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

Présentée pour obtenir le diplôme de

DOCTORAT $3^{ème}$ CYCLE LMD

Spécialité : AUTOMATIQUE

Par :

Sarah KASSIM

THEME

CONTRIBUTION A LA TRANSMISSION NUMERIQUE SÉCURISÉE DE DONNÉES A BASE DE GÉNÉRATEURS DE SÉQUENCES CHAOTIQUES D'ORDRE NON ENTIER

DEVANT LE JURY :

Président	Rachid MANSOURI	*Professeur, Université de Tizi-Ouzou*
Rapporteur	Saïd DJENNOUNE	*Professeur, Université de Tizi-Ouzou*
Co-Rapporteur	Maâmar BETTAYEB	*Professeur, Université de Sharjah (EAU)*
Examinateur	Amar SI AMMOUR	*MCA, Université de Tizi-Ouzou*
Examinateur	Karim KEMIH	*Professeur, Université de Jijel*
Examinateur	Mourad LAHDIR	*MCA, Université de Tizi-Ouzou*
Invité	Hamid HAMICHE	*MCA, Université de Tizi-Ouzou*

ANNÉE : 2018

Remerciements

Ce travail a été effectué au Laboratoire de Conception et Conduite des Systèmes de Production (L2CSP), de l'université Mouloud Mammeri de Tizi-Ouzou.

Je tiens, tout d'abord, à exprimer ma gratitude, ma plus grande reconnaissance et mon profond respect à mon directeur de thèse, Monsieur Saïd Djennoune, Professeur à l'université Mouloud Mammeri de Tizi-Ouzou, qui a dirigé mes travaux de recherche et qui m'a apporté son apport scientifique indéniable, sa confiance, ses judicieux conseils et sa disponibilité, tout au long de l'élaboration de ma thèse. J'ai profité de son approche rigoureuse, de ses précieux et nombreux conseils et de ses qualités humaines. Qu'il trouve ici l'expression de ma profonde reconnaissance.

Je tiens particulièrement à remercier mon co-directeur de thèse, Monsieur Maâmar Bettayeb, Professeur à l'université de Sharjah, pour avoir accepté de m'accueillir dans son laboratoire à l'université de Sharjah et pour ses conseils, ses critiques et sa disponibilité. Je lui suis très reconnaissante de la confiance qu'il a su me témoigner. Je tiens également à remercier toute sa famille pour leur sympathie et leur générosité.

J'exprime mes profonds remerciements à Monsieur Hamid Hamiche pour son soutien permanent et ses encouragements, ses précieux conseils, sa grande disponibilité, son apport scientifique et la qualité exceptionnelle de son encadrement, tout au long de l'élaboration de ma thèse. Je lui en suis très reconnaissante.

J'exprime mes sincères remerciements à Monsieur Rachid Mansouri, Professeur à l'université Mouloud Mammeri de Tizi-Ouzou, qui m'a fait l'honneur de présider le jury de cette thèse. Je n'ai aucun doute que ses riches connaissances et présieuses suggestions et remarques me permetteront d'améliorer ce travail.

Je remercie également Messieurs Amar Si Ammour, Maître de conférences à l'université Mouloud Mammeri de Tizi-Ouzou, Karim Kemih, Professeur à l'université de Jijel, Mourad Lahdir, Maître de conférences à l'université Mouloud Mammeri de Tizi-Ouzou de m'avoir fait l'honneur en acceptant d'embellir ce travail avec leurs remarques et conseils.

Au cours de ces années, j'ai eu la chance de côtoyer de nombreuses personnes du domaine de la transmission sécurisée à base du chaos, avec qui j'ai eu plaisir à travailler pour apporter quelques contributions scientifiques. Je remercie donc tous mes co-auteurs : Hamid Hamiche, Saïd Djennoune, Maâmar Bettayeb, Saïd Guermah, Mourad Lahdir, Ouerdia Megherbi et Jean-Pierre Barbot. De plus, je souhaite remercier toutes les personnes avec qui j'ai pu échanger de manière plus informelle et qui ont indirectement contribué à enrichir mes connaissances, et en particulier Sofiane Hammouche, Lamia Sersour, Aghiles Ardjal, Mohammed Belkaid Boukhatem, Rafik Saddaoui.

Mes remerciements s'adressent également à tous les membres du Laboratoire de Conception et Conduite des Systèmes de Production (L2CSP), en particulier son directeur Redouane Kara, Professeur à l'université Mouloud Mammeri de Tizi-Ouzou, et tous les collègues pour l'excellente ambiance de travail qu'ils ont créé.

Mes sincères remerciements vont aussi à l'équipe de l'université de Sharjah, UAE, en particulier : Qassim Nasir, Professeur associé à l'université de Sharjah, Talal Bonny, Professeur assistant à l'université de Sharjah, et Maha Alla-EDDINE, Ingénieur de Laboratoire, sans oublier Meriam Bettayeb pour m'avoir fait partager leur expérience et leurs encouragements.

Durant ces années, mes parents, ma sœur Ines et mes frères Amine et Nazim, mon mari Aissa, mes proches, ainsi que mes ami(e)s, ont toujours été présents et m'ont apporté leur soutien toutes ces longues années. Qu'ils trouvent ici mes remerciements et toute ma reconnaissance.

Je remercie tous ceux qui de près ou de loin ont contribué à la réalisation de cette thèse.

J'adresse enfin toute ma reconnaissance à ma chère maman, pour sa confiance, son aide, sa compréhension totale et pour les nombreux sacrifices qu'elle a consenti, surtout dans les périodes difficiles durant mes études. Qu'elle trouve ici l'expression de ma reconnaissance et de mon éternelle gratitude.

Notations

Symboles

$\mathbb{N}$:	ensemble des nombre naturels
$\mathbb{Z}$:	ensemble des nombres entiers relatifs
$\mathbb{R}$:	ensemble des nombres réels
K :	clé dans le cas d'un algorithme à clé symétrique
K_e et K_d :	clés de chiffrement/déchiffrement dans le cas d'un algorithmes asymétriques
$E(.)$:	fonction de chiffrement
$D(.)$:	fonction de déchiffrement
t :	variable de temps réel
$x(t)$:	vecteur d'état du modèle d'espace d'état en temps continu
k :	variable de temps discret
$x(k)$:	vecteur d'état du modèle d'espace d'état en temps discret
λ :	exposant de Lyapunov
$\Gamma(\lambda)$:	$(\lambda \in \mathbb{R}^* \backslash \mathbb{Z}_-)$ Fonction Gamma
E_α :	fonction Mittag-Leffler
$E_{\alpha,\beta}$:	fonction Mittag-Leffler à deux paramètres.
$I^k f(t)$:	$(k \in \mathbb{N})$, l'intégration répétée k fois de la fonction $f(t)$
α :	l'ordre d'intégration/dérivation non entier
$I^\alpha f(t)$:	$(\alpha \in \mathbb{R})$, l'intégration non entière d'ordre α de la fonction $f(t)$
$D^\alpha f(t)$:	opérateur de dérivation d'ordre α de la fonction $f(t)$
$\binom{\alpha}{k}$:	$(\alpha \in \mathbb{R}_+)$, binôme de Newton généralisé à des ordres réels
$D^\alpha f(kh)$:	valeur de la dérivée $\alpha^{ème}$ de $f(t)$ à l'instant kh
$D^\alpha x$:	$(x \in \mathbb{R}^n)$, tous les éléments du vecteur x sont dérivés au même ordre α
$D^{[\alpha]} x$:	$(\alpha \in \mathbb{R}^n_+,\ x \in \mathbb{R}^n)$, le $i^{ème}$ élément du vecteur x est dérivé à la $i^{ème}$ composante du vecteur α

h :	période d'échantillonnage
$\mathcal{C}$:	matrice de commandabilité
$\mathcal{O}$:	matrice d'observabilité
Δ :	Opérateur de différence
$\Delta^{\alpha}x$:	tous les éléments du vecteur x sont dérivés au même ordre α
$\Delta^{[\alpha]}x$:	le $i^{ème}$ élément du vecteur x est dérivé à la $i^{ème}$ composante du vecteur α
L :	taille de la mémoire
I_k :	matrice identité de dimension k
$\Vert . \Vert$:	norme
$\mathcal{P}_a(t)$:	facteur d'oubli
s :	opérateur de Laplace
£ :	symbole de la transformation de Laplace
$£^{-1}$:	symbole de la transformation de Laplace inverse
TF :	transformée de Fourier
r_{xy} :	coefficient de corrélation
XOR :	Exclusive OR
χ^2 :	test de Chi^2.

Acronymes

DES :	Data Encryption Standard
3DES :	Triple Data Encryption Standard
AES :	Advanced Encryption Standard
RSA :	Rivest Shamir Adleman
ECB :	Electronique Code Book
CBC :	Cipher Block Chaining
$NPCR$:	taux de changement du nombre de pixels
$UACI$:	moyenne unifiée du changement d'intensité
$PSNR$:	Peak Signal to Noise Ratio

Table des matières

Table des figures

Liste des tableaux

Chapitre 1

Introduction Générale

Avec le développement du commerce électronique, les utilisateurs ont besoin d'authentifier et de garantir la confidentialité de leurs transactions et ainsi protéger les données sensibles transmises à travers des réseaux publics tels que l'Internet. C'est pourquoi, la cryptographie est devenue incontournable et elle continue de jouer un rôle important dans la sécurité et la fiabilité des systèmes de transmission de données [1,2]. La communication sécurisée entre deux parties est effectuée de telle sorte que l'identité de la partie communicante soit confirmée et que la confidentialité ainsi que l'intégrité du message soient maintenues. Par conséquent, la confidentialité, l'authentification et l'intégrité des messages sont trois points clés pour une communication sécurisée. La confidentialité signifie que seuls l'émetteur et le récepteur peuvent comprendre le contenu du message transmis. L'idée est de chiffrer le message par l'émetteur avec des algorithmes de cryptographie. Le message ne peut être déchiffré que par le récepteur prévu, en utilisant une clé particulière. L'authentification signifie que si l'émetteur A et le récepteur B communiquent, l'identité des deux doit être confirmée. L'intégrité des messages signifie qu'à chaque fois que l'émetteur et le récepteur communiquent, il faut s'assurer que le contenu du message n'a pas été modifié.

Depuis longtemps des techniques simples existent mais elles se sont perfectionnées plus récemment, avec le développement de la mécanique dans un premier temps, puis de l'électronique et de l'informatique. Au cours des 30 dernières années, la cryptographie logicielle moderne a connu un développement continu [3,4]. Cette technique de cryptage utilise des systèmes de chiffrement classique (codage informatique au moyen d'algorithmes) soit à clé publique ou à clé secrète. Un certain nombre de techniques de cryptage / décryptage ont été développées, y compris le standard de cryptage des données (DES), Triple-DES, RSA (Rivest, Shamir et Adelman, les inventeurs de la technique), etc [5–8]. Toutefois, le chiffrement des informations au moyen de ces techniques présente des risques, dans la mesure où il est possible, en disposant le temps suffisant, de percer les dites clés. De plus, l'augmentation continue de la vitesse des ordinateurs menace la sécurité de telles procédures. En outre, ces méthodes de chiffrement souffrent du problème de débit faible causé par la lenteur d'exécution des algorithmes de chiffrement [9–11]. C'est pour cette raison que de nouvelles techniques sont en cours de développement afin de surmonter l'obstacle de débit de transmission tout en maintenant le niveau de sécurité élevé. Deux solutions sont proposées ; la cryptographie quantique [12,13] et la cryptographie chaotique [14–17] à laquelle, on s'intéresse dans le présent travail.

Durant ces dernières décennies, les systèmes non linéaires chaotiques ont été appliqués à la cryptographie afin d'augmenter le degré de sécurité. L'étude de ces systèmes est liée à la théorie du chaos qui a connu une grande évolution à partir des années 1960 grâce aux travaux du météorologiste Edward Lorenz [20]. Grâce aux propriétés intrinsèques des systèmes chaotiques, telles que leurs sensibilité aux conditions initiales et le fait qu'ils évoluent dans une large bande de fréquence, les systèmes chaotiques sont de bons candidats pour la cryptographie. En effet, les nombreuses études menées sur les systèmes chaotiques ont montré que, hormis leur comportement aléatoire, ils possèdent des propriétés attrayantes et que le chaos apparaît comme solution prometteuse pour augmenter les performances des systèmes de transmission actuels en termes de débit de transmission et de sécurisation des informations à échanger entre deux correspondants. Bien que ce comportement non périodique paraît complètement aléatoire, son évolution est parfaitement déterministe, de sorte qu'il peut être reproduit à l'identique au niveau du récepteur. Les premiers systèmes qui étaient basés sur la cryptographie chaotique consistaient à superposer à l'information initiale un signal chaotique. Ensuite, le message noyé dans le chaos est envoyé à un récepteur qui connaît les caractéristiques du générateur du chaos. Il ne reste alors plus au destinataire qu'à soustraire le chaos de son message pour retrouver l'information. Depuis lors, plusieurs autres techniques ont été développées. Dans les systèmes de communication, pour réussir une transmission, il est essentiel d'assurer la synchronisation. La synchronisation chaotique cherche à reproduire, au niveau du récepteur, le signal chaotique envoyé par l'émetteur sans aucune connaissance sur son état initial. La synchronisation entre deux systèmes chaotiques est nécessaire pour récupérer l'information transmise, mais elle n'est pas toujours facile à réaliser.

Jusqu'en 1990, la synchronisation des systèmes chaotiques semblait impossible, puisque la notion de synchronisation était réservée jusque-là aux systèmes périodiques, pour désigner deux systèmes dont l'un suit le mouvement de l'autre. Pourtant en 1990, Pecora et Carroll, [21], ont montré que deux systèmes chaotiques identiques avec des conditions initiales différentes peuvent éventuellement se synchroniser s'ils sont couplés d'une certaine manière convenable, c'est à dire sous certaines conditions. Le développement des systèmes de communication utilisant le chaos a commencé donc avec des schémas de synchronisation très simples de circuits électroniques, visant pour le cryptage et la reconstruction simultanés d'un signal d'information. Par la suite, le problème de synchronisation des systèmes chaotiques a été relié au problème standard de l'estimation d'état non linéaire, qui a ouvert la voie à des recherches intensives, motivées par des applications potentielles [22].

Au cours des dernières années, le calcul d'ordre fractionnaire a suscité un intérêt considérable et a trouvé de nombreuses applications dans des études récentes dans divers domaines de la science et de l'ingénierie [23–26]. Avec le développement de cette discipline, l'attention a été portée à l'investigation du comportement chaotique des systèmes d'ordre fractionnaire [27–29]. En effet, en raison de l'interprétation géométrique complexe des effets non locaux des dérivées fractionnaires dans l'espace ou dans le temps [30], les systèmes chaotiques fractionnaires présentent des non linéarités et des degrés de liberté supérieurs aux systèmes chaotiques d'ordre entier. Ces avantages attirent l'attention des chercheurs sur l'application du système chaotique d'ordre fractionnaire dans la communication sécurisée [31]. Effectivement, l'intérêt d'utiliser les systèmes chaotiques d'ordre fractionnaire dans une transmission sécurisée est d'améliorer la sécurité en ajoutant les dérivées d'ordres fractionnaires en tant que nouveaux paramètres à la clé de sécurité. L'identification des paramètres ajoutés est très difficile et plus complexe, ce qui rend le système de chiffrement basé sur des systèmes chaotiques d'ordre fractionnaire avantageux et distinctif par rapport à ceux de l'ordre entier. Pour ces raisons, de nombreux travaux portent sur la synchronisation des systèmes chaotiques d'ordre fractionnaire et leur application à la transmission sécurisée de données sont rapportées dans la littérature [32–34]. Cependant, la transmission sécurisée d'images basée sur des systèmes chaotiques d'ordre fractionnaire constitue un axe de recherche tout à fait nouveau et très prometteur où peu de travaux ont été effectués [35, 36].

Pour les systèmes à temps continu, l'idée de base est de remplacer la dérivée d'ordre entier par une dérivée d'ordre fractionnaire dans certains systèmes d'ordre entier chaotiques non linéaires bien connus. Parmi la liste des systèmes chaotiques d'ordre fractionnaire en temps continu proposée dans la littérature, on trouve le système de Chua, le système de Newton-Leipnik, le système de Lorenz [34]. Même si la théorie et les applications des systèmes chaotiques continus d'ordre fractionnaire sont bien documentées dans la littérature, ce n'est pas le cas des systèmes chaotiques d'ordre fractionnaire en temps discret. La raison en est que l'équation de différence d'ordre fractionnaire est un nouveau sujet et que les rares travaux consacrés à ce domaine concernent le cas linéaire [37, 38]. Très récemment, les systèmes de différences fractionnaires chaotiques commencent à attirer une attention croissante en raison de ses applications potentielles dans la communication numérique sécurisée [28, 39–41]. Effectivement, il est souvent souhaitable de dériver des modèles discrets qui représentent la dynamique des systèmes, qui sont souvent en temps continu. Ceci est principalement dû aux mesures, qui sont habituellement effectuées dans la pratique à des intervalles de temps spécifiques. Plus important encore, les simulations numériques peuvent être effectuées facilement et rapidement, ce qui améliore la vitesse de chiffrement. Toutefois, les recherches sur la synchronisation des systèmes chaotiques à temps discret d'ordre fractionnaire ne sont pas très fructueuses.

1.1 Contributions originales

Les travaux de recherche portés dans cette thèse ont été motivés par le besoin d'élaborer de nouvelles approches de transmission sécurisée basées sur les générateurs de séquences chaotiques d'ordre fractionnaire. Les principaux résultats attendus sont, en premier lieu, le développement d'une nouvelle méthode de synchronisation des systèmes chaotiques discrets d'ordre fractionnaire basée sur l'observateur exact retardé étape par étape [42]. La synthèse de l'observateur dépend de deux conditions : la condition d'observabilité pour retrouver les états du système ; la condition de recouvrement de l'observabilité ("observability matching condition") pour retrouver les états du système et l'information noyée dans le système (inversibilité à gauche du système). Ces deux conditions sont étudiées pour cette catégorie de systèmes [43]. Par la suite, un nouveau schéma de transmission sécurisée efficace et robuste ainsi que quelques variantes ont été élaborés en utilisant la synchronisation par observateurs développée [44–49]. Des résultats de simulation sont ensuite présentés pour mettre en évidence les performances de la méthode proposée. Ces résultats montrent que nos systèmes peuvent résister à différents types d'attaque et qu'ils présentent de bonnes performances.

1.2 Contributions scientifiques de la thèse

La principale contribution de cette thèse consiste à développer une nouvelle approche de synchronisation des systèmes chaotiques discrets d'ordre fractionnaire dans le but de l'appliquer dans un nouveau schéma de transmission sécurisée.
Cette thèse est basée sur les travaux présentés dans les publications suivantes

1.2.1 Publication internationale

– 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, pp. 2473-2489, 2017.

1.2.2 Conférences internationales

- H. Hamiche, S. Kassim, S. Djennoune, S. Guermah, M. Lahdir, M. Bettayeb, *Secure data transmission scheme based on fractional-order discrete chaotic system* , International Conference on Control, Engineering and Information Technology (CEIT'2015). Tlemcen, Algeria, 2015.
- S. Kassim, O. Megherbi, H. Hamiche, S. Djennoune, M. Lahdir, M. Bettayeb, *Secure image transmission scheme using hybrid encryption methods*, International Conference on Automatic Control.Telecommunications and Signals (ICATS'2015). Annaba, Algeria, 2015.
- S. Kassim, H. Hamiche, S. Djennoune, O. Megherbi, M. Bettayeb, *A novel robust image transmission scheme based on fractional-order discrete chaotic systems*, International Workshop on cryptography and its applications (IWCA'16). Oran, Algeria, 2016.
- O. Megherbi, S. Kassim, H. Hamiche, S. Djennoune, M. Bettayeb,*A New Robust Hybrid Transmission Scheme based on the Synchronization of Discrete-Time Chaotic Systems*, International Workshop on cryptography and its applications (IWCA'16). Oran, Algeria, 2016.
- O. Megherbi, S. Kassim, H. Hamiche, S. Djennoune, M. Bettayeb, J-P. Barbot,*Robust Image Transmission Scheme Based on Coupled Fractional-Order Chaotic Maps*, SIAM Conference on Control and Its Applications (CT17), USA, July 10-14, 2017.
- S. Kassim, H. Hamiche, S. Djennoune, M. Bettayeb, *Secure color image transmission scheme based on synchronization of fractional-order discrete-time hyperchaotic systems*, Accepté pour présentation à The International Conference on Fractional Differentiation and its Applications (ICFDA'2018), Amman, The Hashemite Kingdom of Jordan, 16-18 July, 2018.

1.2.3 Chapitre de livre

- H. Hamiche, S. Kassim, O. Megherbi, S. Djennoune, M. Bettayeb, *Secure Digital Data Communication Based on Fractional-Order Chaotic Maps*, Advanced Synchronization Control and Bifurcation of Chaotic Fractional-Order Systems, pp. 438-467, Editeur IGI Global, 2018.

1.3 Organisation de la thèse

Le présent manuscrit est organisé comme suit. L'introduction générale de cette thèse présente l'objectif principal et les motivations pour donner un aperçu général de ce modeste travail.

Le chapitre 1 est consacré à la cryptographie et synchronisation chaotiques. Dans la première partie de chapitre, nous présentons les notions de base de la cryptographie en s'intéressant plus particulièrement à la cryptographie chaotique. Nous traitons également de la théorie du chaos. Une description des caractéristiques essentielles communes à tous les systèmes chaotiques est également donnée. Nous abordons, dans la deuxième partie, la notion de synchronisation tout en présentant les schémas de communications basés sur cette approche. Nous terminons ce chapitre par une description des outils d'évaluation de la sécurité des schémas de transmission sécurisée.

Le chapitre 2 est dédié à l'étude des systèmes chaotiques d'ordre fractionnaire. Dans cette partie, une description de certains outils mathématiques importants dans la théorie des systèmes fractionnaires est donnée. Ensuite, la classe de systèmes chaotiques d'ordre fractionnaire est présentée. Enfin, la synchronisation des systèmes chaotiques d'ordre fractionnaire est abordée.

Dans le chapitre 3, une nouvelle méthode de synchronisation à base d'observateurs des systèmes chaotiques discrets d'ordre fractionnaire est développée en vue de l'appliquer à un schéma de transmission sécurisée de données. Pour ce faire, un observateur retardé étape par étape est conçu. Cet observateur nécessite des conditions : la condition d'observabilité et ; la condition de recouvrement d'observabilité. Ces conditions sont étudiées pour le système chaotique de Hénon modifié d'ordre fractionnaire.

Dans le chapitre 4, un nouveau schéma de transmission sécurisée d'images est introduit. Ce schéma de chiffrement présente une amélioration significative en termes d'efficacité et de sécurité. Une analyse de sécurité est effectuée pour démontrer l'efficacité du système proposé. Par la suite, deux variantes du schéma développé sont proposées où, des simulations numériques sont présentées pour illustrer l'efficacité des schémas proposés.

Enfin, cette thèse est clôturée par une conclusion générale et quelques perspectives.

Chapitre 2

Cryptographie et synchronisation chaotiques

2.1 Introduction

La *cryptologie*, littéralement "l'étude de ce qui est caché", désigne l'étude et la mise en pratique des techniques permettant la réalisation de communications sécurisées en présence de tiers. Cette science est composée de deux branches indissociables. D'une part, la cryptographie, littéralement "écriture des secrets", qui se consacre à créer des systèmes, appelés crypto-systèmes, visant à assurer la confidentialité, l'authentification, l'intégrité et la non répudiation. D'autre part, la *cryptanalyse*, littéralement "investigation des secrets", qui cherche à attaquer les crypto-systèmes, c'est-à-dire à mettre en défaut un ou plusieurs des points précédents.
Au cours des dernières années, une attention particulière a été accordée au développement des techniques pour la communication en utilisant des systèmes dynamiques chaotiques. En effet, les signaux chaotiques sont irréguliers, non périodiques, non corrélés, à large bande et impossible de prévoir à long terme. Ce sont les propriétés exigées en matière de signaux appliqués à des systèmes de communication, en particulier pour des communications à étalement de spectre, des communications multi-utilisateurs, et des communications sécurisées. Un intérêt de recherche croissant peut être observé dans tout les

domaines [14, 16, 50–52].

Ce chapitre apporte une vision globale sur la cryptographie, en s'intéressant plus particulièrement à la cryptographie chaotique. Ensuite, la notion de synchronisation est abordée. Des systèmes de communications basés sur la synchronisation des systèmes chaotiques sont également présentés. Finalement, des outils d'évaluation de la sécurité sont décrits. Ces outils seront utilisés dans le chapitre 4 afin d'analyser la robustesse des systèmes proposés.

2.2 Introduction à la cryptographie

La cryptographie ou science du secret est l'étude de techniques liées à la sécurité de l'information. Les applications de la cryptographie dans la vie courante sont diverses et adaptables à tout type de scénario où deux individus sont capables d'échanger des informations. Le but premier de cette science est de donner la possibilité aux individus de communiquer d'une manière protégée. À cette fin, on suppose que deux personnes disposent d'un canal de communication quelconque par lequel un échange d'informations est possible. Le canal de communication est considéré dans le domaine public et est donc accessible à tout le monde. Il peut être de nature différente suivant le scénario, mais on peut imaginer qu'il s'agisse d'un courrier postal, d'un courrier électronique, d'un câble téléphonique, d'ondes radios, d'une petite annonce dans un journal, etc.

En 1948, Claude Shannon a présenté un modèle mathématique de base d'un cryptosystème [53]. Ce schéma typique de la cryptographie, présenté à la figure 2.1, se compose principalement de deux parties (traditionnellement dénommées Alice et Bob) qui souhaitent échanger des informations confidentielles sur un canal non sécurisé sans qu'un pirate, appelé Ève, en comprenne le sens.

2.2.1 Vocabulaire de base

Cryptologie : Il s'agit d'une science mathématique comportant deux branches : la cryptographie et la cryptanalyse.

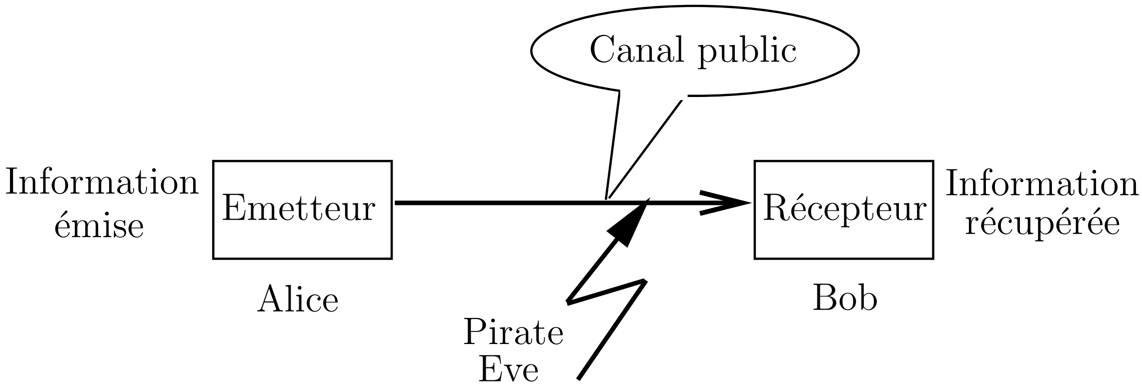


FIGURE 2.1: Schéma d'une communication sécurisée.

Cryptographie : La cryptographie est l'étude des méthodes donnant la possibilité d'envoyer des données de manière confidentielle sur un support donné.

Chiffrement : Le chiffrement consiste à transformer une donnée (texte, message, ...) afin de la rendre incompréhensible par une personne autre que celui qui a crée le message et celui qui en est le destinataire. La fonction permettant de retrouver le texte clair à partir du texte chiffré porte le nom de *déchiffrement*.

Texte chiffré : Appelé également *cryptogramme*, le texte chiffré est le résultat de l'application d'un chiffrement à un texte clair.

Clef : Il s'agit du paramètre impliqué et autorisant des opérations de chiffrement et/ou déchiffrement. Dans le cas d'un algorithme symétrique, la clef est identique lors des deux opérations. Dans le cas d'algorithmes asymétriques, elle diffère pour les deux opérations.

Cryptanalyse : Opposée à la cryptographie, elle a pour but de retrouver le texte clair à partir de textes chiffrés en déterminant les failles des algorithmes utilisés.

Crypto-système : Il est défini comme l'ensemble des clés possibles (espace de clés), des textes clairs et chiffrés possibles associés à un algorithme donné.

L'algorithme est en réalité un triplet d'algorithmes :

- l'un générant les clés K,
- un autre pour chiffrer M, et
- un troisième pour déchiffrer C.

On parle de "décryptage" pour désigner l'action permettant de retrouver le texte clair sans connaître la clef de déchiffrement. On emploie également parfois les termes "cryptage" et "crypter" pour qualifier l'action de chiffrer un message.

2.2.2 Notations

La cryptographie peut être définie comme l'étude des méthodes de chiffrement d'informations et les aspects associés. Elle permet de transmettre des informations confidentielles de manière sécurisée en utilisant des canaux non sécurisés. Le principe de cette étude consiste en l'application d'une fonction de chiffrement E au message à transmettre et le résultat de ce chiffrement, appelé message chiffré, pourra être transmis à l'autre entité qui connait comment déchiffrer ce message chiffré, en utilisant une fonction de déchiffrement D, afin d'obtenir le message clair. Bien sûr, aucune information ne devra être dévoilée sur le message clair si le message chiffré tombe entre les mains du pirate. Pour cela, les fonctions de chiffrement et de déchiffrement doivent rester secrètes. Pour des raisons pratiques, ces fonctions sont décomposées en algorithmes paramétrés par des clés. Dans le cas de chiffrement symétrique, le fonctionnement de ces algorithmes est public et seule la valeur des clés est tenue secrète. En revanche, dans le cas de chiffrement asymétrique, même la clé est publique. La propriété de base de la cryptographie est :

$$M = D_{K_d}(E_{K_e}(M)) \tag{2.1}$$

Où

. M représente le message clair,

. C est le message chiffré,

. K est la clé (dans le cas d'un algorithme à clé symétrique), K_e et K_d dans le cas d'algorithmes asymétriques,

. $E(.)$ est la fonction de chiffrement, et

. $D(.)$ est la fonction de déchiffrement.

Ainsi, avec un algorithme à clé symétrique,

$$M = D(C) \text{ si } C = E(M)$$

2.2.3 Principe de Kerckhoffs

En 1883, Auguste Kerckhoffs a énoncé six principes à respecter pour assurer la confidentialité de la transmission sécurisée, qui ont été formulés dans [55]. Le principe le plus important est celui affirmant que la sécurité du chiffre ne doit pas dépendre de ce qui ne peut pas être facilement changé. En d'autres termes, aucun secret ne doit résider dans l'algorithme mais plutôt dans la clé. Sans celle-ci, il doit être impossible de retrouver le texte clair à partir du texte chiffré. Par contre, si on connaît K, le déchiffrement est immédiat.

2.2.4 Objectifs de la cryptographie

Dans la cryptographie, de nombreux objectifs peuvent être atteints afin d'assurer la sécurité d'un système de communication. Dans une application, ces objectifs peuvent être atteints tous au même temps, ou bien seulement certains d'entre eux. Les principaux objectifs de la cryptographie peuvent être présentés comme suit :

. *Confidentialité :* consiste à garder des données secrètes pour tous ceux qui ne sont pas autorisées à les connaître.

. *Intégrité :* vise à préserver les données de toute altération non autorisée.

. *Authentification :* consiste à faire le lien entre les données et leur expéditeur. L'authentification des entités consiste à s'assurer de leur identité.

. *Non répudiation :* mécanisme qui permet de prouver que l'expéditeur a vraiment envoyé le message, de sorte que le destinataire ne peut pas prétendre que le message n'a pas été envoyé.

. *Signature :* méthode permettant de lier les informations à une entité ou de prouver la paternité de cette dernière.

. *Autorisation :* Le propriétaire donne l'autorisation à quelqu'un d'exécuter une opération en son nom.

. *Contrôle d'accès :* c'est un processus de prévention de l'utilisation non autorisée des ressources, c'est-à-dire qu'il contrôle qui peut avoir accès aux ressources, quand il peut accéder, sous quelles restrictions et conditions l'accès peut être accordé, et enfin, quel est le niveau d'autorisation d'un accès donné.

2.3 Un bref historique

Beaucoup de techniques de cryptographie ont existé au cours des siècles, déclinées en de nombreuses variantes [3, 4]. Les premières utilisations connues de la cryptographie remontent à l'Antiquité, où la plus ancienne race du message chiffré a été retrouvée sur une table en argile sur les bords du Tigre en Irak. Vers 500 ans avant J.-C, des simples chiffres étaient utilisés par les anciens Hébreux. Le plus connu est le chiffre d'Atbash ; ce chiffre est une substitution alphabétique inversée, qui consiste simplement à inverser l'ordre des lettres de l'alphabet. Les Grecs utilisaient une technique de chiffrement dite par transposition. L'outil employé est connu sous le nom de "Scytale" également appelée "bâton de Plutarque", autour duquel ils enroulaient en spires jointives une bande de cuir et y inscrivaient le message. Une fois déroulé, le message est envoyé au destinataire qui doit posséder un bâton identique (diamètre) nécessaire au déchiffrage. Plus tard, aux alentours de 150 ans avant J.-C, l'historien grec Polybe a inventé le carré de Polybe, ce dernier peut être considéré comme l'un des premiers procédés de chiffrement par substitution. Vers 50 ans avant J.-C, Jules César employait une substitution simple avec l'alphabet normal (il s'agissait simplement de décaler les lettres de l'alphabet d'une quantité fixe) dans ses communications secrètes. Ce chiffre était moins robuste qu'Atbash, mais à une époque où très peu de personnes savaient lire, cela suffisait. César écrivait aussi parfois en remplaçant les lettres latines par les lettres grecques. D'autres manières similaires font leur apparition au fil des années, et on peut les classer dans deux grandes catégories : les substitutions mono-alphabétiques ou poly-alphabétiques. Le chiffre de César est une substitution mono-alphabétique car tous les A du message seront toujours remplacés par D , mais on peut citer par exemple le chiffre de Vigenère (1586) dans lequel on ne se contente pas que d'un seul décalage comme pour César, mais de plusieurs. Ainsi, le A n'est pas forcément transformé en la même lettre : on parle de substitution poly-alphabétique.

Au XIV^{ème} siècle (environ 1460), une petite révolution se produit, l'invention de la première machine cryptographique. Elle est inventé par Leon Battista Alberti, l'un des pères du chiffre polyalphabétique. Il a conçu un cadran chiffrant pour simplifier le processus. Ce cadran est constitué de deux disques. L'un, plus grand, est fixe, et l'autre, plus petit, mobile. La circonférence de chacun des disques est divisée en un nombre de parties égales appelées secteurs. Dans chaque secteur du grand disque, les lettres sont écrites en suivant l'ordre alphabétique normal, mais dans un ordre incohérent dans le petit disque. Le principe était de modifier l'alignement des disques, et chaque nouvelle position de ces derniers amène de nouvelles équivalences. Vers 1518, Jean Trithème a écrit un livre sur la cryptologie, il a inventé un chiffre stéganographique et a aussi décrit des chiffres polyalphabétiques sous la forme de tables de substitution rectangulaires. En 1563, Giovanni Battista Della Porta fait apparaître dans ses procédés la première substitution bigrammatique, où deux lettres sont représentées par un seul symbole. Il invente aussi le premier chiffre polyalphabétique. Autour de 1585, Blaise de Vigenère présente un tableau du type Trithème, que l'on dénomme aujourd'hui à tort carré de Vigenère. Ce tableau est basé sur une substitution polyalphabétique, où une clé littérale est utilisée dont chaque lettre indique le décalage alphabétique à appliquer sur les lettres du message clair. Vers 1917, Gilbert S. Vernam a inventé une machine de chiffre polyalphabétique pratique capable d'employer une clé qui est totalement aléatoire et ne se répète jamais (un masque jetable). C'est le seul chiffre, dans nos connaissances actuelles, dont on a prouvé qu'il était indécryptable en pratique et en théorie. Ce procédé exige de devoir produire des millions de clés différentes pour chaque message, ce qui est impraticable. En 1918, Arthur Scherbius a inventé une machine à chiffrer, appelée Enigma. La machine allemande Enigma utilise notamment plusieurs rotors qui agissent indépendamment comme de simples chiffres de substitution, mais qui sont utilisés les uns à la suite des autres, et tournent comme le font les aiguilles d'une montre après que chaque lettre ait été traitée. Cette machine fut utilisée

pendant la seconde guerre mondiale. En 1929, Lester S. Hill publie dans son article [56] le chiffre polygraphique qui porte son nom, où il utilise des matrices est des vecteurs.
Vers le milieu du XX^{ème} siècle, la cryptographie est devenue beaucoup plus mathématique et a été grandement facilitée par l'apparition des premiers ordinateurs. Cette cryptographie moderne est initiée par le travail de Claude Shannon en 1948 sur la théorie mathématique de l'information [54], sur laquelle repose la cryptographie moderne. En 1948, il montre également que même sur un canal véhiculant l'information de manière très altérée il est possible d'ajouter de la redondance afin que le message initial puisse être reconstruit après transmission. Enfin, en 1949, Shannon apporte la première preuve théorique de confidentialité, en lien avec la perfection du code de Vernam [54], qui est une méthode théorique impossible à casser. Au début des années 1970, Horst Feistel a mené un projet de recherche sur les chiffrements itératifs par blocs à l'IBM Watson Research Lab [57, 58], ses travaux ont conduit en 1977 à la proposition de l'algorithme DES, Data Encryption Standard [5], comme standard de chiffrement à clé secrète. Avec l'accroissement de la puissance des ordinateurs, la sécurité de DES a été remise en cause. Ainsi, cet algorithme a été remplacé en 2000 par un nouveau standard appelé AES [19]. En parallèle à ces études, la cryptographie à clé publique a été proposée en 1976 par Whitfield Diffie et Martin Hellmann [7]. Ils ont donné une solution entièrement nouvelle au problème de l'échange de clefs. Ils ont avancé aussi l'idée d'authentification à l'aide d'une fonction à sens unique. En 1978, Ron Rivest, Adi Shamir et Leonard Adleman ont réalisé l'idée de Diffie et Hellman et ont inventé le premier système à clé publique, le système RSA [8]. Cet algorithme est fondé sur la difficulté de factoriser des grands nombres, et la fonction à sens unique utilisée est une fonction "puissance". Depuis lors, la littérature sur ce sujet n'a cessé de développer [59, 60].
Aux alentours des années 1990, une nouvelle technique de chiffrement basée sur le chaos a été proposé dans [61], où l'auteur a utilisé un système chaotique pour générer des séquences de clés aléatoires. En effet, les systèmes chaotiques présentent des propriétés statistiques proches de l'aléatoire en dépit d'être déterministes. Depuis cette proposition, plusieurs travaux sur le chiffrement d'information en utilisant les propriétés du chaos ont

été faits [18, 21, 22, 62, 63, 67]. C'est ainsi que la cryptographie chaotique est née. Il existe d'autres types de cryptographie, tels que la cryptographie quantique [12,13], qui utilise les propriétés de la physique quantique et qui peut être définie comme l'association de deux techniques : la distribution quantique des clés secrètes, et l'utilisation de ces clés dans le codage à masque jetable.

2.4 Cryptographie standard et cryptographie chaotique

Dans cette partie, nous commençons par présenter la cryptographie standard [1]. Cette dernière est composée principalement de deux classes : cryptographie symétrique et cryptographie asymétrique. Par la suite, nous nous intéresserons à la cryptographie chaotique, tout en donnant quelques notions de base concernant le chaos et les systèmes chaotiques.

2.4.1 Cryptographie standard

Malgré la diversité des techniques de cryptographique standard [1, 2], deux grandes classes sont généralement distinguées : la cryptographie asymétrique, aussi appelée cryptographie à clé publique, et la cryptographie symétrique, également appelée cryptographie à clé secrète.

La cryptographie à clé symétrique

Les systèmes de chiffrement symétrique sont synonymes de systèmes à clés secrètes. Le chiffrement à clé secrète utilise pour les échanges entre deux correspondants, une seule clé. Cette clé est utilisée à la fois pour le chiffrement du texte clair et pour le déchiffrement du texte chiffré. La clé, appelée clé secrète ne doit être connue que par les deux interlocuteurs. Pour assurer la sécurité, il faut néanmoins trouver un algorithme dont le déchiffrement soit simple avec la clé, mais particulièrement difficile, voire impossible, sans la connaissance de celle-ci. Le principe du chiffrement symétrique est résumé à la figure 2.2. Les chiffrements symétriques se subdivisent en deux catégories : les chiffrements par blocs et les chiffrements à flots [2]. Dans le cas de chiffrement par blocs, la construction

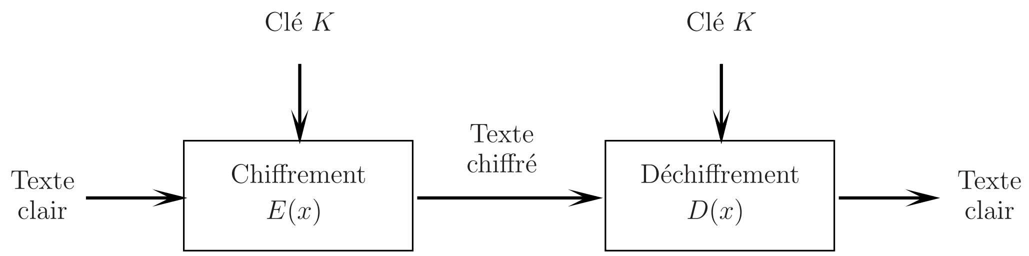


FIGURE 2.2: Principe de chiffrement symétrique.

d'algorithmes repose sur le principe de confusion et diffusion introduit par Claude Shannon [54]. Dans son article fondateur de la cryptographie moderne [54], Claude Shannon a discuté de deux propriétés que devrait vérifier un bon algorithme de chiffrement. Il s'agit de ce qu'il appelle la confusion d'une part et de la diffusion d'autre part. La confusion doit servir à complexifier la dépendance qui existe entre le message clair, la clé et le message chiffré, ceci afin de complexifier le travail statistique d'un attaquant, celui-ci devant en effet obtenir le moins d'information possible sur la clé pour chaque couple clair-chiffré qu'il possède. Cette propriété peut être réalisée en utilisant un algorithme de substitution complexe. La diffusion quant à elle demande que chaque partie du message chiffré dépende de chaque partie du message clair et de la clé, en d'autres termes, de petits changements en entrées doivent avoir un effet important en sortie. Cette propriété peut être établie en utilisant des tables de permutation. Un chiffrement par bloc divise le message clair en blocs de longueur fixe n puis chiffre chacun de ces blocs séparément l'un après l'autre. Les différents blocs sont combinés entre eux via un mode opératoire. Parmi ces modes, nous pouvons citer le mode ECB (*Electronique Code Book*) qui chiffre simplement successivement en parallèle chacun des blocs du texte clair. Un autre mode utilisé est le mode CBC (*Cipher Block Chaining*). Cette fois-ci, avant d'être chiffré, chaque bloc du texte clair est combiné via un ou exclusif avec le texte chiffré du bloc précédent. La seconde catégorie de chiffrement symétrique est le chiffrement à flots. Ce chiffrement traite les données un bit à la fois et fonctionne en générant, à partir de la clé K, une suite de symboles, appelée suite chiffrante, de la même longueur que le message à chiffrer. La suite chiffrante est alors combinée avec le message clair au moyen d'une loi appliquée bit-à-bit. La sécurité de ce type de chiffrement repose sur la qualité de la suite chiffrante générée.

En 1949, Claude Shannon a exposé l'un des critères nécessaires à la sécurité inconditionnelle d'un protocole à clé symétrique : la longueur de la clé doit être au moins aussi longue que le message à chiffrer. Si le critère de Shannon n'est pas respecté, la sécurité ne peut être démontrée formellement. En revanche, les protocoles peuvent être testés contre un grand nombre d'attaques spécifiques, de manière intense. En particulier, les protocoles doivent s'assurer que la clé soit suffisamment longue pour empêcher une attaque dite exhaustive, consistant à tester toutes les clés possibles. Par conséquent, la sécurité est dite calculatoire : le concepteur du protocole essaie de trouver la meilleure attaque contre le système, et estime la durée minimale que prendrait cette attaque pour déterminer la clé. Si cette durée est déraisonnable, le protocole est considéré comme sûr.
De très nombreux protocoles à chiffrement symétrique existent. Citons l'un des plus célèbres, DES (Data Encryption Standard [5]), qui n'est plus utilisé de nos jours car sa clé de chiffrement de 56 bits est trop courte, et autorise une attaque exhaustive très rapide. On considère de nos jours qu'une clé de 80 bits est un minimum, mais une clé de 128, voire 256 bits, est recommandée. Parmi les algorithmes les plus utilisés aujourd'hui, on trouve 3DES (Triple Data Encryption Standard [6]), Blowfish [76] et AES (Advanced Encryption Standard [19]).
Toutefois, cette méthode souffre du problème de la gestion des clés lorsque le nombre d'utilisateurs augmente. La cryptographie asymétrique (ou à clé publique) est venue résoudre le problème de distribution des clés posé par la cryptographie à clé secrète, mais elle présente l'inconvénient d'être bien plus lente que les algorithmes à clé secrète. Dans les algorithmes asymétriques, les clés de chiffrement et de déchiffrement sont distinctes et ne peuvent se déduire l'une de l'autre. On peut donc rendre l'une des deux publique tandis que l'autre reste privée.

La cryptographie à clés asymétriques

La nécessité du partage d'une clé secrète est l'une des limites du chiffrement symétrique ; en effet, il suppose une transmission physique de la clé entre les interlocuteurs, avec les contraintes que ceci comporte. Cette transmission peut en outre être impossible.

Le chiffrement asymétrique offre une solution à ce problème. Le destinataire génère tout d'abord une paire de clés complémentaires : la clé de décodage, appelée clé privée, est conservée par le destinataire, et la clé publique d'encodage est mise à disposition du public sur un serveur de clés authentifié. Si Alice veut envoyer un message codé à Bob, il lui suffit de récupérer la clé publique de Bob sur le serveur, de chiffrer le message avec celle-ci, et d'envoyer le cryptogramme à Bob. Celui-ci peut ensuite le décrypter aisément avec sa clé privée.

Ce type de protocole ne requiert pas de contact a priori pour transmettre un message. En

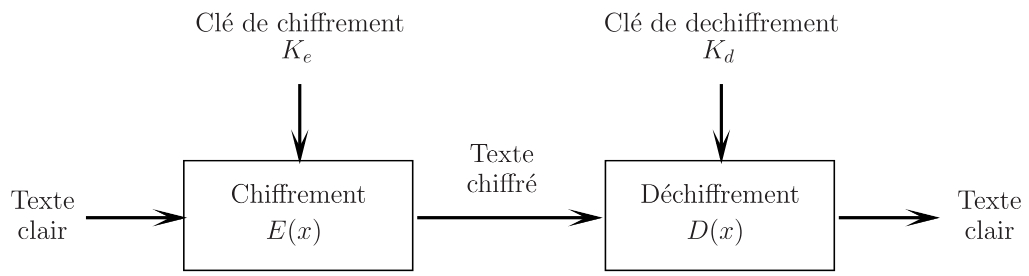


FIGURE 2.3: Principe de chiffrement asymétrique.

revanche, il nécessite des clés beaucoup plus longues que pour le chiffrement symétrique. On considère aujourd'hui que pour une sécurité à assez long terme (typiquement 40 ans), une clé d'au moins 4096 bits devrait être utilisée, ce qui n'est que très rarement le cas en pratique. D'une manière générale, ces chiffrements se basent sur la difficulté de résoudre certains problèmes complexes tels que la factorisation d'entiers [8], le calcul de logarithme discret dans un corps fini [59] ... etc.

