ainsi, la taille minimale de l'espace de clé, notée T_K , est de

$$T_K = (10^{15 \times 3 + 14}) \approx 2^{195}$$

Cette valeur dépasse largement la valeur 2^{100} qui est la taille minimale nécessaire de l'espace de clés pour qu'un système cryptographique puisse résister aux attaques à force brute. A partir de ce résultat, on peut conclure que notre algorithme peut résister à toute sorte d'attaques à force brute.

5.4.6 Qualité du cryptage

Les taux $PSNR$ obtenus pour l'image aux niveaux de gris Cameraman et pour les trois composantes couleurs des images Peppers et Baboon sont respectivement rangés dans les tableaux 5.11 et 5.12. Pour chaque image, Le taux $PSNR$ est calculé entre l'image originale notée I_1 et une autre image I_2 qui représente l'image chiffrée correspondante. Comme nous pouvons le voir, sur chaque tableau, le taux de $PSNR$ entre l'image originale et l'image chiffrée est très faible et inférieure à 10 ce qui traduit une grande différence entre les deux images et une bonne qualité de cryptage.

Image originale I_1	Image I_2	$PSNR(dB)$
Cameraman	I_1 chiffrée	8.3964

TABLE 5.11 – Taux $PSNR$ entre l'image Cameraman et l'images cryptée associée

Image Originale I_1	Image I_2	$PSNR(dB)$			
		R	G	B	Moyenne
Peppers	I_1 chiffrée	9.0700	7.7262	7.7520	8.182
Baboon	I_1 chiffrée	8.4532	8.9716	7.8443	8.4230

TABLE 5.12 – Taux $PSNR$ en utilisant les images Peppers et Baboon

5.4.7 Résultats de l'analyse de la rapidité du système de transmission

L'analyse de la rapidité, dans notre cas, a été effectuée sur un PC de type Intel avec processeur Core(TM) i5-7200U de fréquence 2.5 GHz -2.7 GHz, une RAM de 8 Go et un système d'exploitation Window 10, 64 bits. Pour évaluer la rapidité de notre algorithme de chiffrement, nous avons déroulé ce dernier dix fois consécutives, pour chaque image, et avons relevé à chaque fois, les temps pris pour le cryptage et pour le décryptage. Le tableau 5.13 illustre les temps moyens calculés pour le cryptage et le décryptage de chaque image test. Les temps mis pour le cryptage et le décryptage de l'image transmise est déterminé par les fonction *tic* et *toc* de Matlab.

Comme nous pouvons le voir sur le tableau 5.13, les temps pris pour le chiffrement et pour le déchiffrement, en utilisant notre schéma de transmission, sont très courts pour chaque image test utilisée.

5.4.8 Effet du bruit sur la transmission

Dans notre cas nous avons testé la robustesse du schéma proposé vis-à-vis de deux types de bruits : Un bruit *poivre et sel* et un bruit *gaussien* de différentes densités. Ces bruits sont ajoutés à l'image chiffrée. L'algorithme de décryptage du schéma proposé est

Image	Taille	Temps de cryptage (s)	Temps de décryptage (s)
Cameraman	225×225	0.1629	0.1446
Peppers	$225 \times 225 \times 3$	0.4213	0.4233
Baboon	$229 \times 220 \times 3$	0.4097	0.4194

TABLE 5.13 – Résultats de l'analyse de la rapidité du système de transmission proposé

Type de bruit	PSNR
Poivre et sel (0.005)	31.1948
Poivre et sel (0.05)	21.2066
Gaussien [0 0.02]	13.8983
Gaussien [0 0.05]	11.3398

TABLE 5.14 – Taux PSNR après ajout du bruit à l'image Cameraman

appliqué sur les images chiffrées bruitées. Les tableaux 5.14 et 5.15 donnent les valeur de PSNR entre l'image originale et l'image décrypté. Ces résultats démontrent que le système de transmission est sensible aux bruits.

5.5 Conclusion

La sécurité d'une image est très différentes de celle d'autres données comme les signaux binaires ou fichiers texte à cause de leurs caractéristiques intrinsèques différentes.

Dans ce chapitre, et pour cette raison, nous avons soumis notre système de transmission à plusieurs tests et analyses pour vérifier sa robustesses vis à vis des attaques communes. Ainsi et et après une brève introduction à la cryptanalyse, nous avons défini et présenté un ensemble de tests nécessaires pour étudier la robustesse et les performances d'un système de transmission d'images.

Ces tests ont été appliqués au système de transmission, présenté dans le chapitre précédent. Les résultats de simulation ont démontré que l'algorithme de cryptage proposé à base de systèmes chaotiques discrets d'ordre fractionnaire présente de très bonnes performances en termes de sécurité, de sensibilité aux variations des clés secrètes et peut ainsi résister aux diverses attaques basées sur les analyses statistiques et différentielles.

L'algorithme peut être toutefois renforcé tout en préservant ses performances afin de résister aux différents types de bruits, à d'autres traitements qui risquent de compromettre

Type de bruit	PSNR
Poivre et sel (0.005)	31.1311
Poivre et sel (0.05)	20.9108
Gaussien [0 0.02]	12.9134
Gaussien [0 0.05]	11.4227

TABLE 5.15 – Taux PSNR après ajout du bruit à l'image Peppers

le décryptage de l'image comme la rotation, l'éclaircissement, la compression, etc. et à d'autres attaques. Une fois amélioré, on pourrait ainsi l'implémenter pratiquement sur cartes programmables tels les cartes Arduino, les DSP (Digital Signal Processors) et les circuits FPGAs.

Annexe A : Observabilité des systèmes dynamiques d'ordre fractionnaire

Ce second annexe est consacré à présenter les différentes définitions de l'observabilité proposées dans le cas des systèmes dynamiques d'ordre fractionnaire.

1) Observabilité des systèmes linéaires d'ordre fractionnaire

Dans le cas continu, Bettayeb et Djennoune [292], Matignon et D'Andréa-Novel [293] ainsi que Shamardan et Moubarak [294] ont fourni des résultats d'observabilité des systèmes linéaires d'ordre fractionnaire continus pertinents en utilisant la matrice du Grammien d'observabilité et la condition du rang. Afin de présenter brièvement ces résultats, considérons le système multivariable d'ordre fractionnaire donné par sa représentation d'état :

$$\begin{cases} d^\alpha x(t) &= Ax(t) + Bu(t), \quad x(t_0) = x_0 \\ y(t) &= Cx(t) + Du(t) \end{cases} \quad (5.12)$$

où $u(t) \in \mathbb{R}^m$ est le vecteur d'entrées, $y(t) \in \mathbb{R}^q$ est le vecteur de sorties et $x(t) \in \mathbb{R}^n$ est le vecteur d'état.

Définition 19 [292]

Le système (5.12) est observable sur $[t_0 \quad t_1]$, $t_1 > 0$ si $x(t_0)$ peut être déduit à partir de la connaissance de la sortie $y(t)$ et de l'entrée $u(t)$ pour $t \in [t_0 \quad t_1]$.

Le système (5.12) est observable si le rang de la matrice d'observabilité :

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

est égal à n .

Définition 20 *Le grammien d'observabilité est la matrice symétrique positive W_0 donnée par l'intégrale suivante :*

$$W_0(t_0, t) = \int_{t_0}^t E_\alpha(A^T(\tau)^\alpha) C^T C E_\alpha(A(\tau)^\alpha) d\tau. \quad (5.13)$$

$E_\alpha(\cdot)$ est la fonction de Mittag-Leffler.

Théoreme 23 *Le système (5.12) est observable sur $[t_0 \quad t_1]$ si et seulement si $\text{rang}(\mathcal{O}) = n$*

ou

$$W_0(t_0, t) = \int_{t_0}^t E_\alpha(A^T(\tau)^\alpha) C^T C E_\alpha(A(\tau)^\alpha) d\tau$$

est définie positive pour $t \in [t_0 \quad t_1]$.

Dans le cas de systèmes discrets, l'étude de l'observabilité a été effectuée d'abord par Dzielinski et Sierociuk [295] puis par Guermah *et al.* qui ont étendu leurs recherches au cas non commensurable [296]. Nous rapporterons dans ce qui suit les résultats concernant l'observabilité des systèmes discrets linéaires d'ordre fractionnaire. Le modèle général considéré par les auteurs est donné comme suit :

$$\begin{cases} x(k+1) &= \sum_{j=0}^k A_j x(k-j) + Bu(k), & x(0) = x_0 \\ y(k) &= Cx(k) \end{cases} \quad (5.14)$$

où $x \in \mathbb{R}^n$ est le vecteur d'état, $u(t)$ est l'entrée du système et $y(t)$ est sa sortie.

Dans le cas de systèmes commensurables, la matrice A_j est donnée par

$$A_j = -c_{j+1}I_n \quad (5.15)$$

avec $c_j = (-1)^j \binom{\alpha}{j}$ et I est la matrice identité.

Dans le cas non commensurable, on aura [296] :

$$A_j = \text{diag} - (-1)^{j+1} \begin{pmatrix} \alpha_i \\ j+1 \end{pmatrix}, i = 1, \dots, n. \quad (5.16)$$

Définition 21 [296] :

Le système linéaire discret d'ordre fractionnaire (5.14) est observable à l'instant $k = 0$ si et seulement si, il existe un $K > 0$ tel que l'état x_0 à l'instant $k = 0$ peut être uniquement déterminé par la connaissance de $u(k)$ et $y(k)$, $k \in [0, K]$.

Soit

$$G_k = \begin{cases} I_n & \text{pour } k = 0 \\ \sum_{j=0}^{k-1} A_j G_{k-1-j} & \text{pour } k \geq 1 \end{cases} \quad (5.17)$$

Définition 22 pour le système (5.14), on définit :

– La matrice d'observabilité

$$\mathcal{O}_k = \begin{bmatrix} CG_0 \\ CG_1 \\ CG_2 \\ \vdots \\ CG_{k-1} \end{bmatrix} \quad (5.18)$$

et

– Le Grammien d'observabilité

$$W_O(0, k) = \sum_{j=0}^{k-1} G_j^T C^T C G_j. \quad (5.19)$$

Théoreme 24 [296]

Le système linéaire discret d'ordre fractionnaire (5.14) est observable si et seulement si, il existe un temps fini K , telle que

$$\text{rang}(\mathcal{O}_K) = n$$

ou de manière équivalente

$$\text{rang}(W_O(0, K) = n$$

En outre, l'état initial x_0 à l'instant $k = 0$ est donné par

$$x_0 = W_0^{-1}(0, K) \mathcal{O}_K^T [\tilde{\mathcal{Y}}_K - \mathcal{M}_K \tilde{\mathcal{U}}_K] \quad (5.20)$$

avec

$$\tilde{\mathcal{U}}_K = [u^T(0) \quad u^T(1) \quad \cdots \quad u^T(K-1)]^T$$

,

$$\tilde{\mathcal{Y}}_K = [y^T(0) \quad y^T(1) \quad \cdots \quad y^T(K-1)]^T$$

et

$$\mathcal{M}_K = \begin{bmatrix} 0 & 0 & \cdots & 0 & 0 \\ CG_0B & 0 & \cdots & 0 & 0 \\ CG_1B & CG_0B & \cdots & 0 & 0 \\ CG_2B & CG_1B & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ CG_{K-2}B & CG_{K-3}B & \cdots & CG_0B & 0 \end{bmatrix}$$

.