2.4.2 Cryptographie chaotique

Ces trois dernières décennies ont été marquées par une utilisation massive des systèmes chaotiques pour le chiffrement et la sécurisation des transmissions par le chaos. Ces pratiques étaient possibles grâce à la découverte de la synchronisation des systèmes chaotiques. En effet, deux systèmes chaotiques totalement isolés ne peuvent pas se synchroniser, à cause de leurs sensibilités aux erreurs, même très petites. Alors, un genre de couplage doit être introduit entre les systèmes à synchroniser (émetteur et récepteur). En

1990, Louis Pecora et Thomas Carroll [21] ont proposé un exemple, où un système chaotique et un duplicata d'une partie du système sont synchronisés. Ainsi, la synchronisation des systèmes chaotiques est mise en évidence, ouvrant ainsi la porte à la cryptographie chaotique [14–17, 68–75].

2.4.2.1 Principe de la cryptographie chaotique

La cryptographie chaotique permet de chiffrer et de déchiffrer une information en temps réel en noyant le message dans le signal chaotique. Pour cela, elle utilise les propriétés des dynamiques chaotiques qui sont une évolution temporelle d'aspect bruité et un déterminisme local. Récemment, une variété de systèmes de communication sécurisés basés sur le chaos ont été étudiés. Quelques travaux sont basés sur la structure de Fridrich [77], qui intègre les propriétés de diffusion et de confusion définies par Shannon, [52, 78, 79]. D'autres, sont basés sur la synchronisation des systèmes chaotiques. Cette approche consiste à chiffrer l'information par un signal chaotique pseudo aléatoire généré par l'émetteur (système maître) et utiliser la synchronisation au niveau du récepteur (système esclave) pour récupérer le signal chaotique.
Comparée à la cryptographie classique, la cryptographie chaotique peut apporter quelques avantages en termes de robustesse et de rapidité, surtout en chiffrement symétrique par flux. De plus, la cryptographie chaotique est plus flexible, plus modulaire, et facile à mettre en œuvre, ce qui la rend appropriée pour le chiffrement des images.

2.4.2.2 Généralités sur les systèmes chaotiques

Pendant plusieurs siècles, l'homme pensait qu'une connaissance complète des paramètres d'un phénomène, à un instant donné, lui permettrait d'en prédire l'évolution passée ou à venir, cela sans aucune autre limite de l'imperfection des méthodes expérimentales. Avant le XX^{ème} siècle, les équations linéaires étaient les principaux modèles mathématiques décrivant les phénomènes physiques. Au XVIII^{ème} siècle, Isaac Newton exprima d'une manière explicite la cause de certains mouvements vraisemblablement désordonnés. Selon sa théorie, tout phénomène est causal et pourrait être parfaitement prédictible. Il suffit de résoudre le système d'équations différentielles décrivant ce phénomène. Suite aux succès obtenus en mécanique céleste, Laplace écrivit en 1814 dans l'introduction de son livre [80], *" Nous devons donc envisager l'état présent de l'univers comme l'effet de son état antérieur, et comme la cause de celui qui va suivre..."*. En 1820, le mathématicien Cauchy énonça le théorème général d'existence et d'unicité de la solution d'une équation différentielle. Lipschitz lui donnera sa forme définitive en 1868. Le théorème de Cauchy-Lipschitz indique bien qu'une prévision parfaite est possible, mais uniquement sous réserve de connaître parfaitement la condition initiale. Henri Poincaré résuma aussi ce point de vue : *" Si nous connaissons exactement les lois de la nature et la situation de l'univers à l'instant initial, nous pourrions prédire exactement la situation de ce même univers à un instant ultérieur"*.

La théorie du chaos fait partie des sciences les plus récentes et est devenue l'un des domaines les plus avancés dans la recherche contemporaine [18,81–83]. Les origines de cette nouvelle théorie s'étendent aux mathématiques et physiques des débuts du XX ^{ème} siècle, mais elle a émergé dans les années 1960-70. Poincaré fut l'un des premiers à entrevoir la théorie du chaos [87], il découvrit la notion de sensibilité aux conditions initiales à travers le problème de l'interaction de trois corps célestes. Depuis les années 1960, après la découverte de la théorie par Edward Lorenz [20], elle a pris son essor et a trouvé de nombreuses applications dans les domaines physiques, biologiques, chimiques et économiques ...etc. En 1975, T. Li et J.A. Yorke étaient les premiers auteurs qui ont introduit le terme de *" chaos"* dans leurs article [88] et depuis ce temps, ce mot a été largement utilisé. Depuis lors, le terme chaos s'est trouvé très médiatisé, notamment l'effet papillon qui est souvent invoqué pour faire allusion à de petites causes pouvant avoir de grands effets.

2.4.2.2.1 Définitions et propriétés du chaos

- **Définitions du chaos**

Le mot CHAOS prend origine du terme "$\chi\acute{\alpha}o\varsigma$", utilisé par les Grecs pour décrire l'espace vide infini dont ils ont supposé l'existence avant l'émergence de toutes choses. Le chaos ne signifie pas absence d'ordre ; c'est imbrication d'ordre et de désordre que l'on appelle chaos déterministe.

– **Définitions des systèmes dynamiques**

En général, un système dynamique décrit des phénomènes qui évoluent au cours du temps. Le terme *système* fait référence à un ensemble de variables d'état (dont la valeur évolue au cours du temps) et aux interactions entre ces variables. L'ensemble des variables d'état d'un système permet de construire un espace mathématique appelé *espace de phase*. Ce dernier, qui est une structure correspondante à toutes les trajectoires possibles du système considéré, permet de visualiser les propriétés du systèmes telles que les états stationnaires, les attracteurs, les points périodiques et les bifurcations. Un système dynamique en temps continu est décrit par un système d'équations différentielles, alors qu'en temps discret, on parle d'un système d'équations aux différences finies [89, 90]. Ce système d'équations présente deux types de variables (dynamique et statique). Les variables dynamiques sont les états du système qui changent avec le temps, alors que les variables statiques sont fixes. Si dans ces équations le temps est exprimé explicitement, le système est dit *non autonome* ; et si elles sont non linéaire, le système ne l'est pas non plus.
Les systèmes dynamiques sont classés en deux catégories :

1. Systèmes dynamiques continus (à temps continu),
2. Systèmes dynamiques discrets (à temps discret).

- Systèmes dynamiques à temps continu

Un système dynamique continu est décrit par un système d'équations différentielles ordinaires du premier ordre de la forme :

$$\dot{x}(t) = f(t, x(t)) \tag{2.2}$$

ce qui est une écriture abrégée du système suivant :

$$\begin{cases} \dot{x}_1 = f_1(t, x_1, \dots, x_n) \\ \vdots \\ \dot{x}_n = f_n(t, x_1, \dots, x_n) \end{cases} \tag{2.3}$$

où $f : R^+ \times R^n \to R^n$ désigne la dynamique du système, $x(t) \in R^n$ est le vecteur d'état de dimension n et $t \in R^+$ désigne le temps.
Si la dynamique du système donné par l'équation (2.2) est indépendante de l'instant t considéré, ce type de système est qualifié d'autonome. La dynamique dans ce cas particulier a la forme suivante :

$$\dot{x}(t) = f(x(t)) \tag{2.4}$$

Par un changement de variable approprié, on peut toujours transformer un système dynamique non autonome de dimension n en un système dynamique autonome équivalent de dimension $n + 1$.

- Systèmes dynamiques à temps discret

Un système dynamique discret est celui dans lequel les signaux sont définis à des intervalles de temps discrets. Ce type de système est représenté par des équations aux différences finies ou équations de récurrence, avec le modèle général suivant :

$$x(k + 1) = g(k, x(k)) \tag{2.5}$$

où $g : Z^+ \times R^n \to R^n$ désigne la dynamique du système en temps discret.
En temps discret, on définit aussi le système autonome comme une dynamique ne dépendant pas de l'instant k :

$$x(k + 1) = g(x(k)) \tag{2.6}$$

L'évolution d'un système dynamique unidimensionnel peut être décrite par une fonction itérative appelée en anglais "Map".

2.4.2.2.2 Propriétés du chaos

Les systèmes chaotiques sont des systèmes dont les trajectoires évoluent dans une région bornée présentant un caractère stable mais sans toute fois converger vers un point fixe ou un cycle limite. Ces trajectoires qui restent denses dans cette région sont très sensibles aux conditions initiales : deux conditions initiales très proches conduisent à deux trajectoires qui s'éloignent rapidement l'une de l'autre. Les solutions des équations différentielles non linéaires ne peuvent pas être calculées avec exactitude analytiquement car il n'existe pas de méthode de résolution analytique pour ces équations, sauf pour certaines classes particulières. Elles sont alors déterminées numériquement et le comportement du système est analysé par simulation. En effet, la sensibilité aux conditions initiales, l'attracteur étrange, l'évolution aléatoire et le spectre sont mis en évidence par simulation ou expérimentalement pour caractériser le comportement des systèmes chaotiques. Un système dynamique chaotique inclut les caractéristiques, qui lui sont inhérentes, présentées comme suit [81, 82] :

– **Non linéarité**

Pour un système dynamique non linéaire, les propriétés de stabilité sont essentiellement plus compliquées que dans le cas linéaire. Quand des non linéarités sont présentes, plusieurs caractéristiques peuvent apparaître comme les cycles limites ou le phénomène du chaos. La non linéarité est une condition nécessaire, mais non suffisante pour que le chaos apparaisse. Donc le comportement chaotique doit venir d'un système non linéaire, mais la non linéarité n'implique pas nécessairement le chaos.

– **Déterminisme**

Le comportement chaotique d'un système est généré par une ou plusieurs équations déterministes qui ne font intervenir aucun paramètre aléatoire. Les états passés, présents et futurs du système sont commandés par des lois déterministes. Le déterminisme traduit l'unicité de la solution pour l'équation différentielle d'un système donné, c'est le théorème de Cauchy, mais cela n'empêche quand même pas les systèmes chaotiques d'être imprévisibles.

– **Sensibilité aux conditions initiales**

Une propriété très importante que présentent les systèmes chaotiques est la sensibilité aux conditions initiales, c.à.d. la propriété selon laquelle les évolutions de deux points de départ, aussi proches que l'on veut, seront tellement divergentes qu'il ne sera pas possible de trouver une relation entre leurs deux trajectoires.

Il est en particulier clair que la moindre erreur ou simple imprécision sur la condition initiale interdit de décider à tout temps quelle sera la trajectoire effectivement suivi et, en conséquence, de faire une prédiction autre que statique sur le devenir à long terme du système. Ainsi, bien que l'on traite de systèmes déterministes, il est impossible de prévoir à long terme leurs comportements.

- **Imprévisibilité**

En plus de la sensibilité aux conditions initiales, une autre caractéristique des systèmes chaotiques est que le comportement est imprévisible. Celui-ci correspond à une évolution complexe, non périodique et non prédictible. Cependant, l'observation de la trajectoire dans l'espace des phases, lorsque t tend vers l'infini, décrit une forme particulière qui présente une structure fractale : c'est l'attracteur étrange.

- **Attracteur étrange**

Les systèmes chaotiques ont une dynamique très complexe, mais cette dynamique n'est pas erratique comme dans le cas d'un bruit, Lorsqu'on analyse le système dans l'espace de phase, sa dynamique comporte une certaine régularité qui donne naissance à ce qu'on appelle "attracteur étrange". Dans le plan, ces objets géométriques issus de l'évolution de systèmes chaotiques, sont formés d'une suite infinie de points qui dépendent de la valeur initiale. Au fur et à mesure que le nombre de points augmente, une image se forme dans le plan et devient de plus en plus nette. Cette image n'est ni une courbe ni une surface, c'est en fait un objet intermédiaire constitué de points avec entre eux des espaces inoccupés. L'objet est qualifié d'étrange en raison de sa structure pointilliste et de sa nature fractale. Une valeur différente de la condition initiale conduit a une toute autre suite qui après une courte phase, dessine la même image.

- **Spectre de puissance étalé**

Le spectre de puissance d'un signal chaotique est continu et riche en fréquences, c'est-à-dire il possède une infinité de raies dans ce spectre. Donc, un signal chaotique possède un spectre étalé s'étendant sur une gamme de fréquences, proche du spectre d'un bruit.

- **Bornitude des solutions**

Toutes les solutions des systèmes chaotiques sont des solutions globalement bornées. En effet, la trajectoire du système chaotique que l'on observe dans l'espace des phases reste confinée dans une région bien définie (attracteur étrange), après une période transitoire de durée variable.

2.4.2.2.3 Outils d'étude des systèmes chaotiques

Afin d'étudier les systèmes chaotiques, la communauté scientifique a proposé, entre autres, des solutions avec une approche statistique du problème comme le calcul de la dimension de corrélation, les exposants de Lyapunov ...etc. La dimension de corrélation est un outil qui offre la possibilité de déterminer la dimension de l'attracteur reconstruit à partir d'une série temporelle observée, tandis que les exposants de Lyapunov sont employés pour l'évaluation de l'instabilité propre au phénomène chaotique.
Cette partie a pour but de présenter les différents outils que nous pourrons programmer afin de mettre en évidence certains comportements caractéristiques des systèmes dynamiques non linéaires et, en particulier, les systèmes chaotiques.

– **La section de Poincaré**

La section de Poincaré est un outil mathématique simple permettant de transformer un comportement compliqué dans l'espace de phase en un système dynamique discret dans un espace de dimension inférieure [92]. En effet, lorsqu'on trace les solutions à certains problèmes non linéaires, l'espace de phase peut devenir encombré et la structure fondamentale peut devenir voilée. Pour surmonter ces difficultés, la section de Poincaré a été proposée. Cependant, cela se traduit presque toujours par un travail numérique puisque les solutions analytiques peuvent rarement être trouvées.
Soit un système dynamique continu, décrit dans un espace d'état de dimension n et une surface de dimension $(n-1)$ définie dans cet espace. L'application de Poincaré est le système dynamique en temps discret dont la suite des itérés correspond aux coordonnées des points d'intersections successifs de la trajectoire avec cette surface. L'ensemble des points d'intersections, situés sur la surface représente la section de Poincaré. Si on prend un exemple d'un espace d'états de dimension ≥ 3, la représentation des trajectoires est difficile et on a recours, pour les caractériser, aux sections de Poincaré. Pour cette raison, on coupe l'ensemble des trajectoires par un plan, et chaque fois qu'une trajectoire

traverse ce plan, elle y marque un point. La suite temporelle de points obtenus marque le comportement du système. Ainsi, si la suite temporelle des points converge vers un point d'accumulation, c'est que la coupe passe par l'attracteur ponctuel. Si l'attracteur est cyclique, le plan intersecte le cycle limite en deux points d'accumulation, et les intersections avec la trajectoire se rapprochent alternativement de ces deux points. Si un système de plus de 2 variables manifeste deux pulsations simultanées et indépendantes, les trajectoires s'enroulent autour de la surface d'un tore. Si l'attracteur est chaotique, l'intersection de l'attracteur avec le plan de Poincaré, donne une figure comportant des étirements et repliements de toutes les zones densément occupées. Dans ce cas, aucune trajectoire ne repasse deux fois par le même point, et deux trajectoires ne se superposent jamais [81].

– **Le spectre de Puissance**

Une façon simple de caractériser le chaos consiste à calculer le spectre de puissance, qui représente la répartition de la puissance le long de l'axe des fréquences, de l'évolution temporelle d'une des variables du système [91]. Tout signal $x(t)$, dans le cas continu ($x(k)$ dans le cas discret), peut en effet être représenté comme une superposition de composantes périodiques. Ces dernières sont toujours exprimées en terme de fonctions élémentaires sinus et cosinus. La détermination des amplitudes relatives de ces composantes constitue l'objet de l'analyse spectrale. Le spectre de puissance est simplement la transformée de Fourier de la fonction d'autocorrélation.
La procédure de calcul du spectre de puissance se résume en quatre étapes :

1. Déterminer la moyenne de la variable $x(t)$ ($x(k)$ dans le cas discret), qui représente l'espérance mathématique de $x(t)$ ($x(k)$ dans le cas discret).

$$\begin{cases} m = E[x(t)] & \text{Cas continu} \\ m = E[x(k)] & \text{Cas discret} \end{cases} \tag{2.7}$$

2. Introduire le signal centré sur la moyenne temporelle.

$$\begin{cases} x_c(t) = x(t) - m & \text{Cas continu} \\ x_c(k) = x(k) - m & \text{Cas discret} \end{cases} \tag{2.8}$$

3. Calculer la fonction d'autocorrélation, qui est la covariance entre les variables $x(t)$ et $x(t+\tau)$ ($x(k)$ et $x(k+\tau)$), exprimée sous la forme :

$$\begin{cases} C_{xx}(\tau) = E[x(t)x(t+\tau)] = m^2 + E[x_c(t)x_c(t+\tau)] & \text{Cas continu} \\ C_{xx}(\tau) = E[x(k)x(k+\tau)] = m^2 + E[x_c(k)x_c(k+\tau)] & \text{Cas discret} \end{cases} \tag{2.9}$$

4. En déduire le spectre ou la densité spectrale de puissance d'un signal $x(t)$ ($x(k)$ dans le cas discret), donné par la formule :

$$P_{xx}(f) = TF[C_{xx}(\tau)] \tag{2.10}$$

où TF désigne la transformée de Fourier. Si le signal $x(t)$ est de moyenne non nulle, on adjoint au spectre une raie à l'origine ($f = 0$) d'amplitude m^2. Cette raie à l'origine, qui traduit simplement la présence d'une moyenne non nulle, porte le nom de composante continue du processus.

L'allure générale du spectre de puissance renseigne sur la manière dont évolue le signal $x(t)$ ($x(k)$ dans le cas discret) au cours du temps. Pour un signal périodique, le spectre comporte différentes composantes non-nulles correspondant (en abscisse) à la fréquence fondamentale du signal et ses éventuelles harmoniques. Dans le cas d'un signal chaotique, le spectre sera continu, irrégulier et riche en fréquences, c'est-à-dire il possédera une infinité de raies dans ce spectre. Le spectre de Fourier d'un signal chaotique est un spectre à large bande, analogue à celui d'un bruit.

– **Exposants de Lyapunov**

L'évolution d'un flot chaotique est difficile à appréhender, parce que la divergence des trajectoires sur l'attracteur est rapide. C'est pourquoi, on essaye d'estimer ou même de mesurer la vitesse de divergence ou convergence. Cette vitesse s'appelle l'exposant de

Lyapunov. L'exposant de Lyapunov sert à mesurer le degré de stabilité d'un système et permet de quantifier la sensibilité aux conditions initiales d'un système chaotique [81]. Le nombre d'exposants de Lyapunov est égal à la dimension de l'espace des phases et ils sont généralement indexés du plus grand au plus petit $\lambda_1; \lambda_2; \lambda_3; \ldots$. Ces exposants sont définis ci-après.

Il faut noter que l'existence d'un attracteur nécessite que la dynamique de ce système soit globalement dissipative. Cela signifie que le système doit être caractérisé par une stabilité globale qui correspond à la condition suivante sur le spectre de Lyapunov :

$$\sum_{i=1}^{n} \lambda_i < 0 \tag{2.11}$$

où n désigne la dimension du système. Pour un attracteur non chaotique, les exposants de Lyapunov sont tous négatifs ou nuls ($\lambda_i, i = 1, \ldots, n$) et leurs somme vérifie la condition (2.11). Les attracteurs non chaotiques sont ainsi classés en trois catégories :

- Point d'équilibre asymptotiquement stable : $\lambda_i \leq 0$ pour $i = 1, \ldots, n$.
- Cycle limite stable : $\lambda_1 = 0$ et $\lambda_i < 0$ pour $i = 2, \ldots, n$.
- Tore d'ordre K asymptotiquement stable : $\lambda_1 = \ldots = \lambda_K = 0$ et $\lambda_i < 0, i = K + 1, \ldots, n$.

Dans le cas des systèmes chaotiques continus, un attracteur étrange possèdera toujours au moins un exposant de Lyapunov positif avec la propriété (2.11) vérifiée. De plus, pour un attracteur étrange, un des exposants de Lyapunov est toujours nul. Cela signifie que pour respecter la condition (2.11), un attracteur étrange doit avoir au minimum trois exposants de Lyapunov. Donc, un système continu dans le temps doit être au moins de dimension trois pour produire le chaos. De plus, si le système est de dimension quatre ou plus et il possède deux exposants de Lyapunov positifs avec la propriété (2.11) vérifiée, le système est dit système hyperchaotique. Toutefois, un système chaotique à temps discret de dimension une, où l'exposant de Lyapunov correspondant est positif, peut produire le chaos (exemple de la fonction logistique).

Les divers critères permettant de caractériser la dynamique d'un système non linéaire sont

Régime permanent	Attracteur	Exposants de Lyapunov
Point d'équilibre	Point	$0 > \lambda_1 \geq \ldots \geq \lambda_n$
Périodique	Courbe fermée	$\lambda_1 = 0,\ 0 > \lambda_2 \geq \ldots \geq \lambda_n$
Quasi-périodique	Tore	$\lambda_1 = \ldots = \lambda_i = 0,\ 0 > \lambda_{i+1} \geq \ldots \geq \lambda_n$
Chaotique	Fractal	$\lambda_1 > 0,\ 0 > \lambda_2 \geq \ldots \geq \lambda_n$
Hyperchaotique	Fractal	$\lambda_1 > \lambda_2 > 0,\ 0 > \lambda_3 \geq \ldots \geq \lambda_n$

TABLE 2.1: Différents régimes d'un système dynamique non linéaire.

regroupés dans le tableau 2.1.

– **Cas de Systèmes dynamiques continus**

Considérons le système d'équations différentielles représenté par (2.4). Pour calculer le taux de divergence des trajectoires de ce système, nous supposons que les deux trajectoires (première et deuxième) sont données par $\dot{x_a} = f(x_a)$ et $\dot{x_b} = f(x_b)$, respectivement, et que la différence entre ces deux dernières est notée $d = x_b - x_a$.
La première dérivée de la distance d est donné par :

$$\dot{d} = \dot{x_b} - \dot{x_a} = f(x_b) - f(x_a) \approx f'(x_a)d \tag{2.12}$$

On suppose que la distance d est petite et on développe $f(x_b) = f(x_a + d)$ en série de Taylor :

$$f(x_a + d) = f(x_a) + f'(x_a)(x_b - x_a) = f(x_a) + f'(x_a)d \tag{2.13}$$

On considère aussi que $f'(x_a)$ est constante (ou elle varie très lentement), c'est-à-dire $f'(x_a) \approx \lambda$. Le flot associé à l'équation (2.12), appelé $D(t)$ est donné par :

$$D(t) = d_0 e^{\lambda(t-t_0)} \tag{2.14}$$

où d_0 est la distance initiale entre les trajectoires et t_0 représente l'instant initial. D'après (2.14), il est évident que le signe de λ détermine la convergence ou la divergence des trajectoires. La valeur de λ est calculée d'après la relation suivante :

$$\lambda = \frac{1}{t - t_0} ln \frac{D(t)}{d_0} \tag{2.15}$$

Pour les systèmes non linéaires réels, la condition $f'(x_a) \approx \lambda$ n'est pas vérifiée dans la plupart des cas. Cependant, il est possible de trouver la divergence finale des trajectoires à long terme, c'est-à-dire la limite de (2.15) lorsque t tend vers l'infini :

$$\lambda = \lim_{t \to \infty} \frac{1}{t - t_0} ln \frac{D(t)}{d_0} \tag{2.16}$$

Cette limite est appelée ***exposants de Lyapunov***.

– **Cas de Systèmes dynamiques discrets**

Supposons que la condition initiale x_0 de (2.6) soit affectée d'une erreur infinitésimale E_0. Après k itérations, l'erreur initiale E_0 sera donc amplifiée d'un facteur $\left|\frac{E_k}{E_0}\right|$. Notons que l'erreur diminue lorsque ce facteur est inférieur à 1 et augmente s'il est supérieur à 1. On a la formule suivante :

$$\left|\frac{E_k}{E_0}\right| = \left|\frac{E_k}{E_{k-1}}\right| \left|\frac{E_{k-1}}{E_{k-2}}\right| \cdots \left|\frac{E_2}{E_1}\right| \left|\frac{E_1}{E_0}\right|$$

d'où

$$ln\left(\left|\frac{E_1}{E_0}\right|\right) = \sum_{i=0}^{k} ln\left(\left|\frac{E_i}{E_{i-1}}\right|\right)$$

Il suffit alors de calculer ce produit pour déterminer la façon dont s'amplifie l'erreur initiale. Lyapunov introduit la limite donnée par la formule :

$$\lambda = \lim_{k \to \infty} \frac{1}{k} \sum_{i=0}^{k} ln\left(\left|\frac{dg(x_{i-1})}{dx_{i-1}}\right|\right) \in \mathbb{R} \tag{2.17}$$

– **Diagramme de bifurcation et route vers le chaos**

Un système dynamique non-linéaire peut présenter de multiples comportements (point fixe, oscillations périodiques, quasi-périodiques, chaos) en fonction de la valeur de ses paramètres. Il passe d'un comportement à un autre en fonction des changements de certains paramètres importants du système. Les transitions entre régimes dynamiques se font par bifurcation et le paramètre dont la modification entraîne le changement de régime dynamique est appelé paramètre de bifurcation. L'ensemble de l'évolution dynamique d'un système peut se représenter sous la forme d'un diagramme de bifurcation. Il existe plusieurs scénarios qui décrivent le passage du point fixe au chaos. Nous allons en exposer brièvement trois types d'évolution possible [81].

- **Par doublement de période**

Ce scénario de transition vers le chaos est le plus connu. Par augmentation du paramètre de contrôle du système chaotique, la fréquence du régime périodique double, puis est multipliée par 4, par 8, par 16 etc. Les doublement étant de plus en plus rapprochés, on tend vers un point d'accumulation auquel on obtiendrait hypothétiquement une fréquence infinie. C'est à ce moment que le système devient chaotique.

- **Par intermittences**

Ce scénario via les intermittences se caractérise par l'application erratique de bouffées chaotiques dans un système qui oscille de manière régulière. Le système conserve pendant un certain laps de temps un régime périodique ou pratiquement périodique, c'est-à-dire une certaine "régularité", et il se déstabilise, brutalement, pour donner lieu à une "bouffée" plus tard. On constate que la fréquence et la durée des phases chaotiques ont tendance à s'accroître plus on s'éloignait de la valeur critique de la contrainte ayant conduit à leur apparition. L'intermittence suppose en particulier que le cycle limite (correspondant à l'état périodique d'où est issu ce phénomène de transition) bifurque de façon sous-critique et qu'il n'y ait pas d'attracteur à proximité.

- **Par quasi-périodicité**

Cette route vers le chaos résulte de la "concurrence" de différentes fréquences dans le système dynamique. Dans un système à comportement périodique à une seule fréquence, si nous changeons un paramètre alors il apparaît une deuxième fréquence. Si le rapport entre les deux fréquences est rationnel, le comportement est périodique. Mais, si le rapport est irrationnel, le comportement est quasi périodique. Dans ce cas, les trajectoires couvrent la superficie d'un tore. Alors, on change de nouveau le paramètre et il apparaît une troisième fréquence, et ainsi de suite jusqu'au chaos.

2.4.2.3 Exemples illustratifs

Il existe plusieurs systèmes dynamiques qui sont utilisés pour générer les signaux chaotiques. En effet, dans le cas continu, un système chaotique libre (sans entrée) et sans retard doit posséder au moins trois états. Par ailleurs, dans le cas discret, un système dynamique à un seul état, la fonction logistique par exemple, peut être chaotique. Nous présentons dans ce qui suit deux exemples de systèmes chaotiques : le système chaotique continu de Lorenz et le système chaotique à temps discret de Hénon.

a. Système de Lorenz

Pour illustrer les propriétés d'un système chaotique continu, nous allons traiter l'exemple du système chaotique de Lorenz qui est donné par la représentation d'état suivante [20] :

$$\begin{cases} \dot{x} &= \sigma(y-x) \\ \dot{y} &= rx - y - xz \\ \dot{z} &= xy - bz \end{cases} \tag{2.18}$$

Les valeurs de σ et b sont fixées, respectivement à 10 et 8/3. Le paramètre r, qui est positif, est le paramètre de contrôle. Les points fixes du système (2.18) sont la solution de l'équation suivante :

$$\begin{cases} \sigma(y-x) = 0 \\ rx - y - xz = 0 \\ xy - bz = 0 \end{cases} \Rightarrow \begin{cases} x = y \\ z = (r-1) \\ y^2 = bz \end{cases} \tag{2.19}$$

Pour $r = 1$, nous avons le point fixe $P_0 = (0, 0, 0)$

Dans le cas général :

$$\begin{cases} x = y \\ z = (r-1) \\ y^2 = bz \end{cases} \Rightarrow \begin{cases} x = y \\ z = (r-1) \\ y = \pm\sqrt{b(r-1)} \end{cases} \tag{2.20}$$

Ainsi, le système admet trois points fixes :

$$\begin{cases} P_0 = (0, 0, 0) \\ P_1 = (\sqrt{b(r-1)}, \sqrt{b(r-1)}, r-1) \\ P_2 = (-\sqrt{b(r-1)}, -\sqrt{b(r-1)}, r-1) \end{cases}$$

La figure 2.4 présente la sensibilité aux conditions initiales de l'état x du système (2.18)

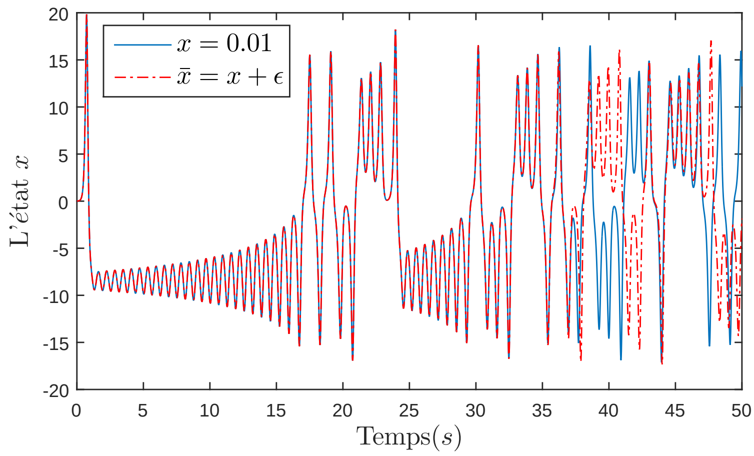


FIGURE 2.4: Sensibilité aux conditions initiales de l'état x du système de Lorenz.

pour $r = 28$, la trajectoire (représentée en bleu) est obtenue pour une condition initiale ($x(0) = 0.01$). Nous remarquons que, pour une petite variation $\epsilon = 10^{-10}$ de cette condition initiale, la trajectoire de $\bar{x}$ (représentée en rouge) diverge de la première courbe. Ce qui démontre la très grande sensibilité aux conditions initiales. L'aspect aléatoire des

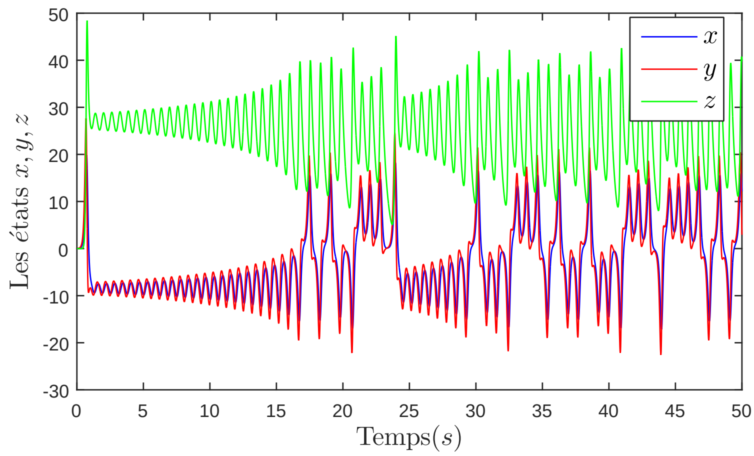


FIGURE 2.5: Aspect aléatoire des états du système de Lorenz.

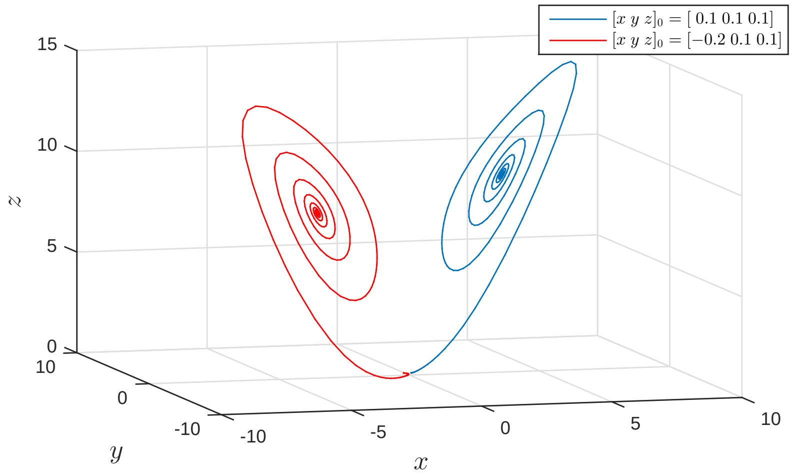


FIGURE 2.6: Plan de phase du système de Lorenz pour $r = 10$.

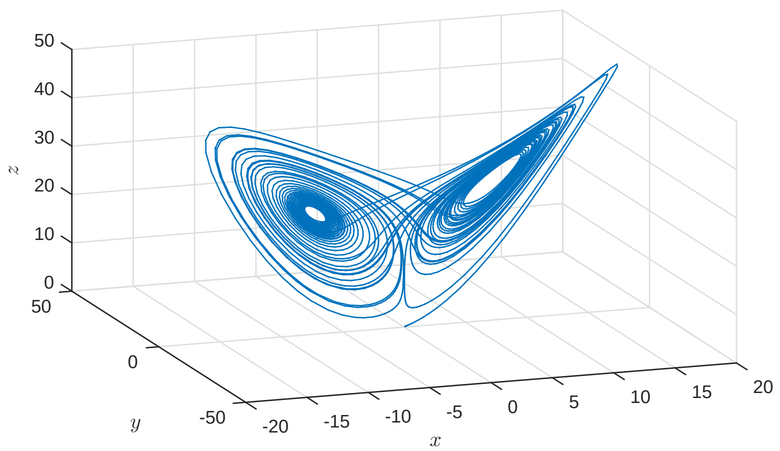


FIGURE 2.7: Plan de phase du système de Lorenz pour $r = 28$.

états x, y, z est illustré par la figure 2.5. Les trajectoires de phases pour différentes valeurs du paramètre r sont présentées par les figures 2.6, 2.7. Ainsi, pour $r = 10$ et à partir des conditions initiales quelconques, les trajectoires d'état convergent vers un des deux points d'équilibre (figure 2.6). Pour $r = 28$, le mouvement n'est pas périodique et l'objet géométrique complexe que l'on observe est un attracteur chaotique (figure 2.7).

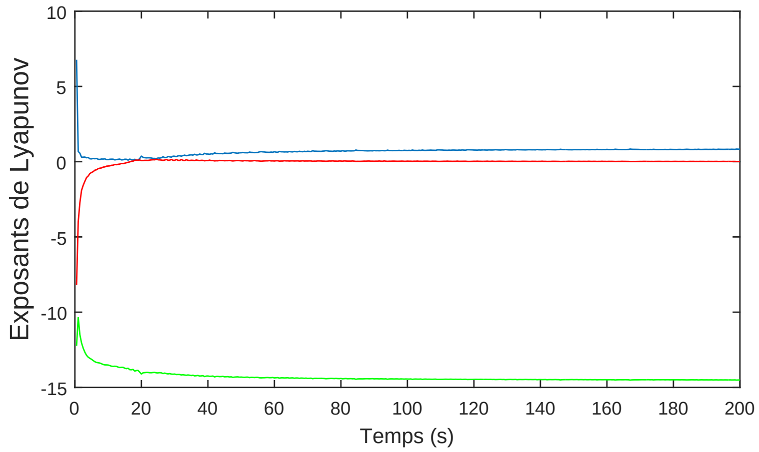


FIGURE 2.8: Exposants de Lyapunov du système de Lorenz.

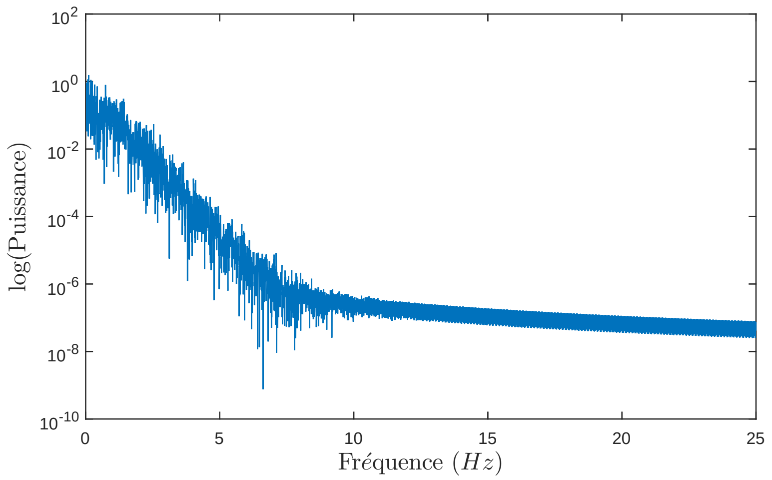


FIGURE 2.9: Spectre de puissance de la variabe x du système de Lorenz

La figure 2.8 présente les exposants de Lyapunov du système de Lorenz pour $r = 28$, où $\lambda_1 = 0.82981$, $\lambda_2 = 0.011796$ et $\lambda_3 = -14.504841$. Le spectre de puissance de la variable x est donné par la figure 2.9.

Le diagramme de bifurcation est présenté par la figure 2.10 qui illustre le comportement

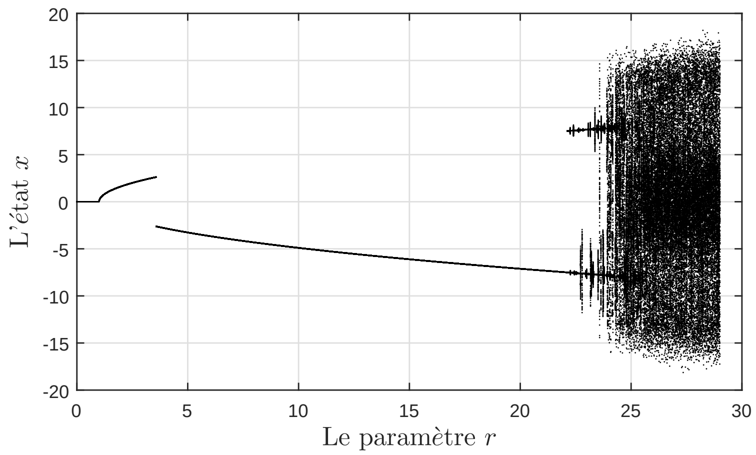


FIGURE 2.10: Diagramme de bifurcation du système de Lorenz.

des orbites du système de Lorenz en variant le paramètre r entre (0, 30). En effet, à partir de cette figure, nous pouvons clairement voir que, lorsque $r \in [0, 1[$, le système possède un seul point d'équilibre (P_0). Toutefois, lorsque $r = 1$, une bifurcation apparaît. Ainsi, pour $r > 1$, les deux autres points d'équilibre (P_1, P_2) sont crées. Par ailleurs, pour $r = r_c = \frac{\sigma(\sigma+b+3)}{\sigma-b-1}$, les deux points d'équilibre se déstabilisent à leurs tours, et lorsque r devient supérieur à r_c le système transite vers un régime chaotique. Dans cet intervalle, le système tourne autour d'un des deux points d'équilibres instables comme si il y convergeait avant de basculer aléatoirement vers l'autre équilibre pour y répéter le même type de comportement. Toutes les trajectoires convergent vers une trajectoire chaotique : l'attracteur étrange.

b. Système de Hénon

Afin de montrer les propriétés d'un système chaotique discret, nous avons choisi le modèle de Hénon. Ce modèle consiste en une itération à deux dimensions, qui est présenté par les équations suivantes [93] :

$$\begin{cases} x(k+1) = 1 - a\,x(k)^2 + y(k) \\ y(k+1) = b\,x(k) \end{cases} \tag{2.21}$$

a et b présentent les paramètres du système, où la valeur de a varie tandis que la valeur de b est fixée à 0.3.

Le système (2.21) possède deux points fixes (Q_1 et Q_2), donnés comme suit :

$$
\begin{aligned}
Q_1 &= \begin{Bmatrix} \frac{1}{2a}(b-1+\sqrt{(1-b)^2+4a} \\ \\ \frac{b}{2a}(b-1+\sqrt{(1-b)^2+4a} \end{Bmatrix} \\
Q_2 &= \begin{Bmatrix} \frac{1}{2a}(b-1-\sqrt{(1-b)^2+4a} \\ \\ \frac{b}{2a}(b-1-\sqrt{(1-b)^2+4a} \end{Bmatrix}
\end{aligned}
\tag{2.22}
$$

Ces deux valeurs sont obtenues à partir de l'équation suivante :

$$
\begin{cases} 1+y-ax^2 & = & x \\ bx & & y \end{cases}
\tag{2.23}
$$

Si l'on calcule les valeurs absolues des valeurs propres de la matrice jacobienne, on trouve que le point fixe Q_2 est un point selle.
Le déterminant $(b-1)^2+4a$ est négatif si $a < a_0 = -\frac{(b-1)^2}{4} = -0.1225$, dans ce cas il n'y a pas de points fixes. Si $a \in \left]-\frac{1}{4}(1-b^2),\ \frac{3}{4}(1-b^2)\right[\ -\ \{0\}$, on a deux points fixes Q_1 et Q_2, dans ce cas le point fixe Q_1 est stable.
Le phénomène de sensibilité aux conditions initiales est illustré par la figure 2.11. Pour les conditions initiales très proches (une différence de l'ordre de 10^{-10}), les deux systèmes évoluent de la même manière dans un premier temps, mais très vite, leur comportement devient différent. La figure 2.12 montre l'aspect aléatoire des états x, y du système de Hénon. Le plan de phase donné par la figure 2.13 présente l'attracteur étrange du système.
Le comportement chaotique du système est justifié par la valeur positive de l'exposant de Lyapunov, cette grandeur est observée sur la figure 2.14. La figure 2.15 présente le spectre de puissance de l'application.

La figure 2.16 nous donne un aperçu de la nature de la trajectoire pour différentes valeurs du paramètre de bifurcation a. Ce diagramme est de type de bifurcation de doublement de période. On remarque que pour toute valeur de $a \in [0\ 0.3675]$, le régime permanent est formé par un point limite stable. Pour $a \in [0.38\ 1.05[$, le diagramme de

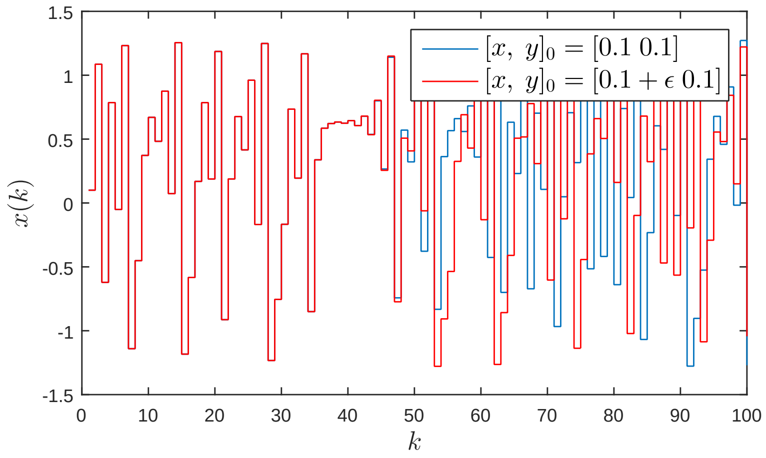


FIGURE 2.11: Sensibilité aux conditions initiales de l'état x du système de Hénon.

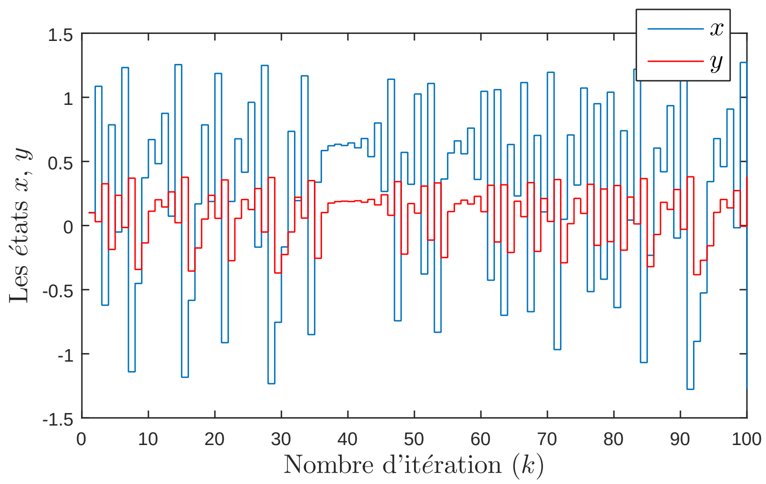


FIGURE 2.12: Aspect aléatoire des états du système de Hénon.

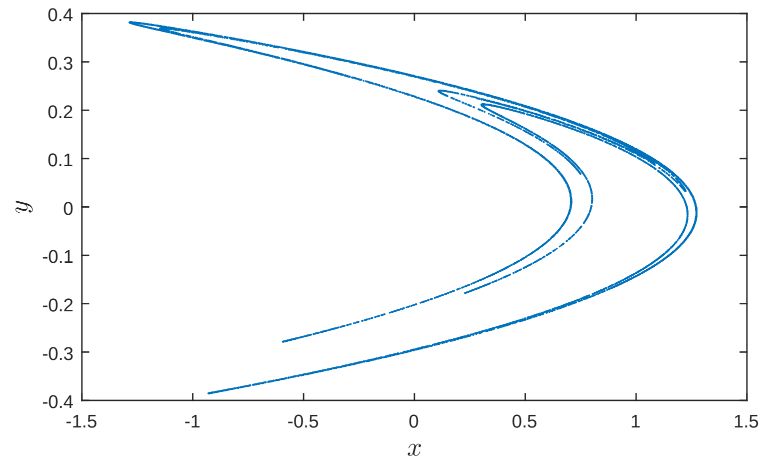


FIGURE 2.13: Plan de phase du système de Hénon pour $a = 1.4$.

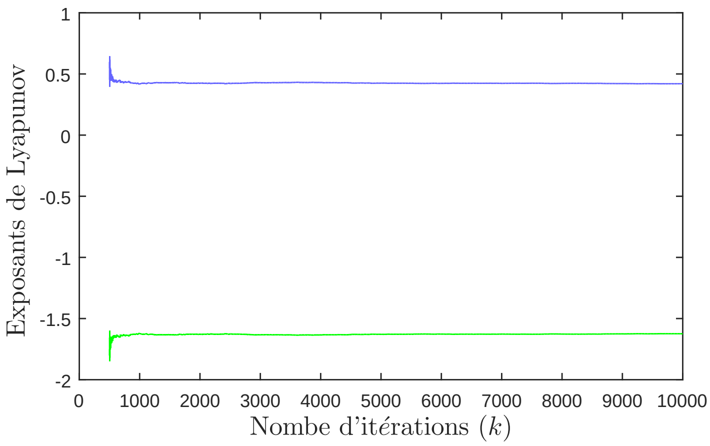


FIGURE 2.14: Exposants de Lyapunov du système de Hénon.