2) Observabilité des systèmes non linéaires d'ordre fractionnaire

Dans le cas non linéaire, plusieurs résultats sur l'observabilité des systèmes d'ordre fractionnaire continus ont été obtenus. Ces résultats sont basés sur la condition de rang et sur le Grammien d'observabilité. Dans [297], des propriétés d'observabilité et une forme canonique observable ont été introduites. Ces propriétés peuvent être déduites à partir d'un système non linéaire d'ordre entier.

Afin de présenter les résultats obtenus, considérons le système non linéaire fractionnaire commensurable suivant :

$$\begin{cases} D^\alpha &= f(x(t)), \quad x(0) = x_0 \\ y(t) &= h(x(t)) \end{cases} \quad (5.21)$$

avec $D^\alpha x(t) = [D^\alpha x_1 \quad D^\alpha x_2 \quad \dots \quad D^\alpha x_n]^T$, $0 < \alpha < 1$ est l'ordre de dérivation, $f(x(t))$ et $g(x(t))$ sont des champs de vecteurs lisses pour $x(t) \in \mathcal{M} \subset \mathbb{R}^n$ avec $\mathcal{M}$ est un ensemble compact contenant l'origine. L'étude de l'observabilité du système (5.21) est basé sur le concept d'indiscernabilité. Des définitions relatives à cette notion ont été fournies dans [297].

Proposition 1 : *Condition du rang d'observabilité [297]*

Le système non linéaire d'ordre fractionnaire (5.21) est localement faiblement observable si la condition du rang suivante

$$\text{rang} \begin{pmatrix} dh \\ dL_f h \\ \vdots \\ dL_f^{n-1} h \\ \vdots \\ dL_f^\infty h \end{pmatrix} = n \quad (5.22)$$

est satisfaite avec $L_f h$ est la dérivée de Lie de h le long du champ de vecteur f donnée par

$$L_f h = \frac{\partial f(x)}{\partial x} h(x)$$

De leur côté, Balachandran et *al.* ont utilisé, dans leur article [298], une fonction matricielle de Mittag-Leffler et le théorème de contraction de Banach pour étudier l'observabilité des systèmes linéaires et non linéaires d'ordre fractionnaire. La définition de l'ordre fractionnaire considérée est celle de Caputo. Le système non linéaire d'ordre fractionnaire étudié par les auteurs est donné comme suit :

$$\begin{cases} D^\alpha &= Ax(t) + f(t, x(t)), \quad t \in [0 \quad T] := J \\ y(t) &= H(x(t)) \end{cases} \quad (5.23)$$

où $x \in \mathbb{R}^n$ est le vecteur d'état, f est un vecteur de fonctions non linéaires continues sur $t \in J$, y est un vecteur de dimension m telle que $m < n$.

Le problème d'observabilité du système a été traité par les auteurs comme suit :

Il est nécessaire de trouver un état inconnu à l'instant présent t à partir de y sur l'intervalle $[\theta, t]$ avec θ est un certain temps passé.

Définition 23 [298]

Le système (5.23) est dit observable à l'instant t , s'il existe $\theta < t$ tel que l'état du système à l'instant t peut être identifié à partir de la connaissance de la sortie du système tout au long de l'intervalle $[\theta, t]$.

Si le système est observable à tout instant $t \in J$, il est dit complètement observable.

Avant de présenter le théorème sur l'observabilité on définit l'équation suivante

$$\begin{aligned}
x(t) &= \int_{\theta}^t G_1(t, \theta, s) y(s) ds \\
&\quad \int_{\theta}^t (t-s)^{\alpha-1} G_2(t, \theta, s) f(s, x(s)) ds.
\end{aligned} \tag{5.24}$$

avec

$$\begin{aligned}
G_1 &= W^{-1}(\theta, t) [E_{\alpha}(A(t-s)^{\alpha})]^2 \\
&\quad \times E_{\alpha}(A^*(t-s)^{\alpha}) H^*,
\end{aligned} \tag{5.25}$$

$$\begin{aligned}
G_2 &= W^{-1}(\theta, t) E_{\alpha, \alpha}(A(t-s)^{\alpha}) W(\theta, s) \\
&\quad \times E_{\alpha}(A^*(t-s)^{\alpha}) H^*,
\end{aligned} \tag{5.26}$$

où $W(\theta, t)$ est la matrice Grammien d'observabilité définie comme suit :

$$W(\theta, t) = \int_{\theta}^t E_{\alpha}(A^* t^{\alpha}) H^* H E_{\alpha}(A t^{\alpha}) dt \tag{5.27}$$

E_{α} est la fonction de Mittag-leffler à un seul paramètre, $E_{\alpha, \alpha}$ est la fonction de Mittag-leffler à deux paramètres et A^* , H^* sont, respectivement, les matrices adjointes des matrices A et H .

Théoreme 25 [298] *Le système (5.23) est globalement (a) observable à l'instant t et complètement (b) observable, si les conditions suivantes sont vérifiées.*

i) *Il existe une constante $c > 0$ telle que*

$$\det(W(\theta, t)) \geq c. \tag{5.28}$$

ii) *L'équation (5.24) a une solution unique pour tout y qui est continu sur $[\theta, t]$*

(a) pour un certain $\theta < t$ dans le cas d'un système observable à l'instant t et

(b) pour tout t et pour un certain $\theta < t$ dans le cas d'un système complètement observable.

Dans le cas de systèmes d'ordre fractionnaire non linéaires discrets, et à notre connaissance, excepté les travaux de Mozyrska et son équipe de recherche, peu de travaux et

d'études de l'observabilité ont été proposés. Dans leur article publié en 2010, D.Mozyrska et *al.* ont défini plusieurs concepts d'observabilité pour les systèmes discrets non linéaires d'ordre fractionnaire [299]. L'espace d'observabilité du système y a été défini et utilisé pour caractériser la relation d'indistinguabilité et différentes formes d'observabilité.

Le système discret non linéaire d'ordre fractionnaire considéré est noté Γ et est défini par les équations suivantes :

$$\begin{cases} D^\Lambda x(k+1) &= f(x(k), u(k)) \\ y(k) &= h(x(k)) \end{cases} \quad (5.29)$$

où de manière équivalente

$$\begin{cases} x(k+1) &= f(x(k), u(k)) - \sum_{j=1}^{k+1} (-1)^j \Lambda_j x(k-j+1), \\ y(k) &= h(x(k)) \end{cases} \quad (5.30)$$

avec $D^\Lambda x(k+1) = \begin{bmatrix} D^{\alpha_1} x_1(k+1) \\ \vdots \\ D^{\alpha_n} x_n(k+1) \end{bmatrix}$, tandis que $\Lambda_j = \text{diag} \left[\begin{pmatrix} \alpha_1 \\ j \end{pmatrix}, \dots, \begin{pmatrix} \alpha_n \\ j \end{pmatrix} \right]$ est

une matrice diagonale et $x(k+1) = (x_1(k+1), x_2(k+1), \dots, x_n(k+1))^T \in \mathbb{R}^n$ est le vecteur d'état du système à l'instant $k+1$.

Remarque 26 *Le système (5.30) est obtenu en appliquant la définition de la différence au sens de Grunwald-Letnikov au système (5.29) dans le cas non commensurable.*

On suppose les fonctions f et g analytiques par rapport à x et on dénote par $J_0(m)$ l'ensemble de toutes les séquences $U = (u_0, u_1, \dots)$ avec $u(k) \in \mathbb{R}^m$. On définit, en outre, les séquences d'applications $F_k : \mathbb{R}^n \times J_0(m) \rightarrow \mathbb{R}^n$ par $F_0(x, U) = x$, $F_{k+1}(x, u) = f(F_k(x, U), u(k)) - \sum_{j=1}^{k+1} (-1)^j \Lambda_j F_{k-j+1}(x, U)$.

Proposition 2 *On dit que deux états $p, q \in \mathbb{R}^n$ sont indistinguables par rapport à Γ si et seulement si $h(F_k(p, U)) = h(F_k(q, U))$ pour toute séquence d'entrées U et pour tout entier non négatif k .*

L'outil principal pour l'étude de l'observabilité est l'espace d'observabilité. Soit $H(\Gamma)$ l'ensemble de toutes les fonctions de la forme $h_i \circ F_k(\cdot, k)$ où $i = 1, \dots, r$, $k \in \mathbb{Z}_+ \cup 0$, h_i est la $i^{\text{ème}}$ composante de h . Ainsi $H(\Gamma)$ est constitué des compositions de h_i avec les applications $F_k(\cdot, U) : \mathbb{R}^n \rightarrow \mathbb{R}^n$.

Proposition 3 [299] $dH(\Gamma)(p) = \sum_{j=1}^n \frac{\partial h_i}{\partial x_j}(F_k(p, U)) \nabla F_{k,j}(p, U) dx$ où $k \geq 0$, $i = 1, \dots, r$ et U est une séquence de commande arbitraire.

Définition 24 [299] Le sous-espace linéaire de l'espace de fonctions analytiques sur $\mathbb{R}^n$ couvert par $H(\Gamma)$ est appelé espace d'observation du système Γ .

Proposition 4 Deux états $p, q \in \mathbb{R}^n$ sont indistinguables par rapport à Γ si et seulement si pour tout $\varphi \in H(\Gamma)$, $\varphi(p) = \varphi(q)$.

Définition 25 [299]

- On dit que Γ est globalement observable si pour tout différents points $p \in \mathbb{R}^n$ et $q \in \mathbb{R}^n$, p et q sont distinguables.
- On dit que Γ est localement observable en $p \in \mathbb{R}^n$ s'il existe un voisinage V de p , tel que pour tout $q \in V \setminus p$, p et q sont distinguables.
- On dit que Γ est localement observable, s'il est localement observable en chaque point de $\mathbb{R}^n$.
- On dit que Γ est localement injective en p , s'il existe un voisinage V de p , tel que pour chaque $q_1, q_2 \in V : \forall \varphi \in H(\Gamma), \varphi(q_1) = \varphi(q_2) \Rightarrow q_1 = q_2$.

La proposition qui suit a été formulée pour les systèmes discrets usuels. Elle ne dépend pas d'une classe de systèmes mais plutôt de l'espace d'observation.

Proposition 5 [299] Soit les conditions suivantes :

1. $\dim dH(\Gamma)(p) = n$

2. $H(\Gamma)$ est injective en p

3. Γ est localement observable en p

Alors $1 \Rightarrow 2 \Rightarrow 3$ et aucune de ces implications ne peut être inversée.

Conclusion Générale

Notre contribution principale dans cette thèse a été de proposer un schéma de synchronisation des systèmes chaotiques discrets d'ordre fractionnaire en utilisant les observateurs impulsifs. Notre intérêt pour les systèmes discrets est justifié par le fait que ces derniers sont naturellement mieux adaptés que les systèmes continus pour la transmission de données numériques.

Notre seconde contribution a été donc de concevoir un système de transmission d'images à base de la synchronisation impulsive des systèmes chaotiques discrets d'ordre fractionnaire. L'objectif assigné a été d'exploiter à la fois les avantages des observateurs impulsifs et ceux des systèmes chaotiques discrets d'ordre fractionnaire.