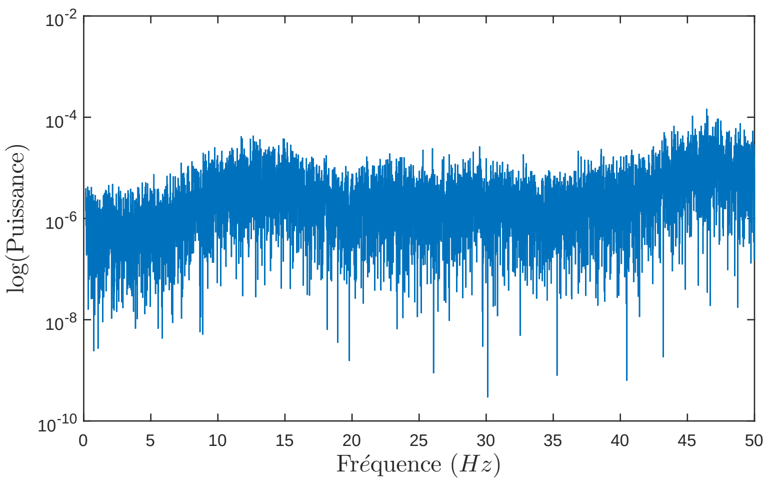


FIGURE 2.15: Spectre de puissance de la variable x du système de Hénon

bifurcation fait ressortir des comportements différents. Dans un premier lieu, l'ensemble des états limites est une solution périodique formé par deux points. Pour le deuxième cas, on observe une augmentation de la dimension de l'ensemble des états limites. Par ailleurs, pour $a \in [1.05\ 1.4]$ le système est dans un état chaotique.

Dans le contexte de chiffrement basé sur le chaos, la récupération de l'information chif-

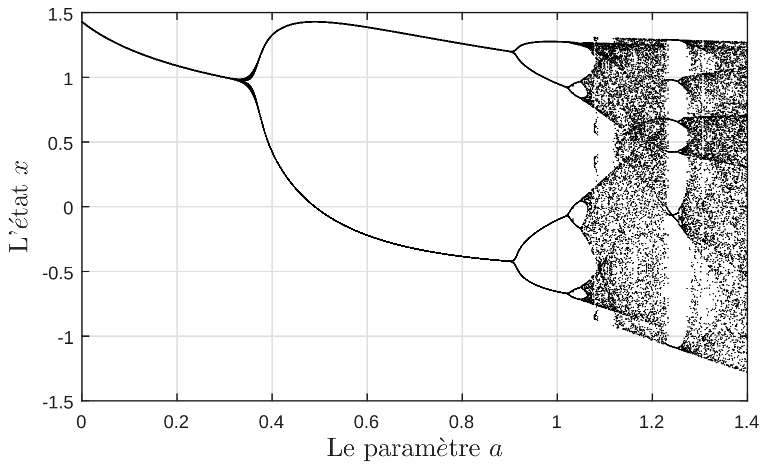


FIGURE 2.16: Diagramme de bifurcation du système de Hénon.

frée nécessite la synchronisation de l'émetteur et du récepteur. Il s'agit alors de garantir la convergence à zero de l'erreur de reconstruction d'état $e(t) = x(t) - \hat{x}(t)$ dans le cas continu ou $e_k = x_k - \hat{x}_k$ dans le discret. La synchronisation des systèmes chaotiques fera l'objet de la section suivante.

2.5 Synchronisation chaotique

Dans le contexte de cryptographie chaotique, le déchiffrement de l'information claire nécessite la synchronisation de l'émetteur et du récepteur. Ici, le mot synchronisation ne doit pas être pris dans le sens des systèmes périodiques. Dans les systèmes périodiques, par exemple deux pendules sont dit synchronisés lorsqu'ils sont en phase. Cependant, dans les systèmes chaotiques, la synchronisation prend place lorsque les trajectoires de deux ou plusieurs systèmes convergent vers la même valeur. A priori, la synchronisation des systèmes chaotiques paraît impossible, notamment à cause du comportement imprévisible à long terme de ces systèmes : ceci est dû à une extrême sensibilité aux conditions initiales. En effet, les trajectoires des systèmes chaotiques issues des conditions initiales légèrement différentes divergent exponentiellement avec le temps, c'est-à-dire que ces systèmes ne sont pas asymptotiquement stables. Toutefois, plusieurs études sur la possibilité de synchroniser le chaos ont été menées. En effet, les premiers travaux sur la synchronisation chaotique ont débuté avec Yamada et Fujisaka [94], qui ont utilisé une approche locale de la synchronisation chaotique. Par la suite, Pecora et Carroll [21] ont défini la synchronisation identique connue sous le nom de synchronisation maître-esclave, développée sur la base de circuits couplés, avec l'un maître et l'autre esclave. Ils ont montré que deux systèmes chaotiques pourraient se synchroniser sous certaines conditions. Une solution plus récente est la méthode de synchronisation généralisée, dont les bases ont été posées dans [97] et qui a ensuite été étudiée dans [98, 104]. Cette approche considère aussi une paire de systèmes configurés en maître-esclave mais cette fois le couplage n'est pas réservé à l'identité. Par la suite, la notion de synchronisation de phase entre deux circuits chaotiques couplés est apparue, dans ce cas la synchronisation vise à réaliser une cohérence de phase entre les variables d'états des systèmes considérés [99]. En parallèle avec ces études, [22, 100] ont montré que le problème de la synchronisation des systèmes chaotiques s'intègre dans le contexte plus général d'estimation d'état non linéaire. Depuis, la synchronisation chaotique a fait l'objet de nombreux travaux de recherche, en particulier dans le domaine de la transmission sécurisée [101].

D'une manière globale, toutes les méthodes de synchronisation sont regroupées sous deux modes de synchronisation, selon la nature de la connexion entre le système maître et le système esclave. Le premier mode repose sur un couplage mutuel (bidirectionnel) entre deux systèmes chaotiques. Le second est appelé couplage unidirectionnel. Dans la synchronisation bidirectionnelle, la boucle de retour est appliquée sur les deux systèmes à la fois. Par contre, dans le cas de la synchronisation unidirectionnelle la boucle de retour est appliquée sur l'un des deux systèmes. Pour expliquer la synchronisation bidirectionnelle et unidirectionnelle de deux systèmes chaotiques, on considère les deux systèmes décrits par l'équation suivante :

$$\begin{aligned} \dot{x}(t) &= f_1(x(t)+)D_1(y(t) - x(t)) \\ \dot{y}(t) &= f_2(y(t)) + D_2(x(t) - y(t)) \end{aligned} \tag{2.24}$$

Avec $x(t) \in R^n$, $y(t) \in R^n$ représentent les états des deux systèmes, et $f_1, f_2 : R^n \to R^n$ des fonctions non linéaires continues. D_1 et D_2 matrices diagonales. Le schéma de couplage des deux systèmes est montré dans les figures 2.17(a) (couplage unidirectionnel) et 2.17(b)(couplage bidirectionnel). Lorsque la synchronisation des deux systèmes est at-

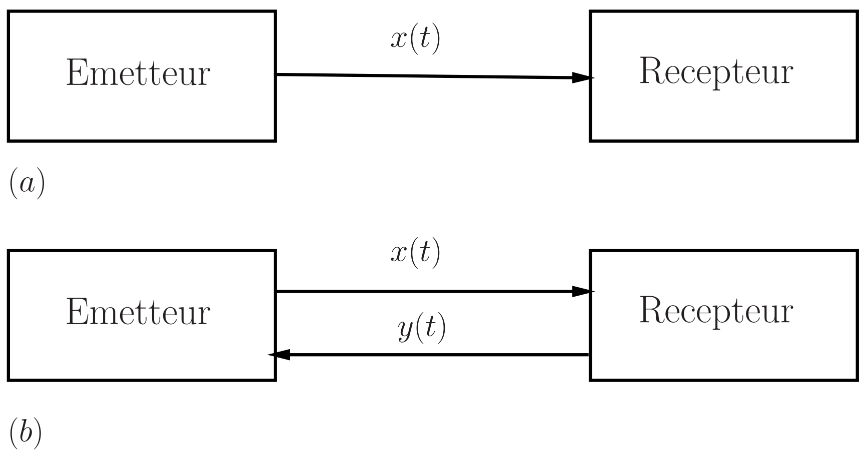


FIGURE 2.17: Schéma de couplage : (a) unidirectionnel, (b) bidirectionnel.

teinte, les termes de couplage $D_1(y(t) - x(t))$ et $D_2(y(t) - x(t))$ deviennent nuls. Cela veut dire que $x = y$ et qu'un comportement commun est obtenu pour les deux systèmes. La synchronisation unidirectionnelle est un cas particulier de la synchronisation bidirectionnelle, elle est définie si $D_1 = 0$ ou $D_2 = 0$.

Dans ce travail de thèse, nous n'abordons que la synchronisation unidirectionnelle de l'émetteur vers le récepteur, ceci afin de réaliser un système de communication, dans lequel la synchronisation joue un rôle principal.

Plusieurs types de synchronisation peuvent être trouvés dans la littérature. Ces différents types peuvent être regroupés dans les catégories suivantes :

2.5.1 Synchronisation complète

Cette synchronisation, connue aussi sous le nom de synchronisation identique, est la forme la plus ancienne et simple de la synchronisation des systèmes chaotiques couplés. Elle consiste en une reproduction parfaite des trajectoires de deux systèmes chaotiques après un régime transitoire, qui est réalisée au moyen d'un signal d'accouplement unidirectionnel, de manière qu'ils restent en phase au cours du temps. Considérons deux systèmes dynamiques

$$\dot{x}_m(t) = f(x_m(t)) \tag{2.25}$$

et

$$\dot{x}_s(t) = f(x_s(t)) \tag{2.26}$$

où $x_m(t), x_s(t) \in R^n$ sont des vecteurs d'état de dimension n.
Alors (2.25) et (2.26) sont identiquement synchronisés si, quelles que soient leurs conditions initiales :

$$\lim_{t\to\infty} |x_s(t) - x_m(t)| = 0 \tag{2.27}$$

Cette catégorie peut être obtenue par différents types de schémas tels que l'approche de Pecora et Carroll [21, 102] que nous expliquerons ci-dessous, la synchronisation par feedback [103], la décomposition active-passive [104, 105], le couplage diffusif et quelques autres méthodes hybrides [106], l'approche utilisant des observateurs [22, 63–66].

L'approche de Pecora et Carroll

Le principe de synchronisation proposé par Pecora et Carroll dans [21] est appelé principe *maître-esclave* (*master-slave)*. En effet, certains systèmes possèdent la propriété d'auto synchronisation, c'est-à-dire qu'on peut les décomposer en deux sous-systèmes, l'un maître, l'autre esclave. Ces derniers peuvent se synchroniser sous l'effet d'un couplage avec signal commun. Considérons à nouveau le système chaotique (système maître), en temps continu, représenté par le modèle dynamique (2.25). Ce système est décomposé en deux sous-systèmes $[x_m = (v, w)]$ de dimensions m et k tel que $n = m + k$.

$$\begin{cases} \dot{v} = g(v, w) \\ \dot{w} = h(v, w) \end{cases} \tag{2.28}$$

où $v = (x_{m_1}, \ldots, u_{m_m})$, $g = (f_1(x_m), \ldots, f_m(x_m))$, $w = (x_{m_{m+1}}, \ldots, x_{m_n})$ et $h = (f_{m+1}(x_m), \ldots, f_n(x_m))$. Considérons maintenant un nouveau sous-système w' (système esclave) identique au sous-système w, dont l'entrée est v :

$$\dot{w}' = h(v, w') \tag{2.29}$$

Ce sous-système w' est un candidat approprié pour se synchroniser avec la dynamique complète initiale. La condition nécessaire et suffisante pour obtenir la synchronisation est que le sous-système w' soit stable, cela signifie que l'ensemble des exposants de Lyapunov du ce sous-système soient négatifs.

Une synchronisation complète peut alors être accomplie seulement si $\lim\limits_{t\to\infty} |w' - w| \to 0$. Ainsi, nous avons :

$$\begin{aligned} \dot{\xi} &= \dot{w} - \dot{w}' \approx h(v, w) - h(v, w') \\ &\approx D_w h(v, w)\xi + O(\xi) \end{aligned} \tag{2.30}$$

où $D_w h$ est la Jacobienne de h par rapport à w.

Le comportement du système (2.30) va dépendre des valeurs propres de la matrice Jacobienne. Du moment que le système est chaotique, des complications vont se présenter. Si les systèmes étaient périodiques, alors les valeurs propres de la matrice de Jacobienne appropriée auraient déterminé la stabilité. Mais dans ce cas, les valeurs propres changent car les variables v et w évoluent de manière chaotique avec le temps. Par conséquent, la moyenne des valeurs propres à chaque instant doit être prise afin de déterminer l'exposant de Lyapunov sur l'ensemble de l'attracteur du sous-système w. Cette moyenne des valeurs propres est appelée *l'exposant conditionnel de Lyapunov* (conditionnel car il dépend des variables chaotiques) [21]. Pecora et Carroll ont mentionné que les systèmes ne se synchroniseraient que si les parties réelles des exposants de Lyapunov étaient négatives [107]. Cependant, la méthode ne mentionne pas les conditions initiales pour lesquelles les systèmes vont se synchroniser. Mais puisque les deux systèmes ont les mêmes attracteurs, avec le temps, les états des systèmes finiront par se rapprocher suffisamment dans l'espace d'état pour que la condition (2.30) soit vraie. Par conséquent, l'exposant de Lyapunov conditionnel ayant une partie réelle négative n'est qu'une condition nécessaire pour atteindre la synchronisation mais pas suffisante.

Vérifions maintenant la méthode de synchronisation de Pecora et Carroll en utilisant le système de Lorenz défini en (2.18), dit "maître". Les valeurs de σ, r et b sont fixées, respectivement, à 10, 28 et 8/3.

Le système (2.18) est décomposé de telle sorte que y soit le signal de couplage pour le système esclave et soit équivalent à v comme expliqué précédemment. Par conséquent, le système esclave conduit par y peut être écrit comme suit :

$$\begin{cases} \dot{\hat{x}} &= \sigma y - \sigma \hat{x} \\ \dot{\hat{z}} &= \hat{x} y - b \hat{z} \end{cases} \tag{2.31}$$

Ainsi, la dynamique d'erreur peut être écrite comme suit :

$$\begin{pmatrix} \dot{e}_x \\ \dot{e}_z \end{pmatrix} = \begin{pmatrix} -\sigma & 0 \\ y & -b \end{pmatrix} \begin{pmatrix} e_x \\ e_z \end{pmatrix} \tag{2.32}$$

La valeur propre de la matrice d'erreur ne dépend pas de la variable de couplage y. Par conséquent, la valeur propre ou l'exposant de Lyapunov du sous-système peut facilement être calculé comme étant $\lambda_1 = -\sigma$, $\lambda_2 = -b$. Cela signifie que les deux exposants sont tout le temps négatifs. Par conséquent, les variables d'erreur $e_x, e_z \to 0$ lorsque $t \to \infty$, permettant ainsi une synchronisation complète de deux systèmes malgré les conditions initiales.

Les résultats de simulation de la synchronisation des systèmes (2.18) et (2.31) sont présentés par les figures (2.18, 2.19 et 2.20). La figure 2.18 présente la synchronisation de l'état x avec son estimé $\hat{x}$, et la figure 2.19 présente la synchronisation de l'état z avec son estimé $\hat{z}$. L'erreur de synchronisation des deux états x, z avec leurs estimés est donnée par la figure 2.20.

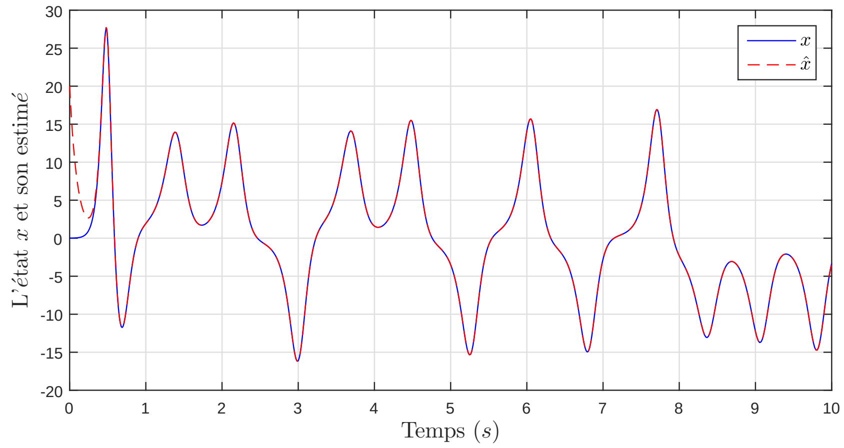


FIGURE 2.18: Synchronisation de l'état x du système de Lorenz avec son estimé $\hat{x}$.

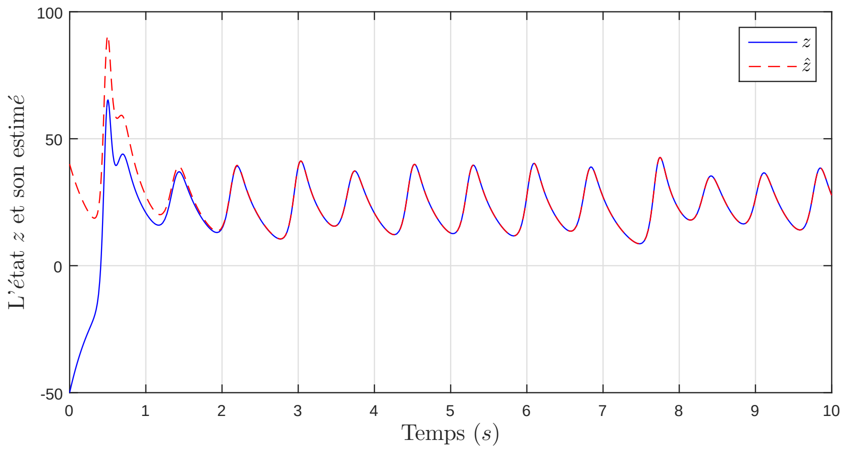


FIGURE 2.19: Synchronisation de l'état z du système de Lorenz avec son estimé $\hat{z}$.

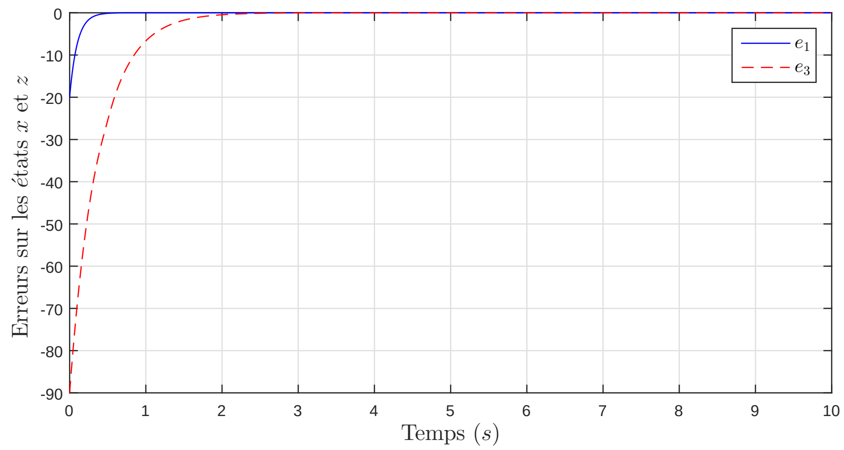


FIGURE 2.20: Erreurs sur les états x et z du système de Lorenz avec leurs estimés $\hat{x}$ et $\hat{z}$, respectivement.

2.5.2 Synchronisation généralisée

La synchronisation généralisée est une généralisation du concept de synchronisation identique. Cette méthode est utilisée dans le cas des systèmes complètement différents, où la sortie d'un système est la fonction de sortie de l'autre système [97,108]. Dans ce cas, les systèmes (2.25) et (2.26) se synchronisent au sens généralisé, s'il existe une transformation Φ tel que :

$$\lim_{t\to\infty} |x_s(t) - \Phi x_m(t)| = 0 \tag{2.33}$$

Il est à noter que la transformation Φ doit être inversible et indépendante des conditions initiales $x_m(0)$ et $x_s(0)$. La synchronisation complète est un cas particulier de la synchronisation généralisée, où la fonction Φ est égale à l'unité.

2.5.3 Synchronisation projective

Cette synchronisation est un cas particulier de la synchronisation généralisée, où la fonction Φ est une fonction linéaire simple $\Phi(x) = \pi x$ [109, 110]. Ce type de synchronisation est utilisé pour les systèmes *partiellement linéaires*, et permet de synchroniser, à un facteur près, les états qui ne peuvent être synchronisés. Ainsi, elle peut être représentée comme suit :

$$\lim_{t\to\infty} |\pi x_m(t) - x_s(t)| = 0 \tag{2.34}$$

2.5.4 Synchronisation retardée

La synchronisation retardée apparaît dans le cas des systèmes chaotiques non identiques faiblement couplés. En effet, il a été démontré qu'il existe un régime de synchronisation retardée [111], où l'état du système esclave converge vers l'état décalé dans le temps du système maître, c'est-à-dire :

$$\lim_{t\to\infty} |x_s(t) - x_m(t-\tau)| = 0 \tag{2.35}$$

où $x_m(t)$ est l'état du système maître (2.25), $x_s(t)$ est l'état du système esclave (2.26) et τ est un retard positif.

2.5.5 Synchronisation de phases

Dans le cas de systèmes périodiques de phases Φ_1 et Φ_2, la synchronisation est exprimée par la relation :

$$|a\ \Phi_1 - b\ \Phi_2| < \varepsilon \tag{2.36}$$

où a, b sont des entiers et ε est une constante positive. Cette notion classique de synchronisation a été récemment étendue au systèmes chaotiques. En effet, dans le cas des systèmes chaotiques non identiques faiblement couplés, la phase du système esclave converge vers celle du système maître mais leurs amplitudes peuvent ne pas être les mêmes. Pour étudier la synchronisation de phase de ces systèmes, il est important de déterminer l'amplitude $A(t)$ et la phase $\Phi(t)$ du signal chaotique. Quelques approches ont été proposées dans [113] afin de calculer ces grandeurs, telle que l'approche analytique. Un signal analytique $\phi(t)$ est une fonction complexe définie par :

$$\phi(t) = s(t) + j\tilde{s}(t) = A(t)e^{j\Phi(t)} \tag{2.37}$$

où $\tilde{s}(t)$ est la transformée de Hilbert de la série temporelle $s(t)$ (V.P. signifie la valeur principale de l'intégrale de Cauchy) :

$$\tilde{s}(t) = \frac{1}{\pi} V.P. \int_{-\infty}^{\infty} \frac{s(\tau)}{t-\tau} d\tau \tag{2.38}$$

Par analogie avec les systèmes périodiques, dans l'expression (2.37), $A(t)$ est l'amplitude du signal $\phi(t)$ et $\Phi(t)$ sa phase.

On dit alors qu'il se produit une synchronisation de phase entre deux systèmes chaotiques couplés si $|a\Phi_1 - b\Phi_2| < \varepsilon$.

2.5.6 Synchronisation par impulsions

On considère le système maître représenté par l'équation (2.25) et on définit une suite d'instants discrets $\{\tau_i, i = 1, 2, \ldots\}$. A chaque instant τ_i, le signal $y_m(t)$ est envoyé par le système maître au système esclave, dont les variables d'état subissent un saut [114]. Le système esclave est définit par le système différentiel impulsif suivant :

$$\begin{cases} \dot{x}_s(t) & = & f_s(x_s(t)), \quad t \neq \tau_i \\ \Delta x_s|_{t=\tau_i} & = & -P(x_m(\tau_i) - x_s(\tau_i)), \quad i = 1, 2, \ldots \end{cases} \tag{2.39}$$

où P est une matrice de gains de contrôle.

2.5.7 Synchronisation à base d'observateur

La synchronisation peut également être réalisée en employant un observateur au niveau du récepteur [22]. L'observateur est un système dynamique virtuel qui permet d'estimer les états d'un système lorsque ces états sont inconnus, c'est à dire inaccessible à la mesure pour des raisons technologiques ou économiques. La synthèse d'observateur des systèmes linéaires a fait l'objet de beaucoup de travaux. Deux principaux observateurs sont utilisés dans le contexte des systèmes linéaires : L'observateur de Kalman pour les systèmes variants dans le temps et l'observateur de Luenberger pour les systèmes linéaires invariants dans le temps. Initialement, Kalman-Bucy ont introduit ce qui est actuellement plus connu sous l'appellation de filtre de Kalman pour la reconstruction d'état d'un système stochastique également utilisé pour des systèmes déterministes [84]. Luenberger a proposé une nouvelle théorie de l'observation dite observateur de Luenberger. Son idée est d'ajouter au modèle (mis sous forme canonique) un terme de correction, entre la sortie et la sortie estimée [85].

Les approches de synthèse d'observateurs linéaires ont fortement inspiré les chercheurs pour généraliser les méthodes déjà développées au cas non linéaire. En effet, la structure de base des observateurs non linéaires proposés est celle de l'observateur de Luenberger. L'observateur le plus largement utilisé pour les systèmes non linéaires est le filtre de

Kalman étendu (EKF) [84]. Cette technique consiste à utiliser les équations du filtre de Kalman (standard) au système non linéaire, linéarisé en utilisant la formule de Taylor du premier ordre. Toutefois, la preuve de convergence de cet estimateur établie pour le cas linéaire ne peut être étendue de manière générale au cas des systèmes non linéaires. Il est à noter que depuis lors, plusieurs observateurs ont été proposés, comme : l'observateur à grand gain [86], l'observateur à mode glissant basé sur la théorie des systèmes à structure variable [18], l'observateur impulsif [115,116], l'observateur dead-beat pour les systèmes en temps discret [117,118] pour lequel on s'intéresse dans le présent travail, et bien d'autres.

La synthèse de l'observateur exploite les informations disponibles, à savoir le modèle dynamique du système étudié, ses entrées et ses sorties mesurées. Lorsqu'une partie (ou la totalité) des entrées n'est pas disponible, l'observateur est dit à entrées inconnues. Le problème à résoudre devient alors plus complexe, puisqu'il s'agit soit d'estimer l'état du système, malgré la présence d'entrées qui interviennent effectivement dans la dynamique du système mais que l'on ne peut pas inclure dans la dynamique de l'observateur, soit d'estimer l'état et les entrées inconnues simultanément. Tous ces observateurs dépendent de plusieurs conditions : la condition d'observabilité pour retrouver les états du système ; la condition de recouvrement de l'observabilité ("observability matching condition") pour retrouver les états du système et l'entrée inconnue (inversibilité à gauche du système). La figure 2.21 illustre ce principe de synchronisation.

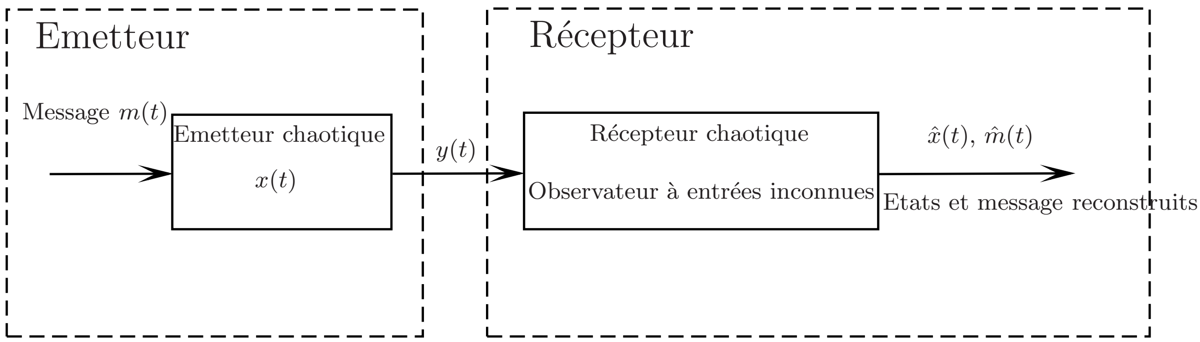


FIGURE 2.21: Principe de synchronisation à base d'observateurs.

Dans ce travail de thèse, notre objectif consiste à concevoir un système de transmission sécurisée basé sur la synchronisation en utilisant un observateur à entrée inconnue que nous développerons en chapitre 3.

2.6 Systèmes de communication basés sur la synchronisation des systèmes chaotiques

La synchronisation des systèmes chaotiques a ouvert la voie à de nombreuses applications parmi lesquelles la transmission sécurisée de données, objet de notre thèse.
Dans ce qui suit, on rappelle les techniques de communication traditionnelles à base du chaos, telles que le masquage chaotique, la modulation paramétrique, la commutation chaotique et le cryptage par injection.

2.6.1 Le masquage chaotique

Cette méthode est la première chronologiquement qui introduit la synchronisation du chaos [62,101,119,120]. Le schéma représentant cette méthode est donné par la figure 2.22. Dans ce schéma, l'émetteur est un système chaotique autonome dont le signal de sortie

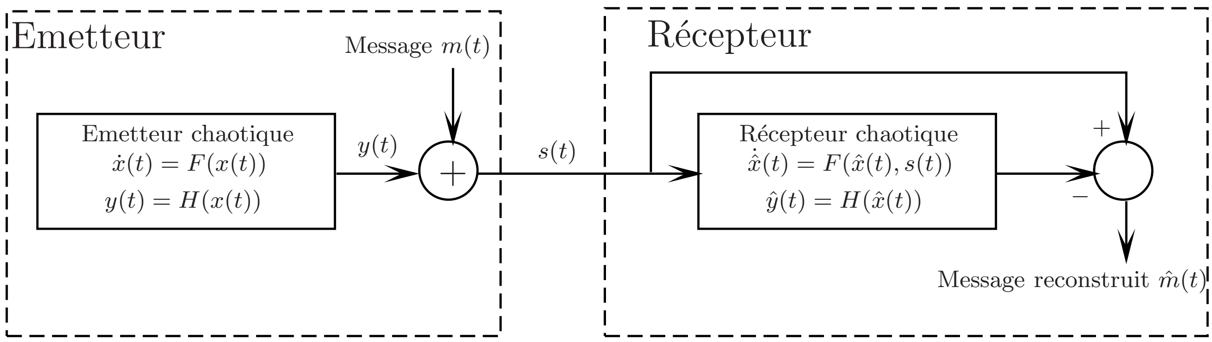


FIGURE 2.22: Schéma représentatif de la technique de masquage chaotique.

$y(t)$ est ajouté au signal du message $m(t)$. La somme des deux signaux est transmise au récepteur à travers le canal de transmission, qui est un canal public. Le récepteur est constitué d'un système chaotique identique à l'émetteur et d'un simple soustracteur. Ainsi, après la synchronisation des deux systèmes chaotiques (émetteur et récepteur), le message est extrait à l'aide d'une opération de soustraction. L'émetteur est donné par la représentation d'espace d'état donnée par :

$$\begin{cases} \dot{x}(t) &= F(x(t)) \\ y(t) &= H(x(t)) \end{cases} \tag{2.40}$$

Le signal de sortie $y(t)$ est une fonction de l'état de l'émetteur $x(t)$. Celui-ci est ajouté à $m(t)$ pour former le signal transmis $s(t)$ qui est donné par :

$$s(t) = y(t) + m(t) \tag{2.41}$$

La dynamique du récepteur, qui est commandée par $s(t)$, est donnée par la représentation d'état suivante :

$$\begin{cases} \dot{\hat{x}}(t) &= F(\hat{x}(t), s(t)) \\ \hat{y}(t) &= H(\hat{x}(t)) \end{cases} \tag{2.42}$$

Lorsque le récepteur se synchronise avec l'émetteur, alors :

$$\lim_{t\to\infty} |\hat{x}(t) - x(t)| = 0 \tag{2.43}$$

Maintenant, le message estimé $\hat{m}(t)$ peut être obtenu par une simple soustraction de la sortie estimée $\hat{y}(t)$ de $s(t)$:

$$\hat{m}(t) = s(t) - \hat{y}(t) \tag{2.44}$$

L'ajout de $m(t)$ à la sortie $y(t)$ de l'émetteur peut provoquer une dégradation de la qualité de la synchronisation au niveau du récepteur puisque le signal de commande n'est pas la sortie de l'émetteur, c'est $s(t)$. Par conséquent, l'amplitude de $m(t)$ doit être très petite par rapport au signal chaotique, sinon, la synchronisation peut ne pas être possible, de plus, le signal chaotique ne pourra plus masquer le spectre du message. Le masquage chaotique a l'avantage de la simplicité et peut être mis en oeuvre très facilement dans les circuits électroniques [101]. Cependant, la méthode de masquage s'est révélée peu sûre et diverses méthodes de cryptanalyse existent [121–125] qui permettent d'estimer la dynamique de l'émetteur et le décodage du signal de message.

2.6.2 La modulation paramétrique

Dans la technique de modulation chaotique, le signal de message est utilisé pour moduler (changer) un ou plusieurs paramètres du système chaotique de l'émetteur de sorte que ses trajectoires continuent de changer dans différents attracteurs chaotiques. Cette méthode est proposée et décrite dans [101, 126–129] et illustrée à la figure 2.23. L'idée est d'utiliser l'espace de bifurcation complexe du système chaotique de sorte que la modification du paramètre due à la modulation du signal de message ne soit pas connue des intrus même s'ils connaissent la structure du système chaotique. La sortie du système chaotique est le signal transmis. Au niveau du récepteur, une synchronisation chaotique

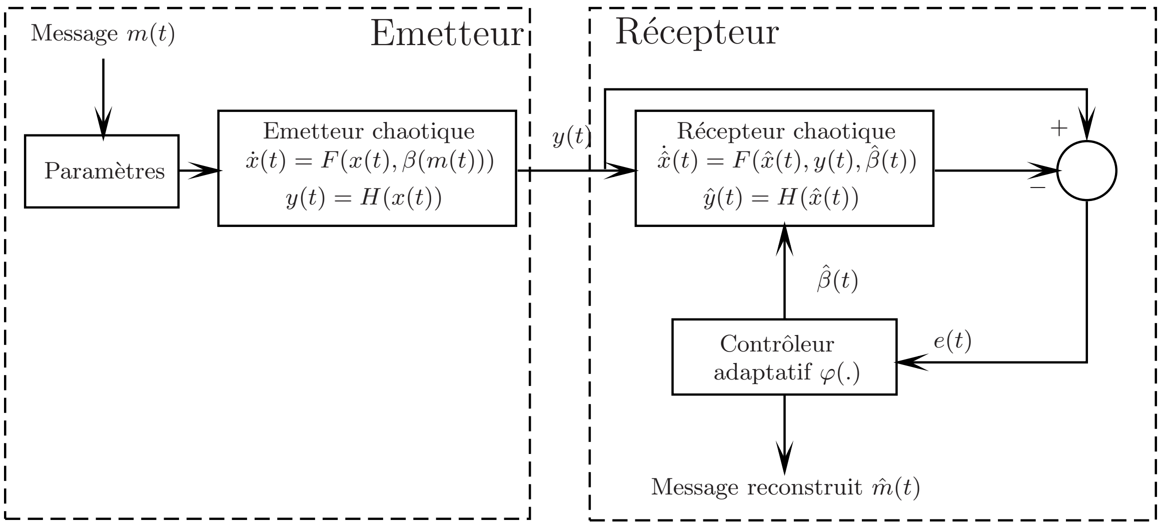


FIGURE 2.23: Schéma représentatif du principe de la modulation.

est effectuée avec un réglage adaptatif du paramètre de telle sorte que l'erreur de synchronisation approche de zéro, récupérant ainsi le signal de message. L'émetteur est donné par la représentation de l'espace d'état suivante :

$$\begin{cases} \dot{x}(t) & = & F(x(t), \beta(m(t))) \\ y(t) & = & H(x(t)) \end{cases} \tag{2.45}$$

Ici, le paramètre β du système est modifié avec $m(t)$, ce qui entraîne différents attracteurs chaotiques. Le signal de sortie $y(t)$ est la fonction de l'état de l'émetteur $x(t)$ et est le signal transmis. Lors de la réception de $y(t)$, la dynamique du récepteur est donnée par la représentation d'espace d'état suivante :

$$\begin{cases} \dot{\hat{x}}(t) & = & F(\hat{x}(t), \hat{\beta}(t)) \\ \hat{y}(t) & = & H(\hat{x}(t)) \\ e(t) & = & \hat{y}(t) - y(t) \\ \hat{\beta}(t) & = & \varphi(e(t)) \end{cases} \tag{2.46}$$

où $\varphi(.)$ est une fonction adaptative accordant le paramètre $\beta(t)$ de telle sorte que $e(t)$ se rapproche de zéro, réalisant ainsi une synchronisation et récupérant le signal de message $\hat{m}(t)$. Bien que la méthode de modulation offre une meilleure sécurité que la méthode de masquage, elle est encore peu sûre par diverses méthodes de cryptanalyse [123, 124, 130–132].

2.6.3 La commutation chaotique

La commutation chaotique est fondamentalement un cas particulier de la technique de modulation paramétrique conçu pour transmettre le message numérique en toute sécurité sur un canal de communication. Dans cette méthode, en fonction de 0 ou 1 à transmettre, les sorties de deux attracteurs chaotiques statistiquement similaires sont prises. Ces deux attracteurs sont générés par les deux systèmes chaotiques qui ont des paramètres légèrement différents mais ayant la même structure. Au niveau du récepteur, le système chaotique est réglé sur le paramètre correspondant à 0 ou 1 et ainsi la synchronisation sera réalisée si le bit correct est transmis sinon il n'y aura pas de synchronisation. Ainsi, en transmettant simplement le signal d'erreur à travers un filtre passe-bas, puis en étalonnant le signal d'erreur, les bits numériques pourraient être récupérés. Cette méthode a été proposée et expliquée dans [133, 134] et illustrée à la figure 2.24. En commutation chaotique, la commutation entre plusieurs attracteurs est également possible [135], transmettant ainsi un symbole dans une durée de T_s. Le nombre de bits N_b qui pourrait être transmis pendant T_s est donné par $N_b = \log_2 M$ où M est le nombre d'attracteurs de commutation. Par conséquent, si nous avons besoin de transmettre 0 ou 1 dans la durée du symbole pour le signal binaire, l'attracteur requis est 2 comme il a été expliqué précé-

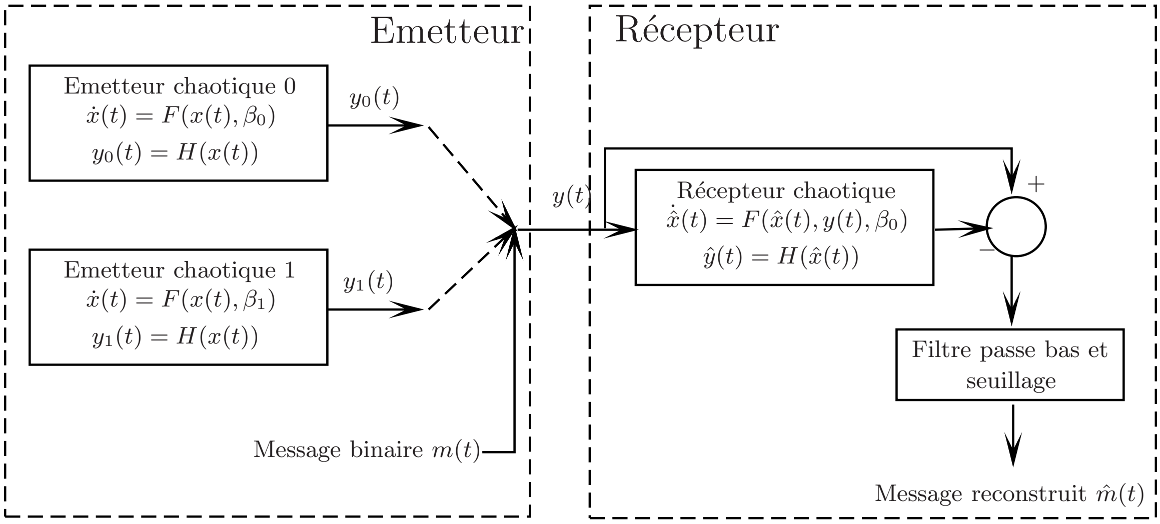


FIGURE 2.24: Schéma représentatif du principe de la commutation.

demment.

T_s doit être suffisamment longue pour garantir que la dynamique chaotique converge vers l'un des attracteurs accordés, sinon la synchronisation ne sera pas possible au niveau du récepteur pour récupérer le message. T_s dépend du plus grand exposant négatif de Lyapunov déterminant le taux de convergence vers l'attracteur. L'émetteur est donné comme :

$$\begin{cases} \dot{x}(t) &= F(x(t), \beta(m(t))) \\ y(t) &= H(x(t)) \end{cases} \tag{2.47}$$

Si le signal binaire $(0, 1)$ doit alors être transmis, nous avons $M = 2$, donc deux paramètres doivent être définis pour β, d'où :

$$\beta(m(t)) = \begin{cases} \beta_0 & \text{si} \quad m(t) = 0 \\ \beta_1 & \text{si} \quad m(t) = 1 \end{cases} \tag{2.48}$$

$y(t)$ est le signal transmis en sortie. Au niveau du récepteur, à la réception du signal, une synchronisation chaotique est effectuée. Le récepteur est donné par :

$$\begin{cases} \dot{\hat{x}}(t) &= F(\hat{x}(t), \beta_0) \\ \hat{y}(t) &= H(\hat{x}(t)) \end{cases} \tag{2.49}$$

Le signal d'erreur de synchronisation sera maintenant :

$$e(t) = \| \hat{y}(t) - y(t) \| \tag{2.50}$$

Ainsi, à partir du signal d'erreur, le message pourrait facilement être récupéré en raison de l'erreur de synchronisation qui existera en raison de la discordance paramétrique. Ce type de récupération de message est le type de détection cohérent. Le message pourrait également être récupéré via un schéma de détection non cohérent où la synchronisation n'est pas requise. L'extraction des bits est faite en regardant les attributs statistiques (tels que la distribution d'énergie du bit, la variance, la moyenne, etc.) du signal transmis auquel l'attracteur correspond [136]. Cependant, ces propriétés statistiques peuvent permettre aux intrus de décoder le message sans aucune connaissance de la dynamique de l'émetteur, le rendant ainsi moins sûr que son homologue, la détection cohérente. Bien que la méthode de commutation chaotique soit robuste vis à vis du bruit et des discordances paramétriques, elle s'est avérée non sûre [122–124, 130, 137, 138].

2.6.4 Méthode par inclusion

Cette technique consiste à injecter le message dans la dynamique de l'émetteur, sans toutefois réaliser une modulation paramétrique. Cette méthode est valable pour transmettre un message de nature binaire ou analogique, mais la puissance de ce dernier doit être suffisamment petite pour ne pas détériorer le comportement chaotique du système. La restauration de l'information se fait par une opération inverse une fois la synchronisation réalisée. Cette méthode est expliquée dans [18, 120, 139, 140] et représentée sur la Figure 2.25.

Dans ce cas, le message est introduit dans la dynamique de l'émetteur comme une entrée. Ainsi, la récupération du message devient un problème d'entrée inconnue dans le cas de la théorie du contrôle où les observateurs sont utilisés. Par conséquent, le système doit, en outre, satisfaire la condition d'observabilité [139, 141–143] ainsi qu'à la propriété d'inversion à gauche [144–146] afin de garantir la possibilité de récupérer tous les états et

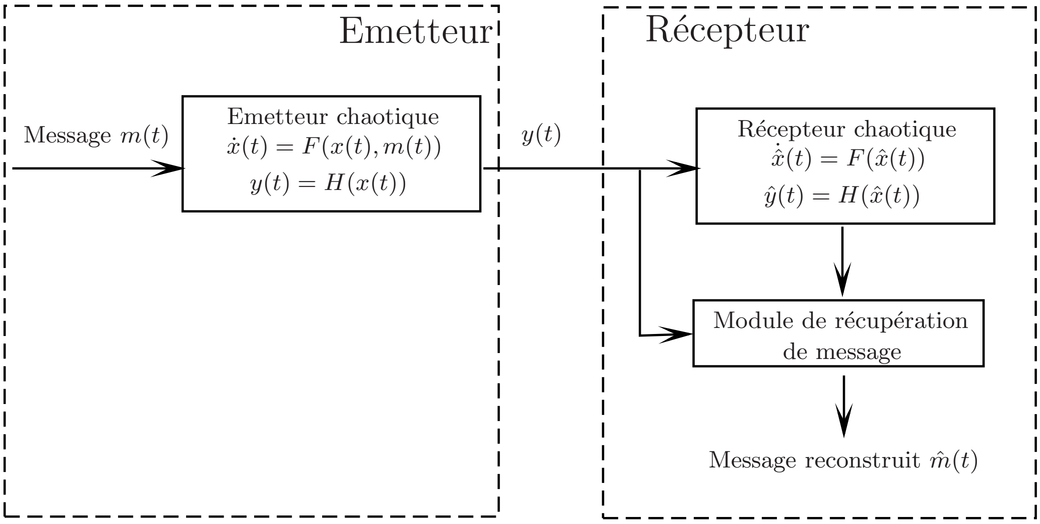


FIGURE 2.25: Schéma représentatif de la méthode par inclusion.

le message d'entrée inconnue au niveau du récepteur à partir de $y(t)$ [64]. L'émetteur est donné par :

$$\begin{cases} \dot{x}(t) &= F(x(t), m(t)) \\ y(t) &= H(x(t)) \end{cases} \tag{2.51}$$

Au récepteur, la dynamique du récepteur est :

$$\begin{cases} \dot{\hat{x}}(t) &= F(\hat{x}(t)) \\ \hat{y}(t) &= H(\hat{x}(t)) \end{cases} \tag{2.52}$$

Maintenant, en appliquant l'inversion comme indiquée dans [120, 139], le message est récupéré sous la condition d'inversion à gauche.

Cette technique par inclusion présente un niveau de sécurité nettement élevé par rapport aux techniques précédentes puisque le signal d'information est masqué dans la dynamique du système maître et que le signal chaotique disponible dans le canal ne porte pas l'information d'une manière directe comme dans le cas de la technique de masquage chaotique. Cependant, cette méthode est également vulnérable à certaines méthodes d'attaque [124] et donc insatisfaisante sans autres modifications.

2.7 Outils d'évaluation de la sécurité

La sécurité d'un schéma de chiffrement est validée par une étape essentielle, qui est la cryptanalyse [125, 132, 138]. Cette dernière, science opposée et complémentaire de la cryptographie, étudie les failles du chiffrement, et cherche à décrypter les messages chiffrés transitant par le canal, sans que les interlocuteurs ne s'en aperçoivent. Dans ce travail de thèse, nous traitons particulièrement la transmission d'images. Pour cette raison, nous donnons dans cette section les définitions des principales analyses connues, et les plus importantes, comme l'analyse des espaces clés, l'analyse statistique et l'analyse différentielle. Ces analyses sont utilisées dans le chapitre 5.

2.7.1 Hypothèse de Kerckhoffs

L'hypothèse fondamentale sous la quelle la cryptanalyse est effectuée est que l'adversaire connaît complètement l'algorithme de chiffrement, à l'exception de la clé secrète qui est inconnue. Dans ce cas, la sécurité du schéma de transmission sécurisée repose entièrement sur la clé secrète [147]. En effet, le but de l'adversaire est d'essayer de briser le message chiffré sans connaître la clé secrète, et cela avec plusieurs niveaux de difficultés en fonction des ressources disponibles :

- *Attaque à texte chiffré uniquement* l'adversaire tente de déduire la clé secrète ou le texte clair en observant seulement le texte chiffré.
- *Attaque à texte clair connu* l'adversaire connaît une séquence du texte clair et la séquence correspondante du texte chiffré.
- *Attaque à texte clair choisi* l'adversaire choisit une séquence du texte clair et analyse la séquence correspondante du texte chiffré.
- *Attaque à texte chiffré choisi* l'adversaire choisit une séquence du texte chiffré et connaît la séquence du texte clair correspondant.