Dans le premier chapitre, nous avons présenté les systèmes chaotiques et décrit leurs caractéristiques essentielles à savoir la sensibilité aux conditions initiales, le déterminisme, l'aspect aléatoire et l'attracteur étrange. Comme notre étude se porte sur les systèmes chaotiques d'ordre fractionnaire, nous avons introduit les concepts et notions de base sur les systèmes d'ordre fractionnaire évoluant en temps continu et discrets. Nous avons ensuite présenté quelques exemples de systèmes chaotiques d'ordre fractionnaire.

Lors du deuxième chapitre, nous avons rappelé les différents régimes de synchronisation entre les systèmes chaotiques d'ordre entier et décrit les différentes stratégies utilisées pour les atteindre. Nous avons ainsi présenté les travaux effectués concernant la technique de synchronisation par observateur impulsif aussi bien dans le cas de systèmes chaotiques

continus que dans le cas de systèmes chaotiques discrets.

Le troisième chapitre de ce travail de thèse a été consacré à la synchronisation des systèmes chaotiques d'ordre fractionnaire. Nous avons retrouvé presque les mêmes méthodes de synchronisations appliquées sur les systèmes chaotiques d'ordre entier à savoir la synchronisation par contrôle actif, la synchronisation par retour, la synchronisation par la méthode de backstepping et la synchronisation impulsive. Par contre, peu de méthodes ont été proposées pour les systèmes chaotiques discrets d'ordre fractionnaire. La synchronisation impulsive entre systèmes chaotiques d'ordre fractionnaire continus peut être établie en utilisant trois approches différentes. La première consiste à appliquer directement les résultats obtenus dans le cas de systèmes chaotiques d'ordre entier au cas de systèmes chaotiques d'ordre fractionnaire. La deuxième approche consiste à modifier la structure du système esclave de manière à obtenir un système d'erreur d'ordre entier et pouvoir utiliser ainsi les résultats de stabilité théoriques développés pour le cas des systèmes impulsifs d'ordre entier. La troisième approche est la plus intéressante car elle est basée sur l'étude de la stabilité des systèmes différentiels impulsifs d'ordre fractionnaire. Nous avons, par conséquent, apporté notre contribution en appliquant la même stratégie aux systèmes chaotiques discrets d'ordre fractionnaire. Nous avons, alors, proposé un observateur impulsif discret d'ordre fractionnaire et avons ensuite étudié la stabilité du système d'erreurs de synchronisation. Les résultats de simulation obtenus montrent que la stabilité de la synchronisation impulsive a été atteinte et que les erreurs de synchronisation ont fini par converger. Les mêmes résultats ont été obtenus par l'implémentation des systèmes maître et esclave synchronisés sur cartes Arduino-Méga.

La deuxième phase de notre travail a été d'utiliser un système chaotique discret d'ordre fractionnaire et son observateur impulsif dans un schéma de transmission d'images. Cette application a fait l'objet du quatrième chapitre de ce manuscrit de thèse. Nous avons entamé le chapitre par quelques définitions relatives au domaine de la cryptographie. Nous avons ensuite dressé une analyse comparative entre les objectifs de la cryptographie

et les propriétés des systèmes chaotiques pour montrer l'apport de la théorie du chaos dans les algorithmes de chiffrement de données et dans la transmission sécurisée. Ensuite, nous avons présenté notre système de transmission. L'algorithme de cryptage, consiste à combiner entre les séquences chaotiques et les pixels de l'image à transmettre. Plusieurs traitements inversibles ont été effectués. Un seul canal a été utilisé pour l'envoi du signal de synchronisation et de l'image chiffrée. Le décryptage, qui a lieu au niveau du récepteur, consiste à inverser les opérations servant au chiffrement et à utiliser les états chaotiques estimés, obtenus grâce à l'observateur impulsif, pour restituer l'image originale. Les premiers résultats de transmission de quelques images tests ont été fournis à la fin du chapitre. Les images ont été bien reconstruites au niveau du récepteur grâce à la synchronisation de celui-ci avec l'émetteur.

La sécurité du schéma de transmission proposé et sa robustesse vis à vis des différentes attaques ont été analysées dans le cinquième chapitre. Après une brève introduction à la cryptanalyse, nous avons présenté les différents tests nécessaires pour vérifier la sécurité d'un algorithme de chiffrement. Les premiers tests sont de type statistiques et servent à comparer entre les distributions des pixels dans les images claire et chiffrée. Plus les propriétés statistiques entre les deux images sont différentes, meilleur est l'algorithme utilisé. La deuxième classe de tests consiste à analyser la sensibilité du système de cryptage par rapport aux variations des clés secrètes. Autrement dit, une insignifiante variation de l'une des clés de cryptage doit donner lieu à une image chiffrée complètement différente. L'image claire, ne pourra, donc, pas être reconstruite. Le troisième type d'analyses concerne l'espace de clés secrètes. La taille de ce dernier doit être assez élevée pour résister aux attaques à force brute. En outre, la qualité du chiffrement a été évaluée en quantifiant la différence entre les images originale et chiffrée. Un autre test concerne la rapidité de la transmission en termes de temps moyens de cryptage et de décryptage. Un algorithme de cryptage doit en effet être rapide et robuste à la fois. Le dernier test consiste à analyser la qualité de l'image déchiffrée en présence de différents types de bruits. Toutes ces analyses ont été appliquées sur le schéma de transmission proposé. Des résultats satisfaisants

ont été obtenus pour les différentes images tests utilisées. Toutefois, notre algorithme est visiblement sensible aux bruits du canal de transmission.

Afin d'améliorer notre travail de thèse à l'avenir, des perspectives peuvent être envisagées que ce soit sur le plan théorique ou sur le plan pratique.

Sur le plan théorique, nous prévoyons de traiter les points suivants :

- Calcul théorique de la période maximale des impulsions de synchronisation au delà de laquelle la convergence du système d'erreurs ne sera plus établie.
- Amélioration de l'algorithme de cryptage pour garantir la robustesse vis à vis des bruits du canal de transmission et d'autres attaques.
- Transmission d'autres données comme la parole ou les vidéos.

Sur le plan pratique, nous projetons à implémenter le schéma de transmission proposé sur cartes programmables telles les cartes Arduino, les DSPs (Digital Signal Processors) et les circuits FPGAs.

Bibliographie

- [1] F. Rodríguez-Henríquez, A. D. Pérez, N. A. Saqib, Ç. K. Koç. A Brief introduction to modern cryptography. Chapitre du livre : Cryptographic Algorithms on Reconfigurable Hardware. *Springer, Boston MA*, pp. 7-33, 2007.
- [2] K. Schmeih. Cryptography and Public Key Infrastructure on the Internet. *John Willey and Sons*, 2003.
- [3] L. Kocarev, S. Lian, Chaos-Based Cryptography, *Springer*, 354, 2011.
- [4] W. Stallings. Cryptography and Network security : Principles and Practices. *Prentice Hall*, 2005.
- [5] S. Vaudeney. A classical Introduction to cryptography : Application for communications security *Springer*, 2006.
- [6] A.S.Hameed. Image encryption based on fractional order Lorenz system and wavelet transform. *Diyala Journal of Engineering Sciences*, 10(01), pp.81-91, 2017.
- [7] C.-C. Chang, M.-S. Hwang, T.-S. Chen. A new encryption algorithm for image cryptosystems. *Journal of Systems and Software*, 58(2), pp. 83-91, 2001.
- [8] R. Martinez-Guerra, C.A. Pérez-Pinacho, G.C. Gomez-Cortés. Synchronization of integral and fractional order chaotic systems. *Springer*, 2015.
- [9] G. Alvarez, S. Li. Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems. *International Journal of Bifurcation and Chaos*, 16(8), pp. 2129-2151, 2006.
- [10] K. Sun. Chaotic secure communication : Principles and Technologies, *Tsinghua University Press and Walter de Gruyter GmbH*, 2015.

- [11] A.Dzielinski, D. Sierociuk. Fractional Order Model of Beam Heating Process and Its Experimental Verification. In : Baleanu D., Guvenc Z., Machado J. (eds) New Trends in Nanotechnology and Fractional Calculus Applications. *Springer*, Dordrecht, 2010.
- [12] H. Sun, A. Abdelwahab, B. Onaral. Linear approximation of transfer function with a pole of fractional power. *IEEE Transactions on Automatic Control*, 29(5), pp. 441-444, 1984.
- [13] G. Liang, X. Liu. A Reduction Algorithm for Fractional Order Transmission Line Modeling with Skin Effect. *International Journal of u- and e- Service, Science and Technology*, 8 (1), pp. 239-250, 2015.
- [14] R.C. Koeller. Application of fractional calculus to the theory of viscoelasticity. *Journal of Applied Mechanics*, 51, pp 229-307, 1984.
- [15] A. G. Radwan, A. M. Soliman, A. S. Elwakil. Design equations for fractional-order sinusoidal oscillators : Four practical circuit examples, *Int. J. Circ. Theor. Appl.*, 36, pp. 473-492, 2008.
- [16] I. Petras. Fractional-Order Nonlinear Systems Modeling, Analysis and Simulation. *Nonlinear Physical Science*, 2011.
- [17] W. M.Ahmad, J.C.Sprott. Chaos in fractional-order autonomous nonlinear systems. *Chaos, Solitons and Fractals*, 16(02), pp. 339-351, 2003.
- [18] W. Zhen, H. Xia, L. Ning, S. Xiao-Na. Image encryption based on a delayed fractional-order chaotic logistic system. *Chinese Physics B*, 21(5), ID050506, 2012.
- [19] H. Hamiche, S. Kassim, O. Megherbi, S. Djennoune, M. Bettayeb. Secure Digital Data Communication Based on Fractional-order Chaotic Maps. Chapitre du livre : A. Boulkroune, S. Ladaci. Advanced Synchronization Control and Bifurcations of Fractional-Order Systems. *IGI Global*, pp. 438-467, 2018.
- [20] P. Muthukumar. Studies on synchronization of fractional-order dynamical systems and its applications in secure communication. Thèse de Doctorat. The Gandhigram rural institute-Deemed University, Inde, 2015.

- [21] L. M. Pecora, T. L. Carroll. Synchronization in chaotic systems, *Physical Review Letters*, 64, pp. 821-825, 1990.
- [22] R. Mainieri, J. Rehacek. Projective synchronization in three-dimensional chaotic systems. *Phys. Rev. Lett.*, 82, pp. 3042-3045, 1999.
- [23] H.U. Voss. Anticipating chaotic synchronization. *Phys. Rev. E*, 61, pp. 5115-5119, 2000.
- [24] N.F. Rulkov, M.M. Sushchik, L.S. Tsimring, H.D.I. Abarbanel. Generalized synchronization of chaos in directionally coupled chaotic systems. *Phys. Rev. E.*, 51, pp. 980-994, 1995.
- [25] H. Nijmeijer, I. M. Y. Mareels. An Observer Looks at Synchronization. *IEEE Transaction on Circuits and Systems-I : Fundamental Theory and Applications*, 44(10), 1997.
- [26] H. Hamiche. Inversion à gauche des systèmes dynamiques hybrides chaotiques : Application à la transmission sécurisée de données. Thèse de Doctorat, université Mouloud Mammeri de Tizi-Ouzou, 2011.
- [27] A. Khadra, X.Z. Liu, X. Shen. Impulsively synchronizing chaotic systems with delay and applications to secure communication. *Automatica*, 41, pp. 1491-1502, 2005.
- [28] A. Ouannas, A.T. Azar, T. Ziar, A.G. Radwan. A Study on Coexistence of Different Types of Synchronization Between Different Dimensional Fractional Chaotic Systems. Chapitre du livre : Fractional Order Control and Synchronization of Chaotic Systems. *Studies in Computational Intelligence*, Springer, 688, 2017.
- [29] C. Goodrich, A.C. Peterson. Discrete fractional calculus. *Springer*, 2015.
- [30] M.K. Shukla, B.B. Sharma. Stabilization of Fractional Order Discrete Chaotic Systems, chapitre du livre *Fractional Order Control and Synchronization of Chaotic Systems*, *Studies in Computational Intelligence*, pp.431-445, 2017.
- [31] M.K. Shukla, B.B. Sharma. Investigation of chaos in fractional order generalized Hyperchaotic Henon map. *AEU-International Journal of Electronics and Communications*, 78, pp.265-273, 2017.

- [32] M. Feki, B. Robert, G. Gelle, M. Colas. Secure digital communication using discrete-time chaos synchronization. *Chaos, Solitons and Fractals*, 18(4), pp. 881-890 2003.
- [33] I. Belmouhoub, M. Djemai, J-P. Barbot. An example of nonlinear discrete-time synchronization of chaotic systems for secure communication. *European Control Conference (ECC)*, Cambridge, UK, 2003.
- [34] A. Razminia, V.J. Majd, D. Baleanu. Chaotic incommensurate fractional order Rössler system : active control and synchronization. *Advances in Difference Equations*, 15, 2011.
- [35] D.A. Vasseur. Biological Chaos and Complex Dynamics. Chapitre du livre : *Oxford Bibliographies in Ecology*, 2012.
- [36] D. Guégan. Chaos in economics and finance. *Annual Reviews in Control*, 33(1), pp. 89-93, 2009.
- [37] A. A. Fahmy. Implementation of the chaotic mobile robot for the complex missions. *Journal of Automation Mobile Robotics and Intelligent Systems*, 6 (2), pp. 8-12, 2012.
- [38] P. Zhou, F. Kuang. A Novel Control Method for Integer Orders Chaos Systems via Fractional-Order Derivative. *Discrete Dynamics in Nature and Society*, ID 217843, 2011.
- [39] F. Zhang, G. Chen, G. Li, J. Kurths. Chaos synchronization in fractional differential systems. *Phil. Trans. R. Soc. A* 371 : 20120155, 2014.
- [40] R. L. Bagley, R. A. Calico. Fractional order state equations for the control of viscoelastically damped structures. *Journal of Guidance, Control, and Dynamics*, 14 (2), pp. 304-311, 1991.
- [41] V.E. Tarasov. Fractional integro-differential equations for electromagnetic waves in dielectric media. *Theoretical and Mathematical Physics*, 158(3), pp. 355-359, 2009.
- [42] D. Kusnezov, A. Bulgac, G.D. Dang. Quantum Levy Processes and Fractional Kinetics. *Phys. Rev. Lett.*, 82, pp. 1136-1139, 1999.

- [43] H. Y. Jia, Z. Q. Chen, G. Y. Qi. Chaotic Characteristics Analysis and Circuit Implementation for a Fractional-order System. *IEEE Transactions on circuits and Systems-I : Regular Paper*, 61(3), 2014.
- [44] K. Alligood, T. Sauer, J. A. Yorke. Chaos : An Introduction to Dynamical Systems, *Springer*, 1997.
- [45] A. Isidori. Nonlinear Control Systems. 3rd edition, *Springer*, 1995.
- [46] H.K. Khalil. Nonlinear Systems : Third Edition. *Prentice Hall*, 2002.
- [47] S.S. Sastry. Nonlinear Systems Analysis, Stability, and Control. *Springer*, 1999.
- [48] D. Rontani. Dynamique Non-Linéaire de Composants Photoniques Cryptographie par Chaos et Multiplexage. Thèse de Doctorat. Supélec, 2001.
- [49] J.D. Farmer. Chaotic attractors of an infinite-dimensional dynamical system, *Physica D*, 4, pp. 366-393, 1982.
- [50] D. Ruelle, F. Takens. On the nature of turbulence, *Commun. Math. Phys.*, 20, pp. 167-192, 1971.
- [51] E. Ott. Strange attractors and chaotic motions of dynamical systems. *Rev. Mod. Phys.*, 53, pp.655-671,1981.
- [52] J. Milnor. On the concept of attractor. *Comm. Math. Phys.*, 99 (2), pp. 177-195, 1985.
- [53] T. Hamaizia, Systèmes Dynamiques et Chaos :Application à l'optimisation a l'aide d'algorithme chaotique. Thèse de Doctorat. Université de Constantine 1, 2013.
- [54] G. Delaporte. Physiques d'Aristote- Tome I. *Paris : l'Harmattan*, 2008.
- [55] J. C. Maxwell, Matter and Motion, 1876.
- [56] H. Poincaré. Sur le problème des trois corps and les équations de la dynamique. *Acta mathematica*, 13, pp.1-270, 1890.
- [57] R. Kautz, Chaos : The science of predictable random motion, *Oxford University Press*, 2011.
- [58] E.N. Lorenz. Deterministic nonperiodic flow, *J. Atmos. Sci.*, 20, pp. 130-141, 1963.

- [59] E.N. Lorenz. Predictability : Does the flab of butterfly's wings in Brazil set off a tornado in Texas. *American Association for the Advancement of Science Conference*, 1972.
- [60] T.Y. Li, J. A. Yorke. Period Three Implies Chaos. *The American Mathematical Monthly*, 82(10), pp. 985-992, 1975
- [61] M. Feigenbaum. Quantitative universality for a class of nonlinear transformation. *J. Stat. Phys.*, 19, pp. 25-52, 1978.
- [62] T. Matsumoto. A chaotic attractor from Chua's circuit. *IEEE Transactions on Circuits and Systems*, 31(12), 1984.
- [63] R. C. Hilborn. Chaos and nonlinear dynamics : An introduction for scientists and engineers. *Oxford University Press*, New York, 2000.
- [64] R. May. Simple mathematical models with very complicated dynamics. *Nature*, 261, pp. 459-467, 1976.
- [65] F. Anstett. Les systèmes dynamiques chaotiques pour le chiffrement : Synthèse et cryptanalyse. Thèse de Doctorat. Université Henri Poincaré Nancy 1, 2006.
- [66] J. M. González-Miranda. Synchronization and control of chaos - An Introduction for Scientists and Engineers. *Imperial College Press*, 2004.
- [67] Y. Chen, A. Y. T. Leung. Bifurcation and Chaos in Engineering. *Springer-Verlag*, 1998.
- [68] R. Kharel. Design and Implementation of Secure Chaotic Communication Systems. Thèse de Doctorat. Université de Northumbria à Newcastle, 2011.
- [69] K. Feltekh. Analyse spectrale des signaux chaotiques. Thèse de Doctorat. École nationale d'ingénieurs de Tunis - ED-STI et Institut National des Sciences Appliquées de Toulouse - EDSYS, 2014.
- [70] G.B. Mindlin, X.-J. Hou, H.G. Solari, R. Gilmore, N.B. Tufilaro. Classification of strange attractors by integers. *Phys. Rev. Lett.*, 64 (20), pp. 2350-2353, 1990.
- [71] B. Mandelbrot. The Fractal Geometry of Nature, *Freeman edition*, 1982.

-
- [72] A. Ouannas, R. Abu-Saris. On Matrix Projective Synchronization and Inverse Matrix Projective Synchronization for Different and Identical Dimensional Discrete-Time Chaotic Systems. *Journal of Chaos*, ID 4912520, 2016.
- [73] G.L. Baker, J.P. Gollub. Chaotic dynamics : an Introduction. Second Edition *CAMBRIDGE University Press*, 1996.
- [74] H. G. Schuster, W. Just. Deterministic Chaos : An Introduction. *Wiley-VCH Verlag*, 1995.
- [75] M. Rosentsein, J. Collins, C. De Luca. A practical method for calculating largest Lyapunov exponents for small data sets. *Physica, D* 65, pp. 117-134, 1993.
- [76] A. Wolf, J. Swift, H. Swinney, J. Vastano. Determining Lyapunov exponents from a time series. *Physica*, 16, pp. 285-317, 1985.
- [77] M.B. Luca. Apport du chaos et des estimateurs d'états pour la transmission sécurisée de l'information. Thèse de Doctorat. Université de Bretagne occidentale, France, 2010.
- [78] J.D. Crawford. Introduction to bifurcation theory. *Rev. Mod. Phys.*, 63, pp. 991-1037, 1991.
- [79] Y. A. Kuznetsov. Elements of applied bifurcation theory. Second edition, *Springer*, 2004.
- [80] J.-P. Eckmann. Roads to turbulence in dissipative dynamical systems. *Rev. Mod. Phys.*, 53, pp. 643-654, 1981.
- [81] B. Pierre, B. Yves, V. Christian. Order within Chaos. *Wiley Interscience*, 1987.
- [82] Y. Pomeau, P. Manneville. Intermittent transition to turbulence in dissipative dynamical systems. *Communications in Mathematical Physics*, 74, pp. 189-197, 1980.
- [83] L.O. Chua, C.W. Wah, A. Huang, G. Zhong. A universal circuit for studying and generating chaos, part I : routes to chaos. *IEEE. Trans. Circuits Syst.*, 40(10), pp. 732-744, 1993.

- [84] S. Newhouse, D. Ruelle, F. Takens. Occurrence of strange Axiom A attractors near quasi-periodic flows on T_m , $m \geq 3$. *Communications in Mathematical Physics*, 64, pp. 35-40, 1978.
- [85] T. Matsumoto, L.O. Chua, R. Tokungara. Chaos via torus breakdown. *IEEE Trans. Circ. Sys.* 34 (3), pp. 240-253, 1987.
- [86] B. Muthuswamy, S. Benerjee. A route to chaos using FPGAs, volume I : Experimental Observations. *Springer*, 2015.
- [87] S. He, H. Wang, K. Sun. Dynamics and Synchronization of the Fractional-Order Hyperchaotic System. Chapitre du livre : A. Boulkroune, S. Ladaci. Advanced Synchronization Control and Bifurcation of Chaotic Fractional-Order Systems. *IGI Global*, pp. 23- 53, 2018.
- [88] EH. Shen, ZJ. Cai, FJ. Gu, Mathematical foundation of a new complexity measure. *Applied Mathematics and Mechanics*, 26 (9), pp 1188-1196, 2005.
- [89] S. He, K. Sun, H. Wang. Complexity Analysis and DSP Implementation of the Fractional-Order Lorenz Hyperchaotic System. *Entropy*, 17, pp. 8299-8311, 2015.
- [90] G.A. Gottwald, I. Melbourne,. A new test for chaos in deterministic systems. *Proc. R. Soc. Lond. A*, 460, pp. 603-611, 2004.
- [91] D. Cafagna, G. Grassi. Fractional-order Chua's circuit : time-domain analysis, bifurcation, chaotic behavior and test for chaos. *International Journal of Bifurcation and Chaos*, 18(03), pp. 615-639, 2008.
- [92] G.W. Leibniz, Letter from hanover, germany, to john wallis. *Mathematische Schriften*, 1697, Reprinted 1962.
- [93] L. Euler. De progressionibus transcentibus, seu quarum termini algebraice dari nequeunt. *Comment. Acad. Sci. Imperialis Petropolitanae*, 5, pp. 36-57, 1738.
- [94] J.B.J. Fourier. Théorie Analytique de la Chaleur. Oeuvres de Fourier, Didot, Paris, 1822.
- [95] K. S. Miller, B. Ross. An Introduction to the Fractional Calculus and Fractional Differential Equations. *John Wiley and Sons*, New York, NY, USA, 1993.