Il existe un autre type d'attaque, appelée recherche de clé exhaustive, qui tente toutes les possibilités pour la clé dans l'espace de clés afin de décrypter complètement le message chiffré. Si l'espace clé d'un chiffrement est relativement petit, cette recherche exhaustive fonctionne facilement. Un bon schéma de transmission sécurisée doit avoir un espace de clés suffisamment important pour pouvoir résister à cette attaque, connue sous le nom de l'attaque par force brute.

2.7.2 Analyse de l'espace de clés

L'espace de clés d'un schéma de transmission sécurisée est le total des clés différentes qui peuvent être utilisées dans la procédure de chiffrement/déchiffrement. Un bon schéma de transmission sécurisée doit être sensible à la clé de chiffrement, et l'espace de clés doit être suffisamment grand pour que les attaques par force brute ne soient pas réalisables.

2.7.3 Analyse de la sensibilité de la clé

L'analyse de la sensibilité de la clé permet de révéler certaines informations concernant la clé secrète d'un schéma de transmission sécurisée. Dans ce type d'analyse, deux clés légèrement différentes sont utilisées pour chiffrer la même image ; par conséquent, les deux images cryptées doivent être complètement indépendantes l'une par rapport à l'autre (faible corrélation). De plus, l'image cryptée ne peut pas être décryptée correctement si la clé secrète est légèrement modifiée à la phase de décryptage. Pour confirmer cette sensibilité, le taux de changement du nombre de pixels $NPCR$ (Number of Pixels Change Rate *en anglais*) et la moyenne unifiée du changement d'intensité $UACI$ (Unified Averaged Changed Intensity *en anglais*) sont utilisés. Ces critères sont définis comme suit :

$$NPCR = \frac{\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} D(i,j)}{M \times N} \times 100 \tag{2.53}$$

$$UACI = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} \frac{C_1(i,j) - C_2(i,j)}{255} \times 100 \tag{2.54}$$

Où M et N représentent respectivement la largeur et la hauteur d'une image. $C_1(i,j)$ et $C_2(i,j)$ sont les valeurs des pixels à la position (i,j) des deux images cryptées dont les clés de chiffrement sont légèrement différentes. C_1 et C_2 sont parfois utilisées comme l'image originale et l'image cryptée. $D(i,j)$ est une matrice de la même taille que C_1 et C_2 tel que : $D(i,j) = 1$ si $C_1(i,j) \neq C_2(i;j)$ sinon $D(i,j) = 0$.

2.7.4 Analyse statistique

L'analyse statistique permet de déchiffrer plusieurs algorithmes de cryptage comme mentionné par Shannon. Cette section se consacre aux attaques dites statistiques qui exploitent plutôt une faiblesse de la partie confusion du chiffrement. Pour cela, nous allons décrire l'analyse des histogrammes ainsi que la corrélation de pixels adjacents.

Analyse des histogrammes

L'histogramme d'une image présente la distribution des intensités des ses pixels, c'est-à-dire le nombre de pixels pour chaque intensité lumineuse. Dans le cas de transmission d'images sécurisée, un crypto-système est considéré comme fort contre cette analyse, si l'histogramme de l'image chiffrée est uniformément réparti. Le test visuel est nécessaire, mais ce n'est pas suffisant. Pour assurer l'uniformité de l'image, le test χ^2 est appliqué (voir l'équation (2.55)) pour confirmer statistiquement l'uniformité de l'histogramme :

$$\chi^2 = \sum_{i=0}^{Q-1} \frac{(o_i - e_i)^2}{e_i} \tag{2.55}$$

Dans l'équation (2.55), Q est le nombre de niveaux, o_i est la fréquence d'occurrence observée de chaque niveau de couleur $(0 - 255)$ sur l'histogramme de l'image chiffrée, et e_i est la fréquence d'occurrence attendue de la répartition uniforme, donnée par $e_i = M \times N \times P/Q$, où M et N présentent la taille de l'image. Pour un bon schéma de transmission sécurisée, la valeur expérimentale du χ^2 doit être inférieure au χ^2 théorique, soit 293 pour $\alpha = 0.05$ (α présente le niveau de signification) et $Q = 256$ [148].

Analyse de corrélation

Les images numériques sont caractérisées par des pixels adjacents très redondants et fortement corrélés. Un schéma de transmission d'image sécurisé efficace doit pouvoir supprimer ce type de relation, c'est-à-dire, les pixels adjacents dans l'image chiffrée doivent avoir une redondance et une corrélation aussi faible que possible. Par conséquent, il convient de tester la corrélation entre les valeurs de deux pixels adjacents de nos images. Nous calculons donc le coefficient de corrélation dans chaque direction par l'équation suivante :

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{2.56}$$

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

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N} E(x_i - E(x))(y_i - E(y)) \tag{2.57}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{2.58}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \tag{2.59}$$

Avec N est le nombre de pixels utilisés.

2.7.5 Entropie d'information

L'entropie d'une information est une caractéristique importante de l'aléatoire. Les valeurs des pixels d'image varient de 0 à 255. Dans un algorithme de chiffrement robuste, la probabilité d'occurrence d'un pixel doit être la même (ou presque la même). Le comportement aléatoire de l'information cryptée peut être évaluée en utilisant l'entropie de l'information définies par :

$$H(C) = \sum_{i=0}^{n} p(c_i)\log_2\frac{1}{p(c_1)} \tag{2.60}$$

Où $H(C)$ est l'entropie de l'image chiffrée C et $p(c_i)$ présente la probabilité d'apparition de la valeur d'information x_i. Pour une véritable source aléatoire qui produit des symboles 2^L, l'entropie doit être L. Par exemple, pour des images à échelle de 256 gris dans les quelles les données de pixels ont 2^8 valeurs possibles, l'entropie d'une véritable image aléatoire doit être 8. Cependant, la valeur d'entropie de l'information pratique est inférieure à celle idéale.

2.7.6 Robustesse par rapport au bruit

Pendant le processus de transmission, l'image chiffrée peut être influencée par le bruit. Par conséquent, le schéma de transmission devrait être capable de résister aux attaques de bruit. Afin d'évaluer les performances d'un système de transmission vis à vis des attaques de bruit, le test de rapport signal sur bruit (PSNR) est effectué. La définition de PSNR est décrite comme suit,

$$PSNR = 10 \times \log_{10}(\frac{255^2}{MSE}) \tag{2.61}$$

où MSE est l'erreur quadratique moyenne entre l'image originale I et l'image déchiffrée I', qui est donnée par

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} [I(i,j) - I'(i,j)]^2 \tag{2.62}$$

2.8 Conclusion

Ce chapitre a été consacré à la description de la cryptographie et de la synchronisation, en s'intéressant plus précisément aux méthodes basées sur le chaos. Pour cela, dans la première partie, nous avons exposé les notions générales de la cryptographie, tout en citant quelques méthodes de chiffrement. En effet, nous avons, dans un premier temps, présenté les méthodes de cryptographie standard. Par la suite, nous avons parlé de la cryptographie chaotique. Dans cette partie, nous avons abordé la notion du chaos et avons donné quelques définitions des systèmes dynamiques et chaotiques, nous avons aussi exposé les caractéristiques du comportement chaotique. Ces caractéristiques, tels que la très grande sensibilité aux conditions initiales et l'aspect aléatoire ... etc., ont fait du chaos un phénomène très intéressant pour cacher les signaux d'informations afin de les transmettre d'une manière sécurisée.

Dans la seconde partie, la notion de synchronisation a été abordée. En effet, ce phénomène permet à deux systèmes chaotiques, ayant la même structure mais forcement des conditions initiales différentes, de reproduire le même signal chaotique. Ce qui rend possible, dans les schémas cryptographiques, la récupération de l'information chiffrée. Dans un premier lieu, nous avons cité quelques types de synchronisation. Ensuite, nous avons présenté différents systèmes de communication basés sur la synchronisation des systèmes chaotiques.

Dans la dernière partie, nous avons présenté quelques outils d'analyse de sécurité des crypto-systèmes chaotiques.

Le prochain chapitre sera consacré à l'étude des systèmes chaotiques d'ordre fractionnaire ainsi que leurs synchronisations.

Chapitre 3

Systèmes chaotiques d'ordre fractionnaire et synchronisation

3.1 Introduction

Le calcul fractionnaire est un sujet mathématique dont l'histoire remonte à plus de 300 ans. Pourtant, son application à l'ingénierie n'a été signalée que ces dernières années [23–25]. L'étude de nombreux systèmes présentant des phénomènes de relaxation, et de diffusion que l'on rencontre dans divers domaines tels que : thermique, mécanique, électrotechnique, chimie des polymères..., révèle, à travers l'établissement des solutions analytiques, un comportement relevant de la dérivation non entière. Celle-ci étant un outil approprié pour la description des propriétés héréditaires des phénomènes physiques. Ainsi, l'idée de l'application des systèmes fractionnaires dans la modélisation des procédés diffusifs apparait évidente [149–153]. En effet, ces systèmes physiques sont caractérisés par les propriétés de *mémoire longue* et *structure de dimension infinie*, ce qui est pris en compte lors de la modélisation, à savoir la représentation de l'espace d'état, de cette manière apparaît une nécessité d'interprétation des conditions initiales [154] et une nécessité de prendre en compte la mémoire du système à partir de l'instant initial. Dans ce cas, nous devons utiliser des variables d'état étendues, que nous appelons les *"pseudo variables d'état"*, au lieu des variables d'état classiques [26, 155].

Au cours des dernières années, la dérivée d'ordre fractionnaire a trouvé de nombreuses applications dans différents domaines. Aujourd'hui, elle est également utilisée dans les schémas de communication sécurisée basés sur la synchronisation des systèmes chaotiques fractionnaires [156, 157]. Il est à noter que les séquences générées à partir des systèmes chaotiques d'ordre fractionnaire sont très complexes. De plus, les ordres non entiers des systèmes chaotiques d'ordre fractionnaire sont très sensibles aux petites variations, ce qui leur permet d'être considérés comme des clés secrètes additionnelles. Ceci permet d'améliorer les performances et d'augmenter l'espace de clés des schémas de transmission sécurisée basés sur ces systèmes, et par conséquent de renforcer la robustesse de ces derniers face aux différentes attaques de cryptanalyse.
Dans ce chapitre, une introduction sur le calcul fractionnaire est présentée, une branche des mathématiques qui est, dans un certain sens, aussi ancienne que le calcul classique que nous connaissons aujourd'hui. Dans un premier temps, certains outils mathématiques importants dans la théorie des systèmes fractionnaires seront introduits. Quelques approches liées à la généralisation des notions de dérivation seront également considérées. Ensuite, la classe de systèmes chaotiques d'ordre fractionnaire sera présentée. Enfin, la synchronisation des systèmes chaotiques d'ordre fractionnaire sera abordée.

3.2 Outils mathématiques de base

Dans cette partie, nous allons présenter quelques notions qui sont très utilisées et qui permettent de fournir des solutions aux problèmes du calcul fractionnaire.

3.2.1 La fonction Gamma

L'une des fonctions de base utilisée dans le calcul fractionnaire est la fonction Gamma d'Euler [24]. Son interprétation est simplement la généralisation du factoriel n ($n!$), et elle permet à n de prendre des valeurs non entières. Cette fonction est définie par :

$$\Gamma(z) = \int_0^\infty t^{z-1} e^{-t} dt \tag{3.1}$$

avec $\Gamma(1) = 1$, $\Gamma(0^+) = +\infty$, $\Gamma(z)$ est une fonction monotone et strictement décroissante pour $0 < z \leq 1$. Une propriété importante de cette fonction est la relation de récurrence suivante :

$$\Gamma(z+1) = z\Gamma(z) \tag{3.2}$$

La fonction Gamma d'Euler généralise la factorielle car $\Gamma(n+1) = n!$, $\forall n \in N$.

3.2.2 La fonction Mittag-Leffler

La fonction de Mittag-Leffler, $E_\alpha(z)$, qui est une généralisation de la fonction exponentielle, est une fonction qui joue un rôle très important dans la théorie du calcul fractionnaire. La fonction de Mittag-Leffler à un seul paramètre a été introduite par G.M Mittag-Leffler [160]. Plus tard, la fonction de Mittag-Leffler généralisée à deux paramètres a été introduite [161, 162], cette dernière est définie par le développement en série suivant

$$E_{\alpha,\beta}(z) = \sum_{k=0}^{\infty} \frac{z^k}{\Gamma(\alpha k + \beta)}\ , \qquad (\alpha > 0, \beta > 0) \tag{3.3}$$

Lorsque $\beta = 1$, la fonction de Mittag-Leffler à un seul paramètre est obtenue, équation (3.4).

$$E_\alpha(z) = \sum_{k=0}^{\infty} \frac{z^k}{\Gamma(\alpha k + 1)}\ , \qquad (\alpha > 0) \tag{3.4}$$

A partir de l'équation (3.4), la fonction exponentielle e est déduite en posant $\alpha = 1$

$$E_1(z) = \sum_{k=0}^{\infty} \frac{z^k}{\Gamma(k+1)} = \sum_{k=0}^{\infty} \frac{z^k}{n!} = e^z \tag{3.5}$$

3.3 Définitions sur l'intégrale et la dérivée d'ordre fractionnaire

Le calcul fractionnaire peut être considéré comme une généralisation du calcul conventionnel [23]. C'est-à-dire que l'opération de dérivation ou d'intégration d'ordre non entier est une généralisation de la dérivation ou intégration classique à des ordres quelconques non entiers, qui peuvent être exprimés au moyen de l'opérateur fondamental ${}_aD_t^\alpha$, dénommé par certains auteurs l'opérateur *differintégration* d'ordre α, où a et t sont les limites de l'opération et $\alpha \in R$. Il est important de mentionner que la signification de l'opérateur dépend du signe de α (positif ou négatif), ce qui correspond respectivement aux opérations de dérivation et d'intégration :

$$
{}_aD_t^\alpha = \begin{cases} \frac{d^\alpha}{dt^\alpha} & \alpha > 0 \\ 1 & \alpha = 0 \\ \int_a^t (d\tau)^{-\alpha} & \alpha < 0 \end{cases} \tag{3.6}
$$

Les notations ${}_{t_0}D^\alpha f(t)$ et $I^\alpha f(t)$ représenteront respectivement l'opérateur de dérivation et d'intégration. Plusieurs définitions de généralisation de la dérivation entière à des ordres réels peuvent être trouvées dans la littérature telles que : les définitions de Riemann-Liouville, Grünwald-Letnikov, Caputo, Weyl ...etc. Dans notre travail, nous nous limiterons aux trois définitions les plus fréquemment utilisées, qui sont : Riemann-Liouville, Caputo et Grünwald-Letnikov. En effet, ces trois définitions ont la même essence et le transfert de l'une à l'autre est possible sous certaines conditions [158].

3.3.1 Intégration d'ordre fractionnaire

C'est la formule qui réduit le calcul de l'intégrale répétée k fois, où k est un nombre entier positif, de la fonction $f(t)$ à une intégrale de convolution due à Cauchy qui forme le point de départ de l'intégrale d'ordre non entier. Cette formule, appelée la formule de Cauchy, est présentée comme suit :

$$
\underbrace{\int_{t_0}^{t} \dots \int_{t_0}^{t}}_{k \text{ fois}} f(t) = I^k f(t) = \frac{1}{(k-1)!} \int_{t_0}^{t} (t-\tau)^{k-1} f(\tau) d\tau \tag{3.7}
$$

Pour généraliser cette formule à un nombre réel $\alpha \in R_+^*$, Riemann a proposé de remplacer la fonction factorielle par la fonction Gamma, qui en est la généralisation aux nombres réels. Ainsi, il a défini l'intégration non entière comme suit :

$$I^{\alpha} f(t) = \frac{1}{\Gamma(\alpha)} \int_{t_0}^{t} (t-\tau)^{\alpha-1} f(\tau) d\tau \tag{3.8}$$

Γ étant la fonction d'Euler définie par l'équation (3.1).

L'intégrale de Riemann-Liouville peut être écrite sous la forme :

$$I^{\alpha} f(t) = \mathcal{P}_a(t) \otimes f(t) \tag{3.9}$$

avec $\mathcal{P}_a(t) = \frac{1}{\Gamma(\alpha)} t^{\alpha-1}$ et $\otimes$ le produit de convolution. Le facteur $\mathcal{P}_a(t)$, appelé dans la littérature *facteur d'oubli*, est égal à 1 lorsque l'ordre $\alpha = 1$ (cas entier) ; en revanche pour α non entier, $\mathcal{P}_a(t)$ permet de moduler la pondération de la fonction $f(t)$ différemment : les valeurs les plus récentes ayant plus de poids que les plus anciennes, et de cette façon prend en compte la mémoire du système.

3.3.2 Dérivation d'ordre fractionnaire des systèmes à temps continu

La dérivation d'ordre non entier est la généralisation de la fonction de dérivation entière à des ordres non entiers quelconques. Différentes définitions de la dérivation d'ordre fractionnaire sont apparues lors du développement de la théorie des calculs d'ordre fractionnaire. Les définitions de Riemann-Liouville [163] et de Caputo [164] sont obtenues à partir de l'intégration non entière de Riemann-Liouville. Une troisième définition de la dérivée non entière d'une fonction, proposée par Grünwald-Letnikov [165], peut être obtenue de façon plus intuitive à partir de la généralisation de la définition de la dérivée entière usuelle.

3.3.2.1 Dérivées de Riemann-Liouville et Caputo

Les définitions de Riemann-Liouville et de Caputo sont obtenues à partir de l'intégration non entière de Riemann-Liouville, donnée par l'équation (3.8), ceci en procédant de deux manières différentes.

Introduisons le nombre entier positif r tel que $r - 1 < \alpha < r$, la définition de Riemann-

Liouville de l'opérateur de dérivation consiste à dériver r fois $I^{r-\alpha}f(t)$. Cela suppose $f(t)$ causale et ses dérivées existent jusqu'à l'ordre r [163]. Cette définition est donnée par :

$$_{t_0}D^{\alpha}f(t) = D^r I^{r-\alpha} f(t) = \frac{d^r}{dt^r}\left[\frac{1}{\Gamma(r-\alpha)}\int_{t_0}^{t}\frac{f(\tau)}{(t-\tau)^{\alpha-r+1}}d\tau\right] \tag{3.10}$$

alors que la définition de Caputo [164] consiste, en premier lieu, à dériver la fonction $f(t)$ à l'ordre entier r, par la suite, intégrer le résultat obtenu à l'ordre non entier $\alpha - r + 1$. La dérivation d'ordre fractionnaire de Caputo est donnée comme suit :

$$_{0}D^{\alpha}f(t) = I^{r-\alpha}D^r f(t) = \frac{1}{\Gamma(r-\alpha)}\int_{0}^{t}\frac{f^{(r)}(\tau)}{(t-\tau)^{(\alpha-r+1)}}d\tau \tag{3.11}$$

avec $f^{(r)}(\tau)$ la dérivée $r^{ème}$ de $f(\tau)$. Cette définition nécessite que la fonction $f(t)$ et ses r dérivées successives soient nulles pour $t \leq 0$, ce qui la rend plus restrictive que la définition de Riemann-Liouville.

La Transformée de Laplace de la fonction causale $f(t)$ pour les deux définitions s'en déduit : pour la définition de Riemann-Liouville :

$$\mathcal{L}[_{0}D^{\alpha}f(t)] = s^{\alpha}\mathcal{L}[f(t)] - \sum_{i=0}^{r-1} s^i D^{\alpha-i-1}f(t)\Big|_{t=0} \tag{3.12}$$

ainsi les conditions initiales, dans le cas de Riemann-Liouville, s'expriment en fonction des valeurs à l'origine des dérivées non entières $D^{\alpha-i-1}f(t)$ de $f(t)$ $(i = 0, 1, \ldots, r-1)$.

Pour la définition de Caputo :

$$\mathcal{L}[_{0}D^{\alpha}f(t)] = s^{\alpha}\mathcal{L}[f(t)] - \sum_{i=0}^{r-1} s^{\alpha-i-1}D^i f(0) \tag{3.13}$$

Dans ce cas, les conditions initiales s'expriment en fonction des valeurs à l'origine des dérivées entières $D^i f(t)$ de $f(t)$ $(i = 0, 1, \ldots, r-1)$. Ces dernières ayant une interprétation physique, s'avère plus appropriée dans le domaine des sciences de l'ingénieur ; en revanche, la définition de Riemann-Liouville qui rencontre la difficulté de lui attribuer un sens géométrique ou physique est utilisée en mathématiques pures.

3.3.2.2 Dérivée de Grünwald-Letnikov

Cette définition se base sur l'obtention de dérivées par différences finies fractionnaires [165, 166] où toute la différence par rapport au cas entier se situe dans l'extension de la factorielle à travers la fonction Gamma. Considérons la fonction en temps continu $f(t)$, sa dérivée d'ordre 1 s'écrit :

$$D^1 f(t) = \lim_{h \to 0} \frac{f(t) - f(t-h)}{h} \tag{3.14}$$

h étant le pas d'échantillonnage.

En dérivant l'équation (3.14) pour une deuxième fois, nous obtiendrons la dérivée d'ordre 2 de la fonction $f(t)$ sous la forme suivante :

$$\begin{aligned} D^2 f(t) &= \lim_{h \to 0} \tfrac{f'(t) - f'(t-h)}{h} \\ &= \lim_{h \to 0} \tfrac{f(t) - 2f(t-h) + f(t-2h)}{h^2} \end{aligned} \tag{3.15}$$

A partir des équations (3.14) et (3.15), la dérivée d'ordre 3 de la fonction $f(t)$ peut être obtenue comme suit :

$$D^3 f(t) = \lim_{h \to 0} \frac{f(t) - 3f(t-h) + 3f(t-2h) - f(t-3h)}{h^3} \tag{3.16}$$

La généralisation à un ordre de dérivation quelconque (entier, réel ou complexe) conduit à la définition proposée par Grünwald en 1867, soit :

$$D^\alpha f(t) = \lim_{h \to 0} \left(\frac{1}{h^\alpha} \sum_{k=0}^{\infty} (-1)^k \binom{\alpha}{k} f(t - kh) \right) \tag{3.17}$$

où la notation $\binom{\alpha}{k}$ désigne le binôme de Newton généralisé à des nombres réels.

$$\binom{\alpha}{k} = \frac{\alpha!}{j!(\alpha - j)!} = \frac{\Gamma(\alpha + 1)}{\Gamma(k+1)\Gamma(\alpha - k + 1)} \tag{3.18}$$

avec $\binom{\alpha}{0} = 1$.

Pour des ordres de dérivations entiers, la formule (3.17) se limite à une combinaison linéaire des $(n+1)$ valeurs de la fonction $f(t-kh)$, $k=0,\dots,n$ donnant ainsi une caractérisation locale. En revanche, dans le cas des ordres non entiers, elle montre que $D^{\alpha}f(t)$ à un instant t donné prend en compte toutes les valeurs de cette fonction à tous les instants du passé $f(t-kh)$, $k=0,\dots,\infty$, de cette fonction, donc revêt un caractère global contrairement à la dérivation entière. Dans le cas où la fonction $f(t)$ est causal, en posant $t=Kh$, cette condition se traduit par $f((K-k)h)=0$ pour $K-k<0$. Ainsi dans l'équation (3.17), la somme étendue de $k=0$ à $k=\infty$ se réduit à la somme étendue de $k=0$ à $k=K$. L'équation (3.17) s'écrit alors sous la forme suivante :

$$D^{\alpha}f(Kh)=\frac{1}{h^{\alpha}}\sum_{k=0}^{K}(-1)^{k}\binom{\alpha}{k}f((K-k)h) \tag{3.19}$$

$D^{\alpha}f(Kh)$ représente la valeur de la dérivée $\alpha^{ème}$ de $f(t)$ à l'instant Kh.
Cette propriété permet d'interpréter les systèmes non entiers comme des systèmes à mémoire longue alors que les systèmes entiers sont considérés comme des systèmes à mémoire courte (nécessite quelques échantillons précédents) [23]. Pour des raisons pratiques, le principe de *"mémoire courte"*, [184], est utilisé afin de surmonter la difficulté de l'évaluation dans un large intervalle de variation de la variable t. Ce principe est énoncé comme suit :

$$D^{\alpha}f(t)\approx\lim_{h\to 0}\left(\frac{1}{h^{\alpha}}\sum_{k=0}^{L}(-1)^{k}\binom{\alpha}{k}f(t-kh)\right) \tag{3.20}$$

La taille de la mémoire L est choisie de sorte qu'elle satisfasse la précision requise de calcul.

3.3.3 Différentiation d'ordre fractionnaire des systèmes à temps discret

Il est bien connu qu'il existe une similarité entre les propriétés du calcul différentiel impliquant l'opérateur $D=\frac{d}{dx}$ et les propriétés du calcul discret impliquant l'opérateur $\Delta f(x)=f(x+1)-f(x)$ qui est connu comme l'opérateur de différence. D'une manière analogue aux dérivées fractionnaires, des définitions de la dérivée fractionnaire discrète ont été données de différentes manières. La différence d'ordre fractionnaire a été mentionnée pour la première fois par Kuttner en 1956 [185].

Pour une séquence de nombres complexes a_n et une constante réelle s, Kuttner a défini la différence d'ordre s comme suit

$$\Delta^s a_n = \sum_{m=0}^{\infty} \binom{-s-1+m}{m} a_{n+m} \tag{3.21}$$

où

$$\binom{t}{m} = \frac{t(t-1)\dots(t-m+1)}{m!}$$

En 1974, Diaz et Osler [186] ont défini la différence fractionnaire comme suit

$$\Delta^\alpha f(x) = \sum_{k=0}^{\infty} (-1)^k \binom{\alpha}{k} f(x+\alpha-k) \tag{3.22}$$

$$\binom{\alpha}{k} = \frac{\Gamma(\alpha+1)}{\Gamma(\alpha-k+1)k!} \tag{3.23}$$

où α est un nombre réel ou complexe.

En 1989, Miller et Ross [25] ont défini les opérateurs de sommation et de différence d'ordre fractionnaire comme présentés ci-dessous respectivement,

$$\Delta^{-\alpha} f(t) = \frac{1}{\Gamma(\alpha)} \sum_{k=a}^{t-\alpha} (t-k-1)^{(\alpha-1)} f(k) \tag{3.24}$$

$$\Delta^\alpha f(t) = \Delta\Delta^{-(1-\alpha)} f(t) = \Delta \frac{1}{\Gamma(1-\alpha)} \sum_{k=a}^{t-1+\alpha} (t-k-1)^{(-\alpha)} f(k) \tag{3.25}$$

où $\alpha > 0$, $a \in R$, $t \in N_{a+\alpha}$ et $t^{(\alpha)} := \frac{\Gamma(t+1)}{\Gamma(t-\alpha+1)}$.

L'équation (3.25) représente la différence d'ordre fractionnaire au sens de Riemann-Liouville. Elle a été introduite, en 2007, par Atici et Eloe [174] en utilisant la définition de sommation d'ordre fractionnaire de Miller et Ross. En 2009, Anastassiou [187] a défini l'opérateur de différence d'ordre fractionnaire selon Caputo comme suit

$$\Delta^{\alpha} f(t) = \Delta^{-(m-\alpha)}\Delta^{m} f(t) = \frac{1}{\Gamma(m-\alpha)} \sum_{k=a}^{t-m+\alpha} (t-\sigma(k))^{(m-\alpha-1)}\Delta^{m} f(k) \tag{3.26}$$

où m est un entier positif tel que $m-1 < \alpha < m$, $\alpha > 0$ et $\sigma(k) = k+1$. L'opérateur de différence d'ordre fractionnaire selon la définition de Grünwald-Letnikov a été défini, en généralisant la différence d'ordre entier à la différence d'ordre fractionnaire [155, 175]. En outre, ce sujet est devenu plus attirant et des discussions approfondies ont été proposées, telles que la série de Taylor [176], les définitions des différences fractionnaires et leurs propriétés [177], la transformée de Laplace [178], les problèmes de valeur initiale [179], le calcul discret des variations [38, 180], le traitement du signal basé sur les dérivées discrètes [181, 182].

Dans ce qui suit, nous présentons deux classes de systèmes d'ordre fractionnaire, linéaire et non linéaire, en utilisant l'opérateur de différence d'ordre fractionnaire au sens de Grünwald-Letnikov. Ainsi, nous allons définir l'opérateur de différence d'ordre fractionnaire, au sens de Grünwald-Letnikov, pour les systèmes à temps discret. Pour cela, nous allons en premier lieu considérer un modèle d'état d'un système linéaire d'ordre entier à temps continu, présenté comme suit :

$$D^{1}x(t) = Ax(t) + Bu(t) \tag{3.27}$$

où $x(t) \in R^{n}$ est le vecteur d'état. Ce modèle peut être représenté en temps discret en utilisant la différence du premier ordre de $x(t)$ [155]. Pour cela, on considère h la période d'échantillonnage. Ainsi, pour $kh \leq t < (k+1)h$, la première dérivée d'ordre entier $D^{1}x(t)$ peut être approximée par la méthode d'Euler explicite comme suit :

$$D^{1}x(t) \approx \Delta^{1}x((k+1)h) = \frac{x((k+1)h) - x(kh)}{h} \tag{3.28}$$

Ainsi, nous pouvons écrire :

$$\begin{aligned} \Delta^1 x((k+1)h) &= \tfrac{Ax(kh)+Bu(kh)-x(hk)}{h} \\ &= A_d x(kh) + Bu(kh) \end{aligned} \tag{3.29}$$

De la même manière, cette discrétisation peut être appliquée à un modèle d'état d'ordre fractionnaire, donné comme suit :

$$\Delta^{[\alpha]} x((k+1)h) = \frac{A_d x(kh) + Bu(kh)}{h} \tag{3.30}$$

où l'ordre fractionnaire α peut être commensurable ou non commensurable. Ainsi, la dérivée d'ordre fractionnaire $D^{[\alpha]}x(t)$ peut être approximée en utilisant la définition de Grünwald-Letnikov.

$$D^{[\alpha]}x(t) \approx \Delta_h^{[\alpha]} x((k+1)h) = \frac{1}{h^\alpha} \sum_{j=0}^{k+1} (-1)^j \binom{\alpha}{j} x((k+1-j)h) \tag{3.31}$$

où $k \in N$ représente le temps discret et $\Delta^\alpha x(k)$ désigne la différence de Grünwald-Letnikov, et le terme $\binom{\alpha}{j}$ est calculé par la relation suivante :

$$\binom{\alpha}{j} = \begin{cases} 1 & pour j = 0 \\ \frac{\alpha(\alpha-1)\cdots(\alpha-j+1)}{j!} & pour j > 0 \end{cases} \tag{3.32}$$

Si on omet h (i.e., on met h=1), nous allons obtenir l'opérateur de différence discret d'ordre fractionnaire comme il est défini dans [155, 183]. En effet, le choix de la période d'échantillonnage h est très important lors de l'élaboration du modèle discrétisé d'un processus donné. h ne doit pas être nécessairement petit, il correspond à un taux d'échantillonnage approprié, déduit de la dynamique du processus, en utilisant des règles et des critères, comme il est exposé par exemple dans [194].

Ainsi, l'opérateur de différence discret d'ordre fractionnaire lorsque $h = 1$ est présenté comme suit :

$$\Delta^{[\alpha]} x(k+1) = \sum_{j=0}^{k+1} (-1)^j \binom{\alpha}{j} x(k+1-j) \tag{3.33}$$

Maintenant, considérons le système non linéaire discret d'ordre entier décrit par la forme suivante :

$$x(k+1) = f(x(k)) + g(x(k))u(k) \tag{3.34}$$

où $x(k) \in R^n$ est le vecteur d'état de dimension n et $u(k) \in R$ l'entrée de commande. $f(x)$ et $g(x)$ sont des champs vectoriels pour $x \in R^n$. Le vecteur d'état est écrit comme

$$x(k) = [x_1(k)\, x_2(k)\ \ldots\ x_n(k)]^T$$

La différence du premier ordre de $x(k+1)$ est définie par :

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

Ainsi, en utilisant l'équation (3.34), nous déduisons

$$\Delta^1 x(k+1) = f(x(k)) + g(x(k))u(k) - x(k) \tag{3.35}$$

La différence d'ordre α de $x(k+1)$ est obtenue de même façon que pour la différence du premier ordre, elle est présentée comme suit :

$$\Delta^{[\alpha]} x(k+1) = f(x(k)) + g(x(k))u(k) - x(k) \tag{3.36}$$

En utilisant la différence d'ordre α donnée par l'équation (3.33), nous obtenons :

$$\Delta^{[\alpha]} x(k+1) = x(k+1) + \sum_{j=1}^{k+1} (-1)^j \binom{\alpha}{j} x(k+1-j) \tag{3.37}$$

Cette équation peut être réécrite sous cette forme :

$$\Delta^{[\alpha]} x(k+1) = x(k+1) - \alpha x(k) + \sum_{j=2}^{k+1} (-1)^j \binom{\alpha}{j} x(k+1-j) \tag{3.38}$$

En substituant l'équation (3.38) dans l'équation (3.36), nous obtenons :

$$x(k+1) = f(x(k)) + g(x(k))u(k) + (\alpha - 1)x(k) - \sum_{j=2}^{k+1}(-1)^j \binom{\alpha}{j} x(k+1-j) \tag{3.39}$$

Introduisons les nouvelles variables $C_p = (-1)^{p+1}\binom{\alpha}{p+1}$ et $p = j-1$. Ainsi, l'équation (3.39) est équivalente à

$$x(k+1) = f(x(k)) + g(x(k))u(k) + (\alpha - 1)x(k) - \sum_{p=1}^{k} C_p x(k-p) \tag{3.40}$$

Remarque 1 *Nous pouvons affirmer que le système (3.40) présente une propriété de mémoire longue et infinie, et nous pouvons facilement vérifier que le coefficient C_p diminue lorsque l'itération p augmente. Alors, il est raisonnable de tronquer la mémoire pour une utilisation pratique facile et pour optimiser le processus de calcul. Par conséquent, le principe de mémoire courte peut être utilisé pour spécifier un système d'ordre fractionnaire plus exploitable. La longueur limitée de la mémoire est indiquée par L.*

Ainsi, le système (3.40) peut être réécrit comme suit :

$$x(k+1) = f(x(k)) + g(x(k))u(k) + (\alpha - 1)x(k) - \sum_{p=1}^{L} C_p x(k-p) \tag{3.41}$$

Remarque 2 *Le modèle défini par (3.40) peut être considéré comme un modèle à temps discret avec des retards dans les états. En effet, le système contient un nombre d'états retardés égal à k.*

3.4 Systèmes d'ordre fractionnaire

Les systèmes d'ordre fractionnaire sont souvent décrits par des équations différentielles d'ordre fractionnaire, mais d'autres concepts peuvent être utilisés, telle que la représen-

tation diffusive introduite par Montseny [152], dans le but de transformer certains opérateurs causaux non standards, tels les intégrations ou dérivations d'ordre fractionnaire, en systèmes dynamiques linéaires entrée-sortie, dans un espace d'état fonctionnel. Cette dernière description présente la propriété de *mémoire longue temporelle* qui se traduit par un effet de mémoire spatiale, c'est à dire : le comportement d'un système fractionnaire résulte d'une infinité de systèmes spatialement distribués. En conséquence, se pose le problème de l'initialisation correcte d'un système fractionnaire qui nécessite une infinité de conditions initiales [154, 188–192]. Celle ci peut être déduite de la représentation diffusive en compatibilité avec la physique du système, ce qui n'est pas le cas si nous considérons la définition de Riemann-Liouville ou celle de Caputo [193].
Dans ce qui suit, nous présentons les systèmes d'ordre fractionnaire à temps continu et à temps discret.

3.4.1 Systèmes d'ordre fractionnaire à temps continu

Tout au début, la plupart des travaux consacrés à l'étude des systèmes d'ordre fractionnaire se sont concentrés sur des représentations en temps continu. La représentation d'état des systèmes continus d'ordre fractionnaire a été introduite dans [167–170]. Cette représentation a été utilisée dans l'analyse des performances du système. La solution des équations du modèle d'état a été obtenue en utilisant la fonction de Mittag-Lefller. Par la suite, la stabilité des ces systèmes a été étudiée [195, 197] et une condition basée sur le principe de l'argument a été établie pour garantir la stabilité asymptotique du système d'ordre fractionnaire. De plus, les propriétés de commandabilité et d'observabilité ont été définies et certains critères algébriques de ces deux propriétés ont été tirés dans [196]. Une autre contribution sur l'analyse de la commandabilité et de l'observabilité d'un système d'ordre fractionnaire commensurable modélisé par des équations d'états fractionnaires est apportée dans [198].
Considérons un système d'ordre non entier, linéaire à temps continu causal et invariant dans le temps décrit par l'approche classique, et défini comme dans le cas entier par trois modèles :

- Équation différentielle généralisée
- Fonction de transfert fractionnaire
- Représentation d'état fractionnaire.

3.4.1.1 Équation différentielle généralisée

Les systèmes linéaires mono-variables à temps invariant d'ordre fractionnaire peuvent en général être décrit par une équation différentielle fractionnaire de la forme [158] :

$$y(t) + \sum_{i=1}^{n} a_i D^{\alpha_i} y(t) = \sum_{j=1}^{m} b_j D^{\beta_j} u(t) + b_0 u(t) \tag{3.42}$$

où D^α désigne l'opérateur de dérivation d'ordre α de Caputo. $u(t) \in R$ et $y(t) \in R$ désignent respectivement l'entrée et la sortie du système, $a_i, b_j \in R, \alpha_i, \beta_j \in R^+$. n et m sont les nombres des termes de chaque partie de l'équation différentielle.
Lorsque les ordres de dérivation de l'équation différentielle fractionnaire α_i, β_j sont tous des multiples entiers d'ordre de base α, le système fractionnaire est dit d'ordre commensurable, sinon, le système est dit d'ordre non commensurable.

Remarque 3 *Le cas des systèmes commensurables est très intéressant en pratique. Il permet d'obtenir une représentation des pseudo-états analogue à celle des systèmes d'ordre entier.*

3.4.1.2 Fonction de transfert non entière

L'application de la transformée de Laplace à l'équation (3.42), avec des conditions initiales nulles, permet de déduire la fonction de transfert [158] :

$$G(s) = \frac{Y(s)}{U(s)} = \frac{b_0 + \sum\limits_{j=1}^{m} b_j s^{\beta_j}}{1 + \sum\limits_{i=1}^{n} a_i s^{\alpha_i}} \tag{3.43}$$

Dans le cas des systèmes d'ordres commensurables, la fonction de transfert est donnée sous la forme suivante :

$$G(s) = \frac{b_0 + \sum_{j=1}^{m} b_j s^{j\alpha}}{1 + \sum_{i=1}^{n} a_i s^{i\alpha}} \tag{3.44}$$

Pour le cas multi-variable, le système d'ordre non entier peut être décrit par une matrice de fonctions de transfert non entières, ou un système d'équations différentielles fractionnaires. Dans le cas de système d'ordre non entier, le terme *ordre d'un système* est remplacé par le terme *dimension d'un système*. En effet, le terme *ordre* utilisé pour désigner l'ordre de dérivation non entier est différent du terme *dimension* que nous utilisons pour la dimension du système ou du modèle d'état.

3.4.1.3 Représentation dans l'espace des pseudo états

Le système d'ordre fractionnaire commensurable peut également être représenté dans l'espace des pseudo états, [155, 167–169], défini comme dans le cas entier par deux équations :

- Une équation d'état où chaque variable d'état $x_i(t)$ est dérivée à l'ordre non entier α.
- Une équation de sortie analogue au cas entier.

Le modèle d'état du système d'ordre non entier s'écrit sous la forme :

$$\begin{cases} D^{\alpha}x(t) &= Ax(t) + Bu(t) \\ y(t) &= Cx(t) + Du(t) \end{cases} \tag{3.45}$$

où $x \in R^n$ désigne le vecteur pseudo-état, $u \in R$ est le vecteur d'entrée présentant la commande, $y \in R$ est la sortie du système et α est l'ordre de dérivation fractionnaire.
La représentation des pseudo états (3.45) n'est pas unique. Des formes similaires aux formes canoniques observables ou commandables d'un modèle entier peuvent être obtenues. Comme les concepts fondamentaux des systèmes d'ordre entier (Commandabilité, Observabilité, Stabilité,...) qui reposent sur la notion d'état et d'état initial. De nom-

breux travaux ont été réalisés afin de résoudre le problème de l'initialisation d'un système d'ordre non entier [154, 189–192]. Dans les travaux de [154, 189, 190], les auteurs se sont basés sur les concepts de "*history function*" et "*intialization function*". Toutefois, leur théorie n'apporte pas de solution au concept d'état. Dans [191, 192], un autre concept a été proposé, celui d'intégrateur d'ordre non entier, qui a permis également d'apporter une solution au problème d'initialisation.

Remarque 4 *Dans la suite de ce manuscrit, on appellera les pseudo états du système d'ordre fractionnaire simplement par les états du système.*

3.4.1.4 Propriétés des systèmes continus d'ordre non entier

3.4.1.4.1 Commandabilité et observabilité des systèmes d'ordre non entier

Les notions de commandabilité et d'observabilité des systèmes linéaires d'ordre fractionnaire commensurable sont étudiées dans [196]. En effet, les auteurs ont montré que les conditions de commandabilité et d'observabilité de la représentation dans l'espace des pseudo états des systèmes continus d'ordre non entier commensurable sont les mêmes que dans le cas des systèmes d'ordre entier. Ainsi, le système (3.49) est commandable si le rang de la matrice de commandabilité

$$\mathcal{C} = [B\ AB\ A^2B\ \ldots\ A^{n-1}B] \tag{3.46}$$

est égale à n. En outre, ce système est observable si le rang de la matrice d'observabilité

$$\mathcal{O} = \begin{bmatrix} C \\ CA \\ CA^2 \\ \vdots \\ CA^{n-1} \end{bmatrix} \tag{3.47}$$

est égale à n.

3.4.1.4.2 Stabilité des systèmes d'ordre non entier

La définition de la stabilité au sens entrée bornée sortie bornée (BIBO), dite aussi stabilité externe, est donnée par la définition suivante [197] :

Définition 1 *Un système est dit BIBO stable si, à une entrée bornée il lui correspond une sortie bornée.*

La condition de stabilité des systèmes d'ordre fractionnaire commensurable est satisfaite, comme dans le cas des systèmes entiers, lorsque l'équation caractéristique du système n'admet aucune racine à partie réelle positive [151]. Dans [197], Matignon a établi une condition de stabilité en raisonnant sur le polynôme entier, de variable complexe p, obtenu à partir de l'équation caractéristique, de variable s, par le changement de variable $p = s^{\alpha}$. Ainsi, la condition de stabilité nécessite que les pôles p du polynôme $D(p)$ vérifient la condition suivante :

$$|arg(p_i)| > \alpha\frac{\pi}{2}, \qquad i = 1, \ldots, n \tag{3.48}$$

Le domaine de stabilité est représenté par la figure 3.1.

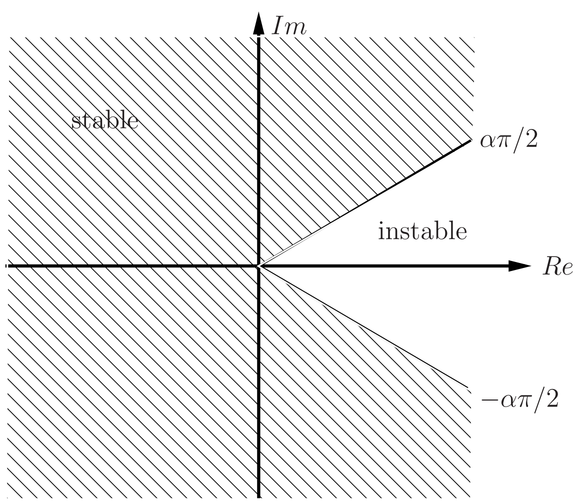


FIGURE 3.1: Domaines de stabilité des systèmes d'ordre fractionnaire approximés par des modèles entiers dans le plan complexe pour $0 < \alpha < 1$.

3.4.1.4.3 Réponse temporelle de l'équation d'état fractionnaire

Étant donné un système fractionnaire d'ordre commensurable $\alpha < 1$ dont le modèle d'état est donné par :

$$\begin{cases} D^\alpha x & = & Ax + Bu, \qquad x(0) = x_0, \\ y & = & Cx + Du \end{cases} \tag{3.49}$$

En calculant la transformation de Laplace de cette équation, en utilisant la définition de Caputo de la dérivation non entière, nous pouvons exprimer la transformation de Laplace du vecteur d'état par :

$$X(s) = (s^\alpha I - A)^{-1} BU(s) + (s^\alpha I - A)^{-1} x_0 \tag{3.50}$$

Nous pouvons alors déterminer l'expression temporelle du vecteur d'état $x(t)$ par :

$$x(t) = \pounds^{-1}[X(s)] = \pounds^{-1}[(s^\alpha I - A)^{-1} BU(s) + (s^\alpha I - A)^{-1} x_0] \tag{3.51}$$

Définissions alors, comme dans le cas entier, la matrice de transition par :

$$\Phi(t) = \pounds^{-1}[(s^\alpha I - A)^{-1}] \qquad \text{pour} \qquad t > 0 \tag{3.52}$$

On obtient finalement :

$$x(t) = \Phi(t) x_0 + \int_0^t \Phi(t - \tau) Bu(\tau) d\tau \tag{3.53}$$

où $\Phi(t)$ est donnée par :

$$\Phi(t) = E_\alpha(At^\alpha) = \sum_{k=0}^{\infty} \frac{A^k t^{k\alpha}}{\Gamma(1 + k\alpha)} \tag{3.54}$$

E_α étant la fonction Mittag-Leffler donnée par l'équation (3.4). En effet, lorsque ($\alpha = 1$) le développement de la somme (3.54) donne e^{At}.

3.4.2 Systèmes d'ordre fractionnaire à temps discret

La représentation en temps continu rencontre certaines limitations. En effet, l'utilisation d'ordinateurs pour la mise en œuvre de systèmes de transmission sécurisée dans des applications réelles est en faveur de l'utilisation de la modélisation en temps discret. Par conséquent, nous avons orienté notre recherche dans cette direction. Dans cette section, nous rappelons quelques résultats obtenus pour le cas des systèmes linéaires d'ordre fractionnaire tels que la représentation d'état, l'observabilité et la commandabilité [171, 183]. L'observabilité des systèmes non linéaires affines en l'entrée d'ordre fractionnaire sera étudiée dans le chapitre 4.