-
- [96] N.H. Abel. Solution De quelques Problèmes a L'aide Intégrales Définies, oeuvres Complètes-1, *Grondahl Christiania*, Norway, pp. 11-18, 1881.
- [97] J. Liouville. Memoire sur le calcul des différentielles à indices quelconques. *J. Ecole Polytechnique* 13, pp. 71-162, 1832.
- [98] B. Riemann. Versuch einer allgemeinen auffassung der integration und differentiation. *Gesammelte Werke*, 1876.
- [99] A. K. Grünwald. Über begrenzte derivationen und deren anwendung. *Zeitschrift für Mathematik und Physik*, 12, pp. 441-480, 1867.
- [100] A. V. Letnikov. Theory of differentiation with an arbitrary index. *Mat. Sb.*, 3, pp. 1-66, 1868.
- [101] O. Heaviside. Electromagnetic theory. *The Electrician printing and publishing company*, ltd., London, 1893. Reprinted by Benn, London 1922.
- [102] H. Weyl. Bemerkungen zum begriff des differentialquotienten gebrochener ordnung vierteljahresschr. *Naturforschende Gesellschaft in Zürich*, 62, pp. 296-302, 1917.
- [103] M. Riesz. L'intégrale de Riemann-Liouville et le problème de Cauchy. *Acta Mathematica*, 81(1), pp. 1-222, 1949.
- [104] M. Caputo. Linear models of dissipation whose q is almost frequency independent-II. *Geophysical Journal of the Royal Astronomical Society*, 13(5), pp. 529-539, 1967.
- [105] K.B. Oldham, J. Spanier. The replacement of fick's laws by a formulation involving semidifferentiation. *J. Electroanal. Chem.*, 26, pp 331-341, 1970.
- [106] I. Podlubny. Fractional-order system and fractional-order controllers. Technical Report UEF-03-94, Institute of Experimental Physics, Academy of Sciences, Slovakia, 1994.
- [107] R.L. Bagley, P.J. Torvik. On the appearance of the fractional derivatives in the behaviour of real materials. *J. Applied Mechanics*, 41, pp. 294-298, 1984.
- [108] V.H. Schmidt, J. E. Drumheller. Dielectric properties of lithium hydrazinium sulfate. *Physical Review B*, 4, pp.4582-4597, 1971.

- [109] J.A. Ochoa-Tapia, F.J. Valdes-Parada, J. Alvarez-Ramirez. A fractional-order Darcy's law. *Physica A : Statistical Mechanics and its Applications*, 374, pp 1-14, 2007.
- [110] B. Goodwine. Modeling a multi-robot system with fractional-order differential equations. *Proceedings- IEEE International Conference Robotics and Automation (ICRA)*, pp 1763-1768, 2014.
- [111] L. J. Sheu. A speech encryption using fractional chaotic systems. *Nonlinear Dynamics*, 65(1-2), pp. 103-108, 2011.
- [112] G. Sarwas. Modelling and Control of Systems with Ultracapacitors Using Fractional Order Calculus. Thèse de Doctorat. Université de Warsaw, 2012.
- [113] H. T. Davis. The theory of linear operators. *Principia Press*, 1936.
- [114] M.S. Abdelouahab. Les systèmes chaotiques à dérivées fractionnaires. Thèse de doctorat, Université de Constantine 1, 2013.
- [115] I. N'Doye. Généralisation du lemme de Gronwall-Bellman pour la stabilisation des systèmes fractionnaires. Thèse de Doctorat. Université Henri Poincaré-Nancy 1, 2011.
- [116] G.M. Mittag-Leffler. Sur la nouvelle fonction $E_\alpha(x)$. *C. R. Académie des Sciences*, 137 pp 554-558, 1903.
- [117] R.P. Agarwal. A propos d'une note de M. Pierre Humbert. *C. R. Académie des Sciences*, 236, pp 2031-2032, 1953.
- [118] R. Gorenflo, A. A. Kilbas, S. V. Rogosin. On the generalized mittag-leffler type functions. *Integral Transform. Spec. Funct.*, 7, pp. 215-224, 1998.
- [119] M. M. Djrbashian. Harmonic Analysis and Boundary Value problems in the Complex Domain. *Operator theory : Advances and applications*, 1st Edition, Birkhäuser, 1993.
- [120] K. B. Oldham, J. Spanier. The Fractional Calculus. *Academic Press*, New York, 1974.
- [121] I. Podlubny. Fractional Differential Equations, *Academic Press*, New York, 1999.
- [122] M. Caputo, F. Mainardi. A new dissipation model based on memory mechanism. *Pure and Applied Geophysics*, 91, pp. 134-137, 1971.

- [123] C.A. Monje, Y.-Q. Chen, B. M. Vinagre, D. Xue, V. Feliu. Fractional-order systems and controls : Fundamentals and Applications. *Springer*, 2010.
- [124] R. Mansouri. Contribution à l'analyse et à la synthèse des systèmes d'ordres fractionnaire par la représentation d'état. Thèse de Doctorat. Université Mouloud Mammeri de Tizi-Ouzou de Tizi-Ouzou, 2008.
- [125] D. Matignon, B. D'Andrea-Novel. Some results on controllability and observability of finite-dimensional fractional differential systems. *Computational Engineering in Systems Applications*, Lille, France, 2, pp. 952-956, 1996.
- [126] D. Mozyrska, E. Pawluszewicz. Local controllability of nonlinear discrete-time fractional order systems. *Bull. Pol. Ac. : Tech.*, 61(01), pp. 251-256, 2013.
- [127] F. Chen, X. Luo, Y. Zhou. Existence results for nonlinear fractional difference equation. *Advances in Difference Eq.*, ID 713201, pp. 1-12, 2011.
- [128] G.A. Anastassiou. Discrete Fractional Calculus and Inequalities. <https://arxiv.org/pdf/0911.3370>, 2009.
- [129] T. Abdeljawad. On Riemann and Caputo fractional differences. *Comp. and Math. with Appl.*, 13(3), pp. 1602-1611, 2011.
- [130] F. M. Atici, P. W. Eloe. Initial value problems in discrete fractional calculus. *Proceedings of the American Mathematical Society*, 137, pp. 981-989, 2009.
- [131] G.-C. Wu, D. Baleanu, H. -P. Xie, F. -L. Chen. Chaos synchronization of fractional chaotic maps based on the stability condition. *Physica A : Statistical Mechanics and its Applications*, 460, pp. 374-383, 2016.
- [132] G.A. Anastassiou. Intelligent Mathematics : Computational Analysis, *Springer*, Berlin, 2011.
- [133] M.T. Holm. The Theory of Discrete Fractional Calculus : Development and Application. University of Nebraska, Lincoln, 2011.
- [134] A.A. Kilbas, H.M. Srivastava, J.J. Trujillo. Theory and application of fractional differential equations. In : vanMill, J. (ed.) North Holland Mathematics Studies. Elsevier, Amsterdam, 2006.

- [135] X. Liao, Z. Gao, H. Huang. Synchronization control of fractional-order discrete-time chaotic systems. *In : European Control Conference (ECC)*, Zürich, Switzerland, 2013.
- [136] S. Guermah, M. Bettayeb, S. Djennoune. Controllability and the observability of linear discrete-time fractional-order systems. *Int. J. Appl.Math. Comput. Sci.*, 18, pp 213-222, 2008.
- [137] A. Dzielinski, D. Sierociuk. Observer for discrete fractional order state-space systems. *In Proceedings of 2nd IFAC Workshop on Fractional Differentiation and its Applications, IFAC FDA'06*, pp 524-529. Porto, Portugal, 19-21 Juillet, 2006.
- [138] A. Dzielinski, D. Sierociuk. Adaptive feedback control of fractional order discrete state-space systems. *In Computational Intelligence for Modelling, Control and Automation, 2005 and International Conference on Intelligent Agents, Web Technologies and Internet Commerce, International Conference on*, 1, pp 804-809, 2005.
- [139] O.E. Rössler. An equation for continuous chaos. *Physics Letters A*, 57(5), pp. 397-398, 1976.
- [140] C.G. Li, G. Chen. Chaos and hyperchaos in fractional order Rössler equations. *Physica A*, 341, pp. 55-61, 2004.
- [141] T. Zhou, Y. Tang, G. Chen. Chen's attractor exists. *International Journal of Bifurcation and Chaos*, 14, 3167-3177, 2004.
- [142] J. G. Lu, G. Chen. A note on the fractional-order Chen system. *Chaos, Solitons and Fractals*, 27, pp. 685-688, 2006.
- [143] O. Megherbi, S. Kassim, H. Hamiche, S. Djennoune. A New robust hybrid transmission scheme based on the synchronization of discrete-time chaotic systems. *In : International Workshop on Cryptography and its Applications (IWCA'16)*, Oran, Algeria, (2016).
- [144] X.-S. Yang. Concept of synchronization in dynamical systems. *Physics Letters A*, 260, pp. 340-344, 1999.
- [145] J. Buck, E. Buck. Synchronous fireflies. *Scientific American*, 234(5), pp. 74-85, 1976.

- [146] T. Danino, O. Mondragón-Palomino, L. Tsimring, J. Hasty. A synchronized quorum of genetic clocks. *Nature*, 463, pp. 326-330, 2010.
- [147] D.P. Taylor. Introduction to "Synchronous Communications". *Proceedings of the IEEE*, 90(8), 2002.
- [148] R.A. Filatov, A.E. Hramov, A.A Koronovskii. Chaotic synchronization in coupled spatially extended beam-plasma systems, *Physics Letters A*, 358(4), pp. 301-308, 2006.
- [149] Y.-N. Li, L. Chen, Z.-S. Cai, X.-Z. Zhao. Chaos Synchronization in the Belousov-Zhabotinsky Chemical Reaction by Adaptive Control Scheme. *chinese journal of chemistry*, 20, pp. 753-759, 2002.
- [150] H. Hamiche, S. Guermah, S. Djennoune, K. Kemih, M. Ghanes, J.-P. Barbot. Chaotic synchronisation and secure communication via sliding-mode and impulsive observers. *International Journal of Modelling, Identification and Control*, 20(4), pp. 305-318, 2013.
- [151] A. Zhu, H. Leung. Cooperation Random Mobile Robots Based on Chaos Synchronization. *Mechatronics, ICM2007 4th IEEE International Conference on*, Kumamoto Japan, 2007.
- [152] C. Huyghens. *Horologium oscillatorium*. 1673.
- [153] A. Ouannas. Sur La Synchronisation des Systèmes Chaotiques Discrets. Thèse de Doctorat. Université Frères Mentouri à Constantine, 2015.
- [154] M. Riaz. Synchronization Control for Master-Slave Systems Subject to Nonlinearities and Time Delay. Thèse de Doctorat. Capital University OF Science and Technology, Islamabad, Pakistan, 2016.
- [155] H. Fujisaka, T. Yamada. Stability theory of synchronized motion in coupled oscillator systems, *Prog. Theor. Phys.*, 69 (1), pp. 32-47, 1983.
- [156] V.S. Afraimovich, N.N. Verichev, M.I. Rabinovich. Stochastic synchronization of oscillation in dissipative systems. *Radiophysics and Quantum Electronics*, 29(9), pp. 1050-1056, 1986.

- [157] T.L. Carroll, L.M. Pecora. Synchronizing chaotic circuits. *IEEE Trans. Circuits Syst. I*, 38(4) pp.453-456, 1991.
- [158] M. Hu, Z. Xu. General scheme for Q-S synchronization of chaotic systems. *Nonlinear Analysis : Theory, Methods and Applications*, 69 (4), pp. 1091-1099, 2008.
- [159] M. G. Rosenblum, A. S. Pikovsky, J. Kurths. Phase synchronization of chaotic oscillators. *Phys. Rev. Lett*, 76, pp. 1804-1807, 1996.
- [160] X. Wu, G. Chen, J. Cai. Chaos synchronization of the master-slave generalized Lorenz systems via linear state error feedback control. *Physica D : Nonlinear Phenomena*, 229(1), pp. 52-80, 2007.
- [161] M.T. Yassen. Controlling, synchronization and tracking chaotic Liu system using active backstepping design. *Physics Letters A*, 360(4-5), pp. 582-587, 2007.
- [162] X. Tan, J. Zhang, Y. Yang. Synchronizing chaotic systems using backstepping design. *Chaos, Solitons and Fractals*, 16 (1), pp. 37-45, 2003.
- [163] G. Abay, T. Aldemir. Synchronization of different chaotic systems using generalized active control. *Electrical and Electronics Engineering ELECO, International Conference on*, Bursa, Turquie, 2009.
- [164] R. Guo. A simple adaptive controller for chaos and hyperchaos synchronization. *Physics Letters A*, 372(34), pp. 5593-5597, 2008.
- [165] S. Chen, J. Lü. Synchronization of an uncertain unified chaotic system via adaptive control. *Chaos, Solitons and Fractals*, 14 (4), pp. 643-647, 2002.
- [166] B.A. Idowu, R. Guo, U. E. Vincent. Adaptive control for the strabilization and synchronization of nonlinear Gyroscopes. *International Journal of Chaos, Control, Modelling and Simulation (IJCCMS)*, 2(2), 2013.
- [167] F. Shi-Hui, L. Qi-Shao, D. Ying. Adaptive H_∞ synchronization of chaotic systems via linear and nonlinear feedback control. *Chinese Physics B*, 21(6), 2012.
- [168] A. Khan, S. Kumar. T-S Fuzzy Modeling and Synchronization of Chaotic Systems. *Journal of Uncertain Systems*, 10(4), pp. 251-259, 2016.

- [169] G. Besaçon. Nonlinear observer and Applications. *Series Lecture Notes in Control and Information Science*, Springer Verlag, Berlin Heidelberg New York, 2007.
- [170] A. Zemouche. Sur l'observation de l'état des systèmes dynamiques non linéaires. Thèse de Doctorat. Université Louis Pasteur Strasbourg I, 2007.
- [171] A.J. Krener, A. Isidori. Linearization by output injection and nonlinear observers. *Systems and Control Letters*, 3 (1), pp. 47-52, 1983.
- [172] F.E. Thau. Observing the state of non-linear dynamic systems. *International Journal of Control*, 17(3), pp 471-479, 1973.
- [173] M. Arcak, P. Kokotović. Nonlinear observers : a circle criterion design and robustness analysis. *Automatica*, 37(12), pp. 1923-1930, 2001.
- [174] W. Lohmiller, J.-J.E. Slotine. On Contraction Analysis for Non-linear Systems. *Automatica*, 34(6), pp. 683-696, 1998.
- [175] C. Hua, X. Guan, X. Li, P. Shi. Adaptive observer-based control for a class of chaotic systems. *Chaos, Solitons and Fractals*, 22, pp. 103-110, 2004.
- [176] I. Belmouhoub, M. Djemai, J.-P. Barbot, K. Busawon. Discrete-time synchronization of chaotic systems for secure communication. *Communication Systems, Networks and Digital Signal Processing (CSNDSP), International Symposium on*, Poznan, Pologne, 2012.
- [177] L. Boutat-Baddas, J.-P. Barbot, D. Boutat, R. Tauleigne. Sliding Mode Observers and Observability Singularity in Chaotic Synchronization. *Mathematical problems in engineering*, pp. 11-31, 2004.
- [178] M. Stork, J. Hrusak, D. Mayer. Discrete-Time Chaotic Systems Impulsive Synchronization and Data Transmission. *Proceedings of the 13th WSEAS International Conference on Systems*, pp. 127-132, 2017.
- [179] A. Khadra, X. Liu, X. Shen. Application of impulsive synchronization to communication security. *IEEE Transactions on Circuits and Systems I : Fundamental Theory and Applications*, 44(10), pp. 341-351, 1997.

- [180] V. Lakshmikantham, D.D. Bainov, P.S. Simeonov. Theory of Impulsive Differential Equations. *Series in Modern Applied Mathematics*, 6, World Scientific, Singapore, 1989.
- [181] T. Yang, L.O. Chua. Impulsive stabilization for control and synchronization of chaotic systems : theory and application to secure communication. *IEEE Transactions on Circuits and Systems I : Fundamental Theory and Applications*, 44(10), pp. 976-988, 1997.
- [182] T. Yang. Impulsive control theory. *Lecture Notes in Control and Information Sciences*, Springer, 2001.
- [183] T. Yang, L.B. C.M. Yang, Yang. Impulsive synchronization of Lorenz systems. *Physics Letters A*, 226(6), pp. 349-354, 1997.
- [184] Y.A. Zheng, Y.B. Nian, Z.R.Liu. Impulsive Control for the Stabilization of Discrete Chaotic System. *Chinese Physics Letters*, 19(9), pp. 1251-1253, 2002.
- [185] H. Hamiche, O. Megherbi, R. Kara, R. Saddaoui, M. Laghrouche, S. Djennoune. A new implementation of an impulsive synchronization of two discrete-time hyperchaotic systems using Arduino-Uno boards. *International Journal of Modelling, Identification and Control*, 28(2), pp. 177-186, 2017 .
- [186] Y.A. Zheng, Y.B. Nian, Z.R.Liu. Impulsive Synchronization of Discrete Chaotic Systems. *Chinese Physics Letters*, 20 (2), pp. 199-201, 2003.
- [187] C. Li, X. Liao, J. Yu ; Synchronization of fractional order chaotic systems. *Phys. Rev. E*, 68, 067203, 2003.
- [188] M.J. Wang, X.Y. Wang. Generalized Synchronization of Fractional order Chaotic Systems. *International Journal of Modern Physics B*, 25 (9), pp. 1283-1292, 2011.
- [189] P. Zhou, W. Zhu. Function projective synchronization for fractional-order chaotic systems. *Nonlinear Analysis : Real World Applications*, 12 (2), pp.811-816, 2011.
- [190] C. Li. Phase and Lag Synchronization in coupled fractional order chaotic oscillators. *International Journal of Modern Physics B*, 21 (30), pp. 5159-5166, 2007.

- [191] Y. Tang, Z. Wang, J. Fang. Pinning control of fractional order weighted complex networks. *Chaos*, 19, 013112, 2009.
- [192] X. Wu, D. Lai, H. Lu. Generalized synchronization of the fractional-order chaos in weighted complex dynamical networks with nonidentical nodes. *Nonlinear Dyn.*, 69, pp. 667-683, 2012.
- [193] S. Bhalekar, V. Daftardar-Gejji. Synchronization of different fractional order chaotic systems using active control. *Commun Nonlinear Sci. Numer. Simulat.*, 15, pp. 3536-3546, 2010.
- [194] D. Matignon. Stability Results For Fractional Differential Equations With Applications To Control Processing. In *Computational Engineering in Systems Applications*, 2, pp. 963-968, 1996.
- [195] G.T. He, M.K. Luo. Dynamic behavior of fractional order Duffing chaotic system and its synchronization via singly active control. *Applied Mathematics and Mechanics*, 33(5), pp. 567-582, 2012.
- [196] A.K. Singh, V.K. Yadav, S. Das. Comparative study of synchronization methods of fractional order chaotic systems. *Nonlinear Engineering*, 5(3), pp.185-192, 2016.
- [197] L. Song, J. Yang, S. Xu. Chaos synchronization for a class of nonlinear oscillators with fractional order. *Nonlinear Analysis*, 72, pp. 2326-2336, 2010.
- [198] G.C. Wu, D. Baleanu, Chaos synchronization of the discrete fractional logistic map. *Signal Processing*, 102, pp. 96-99, 2014.
- [199] B. Xin, L. Liu , G. Hou, Y. Ma. Chaos Synchronization of Nonlinear Fractional Discrete Dynamical Systems via Linear Control. *Entropy*, 19(7), 351, 2017.
- [200] X. Liao, Z. Gao, H. Huang. Synchronization Control of Fractional-Order Discrete-Time Chaotic Systems. *European Control Conference (ECC)*, Zürich, Switzerland, 2013.
- [201] M.K. Shukla, B.B. Sharma. Backstepping based stabilization and synchronization of a class of fractional order chaotic systems. *Chaos, Solitons and Fractals*, 102, pp. 274-284, 2017.

- [202] U.E. Vincent, Chaos Synchronization Using Active Control and Backstepping Control : A Comparative Analysis. *Nonlinear Analysis : Modelling and Control*, 13(2), pp. 253-261, 2008.
- [203] S.H. Hosseinnia, R. Ghaderi, A. Ranjbar, J. Sadati, S. Momani. Synchronization of Gyro Systems via Fractional-Order Adaptive Controller. Chapitre du livre : *New Trends in Nanotechnology and Fractional Calculus Applications*. Springer, Dordrecht, 2010.
- [204] Z. Ruo-Xun, Y. Shi-Ping. Modified adaptive controller for synchronization of incommensurate fractional-order chaotic systems. *Chin. Phys. B*, 21(3), 2012.
- [205] C. Li, Y. Tong. Adaptive control and synchronization of a fractional-order chaotic system. *Pramana-journal of physics*, 80 (4), pp. 583-592, 2013.
- [206] K. Rabah, S. Ladaci, M. Lashab. A novel fractional sliding mode control configuration for synchronizing disturbed fractional-order chaotic systems. *Pramana - J. Phys.*, 89 :46, 2017.
- [207] U.M. Al-Saggaf, M. Bettayeb, S. Djennoune. Super-Twisting Algorithm-Based Sliding-Mode Observer for Synchronization of Nonlinear Incommensurate Fractional-Order Chaotic Systems Subject to Unknown Inputs. *Arabian Journal for Science and Engineering*, 42(7), pp. 3065-3075, 2017.
- [208] L. Huang, L. Wang, D. Shi. Discrete Fractional Order Chaotic Systems Synchronization Based on the Variable Structure Control with a New Discrete Reaching-law. *IEEE/CAA Journal of Automatica Sinica*, 2016.
- [209] M. Bettayeb, U. M. Al-Saggaf, S. Djennoune. High gain observer design for fractional-order non-linear systems with delayed measurements : application to synchronisation of fractional-order chaotic systems. *IET Control Theory and Applications*, 11(17), pp. 3171-3178, 2017.
- [210] A. Kiani-B, K. Fallahi, N. Pariz, H. Leung. A chaotic secure communication scheme using fractional chaotic systems based on an extended fractional Kalman filter. *Nonlinear Sci. Numerical Simulat.*, 14, pp. 863-879, 2007.