3.4.2.1 Représentation des systèmes discrets d'ordre non entier

Dans cette section, nous allons considérer la définition de Grünwald-Letnikov pour définir un système d'ordre fractionnaire à temps discret. Pour ce faire, nous allons considérer les résultats précédents afin de présenter le modèle d'état d'un système linéaire à temps discret d'ordre fractionnaire. Pour commencer, nous considérons le modèle linaire entier donné sous la représentation d'état suivante :

$$x(k+1) = Ax(k) + Bu(k); \qquad x(0) = x_0 \tag{3.55}$$

où $u(k) \in R^m$ est le vecteur d'entrée, $y(k) \in R^q$ le vecteur de sortie et $x(k) \in R^n$ le vecteur d'état : $x(k) = [x_1(k)\ x_2(k)\ \ldots\ x_n(k)]^T$. La différence d'ordre α du système (3.55) est obtenue en suivant les étapes de la section 3.3.3 et en utilisant l'équation (3.33). Ainsi, nous obtenons la représentation suivante :

$$\Delta^\alpha x(k+1) = Ax(k) + Bu(k) - x(k) = A_d x(k) + Bu(k); \qquad x(0) = x_0 \tag{3.56}$$

Dans ce modèle, l'ordre de différentiation α est pris le même pour toutes les variables d'état $x_i(k)$, $i = 1, \ldots, n$ (ordre commensurable). De plus, en utilisant la différence d'ordre α

donnée par l'équation (3.31) on obtient :

$$\Delta^{\alpha} x(k+1) = x(k+1) + \sum_{j=1}^{k+1} (-1)^j \binom{\alpha}{j} x(k+1-j) \tag{3.57}$$

En substituant l'équation (3.56) dans l'équation (3.57), nous obtenons :

$$x(k+1) = A_d x(k) - \sum_{j=1}^{k+1} (-1)^j \binom{\alpha}{j} x(k+1-j) + Bu(k) \tag{3.58}$$

Introduisons une nouvelle variable $C_j = (-1)^j \binom{\alpha}{j}$. Ainsi, l'équation (3.58) est équivalente à

$$x(k+1) = (A_d - C_1 I_n) x(k) - \sum_{j=2}^{k+1} C_j x(k-j+1) + Bu(k) \tag{3.59}$$

D'après la Remarque 1, il est raisonnable de tronquer la mémoire infinie. Ainsi, le système (3.59) peut être réécrit comme suit :

$$x(k+1) = (A_d - C_1 I_n) x(k) - \sum_{j=2}^{L} C_j x(k-j+1) + Bu(k) \tag{3.60}$$

Maintenant, nous allons mettre

$$A_0 = (A_d - C_1 I_n) \tag{3.61}$$

et, pour tout les $j > 0$:

$$A_j = -C_{j+1} I_n \tag{3.62}$$

Cela mène à

$$x(k+1) = A_0 x(k) + A_1 x(k-1) + A_2 x(k-2) + \ldots + A_k x(0) + Bu(k) \tag{3.63}$$

Cette description peut être étendue aux systèmes d'ordre fractionnaire non commensurable, où l'ordre de différentiation est noté $[\alpha]$.

$$\Delta^{[\alpha]}x(k+1) = A_d x(k) + Bu(k)$$

Avec

$$\Delta^{[\alpha]}x(k+1) = \begin{bmatrix} \Delta^{\alpha_1}x_1(k+1) \\ \vdots \\ \Delta^{\alpha_n}x_n(k+1) \end{bmatrix}$$

où $\alpha_i \in R^{*+}$, $i = 1, 2, \ldots$ présentent les ordres fractionnaires. Ici, nous pouvons écrire

$$A_j = diag\{-(-1)^{j+1}\binom{\alpha_i}{j+1}, i = 1, \ldots, n\} \tag{3.64}$$

En utilisant les équations (3.63) et (3.64), nous obtiendrons l'équation d'état suivante :

$$x(k+1) = \sum_{j=0}^{k} A_j x(k-j) + Bu(k); \qquad x(0) = x_0 \tag{3.65}$$

Dans ce modèle, A_j est donné par l'équation (3.62) dans le cas commensurable et par l'équation (3.64) dans le cas non commensurable. L'équation de la sortie correspondante est donnée comme suit :

$$y(k) = Cx(k) \tag{3.66}$$

Considérons G_k de sorte que

$$G_k = \begin{cases} I_n & \text{pour } k = 0 \\ \sum\limits_{j=0}^{k-1} A_j G_{k-1-j} & \text{pour } k \geq 1 \end{cases} \tag{3.67}$$

Ainsi, la solution du système (3.65) est donnée comme suit :

$$x(k) = G_k x(0) + \sum_{j=0}^{k-1} G_{k-1-j} Bu(j) \tag{3.68}$$

La matrice de transition correspondante peut être définie comme suit

$$\Phi(k,0) = G_k, \qquad \Phi(0,0) = G_0 = I_n \tag{3.69}$$

Remarque 5 $\Phi(k,0)$ *présente la particularité d'être variable dans le temps, puisqu'elle est composée d'un nombre de termes* A_j *qui augmente avec* k*. Cela est dû à la caractéristique de l'ordre fractionnaire du modèle, qui prend en compte toutes les valeurs passées de l'état.*

3.4.2.2 Propriétés des systèmes discrets d'ordre non entier

3.4.2.2.1 Commandabilité et observabilité des systèmes d'ordre non entier

Les notions d'accessibilité, de commandabilité et d'observabilité sont bien étudiées dans [183]. En effet, les auteurs ont étendu ces concepts au cas des systèmes linéaires d'ordre fractionnaire à temps discret. Dans ce travail, nous allons présenter, d'une manière générale, ces notions.

Définition 2 *Le système linéaire d'ordre fractionnaire à temps discret modélisé par (3.65) est accessible s'il est possible de trouver une séquence de commande de sorte qu'un état arbitraire puisse être atteint depuis l'origine dans un temps fini.*

Définition 3 *Le système linéaire d'ordre fractionnaire à temps discret modélisé par (3.65) est contrôlable s'il est possible de trouver une séquence de commande de sorte que l'origine puisse être atteinte à partir de n'importe quel état initial dans un temps fini.*

Définition 4 *Pour le système linéaire d'ordre fractionnaire à temps discret modélisé par (3.65), nous définissons ce qui suit :*

1. La matrice de commandabilité

$$\mathcal{C}_k = [G_0B \quad G_1B \quad G_2B \quad \dots \quad G_{k-1}B] \tag{3.70}$$

2. Le Grammien d'accessibilité

$$\mathcal{W}_r(0,k) = \sum_{j=0}^{k-1} G_j B B^T G_j^T, \qquad k \geq 1 \tag{3.71}$$

Il est facile de montrer que $\mathcal{W}_r(0,k) = \mathcal{C}_k \mathcal{C}_k^T$.

3. Le Grammien de commandabilité, à condition que A_0 *soit non singulière*

$$\mathcal{W}_c(0,k) = G_k^{-1} \mathcal{W}_r(0,k) G_k^{-T}, \qquad k \geq 1 \tag{3.72}$$

Dans ce qui quit, nous considérons A_0 non singulière. Ainsi, le système linéaire d'ordre fractionnaire à temps discret modélisé par (3.65) est accessible si et seulement s'il existe un temps fini K tel que : $rang(\mathcal{C}_K) = n$ ou, de manière équivalente, $rang(\mathcal{W}_r(0,K)) = n$. En outre, la séquence d'entrée

$$\mathcal{U}_{\mathcal{K}} = [u^T(K-1)\, u^T(K-2)\, \ldots\, u^T(0)]^T$$

qui transfère $x_0 = 0$ quand $k = 0$ à $x_f \neq 0$ quand $k = K$ est donnée par

$$\mathcal{U}_{\mathcal{K}} = \mathcal{C}_K^T \mathcal{W}_r^{-1}(0,K) x_f \tag{3.73}$$

Remarque 6 *Dans le cas d'un ordre entier, il est bien connu que le rang de* $\mathcal{C}_k$ *ne peut augmenter pour aucun* $k \geq n$. *Cela résulte du théorème de Cayley-Hamilton. Au contraire, dans le cas du système d'ordre fractionnaire linéaire non commensurable à temps discret linéaire (3.65), le rang de* $\mathcal{C}_k$ *peut augmenter pour les valeurs de* $k \geq n$. *En d'autres termes, il est possible d'atteindre l'état final* x_f *en plusieurs étapes supérieures à* n. *Ceci est dû à la nature des éléments* G_k *qui construisent la matrice de contrôlabilité* $\mathcal{C}_k$ *et qui présentent la particularité de varier dans le temps, en ce sens qu'ils sont composés d'un nombre de termes* A_j *croissant avec* k, *comme déjà mentionné dans Remarque 2. Le rang complet de* $(\mathcal{C}_k)$ *peut être atteint dans une étape* $k = K$ *égale ou supérieure à* n.

Ainsi, le système linéaire d'ordre fractionnaire à temps discret modélisé par (3.65) est commandable si et seulement s'il existe un temps fini K tel que $rang(\mathcal{W}_\rceil(0,K)) = n$. De plus, une séquence d'entrée $\mathcal{U}_K = [u^T(K-1)\, u^T(K-2)\, \ldots\, u^T(0)]^T$ qui transfère $x_0 \neq 0$ quand $k = 0$ à $x_f = 0$ quand $k = K$ est donnée par

$$\mathcal{U}_{\mathcal{K}} = -\mathcal{C}_{\mathcal{K}}^T G_K^{-T} \mathcal{W}_c^{-1}(0,K) x_0 \tag{3.74}$$

Définition 5 *Le système linéaire d'ordre fractionnaire à temps discret modélisé par les équations (3.65) et (3.66) est observable à l'instant $k = 0$ si et seulement s'il existe un $K > 0$ tel que l'état x_0 à l'instant $k = 0$ peut être déterminé à partir de la connaissance de u_k, y_k, $k \in [0,K]$.*

Définition 6 *Pour le système d'ordre fractionnaire linéaire à temps discret modélisé par les équations (3.65) et (3.66), nous définissons ce qui suit :*

1. La matrice d'observabilité

$$\mathcal{O}_k = \begin{bmatrix} CG_0 \\ CG_1 \\ CG_2 \\ \vdots \\ CG_{k-1} \end{bmatrix} \tag{3.75}$$

2. Le Grammien d'observabilité

$$\mathcal{W}_o(0,k) = \sum_{j=0}^{k-1} G_j^T C^T C G_j \tag{3.76}$$

Il est facile de montrer que $\mathcal{W}_o(0,k) = \mathcal{O}_k^T \mathcal{O}_k$.

Ainsi, le système linéaire d'ordre fractionnaire à temps discret modélisé par les équations (3.65) et (3.66) est observable si et seulement s'il existe un temps fini K tel que $rang(\mathcal{O}_K) = n$ ou, de manière équivalente, $rang(\mathcal{W}_o(0,K)) = n$. De plus, l'état initial x_0

quand $k = 0$ est donné par

$$x_0 = \mathcal{W}_o^{-1}(0, K)\mathcal{O}_K^T[\mathcal{Y}_K - \mathcal{M}_K\tilde{\mathcal{U}}_K] \tag{3.77}$$

avec

$$\tilde{\mathcal{U}}_K = [u^T(0)\, u^T(1)\, \dots\, u^T(K-1)]^T$$

$$\tilde{\mathcal{Y}}_K = [y^T(0)\, y^T(1)\, \dots\, y^T(K-1)]^T$$

et

$$\mathcal{M}_K = \begin{bmatrix} 0 & 0 & 0 & \dots & 0 & 0 \\ CG_0B & 0 & 0 & \dots & 0 & 0 \\ CG_1B & CG_0B & 0 & \dots & 0 & 0 \\ CG_2B & CG_1B & CG_0B & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \dots & \vdots & \vdots \\ CG_{K-2}B & CG_{K-3}B & CG_{K-4}B & \dots & CG_0B & 0 \end{bmatrix} \tag{3.78}$$

Remarque 7 *D'après le théorème de Cayley-Hamilton, il est bien connu que pour les systèmes d'ordres entiers, le rang de la matrice d'observabilité $\mathcal{O}_k$ ne peut pas augmenter à l'étape $k \geq n$. Ici aussi, il est remarquable que cela ne soit pas vrai dans le cas du système d'ordre fractionnaire non commensurable à temps discret (3.65) et (3.66). En effet, le rang $(\mathcal{O}_k)$ peut augmenter pour les valeurs $k \geq n$. Nous pouvons affirmer que l'observabilité de ce type de systèmes peut éventuellement être obtenue en plusieurs étapes supérieures à n. Cela est dû aux mêmes raisons que celles exposées ci-dessus dans la Remarque 5 pour la commandabilité. Dans [172], la condition d'observabilité pour le système d'ordre fractionnaire à temps discret modélisé par (3.65), avec un ordre non-commensurable, est que le rang de $\mathcal{O}_k$ soit égal au plus à n à l'étape $k = n$. Le résultat montre que le rang complet de $(\mathcal{O}_k)$ peut être atteint dans une étape $k = K$ supérieure à n. Cela peut être considéré comme une extension du résultat précédent dans [172].*

3.5 Systèmes chaotiques d'ordre fractionnaire

Dans cette section, un aperçu sur les systèmes chaotiques d'ordre fractionnaire est donné. Ceux ci présentent l'application la plus importante du calcul fractionnaire dans la théorie du chaos [27–29, 34]. Dans de tels systèmes, non seulement ils contiennent des dérivées fractionnaires, mais ils présentent également des phénomènes liés aux attracteurs étranges observés pour les systèmes chaotiques à dérivée entière. Ces propriétés intrinsèques des systèmes chaotiques peuvent être utilisées dans les schémas de synchronisation et de cryptographie [31, 35, 36]. En effet, le chaos ne peut pas se produire dans les systèmes dynamiques continus lorsque l'ordre total est inférieur à trois. Toutefois, le modèle d'un système chaotique d'ordre fractionnaire peut être réorganisé en trois équations différentielles simples, où les équations contiennent des dérivées fractionnaires. Cependant, l'ordre total du système sera la somme de l'ordre de chaque dérivée fractionnaire de l'état du système, qui par conséquent sera inférieur à 3. Dans [159], le chaos apparaît dans le système de Chua-Hartley pour l'ordre 2.7. Ce qui nous amène à dire qu'on peut observer le phénomène du chaos dans un système dynamique fractionnaire où l'ordre total du système est inférieur à 3.

Dans ce qui suit, nous allons présenter les systèmes non linéaires discrets d'ordre fractionnaire. Ensuite, deux exemples de systèmes fractionnaires seront illustrés ; le premier à temps continu et le deuxième à temps discret. Les calculs des dérivées fractionnaires sont établis en utilisant la méthode de Grünwald-Letnikov.

3.5.1 Exemple d'un système à temps continu

Dans cette partie, nous présentons le système de Lorenz d'ordre fractionnaire. Le système de Lorenz d'ordre entier a été introduit dans le premier chapitre, équation (2.18). Le système de Lorenz d'ordre fractionnaire est donné comme suit [200] :

$$\left\{\begin{array}{lcl} D^{\alpha_1}x(t) & = & \sigma(y(t)-x(t)) \\ D^{\alpha_2}y(t) & = & x(t)(r-z(t))-y(t) \\ D^{\alpha_3}z(t) & = & x(t)y(t)-bz(t) \end{array}\right. \tag{3.79}$$

où $\alpha_1, \alpha_2, \alpha_3$ sont les ordres de dérivation non entiers. L'intégration numérique est réalisée par la méthode d'approximation de Grünwald-Letnikov [158], de pas $h = 0.005s$.

$$\begin{cases} x_k &= [\sigma(y_{k-1} - x_{k-1})]h^{\alpha_1} - \sum\limits_{j=1}^{k} C_{1j}x_{k-j} \\ y_k &= [x_k(r - z_{k-1}) - y_{k-1}]h^{\alpha_1} - \sum\limits_{j=1}^{k} C_{2j}y_{k-j} \\ z_k &= [x_k y_k - b z_{k-1}]h^{\alpha_3} - \sum\limits_{j=1}^{k} C_{3j}z_{k-j} \end{cases} \tag{3.80}$$

où $C_{ij} = (1 - \frac{1+\alpha_i}{j})C_{i\{j-1\}}$, $i = 1, 2, 3$ et $C_{i0} = 1$. Dans [201], un ordre minimal pour lequel le système de Lorenz d'ordre fractionnaire est chaotique est déterminé, avec les paramètres $(\sigma, r, b) = (10, 28, 8/3)$. Ainsi, en considérant $\alpha_1 = \alpha_2 = \alpha_3 = \alpha$, l'ordre commensurable minimal est $\alpha > 0.9941$.

Soit $\alpha_1 = \alpha_2 = \alpha_3 = 0.995$ et $(x_0,\, y_0,\, z_0) = (0.1,\, 0.1,\, 0.1)$, l'attracteur du système de Lorenz d'ordre fractionnaire est présenté par la figure 3.2. La figure 3.3 illustre la sensibilité aux conditions initiales de l'état x du système (3.79), la trajectoire de x (représentée en bleu) est obtenue pour une condition initiale ($x(0) = 0.1$) ; tandis que, la trajectoire de $\bar{x}$ (représentée en rouge) est obtenue pour la même condition initiale mais avec une petite variation $\epsilon = 10^{-10}$. D'après cette figure, nous pouvons dire que le système (3.79) est très sensible aux conditions initiales puisque les deux trajectoires divergent avec le temps. L'aspect aléatoire des états du système (3.79) est présenté par la figure 3.4. Le diagramme de bifurcation est exposé à la figure 3.5 qui présente le comportement des orbites du système (3.79), pour $r \in [0,\, 30]$. Le spectre de puissance de la variable x est donné par la figure 3.6.

3.5.2 Exemple d'un système à temps discret

Maintenant, nous considérons le système de Hénon d'ordre fractionnaire. Les équations d'états du système de Hénon d'ordre entier sont données par l'équation (2.21) du premier chapitre. Le modèle d'état du système de Hénon d'ordre fractionnaire est obtenu

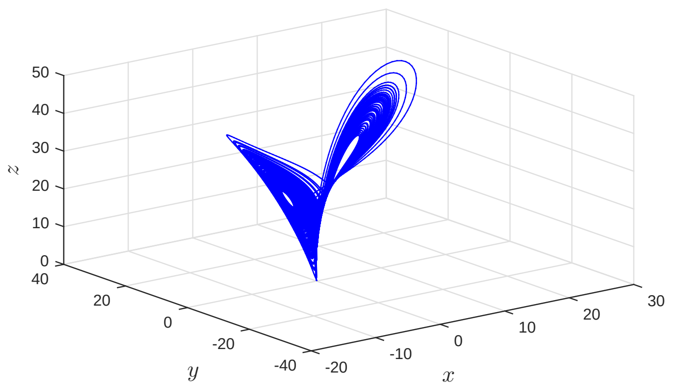


FIGURE 3.2: Attracteur étrange du système de Lorenz d'ordre fractionnaire.

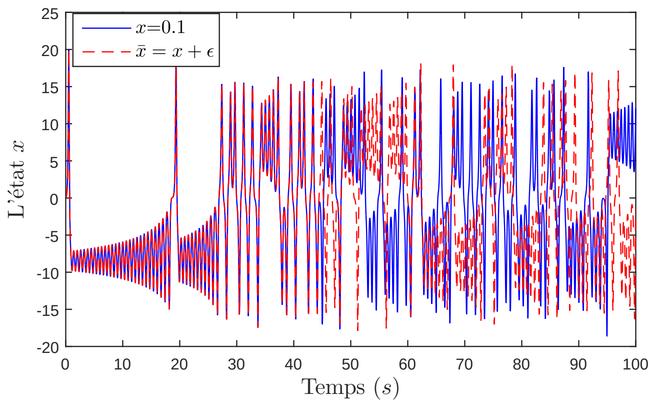


FIGURE 3.3: Sensibilité aux conditions initiales de l'état x du système de Lorenz d'ordre fractionnaire.

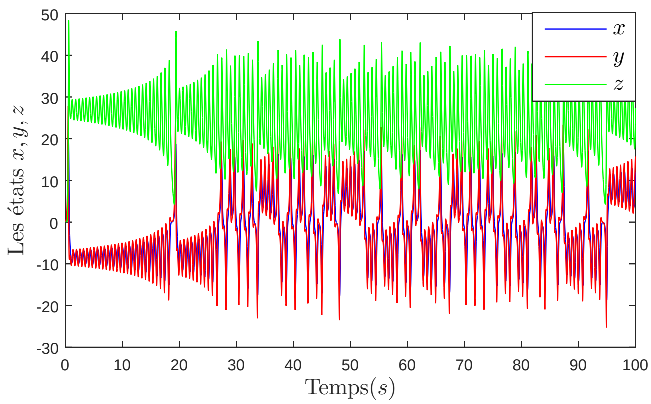


FIGURE 3.4: Aspect aléatoire des états du système de Lorenz d'ordre fractionnaire.

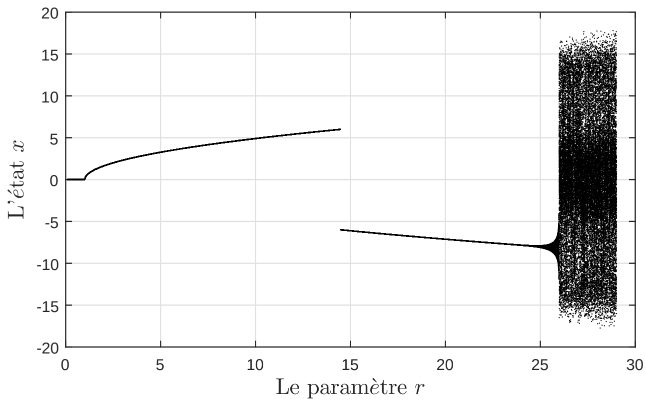


FIGURE 3.5: Diagramme de bifurcation du système de Lorenz d'ordre fractionnaire.

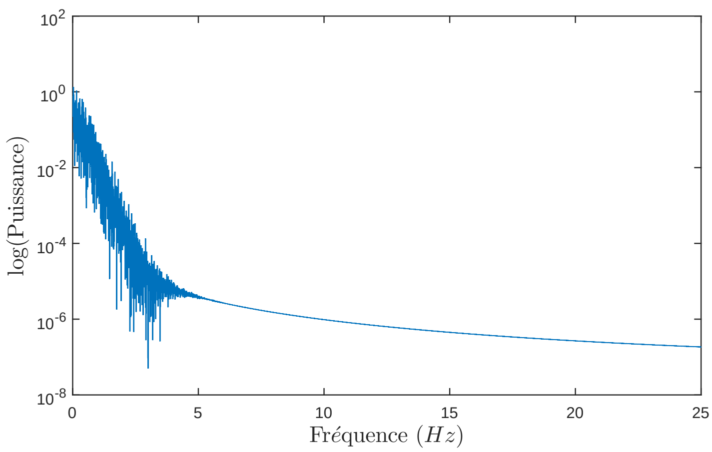


FIGURE 3.6: Spectre de puissance du système de Lorenz d'ordre fractionnaire.

en utilisant la définition de Grünwald-Letnikov et est présenté par les équations suivantes :

$$\begin{cases} x(k+1) = 1 - a\,x(k)^2 + y(k) + (\alpha_1 - 1)x(k) - \sum\limits_{j=1}^{L} C_{1j}x(k-j) \\ y(k+1) = b\,x(k) + (\alpha_2 - 1)y(k) - \sum\limits_{j=1}^{L} C_{2j}y(k-j) \end{cases} \tag{3.81}$$

où les coefficients $C_{ij} = (-1)^j \binom{\alpha_i}{j}$, avec $i = 1, 2$. Les paramètres du système (3.81) a et b sont égal à 1.4 et 0.3, respectivement. α_1 et α_2 représentent les ordres fractionnaires de notre système et ils sont choisis égaux à 0.9 et 0.95, et les conditions initiales sont $(x_0, y_0) = (0.1,\ 0.1)$. L'attracteur du système (3.81) est tracé sur la figure 3.7, et la sensibilité aux conditions initiales de l'état x est présentée par le figure 3.8, où la trajectoire de x (en bleu) est obtenue pour une condition initiale ($x(0) = 0.1$) et la trajectoire de $\bar{x}$ (en rouge) est obtenue pour la même condition initiale mais avec une petite variation $\epsilon = 10^{-10}$. La figure 3.9 illustre l'aspect aléatoire des états du système (3.81). Le diagramme de bifurcation est présenté par la figure 3.10 ; dans cette figure, le comportement des orbites du système (3.79) pour $a \in [0, 1.4]$ est donné. La figure (3.11) expose le spectre de puissance de la variable x.

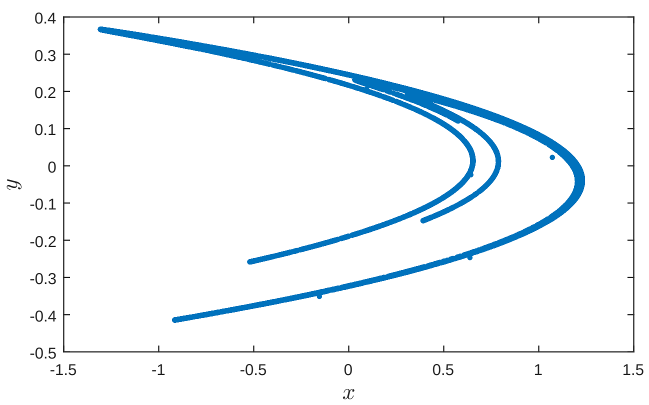


FIGURE 3.7: Attracteur étrange du système de Hénon d'ordre fractionnaire.

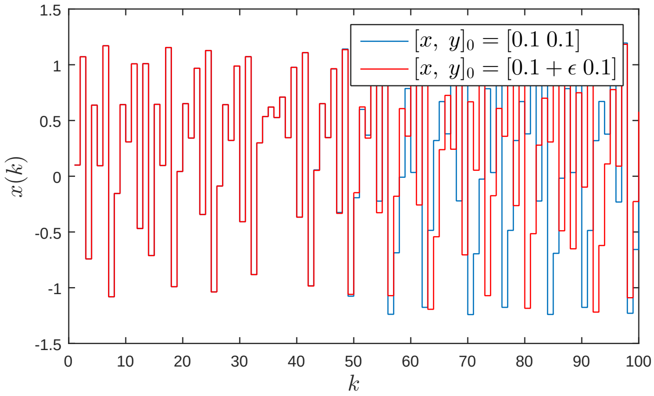


FIGURE 3.8: Sensibilité aux conditions initiales de l'état x du système de Hénon d'ordre fractionnaire.

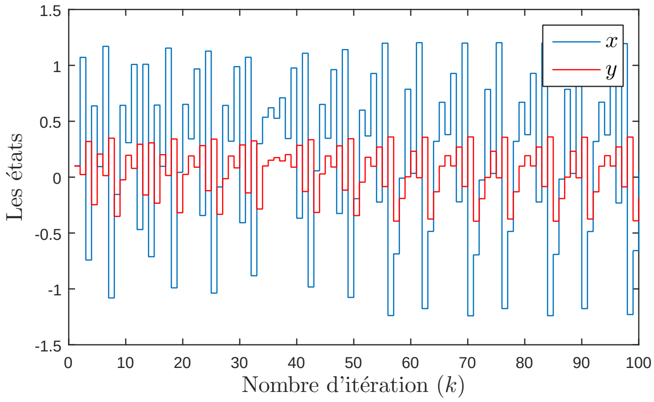


FIGURE 3.9: Aspect aléatoire des états du système de Hénon d'ordre fractionnaire.

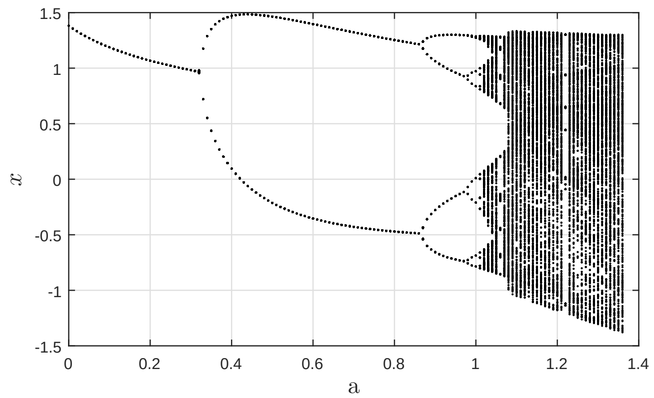


FIGURE 3.10: Diagramme de bifurcation du système de Hénon d'ordre fractionnaire.

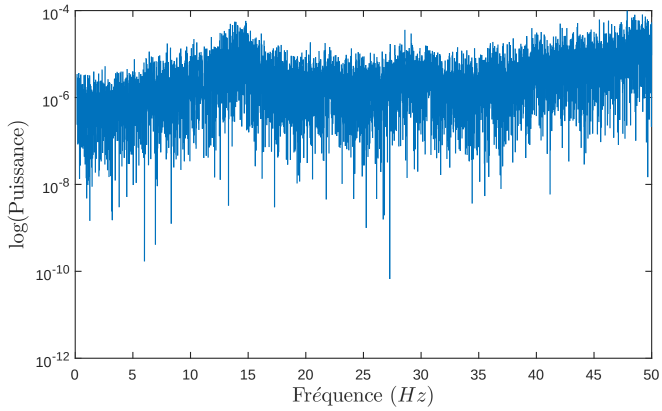


FIGURE 3.11: Spectre de puissance du système de Henon d'ordre fractionnaire.

3.6 Synchronisation des systèmes chaotiques d'ordre fractionnaire

La synchronisation des systèmes chaotiques joue un rôle très important dans différents domaines et spécialement en cryptographie. Avec le développement du calcul fractionnaire, la synchronisation des systèmes chaotiques d'ordre fractionnaire commence à recevoir une considérable attention et est devenue un domaine de recherche très important dû à ses applications potentielles dans les schémas de communications sécurisées. Pour cette raison, beaucoup de chercheurs étudient la possibilité d'étendre les méthodes de synchronisation des systèmes chaotiques d'ordre entier au cas fractionnaire. En effet, plusieurs travaux ont été effectués sur la synchronisation complète des systèmes chaotiques d'ordre fractionnaire. Dans [27], la synchronisation complète du système chaotique de Chen d'ordre fractionnaire a été réalisée en utilisant l'approche de Pecora et Carroll. Cette approche synchronisation a été aussi appliquée pour la fonction logistique d'ordre fractionnaire, avec une méthode de couplage non linéaire dans [28]. Dans [29], la synchronisation des systèmes chaotiques d'ordre fractionnaire à été effectuée en utilisant une commande par feedback linéaire. D'autres méthodes ont été aussi proposées, telles que : commande par mode glissant [202], commande adaptative [203], commande impulsive [204], méthode basée sur Lyapunov [205] et commande robuste H_∞ [217]. De plus, un grand nombre de résultats est obtenu en utilisant l'approche basée sur les observateurs tels que l'observateur

LMI réduit [206], le filtre de Kalman étendu [31] et l'observateur par mode glissant [207]. Un autre type de synchronisation, à savoir la synchronisation projective, a attiré une considérable attention ces dernières années. Ainsi, beaucoup de travaux ont été réalisés. En [208], les auteurs ont proposé une nouvelle approche pour la synchronisation projective, avec des facteurs d'échelle différents, d'un système chaotique d'ordre fractionnaire et ils l'ont appliquée dans le chiffrement d'images. La synchronisation projective généralisée pour deux classes particulières de systèmes chaotiques d'ordre fractionnaire à été proposée dans [209,210]. Par la suite, dans [211], la synchronisation projective retardée des systèmes hyper-chaotiques d'ordre fractionnaire a été examinée. Dans [212], les auteurs ont étudié une fonction de synchronisation projective des systèmes chaotiques d'ordre fractionnaire avec les mêmes dimensions. Par ailleurs, dans [213], une nouvelle méthode de synchronisation projective hybride des systèmes chaotiques d'ordre fractionnaire avec des dimensions différentes à été étudiée. Par ailleurs, des résultats sur la synchronisation de phase des systèmes chaotiques d'ordre fractionnaire ont été obtenus. Dans [214], la synchronisation de phase et anti-phase des systèmes Lü et Liu a été étudiée en utilisant des techniques de la théorie du contrôle actif. Dans [215], les comportements de synchronisation de phase des oscillateurs chaotiques d'ordre fractionnaire a été exploré en employant la transformée d'ondelette. En ce qui concerne la synchronisation retardée, peu de travaux ont été réalisés [211, 216].
Dans ce qui suit, la synchronisation de deux exemples de systèmes chaotiques d'ordre fractionnaire continu et discret est présentée. La méthode utilisée est la l'approche de Pecora et Carroll. Les calculs des dérivées fractionnaires sont établis en utilisant la méthode de Grünwald-Letnikov.

3.6.1 Synchronisation des systèmes chaotiques identiques continus d'ordre fractionnaire

Afin de présenter la synchronisation des systèmes chaotiques identiques d'ordre fractionnaire, nous avons sélectionné la méthode de Pecora et Carrol. Cette méthode est testée sur le système de Lorenz d'ordre fractionnaire (voir l'équation (3.79)).

Considérons le système de Lorenz d'ordre fractionnaire décrit par l'équation (3.79), que nous allons décomposé en deux sous systèmes : maître et esclave. Dans cette configuration, le système maître est donné par le système de Lorenz d'ordre fractionnaire à trois états portant l'indice m, et le système esclave est défini par le sous espace d'état contenant les variables y et z.

$$\left\{\begin{array}{lcl} D^{\alpha_1}x_m(t) & = & \sigma(y_m(t)-x_m(t)) \\ D^{\alpha_2}y_m(t) & = & x_m(t)(r-z_m(t))-y_m(t) \\ D^{\alpha_3}z_m(t) & = & x_m(t)y_m(t)-bz_m(t) \end{array}\right. \tag{3.82}$$

Le système esclave est donné comme suit :

$$\left\{\begin{array}{lcl} D^{\alpha_2}y_s(t) & = & x_m(t)(r-z_s(t))-y_s(t) \\ D^{\alpha_3}z_s(t) & = & x_m(t)y_s(t)-bz_s(t) \end{array}\right. \tag{3.83}$$

Dans cet exemple, nous considérons les ordres fractionnaires $\alpha_1 = \alpha_2 = \alpha_3 = 0.995$, les paramètres des systèmes $(\sigma, r, b) = (10, 28, 8/3)$ et les conditions initiales des systèmes maître et esclave égales à $(x_m, y_m, z_m) = (0.1, 2.5, 4)$ et $(y_s, z_s) = (-9, -15)$. La synchronisation des états y_m et z_m du système maître avec les états y_s et z_s du système esclave est illustrée par la figure 3.12. Les erreurs de synchronisation sont données par la figure 3.13, avec $e_2 = y_m - y_s$ et $e_3 = z_m - z_s$.

3.6.2 Synchronisation des systèmes chaotiques identiques discrets d'ordre fractionnaire

Dans cette partie, nous considérons également la méthode de synchronisation de Pecora et Carroll. Afin d'illustrer ce phénomène pour les systèmes discrets, nous choisissons le système de Hénon modifié d'ordre fractionnaire [42].

Considérons le système de Hénon modifié d'ordre fractionnaire, dont le système maître

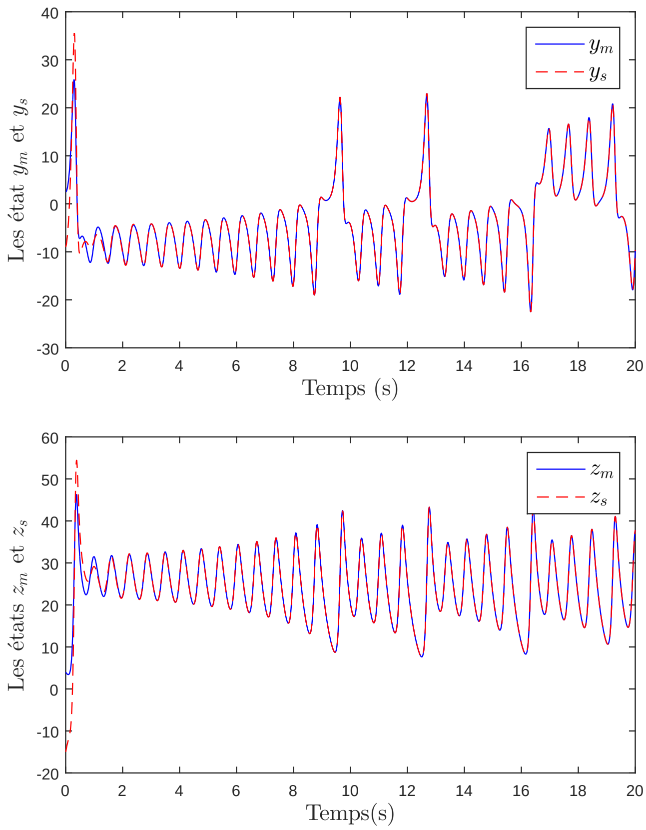


FIGURE 3.12: Synchronisation des états du système de Lorenz d'ordre fractionnaire par la méthode de Pecora et Carrol.

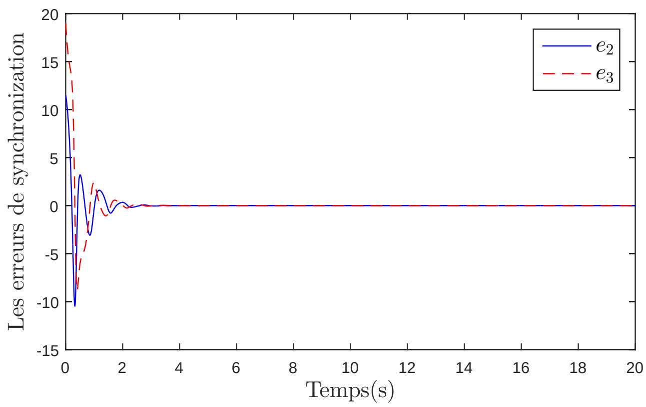


FIGURE 3.13: Erreurs de synchronisation des états du système de Lorenz d'ordre fractionnaire par la méthode de Pecora et Carrol.

est représenté par l'équation suivante :

$$\begin{cases} x_m(k+1) = 1 - a\,y_m(k)^2 - b\,z_m(k) + (\alpha_1 - 1)x_m(k) - \sum\limits_{j=1}^{L} C_{1j}x_m(k-j) \\ y_m(k+1) = x_m(k) + (\alpha_2 - 1)y_m(k) - \sum\limits_{j=1}^{L} C_{2j}y_m(k-j) \\ z_m(k+1) = y_m(k) + (\alpha_3 - 1)z_m(k) - \sum\limits_{j=1}^{L} C_{3j}z_m(k-j) \end{cases} \tag{3.84}$$

Le système esclave est considéré comme suit :

$$\begin{cases} x_s(k+1) = 1 - a\,y_m(k)^2 - b\,z_s(k) + (\alpha_1 - 1)x_s(k) - \sum\limits_{j=1}^{L} C_{1j}x_s(k-j) \\ z_s(k+1) = y_m(k) + (\alpha_3 - 1)z_s(k) - \sum\limits_{j=1}^{L} C_{3j}z_s(k-j) \end{cases} \tag{3.85}$$

Dans cet exemple, nous considérons les ordres fractionnaires $\alpha_1 = 0.95$, $\alpha_2 = 0.9$ et $\alpha_3 = 0.85$, les paramètres des systèmes $(a, b) = (1.6, 0.1)$ et les conditions initiales des systèmes maître et esclave égales à $(x_m, y_m, z_m) = (0.2, 0.5, 0.1)$ et $(x_s, z_s) = (0.8, 1.2)$. La synchronisation des états x_m et z_m du système maître avec les états x_s et z_s du système esclave est illustrée par la figure 3.14. Les erreurs de synchronisation sont données par la figure 3.15, avec $e_1 = x_m - x_s$ et $e_3 = z_m - z_s$.

3.7 Conclusion

Dans la première partie de ce chapitre, nous avons exposé les différentes définitions de l'intégration, dérivation et différentiation d'ordre fractionnaire. Par la suite, nous avons présenté les systèmes d'ordre fractionnaire continu et discret et nous avons abordé les notions d'observabilité et de commandabilité des systèmes d'ordre fractionnaire. Nous avons également cité les systèmes chaotiques d'ordre fractionnaire, et afin de prouver la substance du comportement chaotique dans ces systèmes, deux exemples de systèmes chaotiques d'ordre fractionnaire ont été traités. Enfin, la synchronisation des systèmes chaotiques d'ordre fractionnaire est abordée.

Le chapitre 3 sera consacré à la synchronisation à base d'observateurs des systèmes chao-

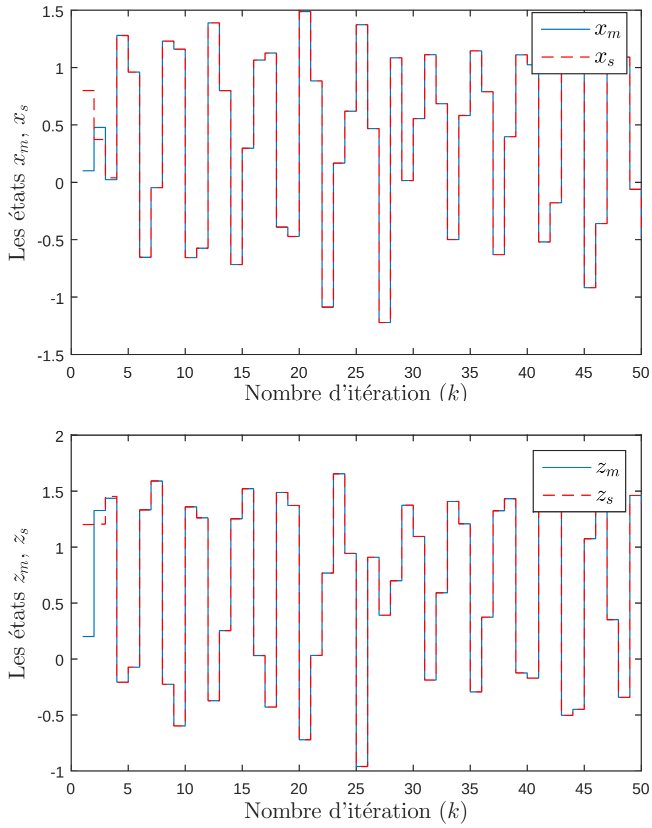


FIGURE 3.14: Synchronisation des états du système de Hénon modifié d'ordre fractionnaire par la méthode de Pecora et Carrol.

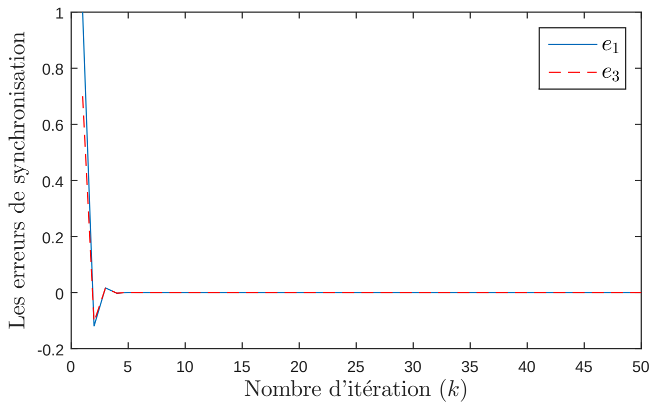


FIGURE 3.15: Erreurs de synchronisation des états du système de Hénon modifié d'ordre fractionnaire par la méthode de Pecora et Carrol.

tiques discrets fractionnaires avec une application à la transmission sécurisée de données.

Chapitre 4

Synchronisation à base d'observateurs des systèmes chaotiques discrets fractionnaires : Application à la transmission sécurisée de données

4.1 Introduction

L'utilisation des systèmes chaotiques d'ordre fractionnaire dans les schémas de transmission sécurisée a conduit les chercheurs à porter un intérêt de recherche de plus en plus important dans le domaine des communications sécurisées. La plupart des schémas de transmission sécurisée par chaos sont basés sur la technique de synchronisation chaotique, où le récepteur est synchronisé avec l'émetteur par l'intermédiaire d'un signal transmis sur un canal public. Depuis lors, plusieurs méthodes de synchronisation chaotique du récepteur avec l'émetteur ont été proposées [27, 200, 206], avec des applications pour sécuriser les communications [208]. La plupart des systèmes basés sur les techniques traditionnelles à base de chaos ont été cassés [125, 218–220]. Afin d'améliorer le niveau de sécurité et de l'augmenter à un degré beaucoup plus élevé, la synchronisation chaotique est généralement combinée avec les techniques de cryptage classique [78, 157].

Ces dernières années, une approche systématique pour la synchronisation et la communication a été proposée, à savoir l'approche basée sur les observateurs [31,172,207]. Dans de tels systèmes de communications chaotiques sécurisées, les problèmes de synchronisation et de communication sont résolus en utilisant le masquage chaotique et la modulation chaotique. L'inconvénient majeur de ces systèmes est lié au spectre du signal. En effet, le spectre correspondant au message chiffré décroît très rapidement avec l'augmentation de la fréquence, présentant un niveau de sécurité inférieur. Par conséquent, la sécurité de ces systèmes est contestable contre diverses attaques, principalement en raison du fait que l'attaquant peut toujours obtenir des informations à partir du signal conducteur pour construire la dynamique de l'émetteur.

Dans une récente recherche [115], les auteurs ont proposé un système de communication chaotique sécurisée fondé sur un schéma de synchronisation avec observateurs (retardé étape par étape et impulsif). L'émetteur est composé d'un système chaotique en temps continu dit de Colpitts et d'un système chaotique en temps discret dit de Hénon modifié. Le récepteur est composé d'un observateur en temps continu et d'un observateur en temps discret. Dans le but de rendre la structure de l'émetteur plus complexe, les états du système en temps continu sont introduits dans la dynamique du système en temps discret. La sortie transmise au récepteur est composée d'un signal dit de synchronisation issu du système en temps continu et d'un signal utile qui contient le message (ajouté par la méthode d'inclusion) issu du système en temps discret. La récupération du message au niveau du récepteur passe d'abord par la synchronisation des deux systèmes en temps continu (de l'émetteur et du récepteur). Toutefois, cette méthode n'est pas robuste contre l'attaque à textes clairs connus et les clés secrètes sont identifiables. Pour résoudre ce problème, les auteurs ont proposé d'introduire des retards (clés secrètes supplémentaires) sur les états continus.

Dans la présente contribution, nous étendons la synchronisation chaotique par observateurs, effectuée dans [115], aux systèmes chaotiques d'ordre fractionnaire. Ainsi, nous proposons une méthodologie de synchronisation des systèmes chaotiques discrets d'ordre fractionnaire à base d'observateurs, plus précisément, l'observateur retardé étape par étape à entrée inconnue. Le fonctionnement correct de cet observateur nécessite l'inversion à gauche du système chaotique, c'est à dire, il dépend de deux conditions et la condition d'observabilité pour estimer les états du système ; la condition de recouvrement d'observabilité pour estimer les états du système et l'information noyée dans ce système (entrée inconnue). Ces notions sont étudiés, pour la première fois, dans le cas des systèmes non linéaires discrets d'ordre fractionnaire. Dans la suite, cet observateur est utilisé dans un nouveau schéma de communication sécurisée basé sur la synchronisation des systèmes chaotiques discrets d'ordre fractionnaire. Les résultats de simulation de la synchronisation de l'émetteur et du récepteur sont donnés à travers une application de cryptage de deux types de signaux (carré et sinusoïdal).

4.2 Inversion à gauche des systèmes chaotiques discrets d'ordre fractionnaire

Dans cette section, nous étudions les notions d'observabilité et de condition de recouvrement des systèmes non linéaires discrets d'ordre fractionnaire [43]. Le problème d'observabilité consiste à pouvoir reconstruire tous les états du système à partir des grandeurs mesurables qui sont les entrées et les sorties. Si le système est observable alors il est possible de construire un système dynamique qui permet de reconstruire le vecteur d'état à partir de la connaissance des entrées et des sorties [221, 222]. Ce système dynamique est dénommé observateur d'état. Quant à la condition de recouvrement, cette propriété permet d'estimer, en plus des états du système, l'entrée (considérée inconnue) appliquée au système [73]. L'objectif à travers ces définitions est de garantir l'inversibilité à gauche des systèmes non linéaires discrets d'ordre fractionnaire. En effet, cette propriété nous permet de réaliser un schéma de transmission sécurisée basé sur la synchronisation par d'observateur. Ce schéma fera l'objet de la section suivante.