- [211] S. Kassim, H. Hamiche, S. Djennoune, M. Bettayeb. A novel secure image transmission scheme based on synchronization of fractional-order discrete-time hyperchaotic systems. *Nonlinear Dyn.*, 88(4), pp. 2473-2489, 2017.
- [212] X. Y. Wang, Y.L. Zhang, D. Lin, N. Zhang. Impulsive synchronisation of a class of fractional-order hyperchaotic systems. *Chinese Physics B*, 20(3), 030506, 2011.
- [213] J. Fu, M. Yu, T.D. Ma. Modified impulsive synchronization of fractional order hyperchaotic systems. *Chin. Phys. B*, 20(12), 120508, 2011.
- [214] T.D. Ma, W.B. Jiang, J. Fu, Impulsive synchronization of fractional order hyperchaotic systems based on comparison system. *Acta Phys. Sin.*, 61(9), 090503, 2012.
- [215] J.G. Liu. A novel study on the impulsive synchronization of fractional-order chaotic systems. *Chin. Phys. B*, 22(6), 060510, 2013.
- [216] M. Bettayeb, S. Djennoune, S. Guermah, M. Ghanes. Structural Properties of Linear Discrete-Time Fractional-Order Systems. *Proceedings of the International Federation of Automatic Control (IFAC)*, Seoul, Korea, (2008).
- [217] B. Liu, H.J. Marquez. Uniform Stability of Discrete Delay Systems and Synchronization of Discrete delay Dynamical Networks via Razumikhin Thechnique. *IEEE Trans. on Circuits and Systems-I :Regular Papers*, 55(9), 2008.
- [218] O. Megherbi, H. Hamiche, S. Djennoune, M. Bettayeb. A new contribution for the impulsive synchronization of fractional-order discrete-time chaotic systems. *Nonlinear Dyn*, 90 (3), pp. 1519 -1533, 2017.
- [219] A.D. Pano-Azucena, J.J. Rangel-Magdaleno, E. Tlelo-Cuautle, A.J. Quintas-Valles. Arduino-based chaotic secure communication system using multi-directional multi-scroll chaotic oscillators. *Nonlinear Dyn*, DOI 10.1007/s11071-016-3184-4, 2016.
- [220] Arduino : www.arduino.cc
- [221] S. Revathy. Secure Crypto System for Image Encryption and Data Embedding using Chaos and BB Equation Algorithm. *International Journal of Computer Science and Mobile Computing*, 3(3), pp. 297-306, 2014.

- [222] S. Somaraj, M. A. Hussain. Performance and Security Analysis for Image Encryption using Key Image. *Indian Journal of Science and Technology*, 8(35), 2015.
- [223] M. Kumar, A. Aggarwal, A. Garg. A review on various digital image encryption techniques and security criteria. *International journal of Computer applications*, 96(13), pp. 19-26, 2014.
- [224] A.S. Dongare, A. S. Alvi, N. M. Tarbani. An Efficient Technique for Image Encryption and Decryption for Secured Multimedia Application. *International Research Journal of Engineering and Technology (IRJET)*, 04 (04), pp. 3186-3190, 2017.
- [225] J.J. Montesinos-García, R. Martínez-Guerra, S.M. Delfín-Prieto. Color image encryption using chaotic systems synchronization. *Electrical Engineering, Computing Science and Automatic Control (CCE), 13th International Conference on*, mexico city, Mexico, 2016.
- [226] S. Wang, W. Sun, C.-Y. Ma, D. Wang, Zheng-Chen. Secure Communication based on a Fractional Order Chaotic System. *International Journal of Security and Its Applications*, 7(5), pp. 205-216, 2013.
- [227] O. Goldreich. Foundation of cryptography : volume 2, basic applications, *Cambridge university press*, 2004.
- [228] M. Abutaha, M. Farajallah, R. Tahboub, M. Odeh. Survey Paper : Cryptography Is The Science Of Information Security. *International Journal of Computer Science and Security (IJCSS)*, 5(3), pp. 298-309, 2011.
- [229] Z. Kotulski, J. Szczepański. Discrete chaotic cryptography (DCC), New method for secure communication, *Annalen der physik*, 6(5), pp. 381-394, 1997.
- [230] E. Biham, A. Shamir. Differential Cryptanalysis of DES-like Cryptosystems, *Journal of Cryptology*, 4(1), pp 3-72, 1991.
- [231] A. Curiger, H. Bonnenberg, R. Zimmermann, N. Felber, H. Kaeslin, W. Fichtner. VINCI : VLSI implementation of the new secret-key block cipher IDEA, *in Custom Integrated Circuits Conference, Proceedings of the IEEE*, 1993.

- [232] P. Patil, P. Narayankar, D.G. Narayan, S. M. Meena. A comprehensive evaluation of cryptographic algorithms : DES, 3DES, AES, RSA and Blowfish. *Procedia Computer Science*, 78, pp. 617-624. Science Direct, 2016.
- [233] C. Chitu, M. Glesner. An FPGA implementation of the AES-Rijndael in OCB/ECB modes of operation. *Microelectronics Journal*, 36(2), p. 139-146, 2005.
- [234] R.L. Rivest, A. Shamir, L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2), pp. 120-126, 1978.
- [235] C. Shannon, Communication Theory of Secrecy Systems, *Bell Systems Technical Journal*, 4, 1949.
- [236] G. Alvarez, P. Montoya, G. Pastor, M. Romera. Chaotic cryptosystems. In Security Technology. *Proceedings, IEEE 33rd Annual 1999 International Carnahan Conference on*, pp. 332-338, 1999.
- [237] G. Alvarez, S. Li. Cryptographic requirements for chaotic secure communications. *International Journal of Bifurcation and Chaos*, 16 (8), pp 2129-2151, 2006.
- [238] L. Kocarev. Chaos-based cryptography : A brief overview. *IEEE Circuits and Systems Magazine*, 1, pp 6-21, 2001.
- [239] S. Wolfram. Cryptography with cellular automata, in Advances in Cryptology - Crypto'85. *Lecture Notes in Computer Science*, Springer-Verlag, Berlin, 1985.
- [240] P. Guan. Cellular automaton public-key cryptosystem. *Complex Systems*, 1, pp. 51-57, 1987.
- [241] R.A.J. Matthews. On the derivation of a "chaotic" encryption algorithm. *Cryptologia*, 13(1), pp. 29-42, 1989.
- [242] M.M. Maqableh. Analysis and Design Security Primitives Based on Chaotic Systems for eCommerce. Thèse de Doctorat. Université de Durham, UK, 2012.
- [243] D.D. Wheeler, R.A.J. Matthews. Supercomputer Investigations of a Chaotic Encryption Algorithm. *Cryptologia*, 15, pp. 140-152, 1991.
- [244] E. Biham. Cryptanalysis of the chaotic-map cryptosystem suggested at EUROCRYPT'91. in Proceedings of the EUROCRYPT'91, Springer, Berlin, 1991.

- [245] B. Preneel, V. Rijmen, A. Bosselaers. Recent developments in the design of conventional cryptographic algorithm. in *Lecturer Notes in Computer Science Springer-Verlag*, Berlin, Germany, pp. 106-131, 1998.
- [246] G. Jakimoski, L. Kocarev. Analysis of some recently proposed chaos based encryption algorithms. *Physics Letters A*, 291(6), 2001.
- [247] D. Yang, X. Liao, Y. Wang, H. Yang, P. Wei. A novel chaotic block cryptosystem based on iterating map with output-feedback. *Chaos, Solitons and Fractals*, 41(1), pp. 505-510, 2009.
- [248] J.A. Martínez-Ñonthea, A. Castañeda-Solisa, A. Díaz-Méndezb, M. Cruz-Irissona, R. Vázquez-Medina. Chaotic block cryptosystem using high precision approaches to tent map. *Microelectronic Engineering*, 90, pp. 168-172, 2012.
- [249] K.-W. Wong. A combined chaotic cryptographic and hashing scheme. *Physics Letters A*, 307(5-6), , pp. 292-298, 2003.
- [250] X. Yi. Hash function based on chaotic tent maps. *Circuits and Systems II : Express Briefs, IEEE Transactions on*, 52(6) : pp. 354-357, 2005.
- [251] D. Xiao, X. Liao, S. Deng. One-way Hash function construction based on the chaotic map with changeable-parameter. *Chaos, Solitons and Fractals*, 24(1). p. 65-71, 2005.
- [252] J. Zhang, X. Wang, W. Zhang. Chaotic keyed hash function based on feedforward-feedback nonlinear digital filter. *Physics Letters A*, 362(5- 6), p 439-448, 2007.
- [253] Zheng F. X.-j. Tian, J.-y. Song, X.-y. LI. Pseudo-random sequence generator based on the generalized Henon map. *The Journal of China Universities of Posts and Telecommunications*, 15(3), p. 64-68, 2008.
- [254] L. Shujuna, M. Xuanqinb, C. Yuanlong. Pseudo-Random Bit Generator Based on Couple Chaotic Systems and its Applications in Stream-Cipher Cryptography, In : Rangan C.P., Ding C. (eds) *Progress in Cryptology, INDOCRYPT 2001. INDOCRYPT 2001. Lecture Notes in Computer Science*, 2247, pp. 316-329, Berlin, Springer-Verlag, 2001.

- [255] N.S. Philip, K.B. Joseph. Chaos for Stream Cipher. *In proceedings of ADCOM 2000 Tata McGraw Hill*, arXiv :cs/0102012, 2001
- [256] A. Skrobek. Cryptanalysis of chaotic stream cipher. *Physics Letters A*, 363(1-2), p. 84, 2007.
- [257] L. Kocarev, G. Jakimoski. Pseudorandom bits generated by chaotic maps. *Circuits and Systems I : Fundamental Theory and Applications, IEEE Transactions on*, 50(1), pp. 123-126, 2003.
- [258] X. Wang, J. Zhang, Y. Fan, W. Zhang. Chaotic Pseudorandom Bit Generator Using n-dimensional Nonlinear Digital Filter. *in Communication Technology, ICCT '06, International Conference on*, Guilin, China, 2006.
- [259] P.-H. Lee, S.-C. Pei, Y.-Y. Chen. Generating Chaotic Stream Ciphers Using Chaotic Systems. *Chinese Journal of Physics*, 41(6), pp. 559-581, 2003.
- [260] L. Kocarev, K. S. Halle, K. Eckert, L. O. Chua, U. Parlitz. Experimental demonstration of secure communications via chaotic synchronization. *International Journal of Bifurcation and Chaos*, 02 (03), pp. 709-713, 1992.
- [261] U. Parlitz, L.O. Chua, L. Kocarev. Transmission of digital Signals by chaotic synchronization. *Int. J. of Bifurcation and Chaos*, 02, pp. 973-977, 1992.
- [262] A. Fradkov, H. Nijmeijer, A. Markov. Adaptive observer-based synchronization for communication. *International Bifurcation and Chaos*. 10(12), 2000.
- [263] S. Li, G. Alvarez, Z. Li, W.A. Halang. Analog Chaos-based Secure Communications and Cryptanalysis : A Brief Survey. *3rd International IEEE Scientific Conference on Physics and Control (PhysCon'2007)*, 2007.
- [264] T. Yang, L.O. Chua. Secure communication via chaotic parameter modulation. *IEEE Transactions on Circuits and Systems I : Fundamental Theory and Applications*, 43(9), pp. 817-819, 1996.
- [265] C.W. Wu, L.O. Chua. A Simple Way to Synchronize Chaotic Systems with Applications to Secure Communication Systems. *International Journal of Bifurcation and Chaos*, 03 (06), pp. 1619-1627, 1993.