4.2.1 Observabilité

Avant de définir l'observabilité des systèmes non linéaires discrets d'ordre fractionnaire, nous présentons en premier lieu l'observabilité des systèmes non linéaires discrets d'ordre entier [221]. Dans ce cas, la notion d'observabilité et la synthèse des observateurs d'état reste un problème encore ouvert malgré l'abondance de travaux rapportés dans la littérature. En effet, une solution systématique est loin d'être établie. Selon la classe du système non linéaire considérée, les définitions d'observabilité ainsi que les méthodes de construction d'observateurs peuvent différer d'une classe à une autre. Par ailleurs, les observateurs proposés sont soumis à des conditions et hypothèses souvent sévères et parfois non remplies par le système (non linéarité lipchitzienne, bornitude des entrées, bornitude des états, ...) supposées pour assurer la stabilité de l'observateur.

Dans ce présent travail, nous considérons la classe des systèmes non linéaires discrets affines en l'entrée représentée comme suit :

$$\begin{cases} x(k+1) &= f(x(k)) + g(x(k))u(k), \qquad x(0) = x_0 \\ y(k) &= h(x(k)) \end{cases} \tag{4.1}$$

où $x \in R^n$, $y \in R$, $u \in R$ sont les vecteurs d'état, de sortie et d'entrée, respectivement, avec $n \in N$ représente l'ordre du système. f, g sont des champs de vecteur et h une fonction scalaire.

Pour pouvoir synthétiser des observateurs d'état dans le cas non linéaire, il faudrait bien évidemment, savoir si la reconstruction du vecteur d'état à partir des entrées/sorties est possible. Il y a lieu aussi de vérifier si les conditions nécessaires et/ou suffisantes d'existence sont remplies. Dans ce cas, l'observabilité est fortement liée à la nature des entrées et des non linéarités.

Comme l'observabilité des systèmes non linéaires dépend de l'entrée appliquée au système, elle est donc définie en premier lieu par le concept d'indistinguabilité [221], dite aussi, indiscernabilité définie comme suit :

Définition 7 ***Indiscernabilité***

Deux états $x^1, x^2 \in R^n$, sont dit indiscernables (noté $x^1 I x^2$) si, pour toute entrée admissible $U_k = \{u(0), u(1), \ldots, u(k)\}$ et $\forall k \geq 0$, les deux trajectoires de sorties produites sont identiques, i.e.,

$$\begin{aligned} & h(f(f(\ldots(f(x^1(0)) + g(x^1(0))u(0)) + \ldots) + g(x^1(k-2))u(k-2)) + g(x^1(k-1))u(k-1)) \\ = \;& h(f(f(\ldots(f(x^2(0)) + g(x^2(0))u(0)) + \ldots) + g(x^2(k-2))u(k-2)) + g(x^2(k-1))u(k-1)) \end{aligned} \tag{4.2}$$

Ainsi, la propriété d'observabilité est définie comme suit [221] :

Définition 8 ***Observabilité***

Le système non linéaire (4.1) est dit observable en $x^0 \in R^n$ si l'ensemble des états indiscernables de x^0 ne contient que x^0.

Les notions d'observabilités locale faible et locale forte ont été définies sur un voisinage d'un point x^0 où toutes les paires d'état sont indiscernables, à savoir [222] :

Définition 9 ***Observabilité locale faible***

Le système non linéaire (4.1) est dit localement faiblement observable en x^0 s'il existe un voisinage $\mathcal{W}$ de x^0 tel que :

$$\forall x \in \mathcal{W} \subset R^n, \quad x I x^0$$

De même, le système non linéaire (4.1) est dit localement fortement observable en x^0 s'il existe un voisinage $\mathcal{W} \subset R^n$ de x^0 tel que :

$$\forall x^1, x^2 \in \mathcal{W}, \quad x^1 I x^2 \text{ implique } x^1 = x^2$$

Une condition de rang a été donnée et définie par le concept d'espace d'observabilité défini comme suit [221] :

Définition 10 ***Espace d'observabilité***

Considérons le système dynamique (4.1). L'espace d'observation de ce système est le plus petit espace vectoriel $O(h)$ des fonctions en R^n donné comme suit :

$$O(h) = [h,\, h \circ f,\, \ldots,\, h \circ f^{(n-1)}]^T \tag{4.3}$$

où "$\circ$" indique la fonction usuelle de composition, "$\circ f^{(j)}$" désigne la fonction f composée j fois.

L'espace des différentielles de $O(h)$, nommée $dO(h)$, est définie comme suit :

$$dO = span\{dh, dh \circ f, \ldots, dh \circ f^{(n-1)}\} \tag{4.4}$$

Définition 11 ***Observabilité au sens du rang.***

Le système dynamique (4.1) est dit observable au sens du rang en $x^0 \in R^n$ si :

$$dim\,(dO(h))(x^0) = n \tag{4.5}$$

Le système (4.1) est localement faiblement observable en x^0 dans un voisinage $\mathcal{W}$ s'il satisfait la condition du rang autour de x^0.

Contrairement au cas linéaire, la condition du rang n'est pas suffisante pour la synthèse d'observateur pour un système non linéaire. Les définitions précédente n'excluent pas l'existence des paires indiscernables par l'entrée u, donc l'observabilité d'un système non linéaire dans ce cas ne suffit pas pour synthétiser un observateur, d'où l'importance d'étudier les propriétés des entrées pour la conception d'observateur. Un cas particulier est celui des entrées pour lesquelles le système ne présente pas des paires indiscernables, défini comme suit :

Définition 12 ***Entrées universelles***

Une entrée u est universelle sur $[0\ k]$ si pour tout couple d'états initiaux distincts $x^1 \neq x^2$ il existe $\theta \in [0\ k]$ tel que :

$$\begin{aligned} & h(f(f(\ldots(f(x^1(0)) + g(x^1(0))u(0)) + \ldots) + g(x^1(\theta-2))u(\theta-2)) + g(x^1(\theta-1))u(\theta-1)) \\ = \; & h(f(f(\ldots(f(x^2(0)) + g(x^2(0))u(0)) + \ldots) + g(x^2(\theta-2))u(\theta-2)) + g(x^2(\theta-1))u(\theta-1)) \end{aligned} \tag{4.6}$$

Si l'entrée est non universelle, elle est dite singulière. Ainsi, une condition d'observabilité plus forte, à savoir l'observabilité uniforme, peut être également définie :

Définition 13 ***Observabilité uniforme***

Un système dont toutes les entrées sont universelles sur $[0\ k]$ est dit uniformément localement observable. Et si $\forall k > 0$, les entrées sont universelles, le système est dit uniformément globalement observable.

Une définition particulière pour la classe des systèmes affines en l'entrée, à savoir la définition d'observabilité différentielle (the drift-observability), a été introduite. Elle s'annonce comme suit :

Définition 14 ***Observabilité différentielle (the drift-observability)*** *[223]*

Le système (4.1) est globalement observable au sens de l'observabilité différentielle si et seulement si :

$$z = \begin{bmatrix} h(x) \\ h \circ f(x) \\ \vdots \\ h \circ f^{(n-1)(x)} \end{bmatrix} = \Phi(x) \tag{4.7}$$

est un difféomorphisme global sur R^n.

Les conditions géométriques d'observabilité globale des systèmes non linéaires n'existent pas. L'observabilité locale est utilisée avec des contraintes sur les entrées (bornitude par exemple).

Maintenant, nous considérons le système non linéaire discret d'ordre fractionnaire affine en l'entrée défini comme suit :

$$\begin{cases} \Delta^{\alpha} x(k+1) & = & f(x(k)) + g(x(k))u(k), \qquad x^0 = 0 \\ y(k) & = & h(x(k)) \end{cases} \tag{4.8}$$

Comme il a été déjà mentionné dans la Remarque 2, le système (4.8) peut être considéré comme un système à états retardés. Ainsi, le système (4.8) est réécrit comme suit :

$$\begin{cases} x(k+1) & = & f(x(k)) + g(x(k))u(k) + (\alpha - 1)x(k) - \sum_{p=1}^{L} C_p x(k-p) \\ y(k) & = & h(x(k)) \end{cases} \tag{4.9}$$

Pour étudier l'observabilité de ces systèmes, nous considérons le système augmenté obtenu a partir du changement de variables suivant [43] :

$$\left\{\begin{array}{lll} Z_1(k) & = & x(k) \\ Z_2(k) & = & x(k-1) \\ \vdots & & \\ Z_{L+1}(k) & = & x(k-L) \end{array}\right. \tag{4.10}$$

où $Z_1, Z_2, \ldots, Z_{L+1} \in R^n$. Ainsi, nous obtenons le système augmenté avec les nouvelles variables présenté comme suit :

$$\left\{\begin{array}{lll} Z_1(k+1) & = & f(Z_1(k)) + g(Z_1(k))u(k) \\ & & +(\alpha-1)Z_1(k) - \sum\limits_{p=1}^{L} C_p Z_{p+1}(k) \\ Z_2(k+1) & = & Z_1(k) \\ \vdots & & \\ Z_j(k+1) & = & Z_{j-1}(k) \\ \vdots & & \\ Z_{L+1}(k) & = & Z_L(k) \\ y(k) & = & h(Z_1(k)) \end{array}\right. \tag{4.11}$$

où $j = 2, \ldots, L+1$.

Le système (4.11) peut être réécrit sous la forme suivante :

$$\left\{\begin{array}{lll} Z(k+1) & = & F(Z(k)) + G(Z(k))u(k) \\ y(k) & = & H(Z(k)) \end{array}\right. \tag{4.12}$$

où $Z(k) = [Z_1, Z_2, \ldots, Z_{L+1}] \in R^{n'}$ est le nouveau vecteur d'état et $n' = n(L+1)$.

Proposition 1 *L'espace d'observabilité $O'(H)$ du système (4.12) est également donné par l'espace linéaire des fonctions en $R^{n'}$ présenté comme suit*

$$O'(H) = [H, H \circ F, \ldots, H \circ F^{(n'-1)}]^T \tag{4.13}$$

Avec F est le champ vectoriel du système augmenté (4.12) et H est la fonction de sortie.

Dans ce cas, l'espace des différentielles de $O'(H)$ est donné comme suit :

$$dO'(H) = span\{dH, dH \circ F, \ldots, dH \circ F^{(n'-1)}\} \tag{4.14}$$

Ainsi, le théorème concernant l'observabilité local des systèmes discrets d'ordre fractionnaire est donné comme suit :

Théorème 1 *[43] Le système non linéaire discret d'ordre fractionnaire modélisé par (4.12) est observable si et seulement si*

$$dim\ (dO'(H)) = n' \tag{4.15}$$

Démonstration 1 *. Supposons $dim\,(dO'(H)) = n'$. Alors, il existe n' fonctions $\Gamma_i(.) = \Gamma_1, \ldots, \Gamma_{n'} \in O$, où $\Gamma_1 = H$, $\Gamma_2 = H \circ F$, ..., $\Gamma_{n'} = H \circ F^{(n'-1)}$, dont les différentielles sont linéairement indépendantes à Z^0. Par continuité, elles restent indépendantes dans un voisinage $\mathcal{W}_{Z^0}$ de Z^0. Par conséquent, $\Gamma_i(.)$ définit une fonction unie de $R^{n'}$ à R, qui est injective dans $\mathcal{W}_{Z^0}$. Soit $Z^1 \in \mathcal{W}_{Z^0}$, si $Z^1 I Z^0$, en particulier, pour chaque $i = 1, \ldots, n'$, alors $\Gamma_i(Z^0) = \Gamma_i(Z^1)$. Par l'injectivité de $\Gamma_i(.)$, $i = 1, \ldots, n'$, il en résulte $Z^0 = Z^1$. Ainsi, Z^0 est un état localement observable.*

4.2.2 Condition de recouvrement d'observabilité

Dans cette partie, nous proposons un nouveau résultat sur la condition de recouvrement d'observabilité pour les systèmes non linéaires discrets d'ordre fractionnaire [43]. Cette condition montre la possibilité d'observer l'entrée inconnue du système à partir de la sortie, mais à condition que cette entrée soit bornée. Pour ce faire, nous commençons par présenter cette condition pour les systèmes d'ordre entier.

Considérons le système non linéaire donné par l'équation (4.1), dans le quel l'entrée est considérée inconnue et bornée. La condition de recouvrement d'observabilité du système (4.1) est donnée dans [18] par la définition suivante.

Définition 15 *La condition de recouvrement d'observabilité du système (4.1) est :*

$$\left((dh)(dh \circ f) \ldots (dh \circ f^{(n-1)})\right)^T g = (0 \ \ldots \ 0 \, *)^T \tag{4.16}$$

où "$*$" signifie un terme non nul partout au voisinage de x_0.

Pour étudier la condition de recouvrement pour le système discret d'ordre fractionnaire défini par (4.9), le théorème suivant est donné :

Théorème 2 *[43] La condition de recouvrement des systèmes non linéaires discrets d'ordre fractionnaire modélisés par (4.9) est :*

$$\left((dh)(dh \circ \tilde{f}) \ldots (dh \circ \tilde{f}^{(n-1)})\right)^T g = (0 \ \ldots \ 0 \, *)^T \tag{4.17}$$

où $\tilde{f} = f(x(k)) + (\alpha - 1)x(k) + \beta(x(k))$ et $\beta(x(k)) \in R^n$ est un vecteur de dimension n des fonction linéaires par rapport aux états retardés $x(k-j)$, avec $j = 1, \ldots, L$, donné par

$$\beta(x(k)) = [\beta_1(x_1(k)), \beta_2(x_2(k)), \ldots, \beta_n(x_n(k))]^T$$

où $\beta_i(x_i(k)) = -\sum_{j=1}^{L} C_{ij} x_i(k-j)$, $i = 1, \ldots, n$, et $C_{ij} = (-1)^{j+1}\binom{\alpha_i}{j+1}$.

Démonstration 2 *Considérons le système (4.9) qui peut être présenté comme suit :*

$$\begin{cases} x(k+1) &= f(x(k)) + g(x(k))u(k) + (\alpha - 1)x(k) + \beta(x(k)) \\ y(k) &= h(x(k)) \end{cases} \tag{4.18}$$

Définissons la dérivée de $\beta_i(x_i)$ par rapport à x_i comme $\frac{d\beta_i(x_i)}{dx_i}$. Comme il a été déjà mentionné, la fonction $\beta_i(x_i)$ est linéaire par rapport à $x_i(k-j)$ et les coefficients C_{ij} sont constants, ainsi nous obtenons

$$\frac{d\beta_i(x_i)}{dx_i} = -\sum_{j=1}^{L} C_{ij} \tag{4.19}$$

Le système (4.18) peut ainsi être réécrit sous la forme suivante :

$$\begin{cases} x(k+1) &= \tilde{f}(x(k)) + g(x(k))u(k) \\ y(k) &= h(x(k)) \end{cases} \tag{4.20}$$

Ainsi, l'application de la Définition.15 complète la démonstration.

4.3 Synthèse de l'observateur discret retardé étape par étape

Dans cette thèse, nous proposons un observateur exact à savoir l'observateur discret retardé étape par étape [42, 43]. Cet observateur permet de reconstruire tout les états et l'entrée inconnue du système d'ordre fractionnaire à partir de la sortie du système transmise et de ses itérés. Dans un premier lieu, nous considérons que l'entrée est connue et nous nous intéressons qu'à la reconstruction des états.
Considérons à nouveau le système chaotique discret d'ordre fractionnaire affine en l'entrée (4.20), mais cette fois-ci nous prenons le champ de vecteur $g(x)$ pour un vecteur constant, appelé B. Ainsi, le système est représenté comme suit :

$$\begin{cases} x(k+1) &= \tilde{f}(x(k)) + Bu(k) \\ y(k) &= h(x(k)) \end{cases} \tag{4.21}$$

La conception d'un observateur à entrée inconnue est réalisable si les conditions données par les hypothèses suivantes sont vérifiées :
Hypothèse 1 Le système (4.21) est observable.
Hypothèse 2 La condition de recouvrement d'observabilité du système (4.21) est vérifiée.
Hypothèse 3 Nous supposons que l'ensemble des entrées appliquées et sorties obtenues, avant $k = 0$, est connu à partir de l'instant $1 - n$, c'est à dire que $y(k)$ et $u(k)$, pour $1 - n < k < 0$, sont connues.
Hypothèse 4 L'entrée inconnue est bornée.

Utilisons le système (4.21) dans sa forme itérative, nous trouvons :

$$\begin{aligned} x(k) &= \tilde{f}(x(k-1)) + Bu(k-1) \\ &= \tilde{f}(\tilde{f}(x(k-2)) + Bu(k-2)) + Bu(k-1) \\ &= \tilde{f}(\tilde{f}(\tilde{f}(x(k-3)) + Bu(k-3)) + Bu(k-2)) + Bu(k-1) \\ &\vdots \\ &= \tilde{f}(\tilde{f}(\ldots(\tilde{f}(x(k-(n-1))) + Bu(k-(n-1))) + \ldots) + Bu(k-2)) + Bu(k-1) \end{aligned} \tag{4.22}$$

Les éléments avancés dans une séquence finie du vecteur de sortie, $y(k)$, sont donnés par :

$$\begin{aligned} y(k) &= h(x(k)) \\ y(k+1) &= h(x(k+1)) = h(\tilde{f}x(k) + Bu(k)) \\ y(k+2) &= h(\tilde{f}x(k+1) + Bu(k+1)) \\ &= h(\tilde{f}(\tilde{f}(x(k)) + Bu(k)) + Bu(k+1)) \\ &\vdots \\ y(k+(n-1)) &= h(x(k+(n-1))) \\ &= h(\tilde{f}(\tilde{f}(\ldots(\tilde{f}(x(k)) + Bu(k)) + \ldots) + Bu(k+(n-3))) + Bu(k+(n-2))) \end{aligned} \tag{4.23}$$

La proposition suivante montre que l'observateur retardé étape par étape est constructible :

Proposition 2 *[43] Supposons que le système chaotique discret d'ordre fractionnaire (4.21) est observable et vérifie la condition de recouvrement d'observabilité et que l'entrée $u(k)$ est bornée. Alors, le système est constructible, c'est-à-dire qu'il existe un système $\Psi : R^n \to R^n$ tel que tout les états, $x(k)$, du système peuvent être exactement reconstruits en termes de la sortie et de l'ensemble fini des entrées appliquées et des sorties obtenues, sous la forme :*

$$x(k) = \Psi(y(k), y(k-1), \ldots, y(k-(n-1)), u(k-1), \ldots, u(k-(n-1))), \qquad k \geq 0 \tag{4.24}$$

où l'ensemble des entrées et sorties $u(k), y(k)$, pour $-n+1 < k \leq 0$, est complètement *connu.*

Démonstration 3 *Selon les hypothèses énoncées, il existe un système Φ tel que l'ensemble des équations,*

$$\begin{bmatrix} y(k) \\ y(k+1) \\ \vdots \\ y(k+(n-1)) \end{bmatrix} = \begin{bmatrix} h(x(k)) \\ h(\tilde{f}x(k)+Bu(k)) \\ \vdots \\ h(\tilde{f}(\tilde{f}(\ldots(\tilde{f}(x(k))+Bu(k))+\ldots)+Bu(k+(n-3)))+Bu(k+(n-2))) \end{bmatrix} \tag{4.25}$$

a une solution $x(k)$, exprimée par une fonction Φ, de la forme :

$$x(k) = \Phi(y(k), y(k+1), \ldots, y(k+(n-1), u(k), \ldots, u(k+(n-2))) \tag{4.26}$$

Si nous appliquons $n-1$ retards dans l'expression (4.26), nous obtenons :

$$x(k-(n-1)) = \Phi(y(k), y(k-1), \ldots, y(k-(n-1)), u(k-1), \ldots, u(k-(n-1))) \tag{4.27}$$

En substituant l'équation (4.27) dans l'équation (4.22), nous trouvons :

$$\begin{aligned} x(k) &= \tilde{f}(\tilde{f}(\ldots(\tilde{f}(\Phi(y(k),y(k-1),\ldots,y(k-(n-1)),u(k-1),\ldots,u(k-(n-1))))+Bu(k-(n-1)))+\ldots)+Bu(k-2))+Bu(k-1) \\ &= \Psi(y(k), y(k-1), \ldots, y(k-(n-1)), u(k-1), \ldots, u(k-(n-1))) \end{aligned} \tag{4.28}$$

Ainsi, il est clair que l'état estimé $x(k)$ peut être exactement reconstruit à partir des entrées/sorties retardées. La preuve est ainsi démontrée.

Dans la deuxième partie de cette section, nous traitons le problème de la reconstruction des états et de l'entrée considérée maintenant inconnue. Pour ce faire, nous considérons la forme observable du système (4.8), donnée comme suit :

$$\begin{cases} \Delta^{\alpha}x(k+1) &= Ax(k) + \Gamma(x(k)) + g(x(k))u(k) \\ y(k) &= Cx(k) \end{cases} \tag{4.29}$$

Les matrices A et C du système sont sous la forme de Brunovski suivante [224] :

$$A = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & 0 & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 0 \end{bmatrix}; \qquad C = [1\ 0\ \dots\ 0] \tag{4.30}$$

Le vecteur de fonctions non linéaires $\Gamma(x(t))$ possède la structure triangulaire suivante

$$\Gamma(x) = \begin{pmatrix} \Gamma_1(x_1) \\ \Gamma_2(x_1, x_2) \\ \Gamma_3(x_1, x_2, x_3) \\ \vdots \\ \Gamma_n(x_1, x_2, x_3, \dots, x_n) \end{pmatrix}$$

et le champ de vecteur $g(x)$ est donné par $g(x) = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ b_n(x) \end{pmatrix}$, avec $b_n(x) \neq 0\ \forall x(k) \in \mathcal{W} \subset R^n$. Cela veut dire que l'entrée inconnue affecte seulement la dynamique de la dernière variable $x_n(k)$. Dans le cas général, les systèmes non linéaires d'ordre fractionnaire ne sont pas donné sous cette forme particulière. Toutefois, si ces systèmes satisfont la condition d'observabilité, cette forme peut être obtenue après un changement de coordonnés approprié. Avec cette forme, l'espace des différentielles de $O_{n-1}(x)$ ne dépend pas de l'entrée inconnue u. Cela implique que l'état $x(k)$ dans l'équation (4.28) ne dépend pas de l'entrée, i.e.,

$$x(k) = \Psi(y(k), y(k-1), \dots, y(k-(n-1))) \tag{4.31}$$

L'état $x(k)$ est uniquement reconstruit à partir de la sortie. L'entrée $u(k)$ apparaît explicitement dans l'équation suivante :

$$y(k+n) = \tilde{\Gamma}(x(k)) + b_n(x(k))u(k) \tag{4.32}$$

où $\tilde{\Gamma}(x(k))$ est la fonction composée de $\Gamma_i(x(t))$, $i = 1, 2, \ldots, n$. La relation (4.32) signifie que l'entrée dépend des sorties avancées. Il s'ensuit que, si $b(x) \neq 0$, $\forall x(k) \in \mathcal{W} \subset R^n$, l'entrée inconnue $u(k)$ peut être exactement reconstruite après n retard à partir de l'état estimé $x(k)$ et des sorties passées.

4.4 Application de la synchronisation à base d'observateur à la transmission sécurisée de données

Dans cette section, un nouveau schéma de transmission sécurisée basé sur la synchronisation des systèmes chaotiques discrets d'ordre fractionnaire est proposé [42]. Le système chaotique utilisé est le système de Hénon modifié d'ordre fractionnaire. Dans ce qui suit, la méthode développée est présentée.

4.4.1 Présentation du système de Hénon modifié d'ordre fractionnaire

Considérons le système de Hénon modifié d'ordre entier donné par l'équation suivante :

$$\begin{cases} x_1(k+1) &= a - x_2^2(k) - b\,x_3(k) \\ x_2(k+1) &= x_1(k) \\ x_3(k+1) &= x_2(k) \\ y(k) &= x_2(k) \end{cases} \tag{4.33}$$

où $x = [x_1,\, x_2,\, x_3]^T \in R^3$ est le vecteur d'état et $y(k) \in R$ est la sortie.

En utilisant l'équation (3.40), le système de Hénon modifié d'ordre fractionnaire est exprimé par :

$$\begin{cases} x_1(k+1) &= a - x_2^2(k) - b\,x_3(k) + (\alpha_1 - 1)x_1(k) - \sum\limits_{j=1}^{L} C_{1j}x_1(k-j) \\ x_2(k+1) &= x_1(k) + (\alpha_2 - 1)x_2(k) - \sum\limits_{j=1}^{L} C_{2j}x_2(k-j) \\ x_3(k+1) &= x_2(k) + (\alpha_3 - 1)x_3(k) - \sum\limits_{j=1}^{L} C_{3j}x_3(k-j) \\ y(k) &= x_2(k) \end{cases} \tag{4.34}$$

où $0 < \alpha_i < 1$, $i = 1, 2, 3$. En posant $\beta_i(x_i(k)) = -\sum\limits_{j=1}^{L} C_{ij}x_i(k-j)$, $i = 1, 2, 3$. Le système (4.34) peut être réécrit sous la forme suivante :

$$\begin{cases} x_1(k+1) &= a - x_2^2(k) - bx_3(k) + (\alpha_1 - 1)x_1(k) + \beta_1(x_1(k)) \\ x_2(k+1) &= x_1(k) + (\alpha_2 - 1)x_2(k) + \beta_2(x_2(k)) \\ x_3(k+1) &= x_2(k) + (\alpha_3 - 1)x_3(k) + \beta_3(x_3(k)) \\ y(k) &= x_2(k) \end{cases} \tag{4.35}$$

Le système (4.35) fait preuve d'un comportement hyper-chaotique pour les ordres $\alpha_1 = 0.85$, $\alpha_2 = 0.8$ et $\alpha_3 = 0.8$, et pour les paramètres $a = 1.55$, $b = 0.1$. Les conditions initiales $x_1(0) = -0.1$, $x_2(0) = 0.5$ et $x_3(0) = 0.1$ sont choisies à l'intérieur du bassin d'attraction. En effet, le calcul des exposants de Lyapunov démontre la présence de l'hyper-chaos, puisque deux exposants de Lyapunov positifs sont trouvés. Dans notre travail, nous avons adapté l'algorithme de Wolf et al. [225] à notre système. Pour simplifier les calculs, nous choisissons la taille de la mémoire du système $L = 1$. Ainsi, le système augmenté correspondant, en utilisant le changement de variables (4.10), présentera 6 états et 6 exposants de Lyapunov. Les exposants de Lyapunov du système (4.35) sont présentés par la figure 4.1, où deux exposants sont positifs ($\lambda_1 = 0.0656$, et $\lambda_2 = 0.020$), ce qui prouve le comportement hyper-chaotique du système.

Le comportement chaotique du système (4.35) est illustré par les résultats de simulation suivants. La sensibilité aux condition initiales du système est présentée par les figures 4.2 et 4.3 ; dans la première figure, le phénomène est illustré pour une petite variation dans

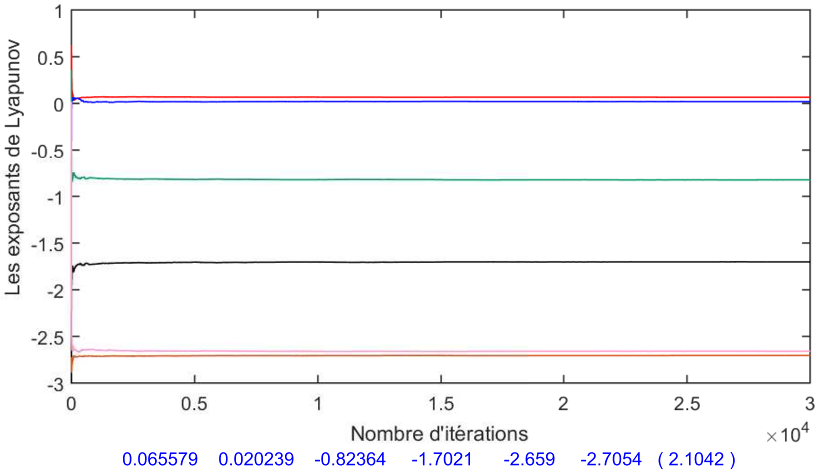


FIGURE 4.1: Les exposants de Lyapunov du système de Hénon modifié d'ordre fractionnaire.

l'ordre α_1, et dans la deuxième figure, c'est le paramètre a qui est légèrement modifié. Le diagramme de bifurcation est donné par la figure 4.4, il est obtenu en variant le paramètre a du système (4.35). En effet, ce système présente un comportement chaotique lorsque $a \in [1.3, 1.7]$. Le plan de phase (x_1, x_3) est exposé dans la figure 4.5.

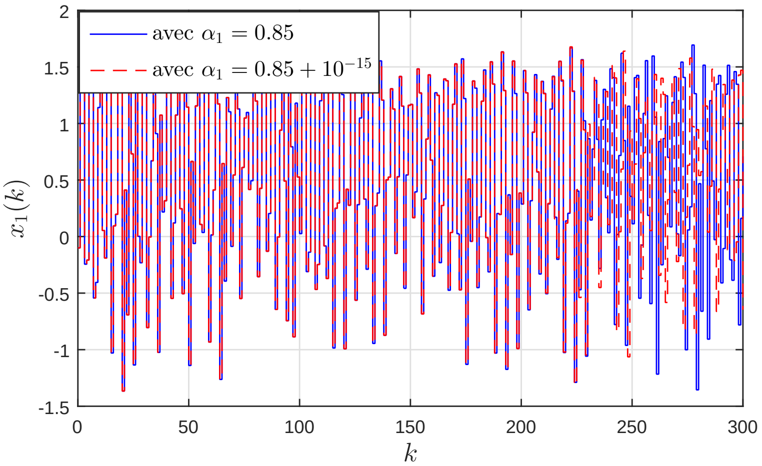


FIGURE 4.2: L'état x_1 du système de Hénon modifié d'ordre fractionnaire pour une petite variation de l'ordre α_1.

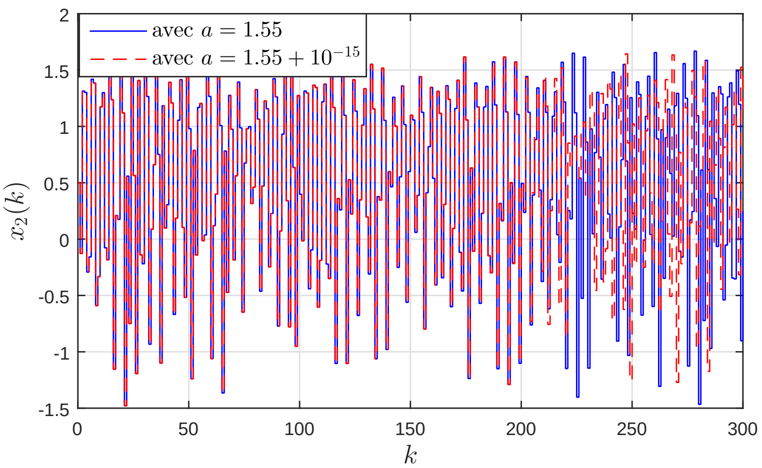


FIGURE 4.3: L'état x_2 du système de Hénon modifié d'ordre fractionnaire pour une petite variation du paramètre a.

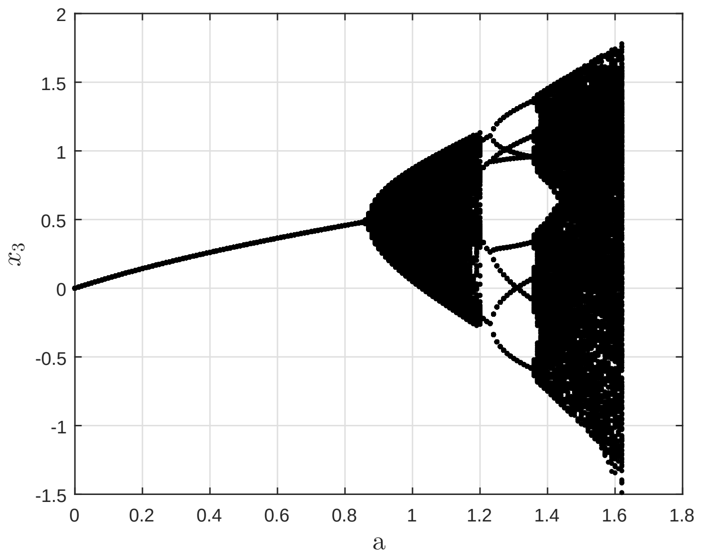


FIGURE 4.4: Le diagramme de bifurcation de l'état x_3 du système de Hénon modifié d'ordre fractionnaire pour $a \in [0, 1.7]$.

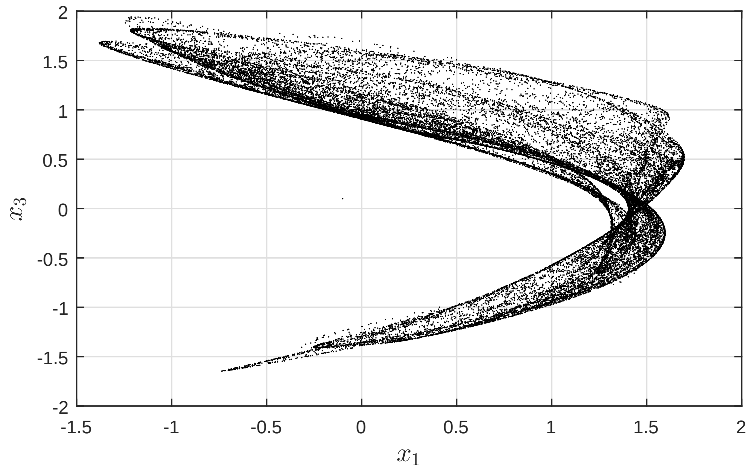


FIGURE 4.5: Le plan de phase des états x_1, x_3 du système de Hénon modifié d'ordre fractionnaire.

4.4.2 Observabilité du système de Hénon modifié d'ordre fractionnaire

Pour étudier l'observabilité du système (4.35), nous utilisons le changement de variables donné par l'équation(4.10). Ainsi, nous obtenons le système augmenté correspondant. Afin de simplifier les équations du système, nous choisissons $L = 1$ [43]. Les équations d'état du système initial sont donné comme suit :

$$\begin{cases} x_1(k+1) &= a - x_2^2(k) - bx_3(k) + (\alpha_1 - 1)x_1(k) - C_{11}x_1(k-1) \\ x_2(k+1) &= x_1(k) + (\alpha_2 - 1)x_2(k) - C_{21}x_2(k-1) \\ x_3(k+1) &= x_2(k) + (\alpha_3 - 1)x_3(k) - C_{31}x_3(k-1) \\ y(k) &= x_2(k) \end{cases} \tag{4.36}$$

Après le changement de variables déjà présenté, nous obtenons le système augmenté comme suit :

$$\left\{\begin{array}{lcl} z_1(k+1) & = & a - z_2^2(k) - bz_3(k) + (\alpha_1 - 1)z_1(k) - C_{11}z_4(k) \\ z_2(k+1) & = & z_1(k) + (\alpha_2 - 1)z_2(k) - C_{21}z_5(k) \\ z_3(k+1) & = & z_2(k) + (\alpha_3 - 1)z_3(k) - C_{31}z_6(k) \\ z_4(k+1) & = & z_1(k) \\ z_5(k+1) & = & z_2(k) \\ z_6(k+1) & = & z_3(k) \\ y(k) & = & z_2(k) \end{array}\right. \tag{4.37}$$

En utilisant la Proposition 1, l'espace des différentielles de $O'(H)$ du système (4.37) est obtenue comme suit :

$$dO' = span\{dH, dH \circ F, dH \circ F^2, \dots, dH \circ F^5\} \tag{4.38}$$

où :

$$dO' = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & -0.2 & 0 & 0 & 0.08 & 0 \\ -0.35 & \gamma_1 & -0.1 & 6.375 \times 10^{-2} & -0.016 & 0 \\ \gamma_2 & \gamma_3 & 0.055 & -2.2312 \times 10^{-2} & \gamma_4 & -0.008 \\ \gamma_5 & \gamma_6 & \gamma_7 & \gamma_8 & \gamma_9 & 4.4 \times 10^{-3} \\ \gamma_{10} & \gamma_{11} & \gamma_{12} & \gamma_{13} & \gamma_{14} & \gamma_{15} \end{pmatrix}$$

$$
\begin{cases}
\gamma_1 &= 0.12 - 2z_2 \\
\gamma_2 &= 0.23625 - 2z_2 \\
\gamma_3 &= 1.5z_2 - 2z_1 - 0.16z_5 - 0.14 \\
\gamma_4 &= 9.6 \times 10^{-3} - 0.16z_2 \\
\gamma_5 &= 2.2z_2 - 4z_1 - 0.32z_5 - 0.19775 \\
\gamma_6 &= 2.2z_1 - 0.92z_2 + 0.2z_3 - 0.1275z_4 + 0.152z_5 - 2z_2\gamma_2 + 2z_2^2 - 3.0074 \\
\gamma_7 &= 0.2z_2 - 4.2625 \times 10^{-2} \\
\gamma_8 &= 1.506 \times 10^{-2} - 0.1275z_2 \\
\gamma_9 &= 0.152z_2 - 0.32z_1 - 2.56 \times 10^{-2}z_5 - 1.12 \times 10^{-2} \\
\gamma_{10} &= 5.6z_1 - 2.1375z_2 + 0.6z_3 - 0.3825z_4 + 0.376z_5 - 2z_2\gamma_2 + 6z_2^2 - 9.1627 \\
\gamma_{11} &= 0.888z_2 - 1.2175z_1 - 0.3z_3 + 0.1658z_4 - 0.056z_5 + 0.016z_6 + 0.4z_2\gamma_2 + (12z_2 \\
&\quad -1.3925)(z_1 - 0.2z_2 + 0.08z_5) + 2z_2(4z_1 - 2.2z_2 + 0.32z_5 + 0.1978) - 2.6z_2^2 \\
&\quad +3.958 \\
\gamma_{12} &= 0.6z_1 - 0.3z_2 + 0.048z_5 + 0.0327 \\
\gamma_{13} &= 0.16575z_2 - 0.3825z_1 - 3.06 \times 10^{-2}z_5 - 1.2606 \times 10^{-2} \\
\gamma_{14} &= 0.376z_1 - 0.1296z_2 + 0.048z_3 - 3.06 \times 10^{-2}z_4 + 2.432 \times 10^{-2}z_5 - 0.16z_2\gamma_2 \\
&\quad +0.48z_2^2 - 0.7366 \\
\gamma_{15} &= 0.016z_2 - 3.41 \times 10^{-3}
\end{cases}
$$

En appliquant le théorème 1, nous obtenons

$$dim\, dO' = 6 \tag{4.39}$$

Il est à noter que l'observabilité du système (4.37) est vérifiée pour une taille de mémoire $L > 1$. Par conséquent, le système (4.37) est observable, ainsi, nous déduisons que le système (4.35) est observable, ce qui garantit l'estimation de tout ses états. Ce résultat motive le choix de la sortie $y(k) = x_2(k)$.

4.4.3 Condition de recouvrement du système de Hénon modifié d'ordre fractionnaire

Dans cette section, nous vérifions la condition de recouvrement du système (4.35) [43]. Pour ce faire, nous insérons l'entrée, qui correspond au message secret dans notre application, au troisième état de notre système. De cette manière, le système (4.35) va être réécrit comme suit :

$$\begin{cases} x_1(k+1) &= a - x_2^2(k) - bx_3(k) + (\alpha_1 - 1)x_1(k) + \beta_1(x_1(k)) \\ x_2(k+1) &= x_1(k) + (\alpha_2 - 1)x_2(k) + \beta_2(x_2(k)) \\ x_3(k+1) &= x_2(k) + (\alpha_3 - 1)x_3(k) + \beta_3(x_3(k)) + u(k) \\ y(k) &= x_2(k) \end{cases} \tag{4.40}$$

Ainsi, nous avons :

$$g(x(k)) = B = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

Maintenant, nous allons calculer $[dh \quad dh \circ \tilde{f} \quad dh \circ \tilde{f}^{(2)}]^T$. Pour ce faire, il faut d'abord calculer $h(x)$, $h \circ \tilde{f}(x)$ et $h \circ \tilde{f}^{(2)}(x)$

$$\begin{cases} h(x) &= x_2(k) \\ h \circ \tilde{f}(x) &= x_2(k+1) \\ &= x_1(k) + (\alpha_2 - 1)x_2(k) - \sum_{j=1}^{L} C_{2j} x_2(k-j) \\ h \circ \tilde{f}^{(2)}(x) &= x_1(k+1) + (\alpha_2 - 1)x_2(k+1) - \sum_{j=1}^{L} C_{2j} x_2(k-j+1) \\ &= a - x_2^2(k) - bx_3(k) + (\alpha_1 - 1)x_1(k) - \sum_{j=1}^{L} C_{1j} x_1(k-j) \\ &\quad +(\alpha_2 - 1)[x_1(k) + (\alpha_2 - 1)x_2(k) - \sum_{j=1}^{L} C_{2j} x_2(k-j)] \\ &\quad - \sum_{j=1}^{L} C_{2j} x_2(k-j+1) \end{cases} \tag{4.41}$$

Ainsi, nous obtenons

$$\begin{pmatrix} dh \\ dh \circ \tilde{f} \\ dh \circ \tilde{f}^{(2)} \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & \sigma_1 & 0 \\ \sigma_2 & \sigma_3 & -b \end{pmatrix} \tag{4.42}$$

où

$$\left\{ \begin{array}{lcl} \sigma_1 & = & (\alpha_2 - 1) - \sum\limits_{j=1}^{L} C_{2j} \\ \sigma_2 & = & \alpha_1 + \alpha_2 - 2 - \sum\limits_{j=1}^{L} C_{1j} \\ \sigma_3 & = & (\alpha_2 - 1)^2 - 2x_2 - (\alpha_2 - 1)(-\sum\limits_{j=1}^{L} C_{2j}) - \sum\limits_{j=1}^{L} C_{2j} \end{array} \right.$$

En utilisant l'équation (4.17), donnée par le théorème 2, nous obtenons

$$\begin{pmatrix} dh \\ dh \circ \tilde{f} \\ dh \circ \tilde{f}^{(2)} \end{pmatrix} g = \begin{pmatrix} 0 & 1 & 0 \\ 1 & \sigma_1 & 0 \\ \sigma_2 & \sigma_3 & -b \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ -b \end{pmatrix} \tag{4.43}$$

Il est clair que $b \neq 0$, ce qui prouve que la condition de recouvrement est satisfaite. De cette manière, le choix du vecteur d'entrée $g(x)$ est satisfaisant.

4.4.4 Schéma de transmission sécurisée proposé

Dans cette section, nous proposons un schéma de transmission sécurisée de données basé sur la synchronisation des systèmes chaotiques d'ordre fractionnaire à l'aide d'observateur [42]. Le diagramme bloc de notre schéma est présenté par la figure 4.6. Ce dernier est composé principalement d'un émetteur et d'un récepteur.

Au niveau de l'émetteur, qui correspond au système de Hénon modifié d'ordre fractionnaire (4.40), le message est chiffré en utilisant la méthode de chiffrement par inclusion (décrite au chapitre 1). Dans notre travail de thèse, le message est ajouté dans la troisième dynamique du système et ceci afin de satisfaire la condition de recouvrement. Par contre, le signal transmis au récepteur est l'état x_2. Il est important de noter que le message doit être bornée et assez petit afin de préserver le comportement chaotique. Dans notre cas, nous choisissons deux types de signaux (rectangulaire et sinusoïdale). Comme montré

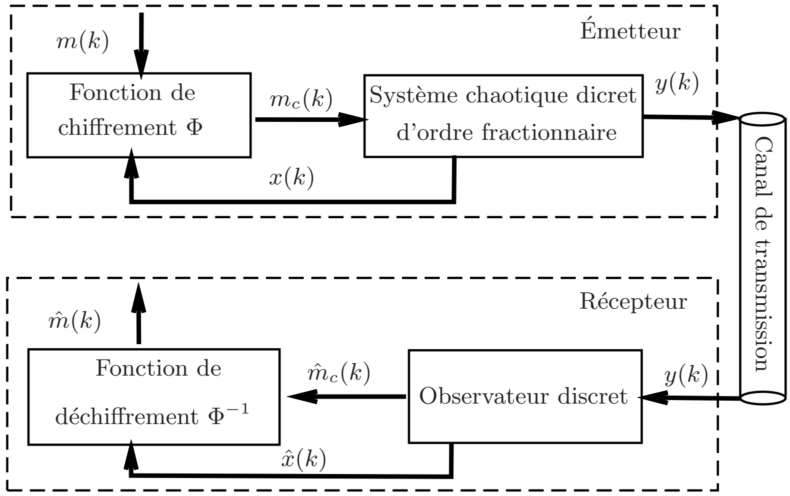


FIGURE 4.6: Le diagramme bloc du schéma de transmission sécurisée.

dans la figure 4.6, le message $m(k)$ est d'abord chiffré par une fonction de chiffrement Φ, puis, introduit dans la troisième dynamique du système (4.40). Ainsi, nous obtenons :

$$\begin{cases} x_1(k+1) &= a - x_2^2(k) - bx_3(k) + (\alpha_1 - 1)x_1(k) + \beta_1(x_1(k)) \\ x_2(k+1) &= x_1(k) + (\alpha_2 - 1)x_2(k) + \beta_2(x_2(k)) \\ x_3(k+1) &= x_2(k) + (\alpha_3 - 1)x_3(k) + \beta_3(x_3(k)) + m_c(k) \\ y(k) &= x_2(k) \end{cases} \tag{4.44}$$

où $m_c(k)$ est choisit tel que :

$$\begin{aligned} m_c(k) &= \Phi(x_1(k), x_3(k), m(k)) \\ &= m(k) + cx_1(k) + dx_3(k) + ex_1^2(k) + fx_3^2(k) + gx_1(k)x_3(k) + hx_1^2(k)x_3(k) \end{aligned} \tag{4.45}$$

avec c, d, e, f, g et h sont les nouvelles clés secrètes du système (4.44). Afin de préserver le comportement chaotique de notre système, ces clés sont choisies avec précaution.
Au niveau du récepteur, en se basant sur les travaux de [118], un observateur retardé étape par étape est réalisé pour résoudre le problème de synchronisation, et pour permettre la reconstruction des états et de l'entrée inconnue (message). Pour cette fin, nous présentons la proposition suivante :

Proposition 3 *[43] Supposons que le système chaotique discret d'ordre fractionnaire*

(4.44) soit observable et vérifie la condition de recouvrement d'observabilité. Alors, le système est constructible, c'est-à-dire qu'il existe un système $\phi : R \to R^3$ tel que l'état $x(k)$ du système peut être exactement reconstruit en termes de sortie et de l'ensemble fini de sorties obtenues, sous la forme :

$$\begin{aligned}
xo_2 &= \phi_2(y(k)) \\
&= y(k) \\
xo_1(k-1) &= \phi_1(y(k), y(k-1)) \\
&= y(k) - (\alpha_2 - 1)y(k-1) - \beta_2(y(k-1)) \\
xo_3(k-2) &= \phi_3(y(k), y(k-1), y(k-2)) \\
&= \tfrac{1}{b}(a - y^2(k-2) + (\alpha_1 - 1)(y(k-1) - (\alpha_2 - 1)(y(k-2) - \beta_2(y(k-2))) \\
&\quad -y(k) + \beta_1(\phi_1(y(k-1), y(k-2))) + (\alpha_2 - 1)y(k-1) + \beta_2(y(k-1)))
\end{aligned} \tag{4.46}$$

où $\phi = [\phi_1, \phi_2, \phi_3]^T$.
De plus, il existe un autre système ψ tel que l'entrée inconnues $mo_c(k)$ du système peut être exactement reconstruite en termes d'états estimés obtenus sous la forme :

$$\begin{aligned}
mo_c(k-3) &= \psi(xo_1, xo_2, xo_3) \\
&= xo_3(k-2) - xo_2(k-3) - (\alpha_3 - 1)xo_3(k-3) + \beta_3(xo_3(k-3))
\end{aligned} \tag{4.47}$$

Démonstration 4 *Réécrivons le système (4.44) comme suit :*

$$\left\{ \begin{aligned}
x_1(k+1) &= f_1(x_1(k), x_2(k), x_3(k)) \\
x_2(k+1) &= f_2(x_1(k), x_2(k)) \\
x_3(k+1) &= f_3(x_2(k), x_3(k)) + m_c(k) \\
y(k) &= x_2(k)
\end{aligned} \right. \tag{4.48}$$

Il est clair que l'état estimé xo_2 peut être exprimé comme suit :

$$\begin{aligned}
xo_2(k) &= y(k) \\
&= \phi_2(y(k))
\end{aligned} \tag{4.49}$$

Si nous appliquons un retard sur le deuxième état du système (4.48), nous obtenons :

$$\begin{aligned} xo_2(k) &= f_2(xo_1(k-1), xo_2(k-1)) \\ &= xo_1(k-1) + (\alpha_2 - 1)xo_2(k-1) + \beta_2(xo_2(k-1)) \end{aligned} \tag{4.50}$$

avec $\beta_2(xo_2(k-1)) = \sum_{j=1}^{L} C_{2j} xo_2(k-j-1)$.
Ensuite, à partir de l'équation (4.50), nous pouvons déduire $xo_1(k-1)$ *comme suit :*

$$\begin{aligned} xo_1(k-1) &= y(k) - (\alpha_2 - 1)y(k-1) - \beta_2(y(k-1)) \\ &= \phi_1(y(k), (k-1)) \end{aligned} \tag{4.51}$$

Si nous appliquons deux retards sur le premier état du système (4.48), nous obtenons :

$$\begin{aligned} xo_1(k-1) &= f_1(xo_1(k-2), xo_2(k-2), xo_3(k-2)) \\ &= a - xo_2^2(k-2) - bxo_3(k-2) + (\alpha_1 - 1)xo_1(k-2) + \beta_1(xo_1(k-2)) \end{aligned} \tag{4.52}$$

avec $\beta_1(xo_1(k-2)) = \sum_{j=1}^{L} C_{1j} xo_1(k-j-2)$.
Ainsi, à partir de l'équation (4.52), nous pouvons déduire $xo_3(k-2)$ *comme suit :*

$$\begin{aligned} xo_3(k-2) &= \tfrac{1}{b}[a - y^2(k-2) + (\alpha_1 - 1)(y(k-1) - (\alpha_2 - 1)(y(k-2) - \beta_2(y(k-2))) \\ &\quad -y(k) + \beta_1(xo_1(k-2)) + (\alpha_2 - 1)y(k-1) + \beta_2(y(k-1))] \\ &= \phi_3(y(k), y(k-1), y(k-2)) \end{aligned} \tag{4.53}$$

Si nous appliquons trois retards sur le troisième état du système (4.48), nous obtenons :

$$\begin{aligned} xo_3(k-2) &= f_3(x_2(k-3), x_3(k-3)) + m_c(k-3) \\ &= xo_2(k-3) + (\alpha_3 - 1)xo_3(k-3) + \beta_3(xo_3(k-3)) + mo_c(k-3) \end{aligned} \tag{4.54}$$

avec $\beta_3(xo_3(k-3)) = \sum_{j=1}^{L} C_{3j} xo_3(k-j-3)$. *En utilisant les états estimés* xo_1, xo_2, xo_3 *et* *à partir de l'équation (4.54), l'entrée estimée est obtenue comme suit :*

$$\begin{aligned} mo_c(k-3) &= xo_3(k-2) - xo_2(k-3) - (\alpha_3 - 1)xo_3(k-3) + \beta_3(xo_3(k-3)) \\ &= \psi(xo_1, xo_2, xo_3) \end{aligned} \quad (4.55)$$

C'est ce qu'il faut démontrer.

Finalement, le déchiffrement du message chiffré est effectué en utilisant la fonction de déchiffrement Φ^{-1}. Ainsi, le message $m(k)$ est obtenu comme suit :

$$\begin{aligned} mo(k) &= \Phi^{-1}(xo_1(k), xo_3(k), mo_c(k)) \\ &= mo_c(k) - cxo_1(k) - dxo_3(k) - exo_1^2(k) - fxo_3^2(k) - gxo_1(k)xo_3(k) - hxo_1^2(k)xo_3(k) \end{aligned} \quad (4.56)$$

4.4.5 Résultats de simulation

Dans ce qui suit, nous présentons les résultats de simulation de la synchronisation des états d'émetteur donné par l'équation (4.44) et de son observateur donné par les équations (4.46)et (4.47). Les clés additionnelles c, d, e, f, g et h sont choisies $c = d = e = f = g = h = 0.1$. Le message original à transmettre est dans un premier temps un signal rectangulaire d'amplitude 1.5. Ensuite, un signal sinusoïdale d'amplitude 0.5 est envoyé. Dans ces simulations, nous avons choisi la période d'échantillonnage égale à $0.04s$. Les résultats de simulation de la reconstruction des états $x_1(k)$, $x_3(k)$ et $m(k)$ de l'émetteur sont exposés sur les figures (4.7 et 4.8), (4.9 et 4.10) et (4.11 et 4.12), respectivement. La réponse de l'état transmis x_2 est présentée par les figures (4.13 et 4.14), et son spectre de puissance est donné dans les figures (4.15 et 4.16).

4.5 Conclusion

Dans ce chapitre, nous avons présenté une méthode de synchronisation à base d'un observateur retardé étape par étape. La méthode de synthèse de l'observateur repose sur les deux conditions : condition d'observabilité et condition de recouvrement d'observabi-

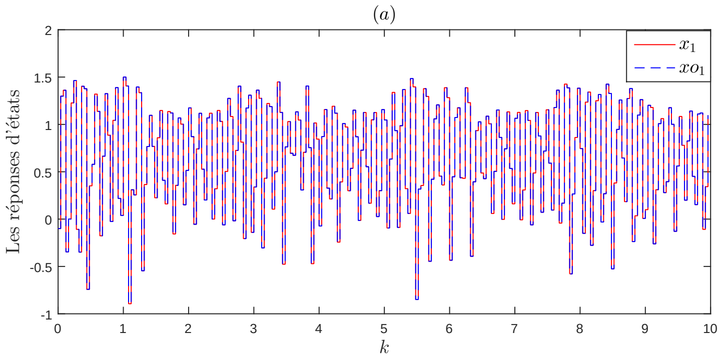


FIGURE 4.7: Réponses des états $x_1(k)$ (Émetteur) et $xo_1(k)$ (Récepteur) pour une entrée rectangulaire.

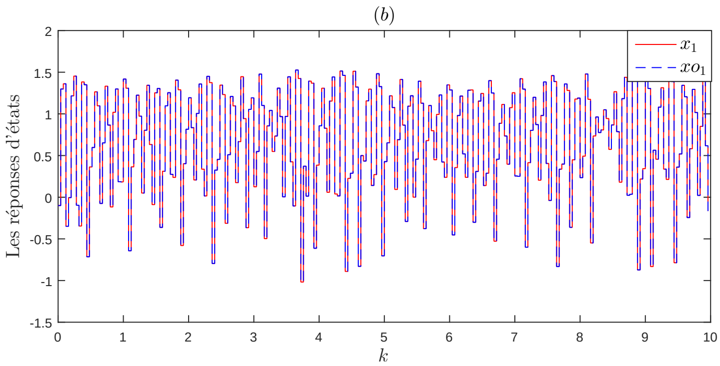


FIGURE 4.8: Réponses des états $x_1(k)$ (Émetteur) et $xo_1(k)$ (Récepteur) pour une entrée sinusoïdale.

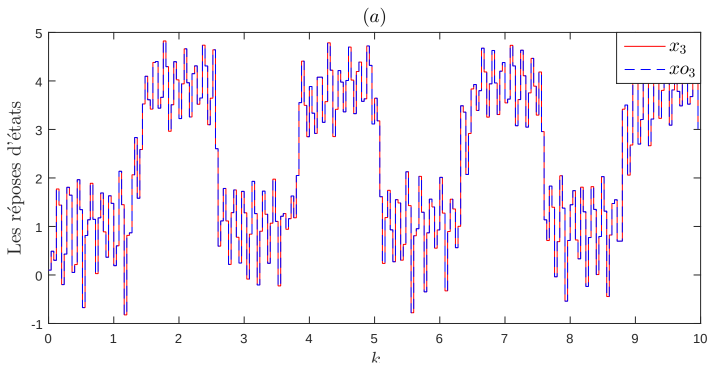


FIGURE 4.9: Réponses des états $x_3(k)$ (Émetteur) et $xo_3(k)$ (Récepteur) pour une entrée rectangulaire.

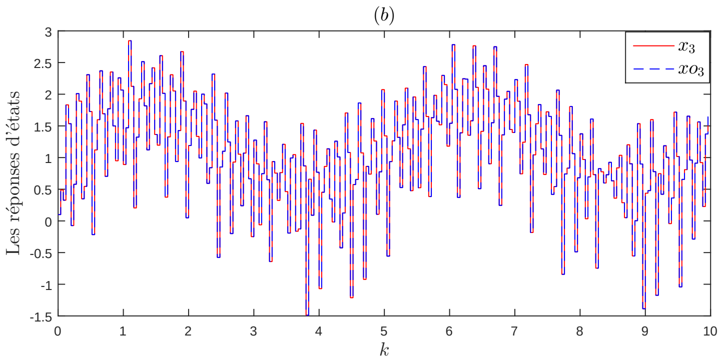


FIGURE 4.10: Réponses des états $x_3(k)$ (Émetteur) et $xo_3(k)$ (Récepteur) pour une entrée sinusoïdale.

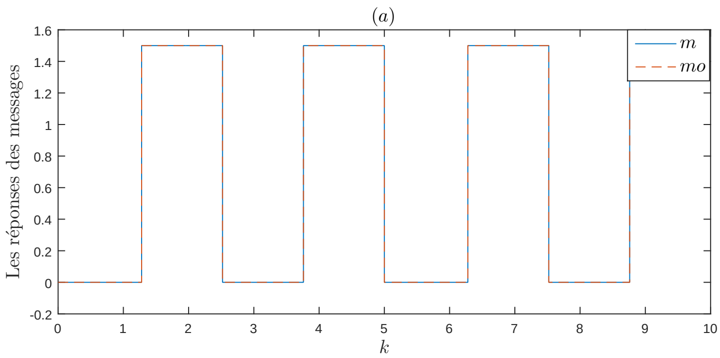


FIGURE 4.11: Réponses des messages $m(k)$ (Émetteur) et $mo(k)$ (Récepteur) pour une entrée rectangulaire.

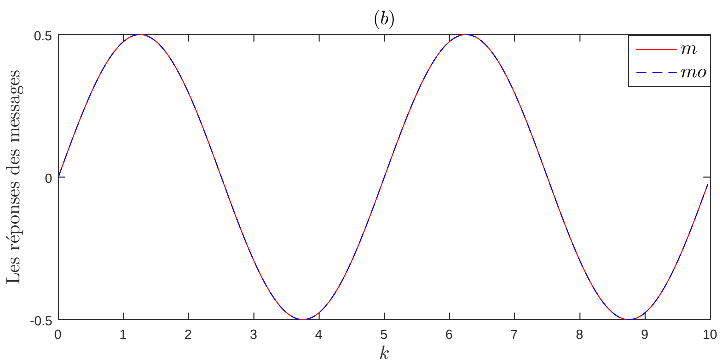


FIGURE 4.12: Réponses des messages $m(k)$ (Émetteur) et $mo(k)$ (Récepteur) pour une entrée sinusoïdale.

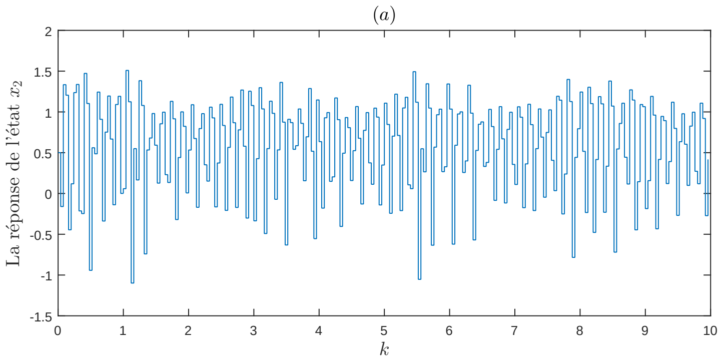


FIGURE 4.13: Réponse de l'état transmis $x_2(k)$ pour une entrée rectangulaire.

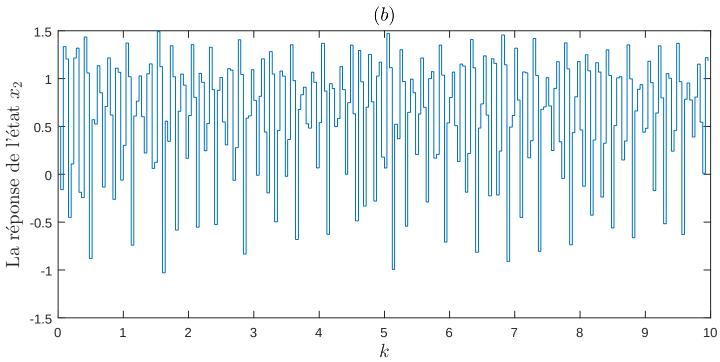


FIGURE 4.14: Réponse de l'état transmis $x_2(k)$ pour une entrée sinusoïdale.

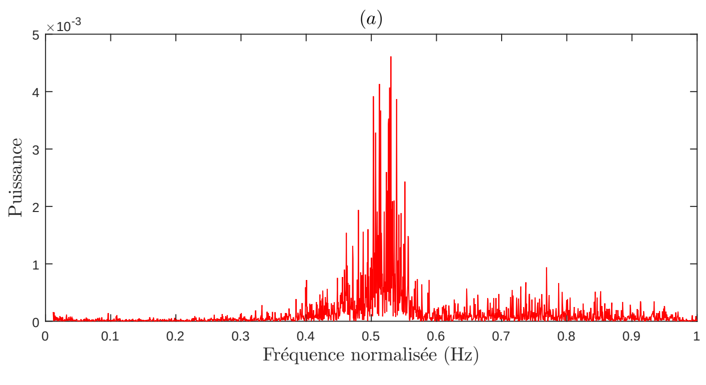


FIGURE 4.15: Spectre de puissance de l'état transmis x_2 pour une entrée rectangulaire.

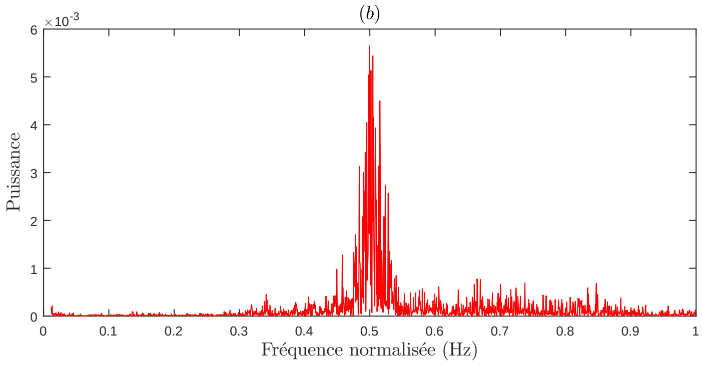


FIGURE 4.16: Spectre de puissance de l'état transmis x_2 pour une entrée sinusoïdale.

lité. Ces deux conditions sont étudiées pour le cas des systèmes chaotiques discrets d'ordre fractionnaire. Ensuite, nous avons appliqué l'observateur élaboré dans un nouveau schéma de communication chaotique sécurisée pour transmettre en sécurité des signaux.

Dans le chapitre 4, nous présenterons quelques schémas de communication sécurisée d'images basés sur cette méthode de synchronisation.

Chapitre 5

Schémas de transmission sécurisée d'images et analyse de performances

5.1 Introduction

Dans ce chapitre, nous proposons quelques schémas de transmission sécurisée d'images basés sur la synchronisation des systèmes chaotiques d'ordre fractionnaire. Le principe de ces schémas est de considérer un système chaotique au niveau de l'émetteur. Ensuite, on injecte l'information utile (qui est une image) dans la dynamique d'un système chaotique par inclusion, puis, de transmettre la sortie du système utilisé au récepteur. Il est à noter que cette sortie ne dépend pas de l'entrée. Le récepteur, qui est un observateur étape par étape, permet de reconstruire étape par étape les états du système et l'information d'origine à partir de la sortie et de ses itérés. De cette idée, nous proposons quelques schémas de transmission sécurisée robustes. En premier lieu, nous proposons un système de chiffrement sûr à une seule voie. Par la suite, quelques variantes du schéma développé seront présentées. L'efficacité des schémas proposés ainsi que les analyses de robustesse aux différentes méthodes d'attaques connues sont effectuées à l'aide du logiciel Matlab afin de prouver que les schémas de communication proposés possèdent de bonnes performances en terme de sécurité.

5.2 Schéma de transmission sécurisée d'images à une voie

À travers cette section, nous présentons un nouveau schéma de transmission sécurisée d'images basé sur la synchronisation des systèmes chaotiques d'ordre fractionnaire [43]. Ce schéma est composé principalement de deux blocs : émetteur et récepteur. Au niveau de l'émetteur, le système chaotique de Hénon modifié d'ordre fractionnaire est utilisé afin de chiffrer et de transmettre l'image originale ; les paramètres et les ordres fractionnaires du système constituent les clés de chiffrement et de déchiffrement qui seront partagés avec le récepteur. Au niveau de ce dernier, un observateur retardé étape par étape est utilisé. Le déchiffrement de l'image chiffrée ne peut être effectuer que si l'émetteur et le récepteur sont synchronisés. La performance du schéma de transmission proposé est mise en évidence par le fait qu'un seul canal de transmission est utilisé pour la synchronisation en plus de la résistance aux différentes attaques de cryptanalyse. Le schéma global du système de transmission sécurisée proposé est présenté par la figure 5.1. Dans ce qui suit, les deux blocs sont décrits.

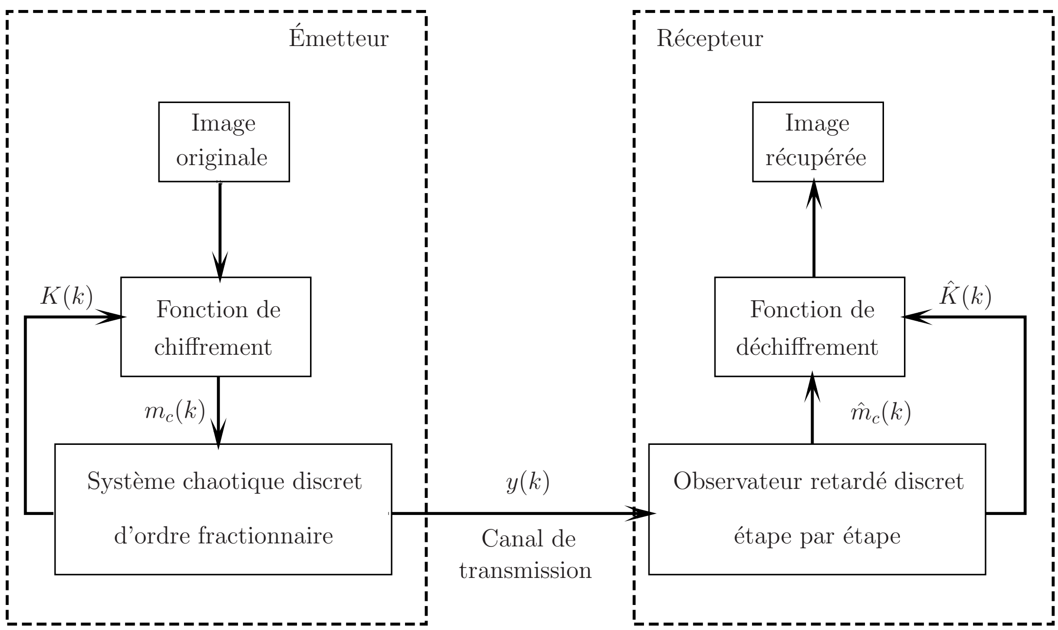


FIGURE 5.1: Schéma de transmission sécurisée d'images à une voie

5.2.1 Étude de l'émetteur

Au niveau de l'émetteur, le système chaotique de Hénon modifié d'ordre fractionnaire (4.40) génère des signaux chaotiques $\{x_1, x_2, x_3\}$. À partir de ces signaux, nous utilisons les séquences pseudo-aléatoires $\{x_1, x_3\}$ pour chiffrer l'image originale dans le but d'obtenir une image chiffrée. Pour ce faire, nous employons l'opération XOR comme fonction de chiffrement. Le choix de de cette opération est justifié par la simplicité de chiffrement et de déchiffrement. Dans le but de rendre la structure de l'émetteur plus complexe, l'image chiffrée (la sortie de l'opération XOR) est introduite dans la dynamique du système chaotique par la méthode d'inclusion. La procédure complète de l'algorithme de chiffrement du schéma proposé est décrite comme suit :

Étape 1 :

Nous présentons l'image originale par une matrice $A_{M\times N}$ (où M et N présentent le nombre de lignes et de colonnes de l'image). Ensuite, nous concaténons les lignes de la matrice afin d'obtenir un vecteur $A = \{A_1, A_2, \ldots, A_{M\times N}\}$. Ce vecteur est converti en binaire,

$$B(k) = de2bi(A(k)) = \{B_1, B_2, \ldots, B_{M\times N\times 8}\} \tag{5.1}$$

où *de2bi* est une commande Matlab permettant de convertir des nombres décimales en vecteurs binaires.

Étape 2 :

Nous considérons le système de Hénon modifié d'ordre fractionnaire (4.40). En itérant ce système $N_f = M \times N \times 8$ itérations, nous obtenons les séquences $\{x_1(k), x_3(k)\}$ que nous utilisons comme suit :

$$\begin{aligned} C(k) &= cx_1^2(k) + d(x_1(k) + x_3(k)) + ex_3^2(k) \\ D(k) &= mod((fC(k) - gC(k)) \times 10^{12}, 255) \\ K(k) &= de2bi(round(D(k))) \end{aligned} \tag{5.2}$$

où c, d, e, f et g sont des clés secrètes supplémentaires et $mod(x, y)$ renvoie le résidu après la division x/y, $round(x)$ arrondit l'élément x au plus proche entier, $abs(x)$ renvoie la valeur absolue de x.

Étape 3 :

Nous chiffrons l'image originale en utilisant la fonction XOR, présentée par le symbole $\oplus$. La séquence chiffrée $m_c(k)$ est obtenue comme suit :

$$m_c(k) = B(k) \oplus K(k) \tag{5.3}$$

Étape 4 :

La séquence chiffrée $m_c(k)$ est introduite dans la troisième dynamique du système (4.40) comme une entrée. Ainsi, nous obtenons :

$$\left\{\begin{array}{lcl} x_1(k+1) & = & a - x_2^2(k) - bx_3(k) + (\alpha_1 - 1)x_1(k) + \beta_1(x_1(k)) \\ x_2(k+1) & = & x_1(k) + (\alpha_2 - 1)x_2(k) + \beta_2(x_2(k)) \\ x_3(k+1) & = & x_2(k) + (\alpha_3 - 1)x_3(k) + \beta_3(x_3(k)) + m_c(k) \\ y(k) & = & x_2(k) \end{array}\right. \tag{5.4}$$

Étape 5 :

La variable d'état $x_2(k)$ considérée comme sortie du système (5.4) est envoyée au récepteur.

5.2.2 Étude du récepteur

Le récepteur, dans notre travail, consiste en un observateur étape par étape ayant pour rôle la récupération de tous les états ainsi que l'information noyée dans le système chaotique de l'émetteur. Cette récupération est possible que lorsque l'émetteur et le récepteur sont synchronisés. Nous avons déjà vérifié l'observabilité et la condition de recouvrement d'observabilité de notre système. Ainsi, nous allons utiliser le même observateur décrit dans le chapitre 3 donné par les équation suivantes :

$$\left\{\begin{array}{lcl}\hat{x}_2 & = & y(k) \\ \hat{x}_1(k-1) & = & y(k)-(\alpha_2-1)y(k-1)-\beta_2(y(k-1)) \\ \hat{x}_3(k-2) & = & \frac{1}{b}(a-y^2(k-2)+(\alpha_1-1)(y(k-1)-(\alpha_2-1)(y(k-2)-\beta_2(y(k-2))) \\ & & -y(k)+\beta_1(\hat{x}_1(k-2))+(\alpha_2-1)y(k-1)+\beta_2(y(k-1))) \\ \hat{m}_c(k-3) & = & \hat{x}_3(k-2)-\hat{x}_2(k-3)-(\alpha_3-1)\hat{x}_3(k-3)+\beta_3(\hat{x}_3(k-3))\end{array}\right. \tag{5.5}$$

De cette manière, nous récupérons les états $\hat{x}_1$ et $\hat{x}_3$ ainsi que l'image chiffrée $\hat{m}_c$. Le déchiffrement de l'image chiffrée est effectué de la même manière que le chiffrement de l'image originale, sauf que dans ce cas la clé $\hat{K}(k)$, comme montrée dans la figure 5.1, est obtenue à partir des états estimés $\hat{x}_1, \hat{x}_3$ par l'observateur étape par étape.

5.2.3 Résultats de simulation

Afin de tester le schéma de transmission sécurisée proposé, nous présentons quelques résultats de simulation. Dans un premier temps, nous donnerons les résultats de simulation sur la synchronisation de l'émetteur et le récepteur. Ensuite, les analyses de sécurité (voir chapitre 1) sont effectuées pour confirmer la robustesse du schéma présenté.

4.2.3.1 Résultats de la synchronisation de l'émetteur et le récepteur

Dans cette partie, les résultats de simulation sur la synchronisation des deux systèmes (5.4) et (5.5) sont présentés. Les paramètres et les ordres du système (5.4) sont choisis tels que : $a = 1.6$, $b = 0.1$, $\alpha_1 = 0.97$, $\alpha_2 = 0.94$ et $\alpha_3 = 0.91$. Les conditions initiales $x_1(0) = 0.2$, $x_2(0) = 0.5$ et $x_3(0) = 0.1$ sont choisies à l'intérieur du bassin d'attraction. Les nouveaux paramètres c, d, e, f et g du système (5.4) sont choisis : $c = 7.1$, $d = 11.08$, $e = 17$, $f = 5.2$, $g = 3.15$. Le message à masquer est une image au niveau de gris de dimension 128×128. Les résultats de synchronisation des états x_1, x_3 et l'entrée inconnue chiffrée m_c sont donnés respectivement par les figures (5.2), (5.3) et (5.4). La reconstruction est obtenue étape par étape et d'une manière parfaite. Il est à noter que les états reconstruits $\hat{x}_1$ et $\hat{x}_3$ du système constituent la clé secrète $\hat{K}$. Cela permet de prouver que la reconstruction du message m dépend de la synchronisation des états et de l'entrée inconnue du système (5.4) et de son observateur (5.5).

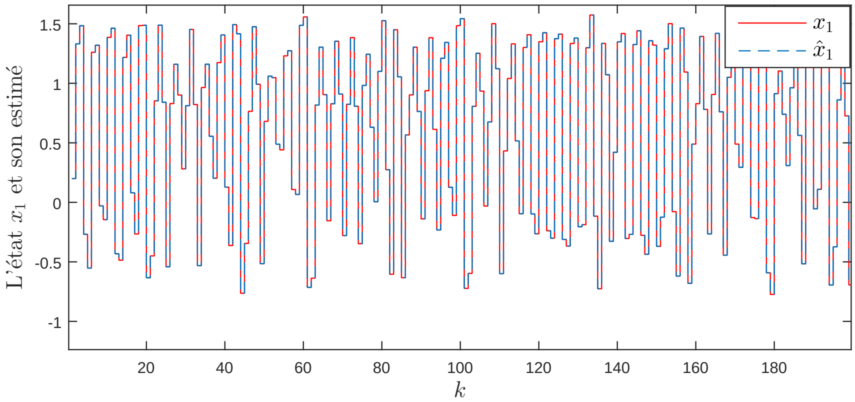


FIGURE 5.2: Résultats de simulation sur la synchronisation de l'état x_1 et son estimé $\hat{x}_1$.

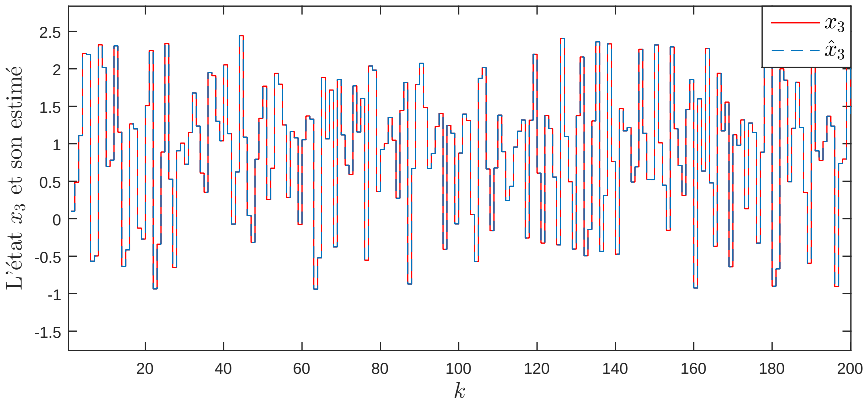


FIGURE 5.3: Résultats de simulation sur la synchronisation de l'état x_3 et son estimé $\hat{x}_3$.

4.2.3.2 Analyse de sécurité

En appliquant un algorithme de chiffrement sur une image, les pixels de l'image chiffrée doivent être différents et indépendants (faible corrélation) de ceux de l'image originale. Ceci peut être visible par simple visualisation de l'image chiffrée. La simple inspection visuelle reste insuffisante pour juger le chiffrement d'une image. On peut classer les métriques d'évaluation du degré de cryptage en analyse statistique, l'entropie d'information et une analyse de la sensibilité et de l'espace de la clé secrète.

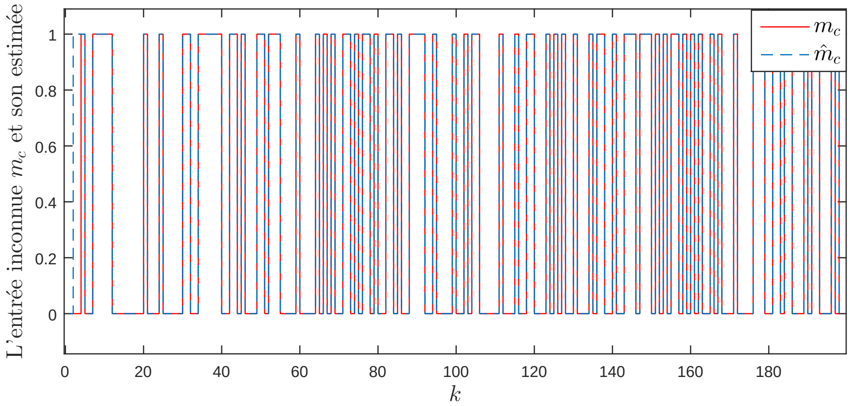


FIGURE 5.4: Résultats de simulation sur la synchronisation de l'entrée inconnue m_c et son estimée $\hat{m}_c$.

Dans tout ce qui suit l'image que nous avons chiffré est l'image de Lena de type BMP de taille 128×128.

4.2.3.2.1 Analyse statistique

L'analyse statistique permet de déchiffrer plusieurs algorithmes de cryptage comme il a été mentionné dans [54]. Durant cette partie, nous allons étudier l'histogramme des images originale, chiffrée et déchiffrée ainsi que la corrélation de pixels adjacents.

- ***Analyse des histogrammes***

Un histogramme est la distribution des intensités des pixels d'une image, c'est-à-dire le nombre de pixels pour chaque intensité lumineuse. Les figures 5.5(a,b et c) représentent respectivement l'histogramme de Lena originale, les histogrammes des images chiffrée et déchiffrée par l'algorithme étudié. Nous pouvons apercevoir que la distribution des pixels de l'image chiffrée est uniforme et considérablement différente de celle de l'image originale. Pour assurer l'uniformité de l'image, le test χ^2 est appliqué (voir l'équation (2.55)) pour confirmer statistiquement l'uniformité de l'histogramme. Ainsi, le résultat du test de χ^2 de l'histogramme de l'image chiffrée 5.5(b), avec un niveau de signification de 0.05, est obtenu égal à 246.06. Il est clair que cette valeur est inférieure à la valeur de χ^2 théorique, soit 293 pour $\alpha = 0.05$, de cette manière nous pouvons conclure que la distribution de l'algorithme testé est uniforme, ce qui prouve que la méthode proposée ne révèle aucune information pour l'analyse statistique.

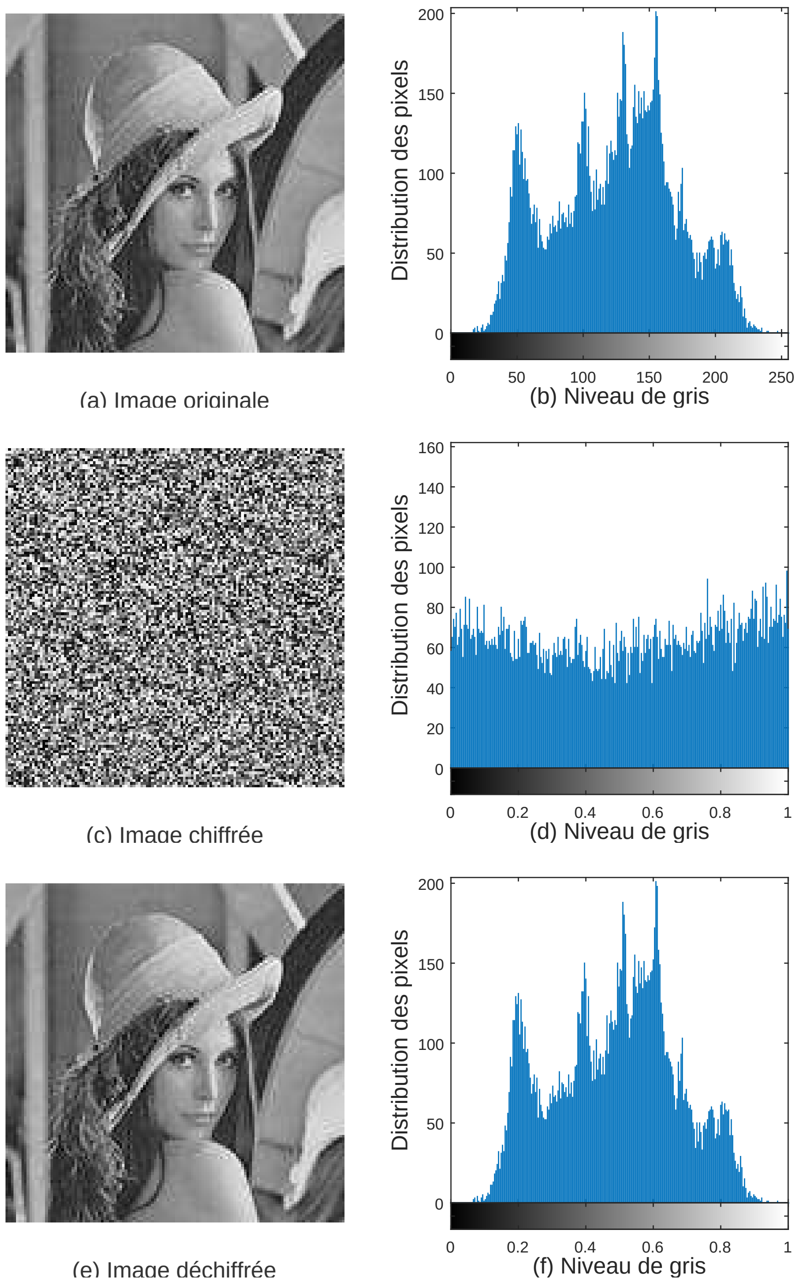


FIGURE 5.5: Analyse par histogramme de l'image de Lena (niveau de gris). (a) image originale, (b) histogramme de l'image originale, (c) image chiffrée, (d) histogramme de l'image chiffrée, (e) image déchiffrée, (f) histogramme de l'image déchiffrée.

	Direction	Image originale	Image chiffrée
Image de Lena	Horizontale	0.8939	−0.0127
	Verticale	0.9523	−0.0293
	Diagonale	0.8550	0.0047

TABLE 5.1: Coefficients de corrélation des pixels adjacents dans les trois directions.

- ***Corrélation des pixels adjacents***

Le calcul du coefficient de corrélation entre les pixels permet l'évaluation de la qualité de cryptage des crypto-systèmes. Si deux pixels sont étroitement associés, le coefficient de corrélation sera proche de 1 ou -1. Une valeur proche de 0 indique que les deux pixels ne sont pas liés et on ne peut pas prévoir l'un de l'autre. Cette métrique est calculée à partir de la formule de r_{xy} (voir équation 2.56).

Nous avons calculé le coefficient de corrélation de 3000 pixels adjacents des images originale, chiffrée, et déchiffrée prisent horizontalement, verticalement et diagonalement. Le Tableau 5.1 regroupe les coefficients de corrélation obtenus. Le coefficient de corrélation mesuré pour l'image originale est proche de 1, alors que le coefficient de corrélation pour l'image chiffrée est proche de 0, on en déduit que le chiffrement a atténué considérablement la corrélation entre les pixels de l'image chiffrée.

La figure 5.6 représente les distributions des corrélations des pixels adjacents dans les directions horizontale, verticale et diagonale de l'image originale et l'image chiffrée. Cette figure confirme les résultats du Tableau 5.1, puisque la distribution des intensités des pixels de l'image originale se concentre sur la diagonale, les pixels sont alors fortement corrélés, tandis que ceux de l'image cryptée sont non-corrélés et ont une distribution uniforme.

4.2.3.2.2 Entropie d'information

L'entropie est utilisée pour mesurer la quantité d'information. Plus une information est ordonnée, plus est faible son entropie ; inversement, plus une information est confuse, plus est élevée l'entropie. Les entropies d'informations de l'image originale de Lena et l'image chiffrée correspondante sont calculées en utilisant l'équation (2.60) donnée au premier

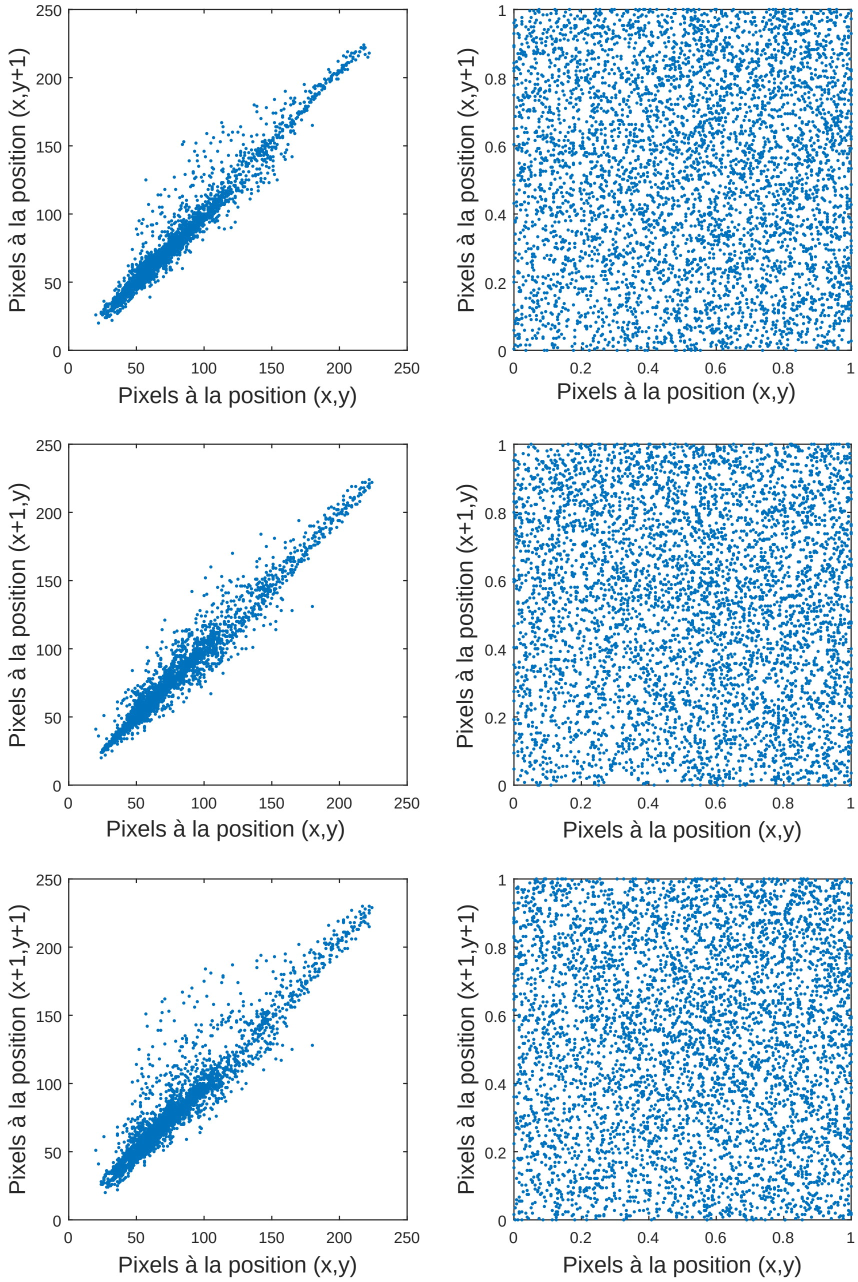


FIGURE 5.6: Distribution de corrélation des pairs de pixels adjacents dans les images originale et chiffrée de Lena (niveau de gris). (a) la corrélation des pixels horizontalement adjacents dans l'image originale, (b) la corrélation des pixels horizontalement adjacents dans l'image chiffrée, (c) la corrélation des pixels verticalement adjacents dans l'image originale, (d) la corrélation des pixels verticalement adjacents dans l'image chiffrée, (e) la corrélation des pixels diagonalement adjacents dans l'image originale, (f) la corrélation des pixels diagonalement adjacents dans l'image chiffrée.

	Image originale	Image chiffrée
Image de Lena	7.4514	7.9815

TABLE 5.2: Entropie d'information des images originale et chiffrée.

chapitre. Les résultats obtenus sont listés dans le tableau 5.2. À partir de ce tableau, il est clair que l'entropie est proche de 8, donc le schéma de transmission proposé a une bonne propriété d'entropie d'information.

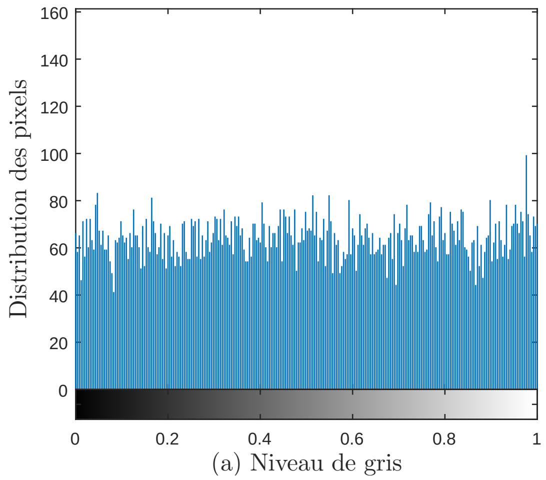
4.2.3.2.3 Analyse de la sensibilité de la clé

Tout algorithme de cryptage fiable doit être extrêmement sensible au changement mineur de la clé secrète pour garantir, dans une certaine mesure, la sécurité contre les attaques par force brute. La sensibilité de la clé d'un crypto-système peut être observée par deux méthodes différentes :

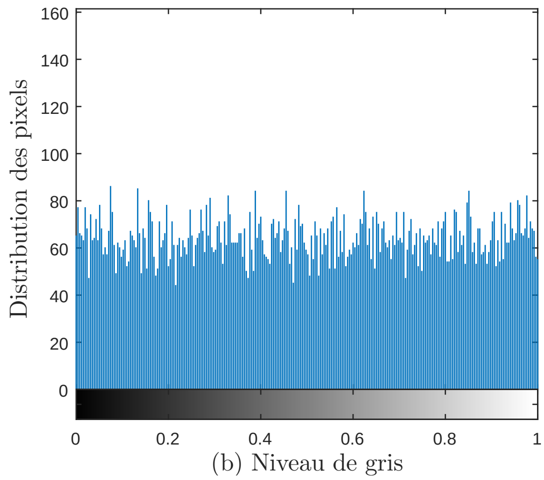
- L'image cryptée doit être très sensible à la clé secrète ; i.e. si on utilise deux clés légèrement différentes pour crypter la même image, alors les deux images cryptées doivent être complètement indépendantes l'une par rapport à l'autre (faible corrélation).
- L'image cryptée ne peut pas être décryptée correctement si la clé secrète est légèrement modifiée à la phase de décryptage.

La figure 5.7 contient les histogrammes de l'image de Lena cryptée par deux clés légèrement différentes au niveau du paramètre $b((a)b = 0.1, (b)b = 0.1 + 10^{-15})$. Le changement d'une seule valeur donne alors deux histogrammes totalement différents avec un très faible coefficient de corrélation entre les deux images ($r_{xy} = -0.0013$). Pour confirmer cette sensibilité, nous avons calculé les taux $NPCR$ et $UACI$ ainsi que le coefficient de corrélation r_{xy} pour des clés différentes uniquement au niveau de quelques paramètres. Les résultats obtenus sont présentés dans le tableau 5.3.

Nous avons essayé de plus de décrypter deux images en employant pour l'une la vraie clé secrète et pour la deuxième une clé légèrement différente. Nous remarquons que le



(a) Niveau de gris



(b) Niveau de gris

FIGURE 5.7: Histogrammes de Lena cryptée : (a) Image chiffrée avec $b = 0.1$ (b) Image chiffrée avec $a = 0.1 + 10^{-15}$.

Clé secrète	$NPCR(\%)$	$UACI(\%)$	r_{xy}
La bonne clé	0	0	1
Paramètre modifié $b + 10^{-15}$	99.4141	33.3693	-0.00013
Ordre fractionnaire modifié $\alpha_3 + 10^{-15}$	99.2188	33.5811	-0.0056
Coefficient modifié $g + 10^{-13}$	99.8047	34.3873	-0.0152

TABLE 5.3: $NPCR$, $UACI$ et r_{xy} de deux images chiffrées par des clés légèrement différentes.

Clé secrète	$NPCR(\%)$
La bonne clé	8.86
Paramètre modifié $a + 10^{-15}$	99.73
Ordre fractionnaire modifié $\alpha_1 + 10^{-15}$	99.64
Coefficient modifié $f + 10^{-13}$	99.80

TABLE 5.4: $NPCR$ de l'image originale les images déchiffrées par des clés différentes.

processus de décryptage a échoué lorsque la clé secrète est légèrement modifiée et que l'image décryptée est totalement brouillée (figure 5.8). Pour confirmer cette sensibilité, nous avons calculé le taux de changement du nombre de pixels $NPCR$. Les résultats obtenus sont présentés dans le tableau 5.4. Ainsi, nous concluons que les images cryptées par l'algorithme proposé ont une extrême sensibilité à la clé secrète et ne sont pas vulnérable aux attaques par force brute.

4.2.3.2.4 Analyse de l'espace de la clé

L'espace de la clé d'un algorithme de chiffrement/déchiffrement est le total des clés différentes qui peuvent être utilisées dans la procédure de chiffrement/déchiffrement. Il doit être assez large (supérieur à 128 bits) pour s'assurer qu'une attaque par force brute est non faisable.