- [266] O. Megherbi, Etude et réalisation d'un système sécurisé à base de systèmes chaotiques, Mémoire de Magister, Université Mouloud Mammeri de Tizi-Ouzou, 2013.
- [267] L.J. Sheu, W.C. Chen, Y.C. Chen, W.T. Weng. A Two-Channel Secure Communication Using Fractional Chaotic Systems. *International Journal of Mathematical, Computational, Physical, Electrical and Computer Engineering*, 4(5), pp.584-588, 2010.
- [268] L.L. Huang, J. Zhang, S.S. Shi. Circuit simulation on control and synchronization of fractional order switching chaotic system. *Mathematics and Computers in Simulation*, 113, pp. 28-39, 2015.
- [269] P. Muthukumar, P. Balasubramaniam, K. Ratnavelu. Synchronization and an application of a novel fractional order King Cobra chaotic system. *CHAOS* 24, ID 033105, 2014.
- [270] X. Huang, T. Sun, Y. Li, J. Liang. A Color Image Encryption Algorithm Based on a Fractional-Order Hyperchaotic System, *entropy*, 17(1), pp. 28-38, 2015.
- [271] W. Zhen, H. Xia, L. Yu-Xia, S. Xiao-Na. A new image encryption algorithm based on the fractional-order hyperchaotic Lorenz system. *Chin. Phys. B*, 22 (1), ID 010504, 2013
- [272] Z. Liu, T. Xia, J. Wang. Fractional two-dimensional discrete chaotic map and its applications to the information security with elliptic-curve public key cryptography. *Journal of Vibration and Control*, pp. 1-28, 2017.
- [273] H. Hamiche, S. Guermah, S. Kassim, M. Lahdir, S. Djennoune, M. Bettayeb. Secure data transmission scheme based on fractional-order discrete chaotic system. *Control, Engineering and Information Technology (CEIT), 2015 3rd International Conference on*, Tlemcen, Algérie, 2015.
- [274] S. Djennoune, S. Guermah, A. Si Ammour, H. Hamiche, L. Feddal, S. Merbouti. Synchronization of the fractional-order chaotic Chua's system via sliding mode observer. *Systems and Control (ICSC), 3rd International Conference on*, pp. 111-116, 2013.

- [275] O. Megherbi, S. Kassim, H. Hamiche, S. Djennoune, M. Bettayeb, J.-P. Barbot. Robust image transmission based on Coupled Fractional-Order Chaotic maps. *Siam conference on Control and its applications*, USA, 2017.
- [276] Y. Xu, H. Wang, Y. Li, B. Pei. Image encryption based on synchronization of fractional chaotic systems. *Science and Numerical Simulation*, 19(10), pp. 3735-3744, 2014.
- [277] M. Ahmad, H.D. Alsharari, M. Nizam. Security Improvement of an Image Encryption Based on mPixel-Chaotic-Shuffle and Pixel-Chaotic-Diffusion. *European Journal of Scientific Research*, 98(3), 2013.
- [278] A. M.N. Alzubaidi. Color Image Encryption and Decryption using Pixel Shuffling with Henon Chaotic System. *International Journal of Engineering Research and Technology (IJERT)*, 3(3), 2014.
- [279] C. Kaufmann, R. Perlman, M. Speciner. Network Security : Private Communication in a Public World. *Prentice Hall*, second edition, 2003.
- [280] B. Schneier. Applied cryptography :protocols, algorithms and source code in C. *John Wiley and Sons*, 2007.
- [281] N.K. Pareek. Design and Analysis of a Novel Digital Image Encryption Scheme, International. *Journal of Network Security and Its Applications (IJNSA)*, 4 (2), pp. 95-108, 2012.
- [282] A. Beloucif. Contribution à l'étude des mécanismes cryptographiques. Thèse de Doctorat. Université de Batna 2, 2016.
- [283] A. Jolfaei, A. Mirghadri. Image Encryption Using Chaos and Block Cipher. *Computer and Information Science*, 4(1), pp. 172-185, 2011.
- [284] J. He, S. Yu, J. Cai. A Method For Image Encryption Based on Fractional-order hyperchaotic systems. *Journal of Applied Analysis and Computation*, 5(2), pp.197-209, 2015.
- [285] L. Liu, S. Miao. A new image encryption algorithm based on logistic chaotic map with varying parameter, *Springerplus*, 5 : 289, 2016.

- [286] M. Farajallah, S. El Assad. Fast and Secure Chaos-Based Cryptosystem for Images. *International Journal of Bifurcation and Chaos*, 26 (2), 21 pages, 2016.
- [287] B. Stoyanov, K. Kordov. Image Encryption Using Chebyshev Map and Rotation Equation, *Entropy*, 17, pp. 2117-2139, 2015.
- [288] G. Chen, Y. Mao, C.K. Chui. A symmetric image encryption scheme based on 3D chaotic cat maps. *Chaos, Solitons and Fractals*, 21, pp. 749-761, 2004.
- [289] J. Ahmad, F. Ahmed. Efficiency Analysis and Security Evaluation of Image Encryption Schemes. *International Journal of Video and Image Processing and Network Security IJVIPNS-IJENS*, 12(04), pp. 18-31, 2012.
- [290] N.A. Abbas. Image encryption based on independant component analysis and Arnold's cat map. *Egyptian Informatics Journal*, 17(1), pp. 139-146, 2015.
- [291] K. Singh, K. Kaur. Image encryption using chaotic maps and DNA addition operation and noise effects on it. *International journal of computer applications*, 23(6), pp. 17-24, 2011.
- [292] M. Bettayeb, S. Djennoune. New Results on the Controllability and Observability of Fractional Dynamical Systems. *Journal of Vibration and Control*, 14(9-10), pp. 1531-1541, 2008.
- [293] D. Matignon, B. D'Andrea-Novel. Observer-based for fractional differential systems. *In Proc. IEEE Conf. Decision and Contr.*, San Diego, USA, 1997.
- [294] A. B. Shamardan, M. R. A. Moubarak. Controllability and observability for fractional control systems. *Journal of Fractional Calculus*, 15, pp. 25-34, 1999.
- [295] A. Dzielinski, D. Sierociuk. Reachability, controllability and observability of the fractional order discrete state space system. *Proceedings of the IEEE/IFAC International Conference on Methods and Models in Automation and Robotics, MMAR'2007*, Szczecin, Poland, pp. 129-134, 2007.
- [296] S. Guermah, S. Djennoune, M. Bettayeb. Controllability and Observability of Linear Discrete-time Fractional-order Systems. *Int. J. Appl. Math. Comput. Sci.*, 18(2), pp. 213-222, 2008.

-
- [297] N. Djeghali, S. Djennoune, M. Bettayeb, M. Ghanes, J.-P. Barbot. Observation and sliding mode observer for nonlinear fractional-order system with unknown input. *ISA Transactions*, 63, pp. 1-10, 2016.
- [298] K. Balachandran, V. Govindaraj, M. Rivero, J. A. T. Machado, J. J. Trujillo. Observability of Nonlinear Fractional Dynamical Systems. *Hindawi Publishing Corporation, Abstract and Applied Analysis*, ID 346041, 7 pages, 2013.
- [299] D. Mozyrska, Z. Bartosiewicz. On Observability of Nonlinear Discrete-Time Fractional-Order Control Systems. *In : New Trends in Nanotechnology and Fractional Calculus Applications*. Springer, Dordrecht, 2010.

Résumé :

Dans ce travail de thèse, notre contribution vise à traiter le problème de la synchronisation des systèmes chaotiques discrets d'ordre fractionnaire. Cette synchronisation entre l'émetteur dit « maître » et le récepteur dit « esclave » a pour objectif d'assurer une transmission sécurisée de données. La méthode de synchronisation développée dans notre cas est basée sur l'utilisation d'observateurs impulsifs. Le principe de cette approche est de concevoir un observateur discret d'ordre fractionnaire afin de reconstruire les états d'un système chaotique d'ordre fractionnaire, à des instants discrets. Il s'agit en d'autres termes d'établir la synchronisation en utilisant de courts échantillons des états du système maître. Des conditions suffisantes ont été définies pour atteindre la stabilité des erreurs de synchronisation et garantir ainsi la synchronisation entre le système maître et l'observateur impulsif d'ordre fractionnaire. Subséquemment, le schéma de synchronisation a été inclus dans un système de communication à un seul canal pour chiffrer puis transmettre une image couleur. Au niveau de l'émetteur, l'algorithme de cryptage utilise les états chaotiques du système chaotique d'ordre fractionnaire maître pour chiffrer l'image originale à travers plusieurs opérations réversibles. Du côté récepteur, l'algorithme de décryptage consiste en l'utilisation des états chaotiques estimés par l'observateur impulsif pour effectuer l'inverse des étapes du cryptage. Afin d'illustrer l'efficacité du schéma de transmission proposé, des analyses et des tests ont été réalisés pour étudier sa robustesse et sa sécurité face aux éventuelles intrusions. Les résultats obtenus montrent que le système cryptographique proposé est robuste et peut résister à plusieurs types d'attaques.

Mots-clés : Synchronisation impulsive, Systèmes chaotiques discrets d'ordre fractionnaire, Observateurs impulsifs discrets, Transmission sécurisée à base du chaos, Systèmes discrets à retards, Robustesse.

Abstract :

In this thesis work, our contribution aims to address the synchronization issue of fractional-order discrete chaotic systems. The purpose of this synchronization between a transmitter called « master » and a receiver called « slave » is to ensure secure data transmission. The synchronization method developed in our case is based on the use of impulsive observers. The principle is to design a fractional-order discrete observer in order to reconstruct the states of a fractional-order chaotic map at discrete instants. In other terms, it consists of the use of short samples of the master system states to establish the synchronization. Sufficient conditions have been defined to reach the stability of synchronization errors and guarantee, thus, the synchronization between the master system and the fractional-order impulsive observer. Subsequently, the synchronization scheme has been included in a single-channel communication system to cipher and to transmit a color image. At the transmitter level, the encryption algorithm uses the chaotic states of the master fractional-order chaotic map to cipher the plain image through several reversible operations. At the receiver side, the decryption algorithm consists of the use of the chaotic states estimated by the impulsive observer to perform the reverse of the encryption steps. Furthermore, some analysis and tests have been carried out to study the robustness and the security of the transmission scheme against eventual intrusion. The obtained results show that the proposed cryptosystem is robust and can withstand several types of attacks.

Keywords : Impulsive synchronization, Fractional-order chaotic maps, Discrete impulsive observers, Chaos-based secure transmission, Delayed discrete systems, Robustness.