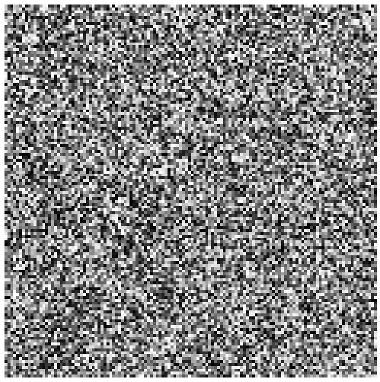
Dans notre travail, la clé est composée de 3 parties :

- Les paramètres du système (a, b).
- Les ordres fractionnaires du système (α_1, α_2).
- Les paramètres additionnels (c, d, e, f, g).

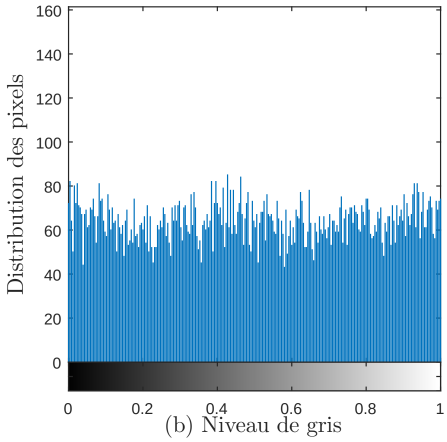
Le tableau 5.5 présente la sensibilité de tout les paramètres de la clé du système, où la taille de l'intervalle de variation de chaque paramètre est $s_i = 0.1$. Ainsi, la taille N de l'espace de la clé est calculé comme suit :

$$N = \prod_{i=1}^{9} = 10^{(14\times4+12\times2+11\times3)} = 10^{113} >> 2^{100} \tag{5.6}$$

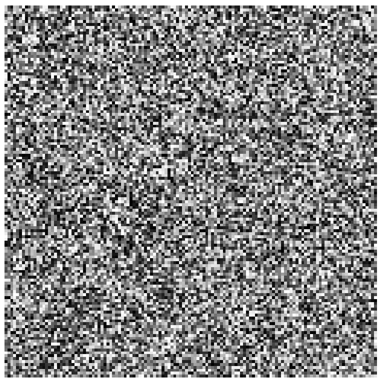
On remarque que l'espace de la clé est suffisamment grand pour résister aux attaques par force brute.



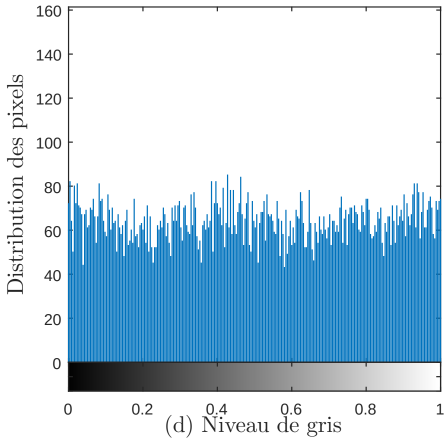
(a) Paramètre a incorrect



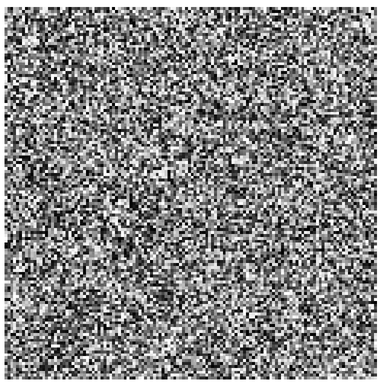
(b) Niveau de gris



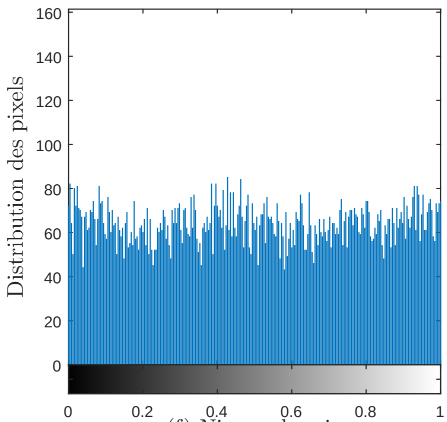
(c) Order fractionnaire α_1 incorrect



(d) Niveau de gris



(e) Coefficient f incorrect



(f) Niveau de gris

FIGURE 5.8: Déchiffrement de Lena chiffrée par différentes clés (a) Paramètre a incorrect (c) Ordre fractionnaire α_1 incorrect (e) Coefficient f incorrect (b), (d) et (e) Niveau de gris.

Paramètres p_i	Sensibilité S_i	Nb. de possibilités : $(N_i = s_i \times S_i^{-1})$
$a = 1.6$	$S_1 = 10^{-15}$	$N_1 = 10^{14}$
$b = 0.1$	$S_2 = 10^{-15}$	$N_2 = 10^{14}$
$\alpha_1 = 0.97$	$S_3 = 10^{-15}$	$N_3 = 10^{14}$
$\alpha_2 = 0.94$	$S_4 = 10^{-15}$	$N_4 = 10^{14}$
$c = 7.1$	$S_5 = 10^{-12}$	$N_5 = 10^{11}$
$d = 11.08$	$S_6 = 10^{-12}$	$N_6 = 10^{11}$
$e = 17$	$S_7 = 10^{-12}$	$N_7 = 10^{11}$
$f = 5.2$	$S_8 = 10^{-13}$	$N_8 = 10^{12}$
$g = 3.15$	$S_9 = 10^{-13}$	$N_9 = 10^{12}$

TABLE 5.5: Sensibilité aux paramètres

4.2.3.2.5 Robustesse par rapport au bruit

Dans cette section, le coefficient PSNR est utilisé pour analyser la qualité visuelle de l'image décryptée par rapport à l'image originale (voir l'équation (2.61)). Plus la valeur PSNR est élevée, moins la distorsion est importante pour l'image originale. En effet, lorsque la valeur de PSNR ≥ 30, l'œil humain ne peut pas percevoir des différences entre l'image originale et l'image déchiffrée. Lorsqu'aucune attaque ne se produit, la valeur PSNR de l'image déchiffrée (figure 5.5(e)) est de 87.30. Dans ce qui suit, nous testons la robustesse du schéma proposé par rapport à deux types de bruit : le bruit Poivre & Sel et le bruit Gaussien, qui sont ajoutés à l'image chiffrée. Ainsi, nous ajoutons le bruit Poivre & Sel avec différentes densités de bruit, c'est-à-dire 0.001 et 0.01 à l'image chiffrée. De plus, un bruit blanc gaussien avec une valeur moyenne 0 et deux différentes valeurs de variance (0.02 et 0.05) est ajouté à l'image chiffrée. Le tableau 5.6 affiche les valeurs PSNR de l'image décryptée lorsque l'image chiffrée est attaquée par différents bruits. Les résultats démontrent que le schéma de transmission proposé peut résister à l'attaque du bruit.

	PSNR de l'image de Lena en Décibel
Déchiffrée sans bruit	87.30
Bruit Poivre & Sel 0.001	38.12
Bruit Poivre & Sel 0.01	28.47
Bruit Gaussien [0, 0.02]	43.62
Bruit Gaussien [0, 0.05]	23.94

TABLE 5.6: $PSNR$ de l'image déchiffrée sous différents types de bruit.

5.3 Variantes du schéma de transmission sécurisée proposé

A travers cette section, de nouveaux schémas de transmission sécurisée sont présentés. Ceux-ci présentent des variantes du schéma développé dans la section précédente. Dans le premier schéma, un autre type de synchronisation, à savoir la synchronisation impulsive, est utilisé en plus de la synchronisation à base d'observateur étape par étape [47]. Le schéma de transmission sécurisée est basé sur des systèmes chaotiques d'ordre fractionnaire couplés et la transmission est effectuée à deux voies. Le deuxième schéma proposé est basé sur la structure de confusion-diffusion, où les clés secrètes utilisées sont générées à partir du système chaotique de Hénon modifié d'ordre fractionnaire. Lors du déchiffrement, l'observateur étape par étape est utilisé pour assurée la synchronisation et la reconstruction des clés secrètes. Dans ce qui suit, les deux schémas seront présentés ainsi que les résultats de simulation et de performance.

5.3.1 Schéma de transmission sécurisée basé sur des systèmes chaotiques d'ordre fractionnaire couplés

Dans cette partie, nous présentons un nouveau schéma de communication sécurisée basé sur la synchronisation des systèmes chaotiques d'ordre fractionnaire couplés en utilisant des observateurs [47,49]. Le principe du schéma de communication sécurisée proposé est illustré par la figure 5.9. Au niveau de l'émetteur, deux systèmes chaotiques discrets d'ordre fractionnaire sont utilisés : le premier système (Lozi d'ordre fractionnaire) per-

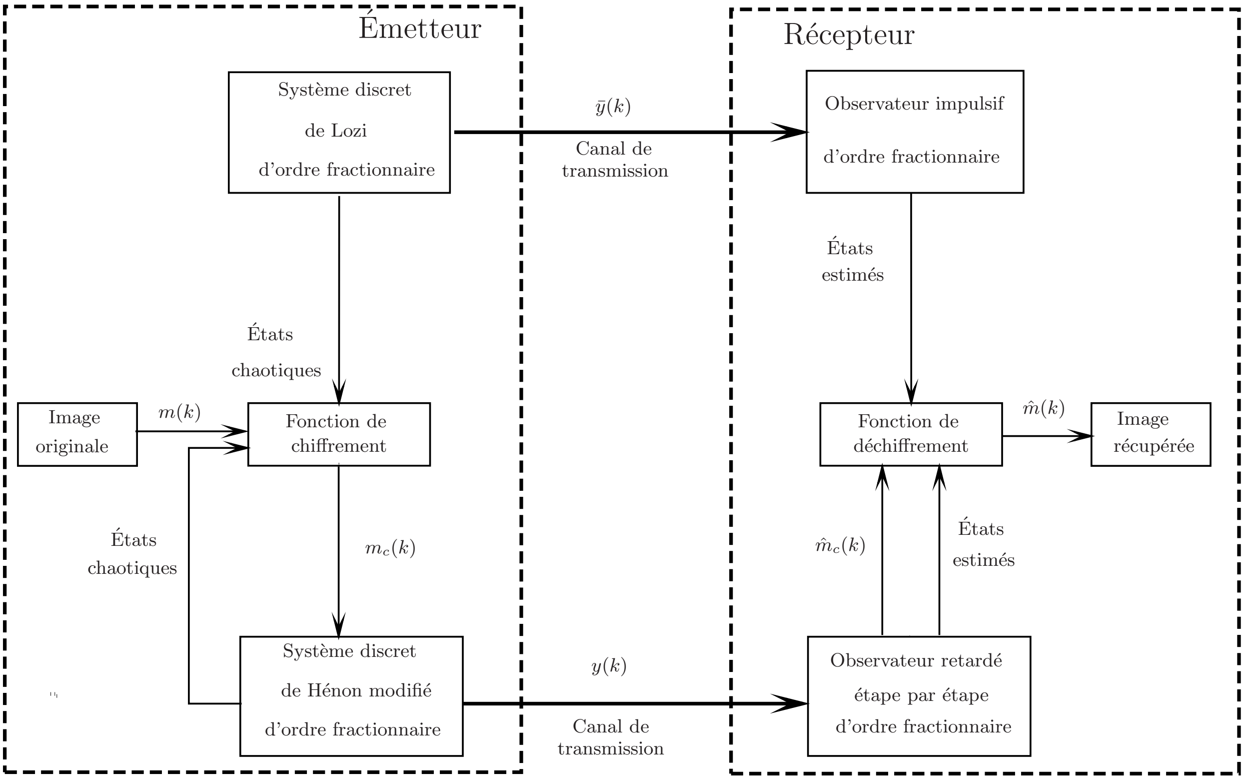


FIGURE 5.9: Schéma de transmission sécurisée C.

met de générer une partie de la clé secrète du crypto-système, pendant que le deuxième système (Hénon modifié d'ordre fractionnaire) génère l'autre partie. Par la suite, l'image originale est chiffrée à l'aide de l'opération XOR (de même pour le déchiffrement). Après cela, l'image chiffrée est insérée dans la dynamique du deuxième système chaotique. Les sorties des deux systèmes sont ensuite envoyées au récepteur. Au niveau de ce dernier, deux types d'observateurs sont utilisés : l'observateur du premier système est un observateur impulsif, tandis que l'observateur étape par étape développé précédemment est utilisé pour le deuxième système. Dans ce qui suit, nous présentons l'émetteur et le récepteur du notre schéma de transmission.

4.3.1.1 Étude de l'émetteur

Au niveau de ce bloc, les systèmes chaotiques de Lozi et de Hénon modifié d'ordre fractionnaire sont utilisés. Considérons le système de Lozi d'ordre fractionnaire donné par la représentation d'état suivante :

$$\begin{cases} z_1(k+1) &= 1 - \bar{a}|z_1(k)| + \bar{b}z_2(k) + (\bar{\alpha_1} - 1)z_1(k) + \beta_1(z_1) \\ z_2(k+1) &= z_1(k) + (\bar{\alpha_2} - 1)z_2(k) + \beta_2(z_2) \\ \bar{y}(k) &= z_1(k) \end{cases} \tag{5.7}$$

avec $z = [z_1\ z_2]^T \in R^2$ est le vecteur d'état, $\bar{y}$ est le premier signal de sortie et $\beta_1(z_1)$, $\beta_2(z_2)$ sont définis par $\beta_1(z_1) = \sum_{p=1}^{L} C_{p1}z_1(k-p)$ et $\beta_2(z_2) = \sum_{p=1}^{L} C_{p2}z_2(k-p)$. Nous prenons les conditions initiales $z_1(0)$ et $z_2(0)$ égales à 0.2 et 0.5, respectivement. Les paramètres et l'ordre commensurable du système sont choisis tels que : $\bar{a} = 1.7$, $\bar{b} = 0.5$ et $\bar{\alpha}_1 = \bar{\alpha}_2 = 0.95$ et la mémoire du système est fixée à 5 ($L = 5$). L'attracteur étrange de notre système est présenté à la figure 5.10. Le deuxième système considéré est le système de Hénon

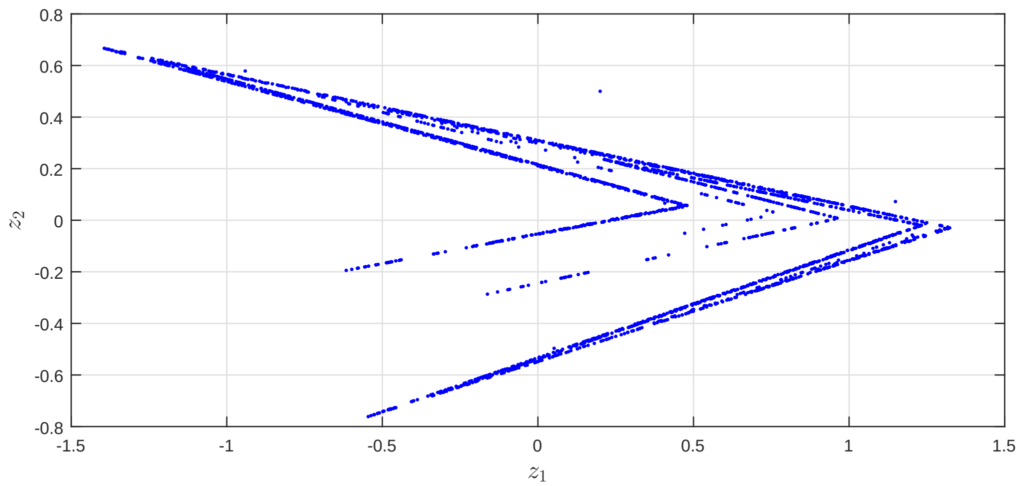


FIGURE 5.10: L'attracteur étrange du système de Lozi d'ordre fractionnaire.

modifié présenté par l'équation (4.40), où les conditions initiales et les paramètres sont pris : $x_1(0) = -0.1$, $x_2(0) = 0.5$, $x_3(0) = 0.1$, $a = 1.5$ et $b = 0.1$. Les ordres fractionnaires sont choisis $\alpha_1 = 0.85$, $\alpha_2 = 0.9$ et $\alpha_3 = 0.75$ et la taille de la mémoire $L = 5$.

Considérons l'image originale donnée sous forme de vecteur binaire $B(k)$, tel qu'il était déjà présenté par l'équation (5.1). Le principe du schéma proposé est de générer une clé secrète, de la même taille que le message $B(k)$, à partir des séquences x_1, x_3, z_2 des deux systèmes chaotiques d'ordre fractionnaire. Ainsi, nous procédons comme suit :

$$\begin{aligned} C(k) &= cx_1(k) + dx_3(k) + ez_2(k) + fx_1(k)z_2(k) + gx_3(k)z_2(k) + hx_1(k)x_3(k)z_2(k) \\ D(k) &= mod((C(k) - floorC(k)) \times 10^{12}, 255) \\ K(k) &= de2bi(round(D(k))) \end{aligned} \tag{5.8}$$

où c, d, e, f, g et d sont considérés comme les nouvelles clés secrètes. Une fois la clé est générée, le message clair est chiffré par la clé secrète en utilisant l'opération XOR, afin d'obtenir une séquence chiffrée $m_c(k)$:

$$m_c(k) = B(k) \oplus K(k) \tag{5.9}$$

Par la suite, le message chiffré est introduit dans la troisième dynamique du système de Hénon modifié d'ordre fractionnaire. Ainsi, nous obtenons :

$$\begin{cases} x_1(k+1) &= a - x_2^2(k) - bx_3(k) + (\alpha_1 - 1)x_1(k) + \beta_1(x_1(k)) \\ x_2(k+1) &= x_1(k) + (\alpha_2 - 1)x_2(k) + \beta_2(x_2(k)) \\ x_3(k+1) &= x_2(k) + (\alpha_3 - 1)x_3(k) + \beta_3(x_3(k)) + m_c(k) \\ y(k) &= x_2(k) \end{cases} \tag{5.10}$$

Finalement, les deux variables de sorties $y(k)$ et $\bar{y}(k)$ sont envoyées au récepteur.

4.3.1.2 Étude du récepteur

Dans cette partie, nous présentons les observateurs utilisés pour récupérer les états des systèmes chaotiques d'ordre fractionnaire de Lozi et de Hénon modifié. Pour reconstruire l'état du système de Lozi d'ordre fractionnaire, un observateur impulsif est utilisé [116]. Le rôle de ce dernier consiste en l'utilisation d'un train d'impulsions, puis reproduire les états du système à l'arrivée de chaque impulsion. Ainsi, l'observateur impulsif du système

(5.7) peut être donné comme suit :

$$\begin{cases} \hat{z}_1(k+1) & = & 1-\bar{a}|\hat{z}_1(k)|+\bar{b}\hat{z}_2(k)+(\bar{\alpha}_1-1)\hat{z}_1(k)+\hat{\beta}_1(\hat{z}_1) & \text{pour } k \neq k_i \\ \hat{z}_2(k+1) & = & \hat{z}_1(k)+(\bar{\alpha}_2-1)\hat{z}_2(k)+\hat{\beta}_2(\hat{z}_2) & \\ \hat{z}(k_{i+}) & = & \hat{z}(k_i)-B(k_i)e(k_i) & \text{pour } k = k_i \end{cases} \tag{5.11}$$

avec $\hat{z} = [\hat{z}_1\ \hat{z}_2]^T \in R^n$ est le vecteur d'états estimés. Les sauts dans les variables d'état se produisent à des instants $k = k_i$, $i = 1, 2, \ldots,$. Nous définissons k_{i+} et k_{i-}, respectivement, comme les instants qui précèdent ou suivent l'arrivée de chaque impulsion. $e(k)$ désigne l'erreur de synchronisation entre le système de Lozi d'ordre fractionnaire et son observateur, tel que : $e(k) = z(k) - \hat{z}(k)$. $B(k_i)$ est une matrice symétrique contenant des paramètres de contrôle agissant lorsque l'impulsion k_i se produit, $B(k_i) = \begin{pmatrix} b_1(k_i) & 0 \\ 0 & b_2(k_i) \end{pmatrix}$.
Dans notre cas, nous n'avons utilisé que des échantillons de l'état z_1 pour le contrôle impulsif. Par conséquent, le paramètre de contrôle est constitué du paramètre $b_1(k_i)$. En outre, il a été pris constant i.e : $b_1(k_1) = b_1(k_2) = \ldots = b_1(k_i)$. La distance entre deux impulsions successives est supposée constante et est notée T.
Pour le deuxième système, nous utilisons l'observateur étape par étape présenté à la section 5.2.2 . Les états $\hat{x}_1(k)$ et $\hat{x}_3(k)$ et le message chiffré $m_c(k)$ sont estimés de la même manière que ceux présentés dans le section 5.2.2 par l'équation (5.5). Une fois le message m_c reconstruit, son déchiffrement est effectué par l'opération XOR à l'aide de la clé $\hat{K}(k)$. Cette clé est obtenue de la même manière que $K(k)$ qui est exprimée par l'équation (5.8), mais cette fois ci en utilisant les états estimés par les observateurs impulsif et étape par étape. Il est à noter que la reconstruction de $\hat{K}(k)$ dépend de la synchronisation des deux systèmes chaotiques et de la connaissance des clés secrètes additionnelles (c, d, e, f, g, h).

4.3.1.3 Résultats de simulation et analyse de sécurité

Le message clair à transmettre est l'image de Légumes verts au niveau de gris de taille 128×128. Dans cette partie, nous commençons par présenter la synchronisation des états des deux systèmes Hénon modifié et Lozi d'ordre fractionnaire. Les résultats de simulation sur la synchronisation des deux systèmes (4.40) et (5.7) sont obtenus pour les mêmes valeurs de paramètres et ordres fractionnaires. Les nouvelles clés sont choisies : $c = 9.23$, $d = 1.87$, $e = 13.4$, $f = 0.01$, $g = 0.15$ et $h = 3.91$. L'image de Légumes verts est convertie en vecteur de valeurs binaires $B(k)$, ainsi la taille de $B(k) = 128 \times 128 \times 8$. Les résultats de synchronisation des états x_1, x_3, z_2 et l'entrée inconnue chiffrée m_c sont donnés sur les figures (5.11),(5.12), (5.13) et (5.14), respectivement. Une fois la synchronisation est achevée, la clé $\hat{K}(k)$ est trouvée. Par conséquent, l'image originale est reconstruite.

Dans ce qui suit, nous analysons le schéma proposé contre les différents types d'attaque

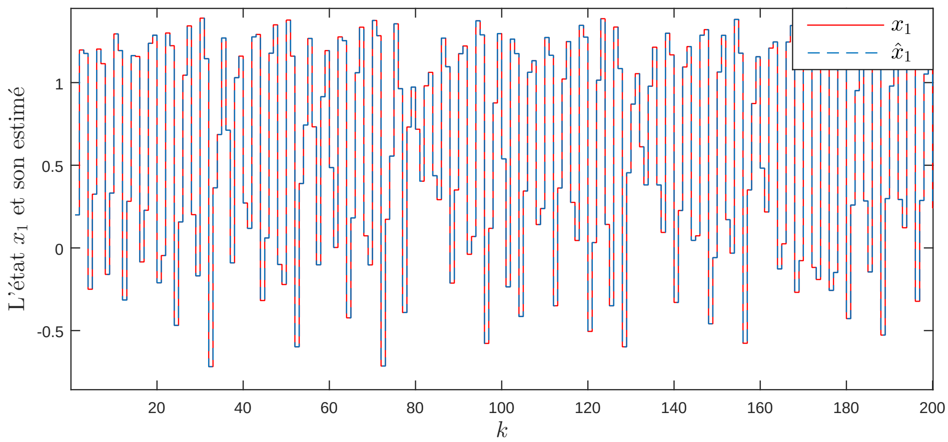


FIGURE 5.11: Résultats de simulation sur la synchronisation de l'état x_1 et son estimé $\hat{x}_1$.

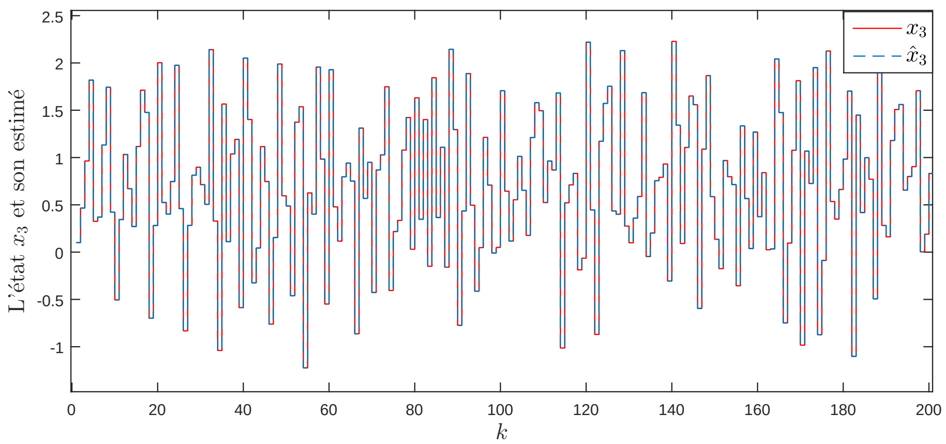


FIGURE 5.12: Résultats de simulation sur la synchronisation de l'état x_3 et son estimé $\hat{x}_3$.

de cryptanalyse.

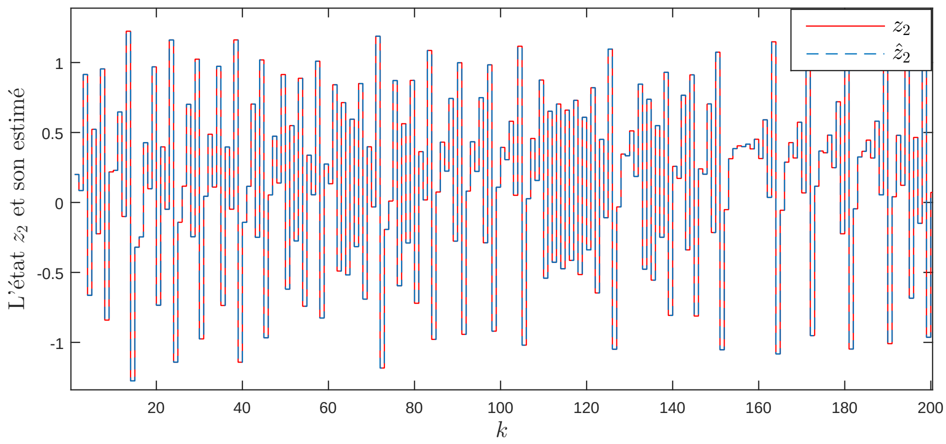


FIGURE 5.13: Résultats de simulation sur la synchronisation de l'état z_2 et son estimé $\hat{z}_2$.

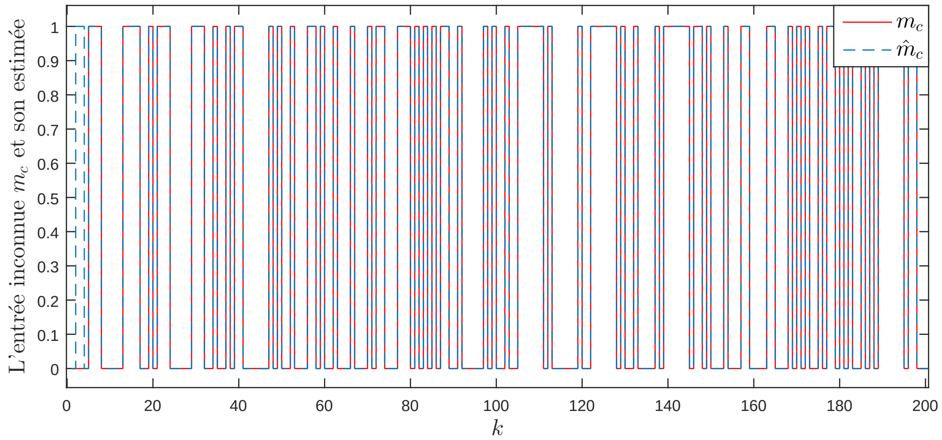


FIGURE 5.14: Résultats de simulation sur la synchronisation de l'entrée inconnue m_c et son estimée $\hat{m}_c$.

		Image originale	**Image chiffrée**
Image de Légumes verts	Horizontal	0.9911	0.0075
	Vertical	0.9848	-0.0216
	Diagonal	0.9755	0.0088

TABLE 5.7: Coefficients de corrélation des images originale et chiffrée.

- Analyse statistique

L'analyse des histogrammes ainsi que la corrélation des pixels adjacents sont exposées dans cette partie. Les histogrammes de l'image originale, chiffrée et déchiffrée sont donnés par la figure 5.15. L'uniformité de l'histogramme de l'image chiffrée est démontrée par le test χ^2 (voir l'équation(2.55)), ainsi, nous obtenons, pour un niveau de signification de $\alpha = 0.05$, la valeur de $\chi^2 = 261.25$. De cette manière, nous pouvons affirmer le bon chiffrement de l'image originale. De plus, nous calculons les coefficients de corrélation des 3000 pixels adjacents des images originale, chiffrée et déchiffrée dans les différentes directions. Les résultats obtenus sont présentés dans le tableau 5.7. La distribution des corrélations des pixels adjacents dans les trois directions (horizontale, verticale et diagonale) des images originale et chiffrée est donnée par la figure 5.16.

- Entropie d'information

En utilisant l'équation (2.60), nous avons obtenu l'entropie de l'image originale égal à 6.9997. Tandis que pour l'image chiffrée, l'entropie est très proche de 8 et est égal à 7.9884. Les résultats obtenus prouve la bonne propriété d'entropie du schéma de communication proposé.

- Analyse de la sensibilité de la clé

Pour analyser la sensibilité de la clé, nous avons déchiffré l'image de Légumes verts chiffrée par une clé légèrement différentes au niveau du paramètre ($\bar{\alpha}_2$). L'image obtenue est complètement brouillée (figure 5.17), ce qui illustre la très grande sensibilité de notre schéma aux petits changements de la clé secrète. Nous avons également calculé le taux de changement du nombre de pixels $NPCR$ entre l'image originale et chiffrée, et nous

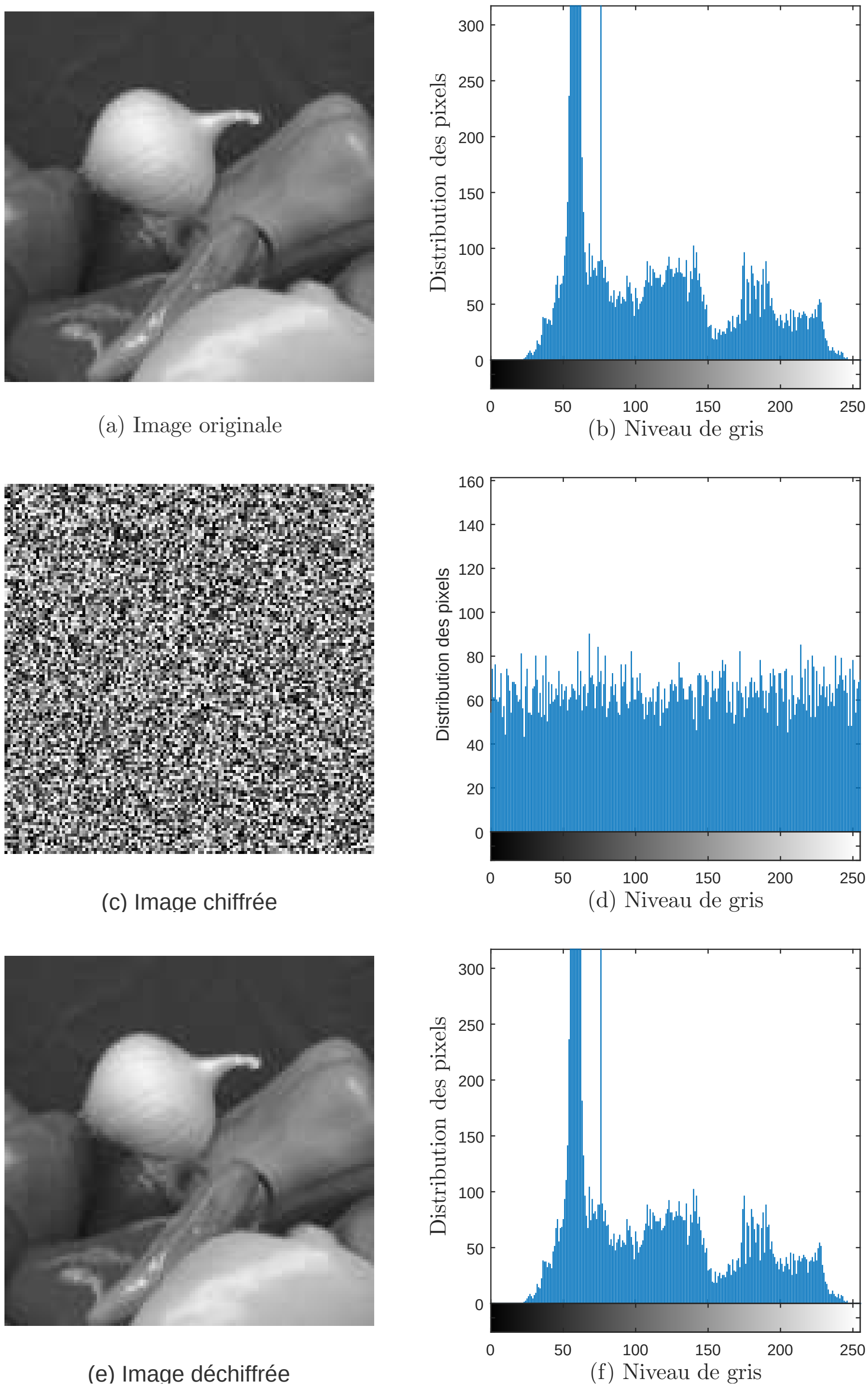


Figure 5.15: Analyse par histogramme de l'image de Légumes verts. (a) image originale, (b) histogramme de l'image originale, (c) image chiffrée, (d) histogramme de l'image chiffrée, (e) image déchiffrée, (f) histogramme de l'image déchiffrée.

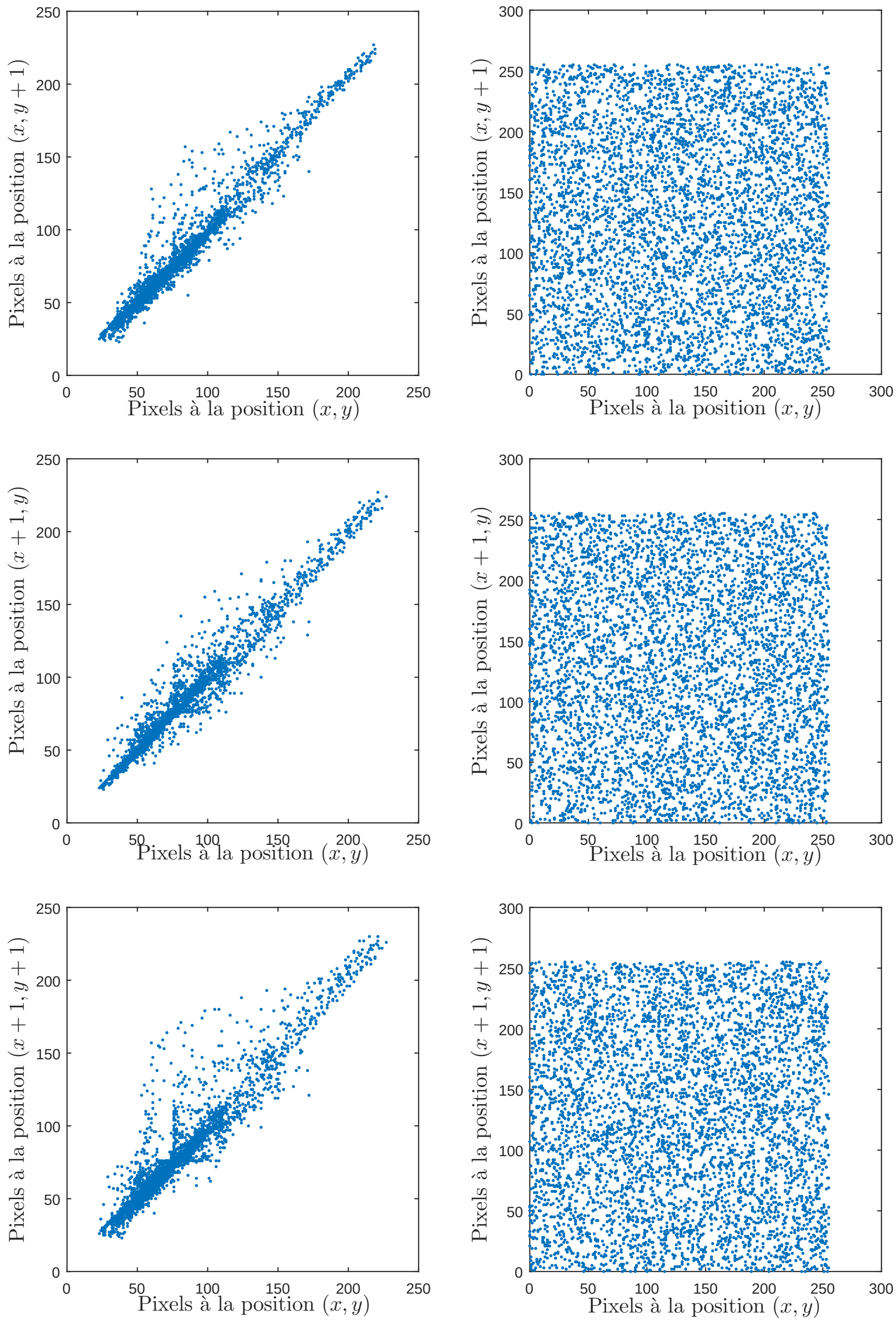
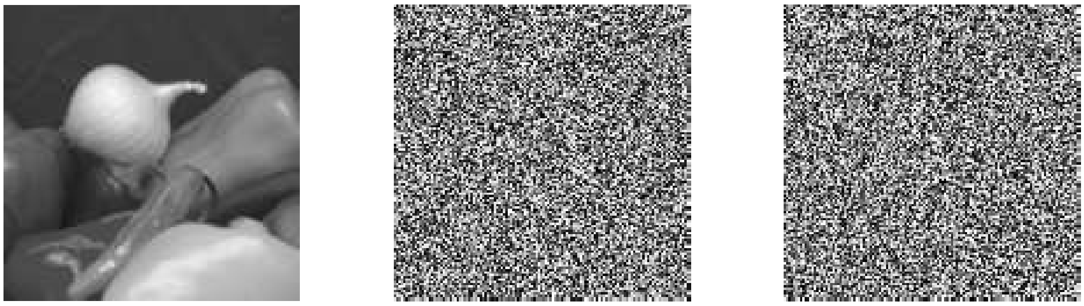


FIGURE 5.16: Distribution de corrélation des pairs de pixels adjacents dans les images originale et chiffrée de Légumes verts. (a) la corrélation des pixels horizontalement adjacents dans l'image originale, (b) la corrélation des pixels horizontalement adjacents dans l'image chiffrée, (c) la corrélation des pixels verticalement adjacents dans l'image originale, (d) la corrélation des pixels verticalement adjacents dans l'image chiffrée, (e) la corrélation des pixels diagonalement adjacents dans l'image originale, (f) la corrélation des pixels diagonalement adjacents dans l'image chiffrée.

l'avons trouvé égal à 99.7925%.



(a) Image originale (b) Image chiffrée (c) Image déchiffrée

FIGURE 5.17: L'image de Légumes verts déchiffrée par une clé légèrement différente.

- Analyse de l'espace de la clé

Dans ce schéma proposé, la clé secrète est composée de :

– Les paramètres et les ordres fractionnaires du système de Hénon modifié d'ordre fractionnaire $(a, b, \alpha_1, \alpha_2)$.
– Les paramètres et les ordres fractionnaires du système de Lozi d'ordre fractionnaire $(\bar{a}, \bar{b}, \bar{\alpha_1}, \bar{\alpha_2})$.
– Les clés additionnelles (c, d, e, f, g, h).

La sensibilité de chaque paramètre de la clé du système, où la taille de l'intervalle de variation est $s_i = 0.1$, est présentée au tableau 5.8. De cette manière, la taille N de l'espace de la clé est obtenu :

$$N = \prod_{i=1}^{14} = 10^{(14\times 8+11\times 6)} = 10^{178} >> 2^{100} \tag{5.12}$$

Paramètres p_i	Sensibilité S_i	Nb. de possibilités : $(N_i = s_i \times S_i^{-1})$
$a = 1.5$	$S_1 = 10^{-15}$	$N_1 = 10^{14}$
$b = 0.1$	$S_2 = 10^{-15}$	$N_2 = 10^{14}$
$\bar{a} = 1.7$	$S_3 = 10^{-15}$	$N_3 = 10^{14}$
$\bar{b} = 0.5$	$S_4 = 10^{-15}$	$N_4 = 10^{14}$
$\alpha_1 = 0.85$	$S_5 = 10^{-15}$	$N_5 = 10^{14}$
$\alpha_2 = 0.9$	$S_6 = 10^{-15}$	$N_6 = 10^{14}$
$\bar{\alpha}_1 = 0.95$	$S_7 = 10^{-15}$	$N_7 = 10^{14}$
$\bar{\alpha}_2 = 0.95$	$S_8 = 10^{-15}$	$N_8 = 10^{14}$
$c = 9.23$	$S_9 = 10^{-12}$	$N_9 = 10^{11}$
$d = 1.87$	$S_{10} = 10^{-12}$	$N_{10} = 10^{11}$
$e = 13.4$	$S_{11} = 10^{-12}$	$N_{11} = 10^{11}$
$f = 0.01$	$S_{12} = 10^{-12}$	$N_{12} = 10^{11}$
$g = 0.15$	$S_{13} = 10^{-12}$	$N_{13} = 10^{11}$
$h = 3.91$	$S_{14} = 10^{-12}$	$N_{14} = 10^{11}$

TABLE 5.8: Sensibilité aux paramètres

5.3.2 Un nouveau schéma de chiffrement/déchiffrement d'images en couleur basé sur la synchronisation des systèmes chaotiques d'ordre fractionnaire

À travers cette partie, un nouveau schéma de chiffrement/déchiffrement d'images en couleur basé sur la synchronisation des systèmes chaotiques d'ordre fractionnaire est présenté [48]. La méthode proposée est basée sur la structure de permutation-diffusion. Les paramètres et les ordres fractionnaires du système chaotique jouent le rôle de clés secrètes du crypto-système. Le principe du schéma de communication sécurisée proposé est illustré par la figure 5.18. Durant le chiffrement, nous considérons le système hyper-chaotique de Hénon modifié d'ordre fractionnaire (4.35), où $a = 1.6$, $b = 0.1$, $\alpha_1 = 0.97$, $\alpha_2 = 0.94$ et $\alpha_3 = 0.91$. Ce système est utilisé afin de générer des séquences pseudo-aléatoires que nous utilisons pour permuter et chiffrer les pixels de l'image originale. La fonction de chiffrement utilisée est l'opération XOR. La procédure complète de l'algorithme de chiffrement est présentée comme suit :

. **Première étape :**

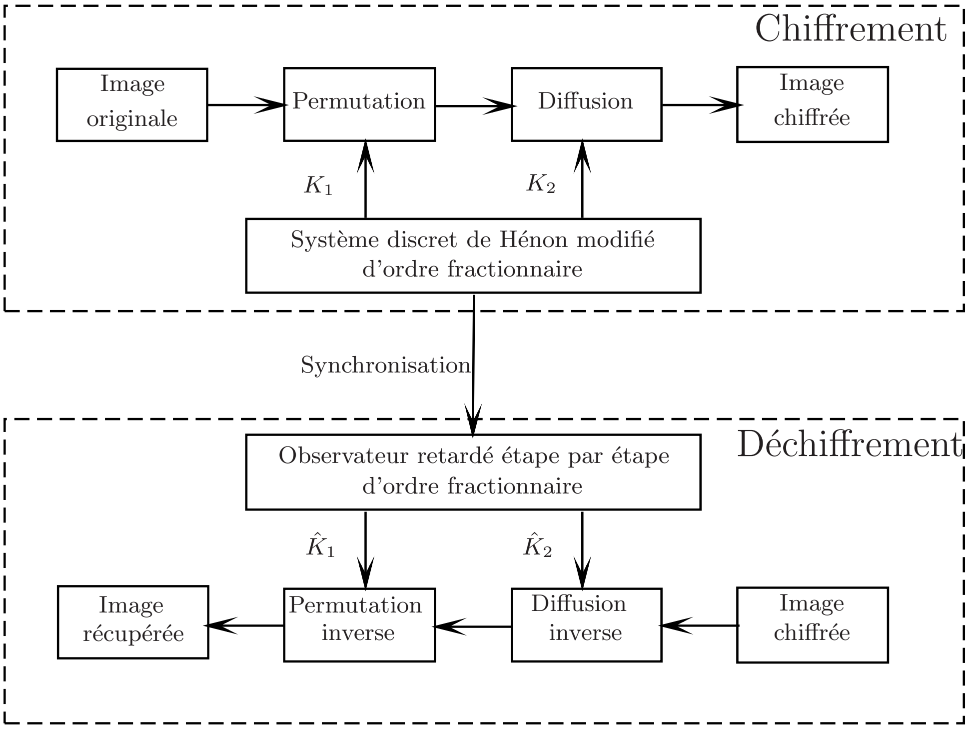


FIGURE 5.18: Schéma de transmission sécurisée D.

Considérons l'image en couleur originale d'un nombre de taille $M \times N$. Dans un premier temps, l'image originale est convertie en 3 images au niveau de gris (rouge, vert, bleu). Ensuite, nous présentons les 3 images par 3 matrices de taille $(M \times N)$, où M et N présentent le nombre de lignes et de colonnes de l'image. Par la suite, nous concaténons les lignes des 3 matrices et nous les associons afin d'obtenir un vecteur $A = \{A_1, A_2, \ldots, A_{M \times N \times 3}\}$.

. **Deuxième étape :**

Le système de Hénon modifié d'ordre fractionnaire (4.35) est considéré afin d'obtenir les séquences chaotiques (x_1, x_2, x_3). Un pré-traitement des séquences obtenues est effectué comme suit :

1.
$$\begin{aligned} B_1(k) &= cx_1^2(k) + d(x_1(k) + x_3(k)) + ex_3^2(k) \\ B_2(k) &= mod((fB_1(k) - gB_1(k)) \times 10^{12}, 255) \\ K_1(k) &= sort(B_2(k)) \end{aligned} \tag{5.13}$$

2.
$$K_2(k) = de2bi(B_2(k)) \tag{5.14}$$

avec c, d, e, f et g sont les nouvelles clés secrètes, où $c = 0.1$, $d = 0.1$, $e = 0.1$, $f = 0.1$ et $g = 0.1$, et *sort* est une commande Matlab permettant de ranger les éléments d'un vecteur.

. **Troisième étape :**

Au niveau de cette étape, l'image originale $A(k)$ est permuté en utilisant le vecteur $K_1(k)$ donné par l'équation (5.13), qui correspond à un vecteur brouillé. Ainsi, l'image permutée est obtenue, nommée $C(k)$.

. **Quatrième étape :**

L'image permutée est maintenant convertie en binaire,

$$D(k) = de2bi(C(k)) = \{C_1, C_2, \ldots, C_{M\times N\times 24}\} \tag{5.15}$$

Par la suite, nous chiffrons l'image permutée $D(k)$ par la clé $K_2(k)$. La fonction de chiffrement correspond à l'opération XOR.

$$m_c(k) = D(k) \oplus K_2(k) \tag{5.16}$$

Enfin, l'image chiffrée obtenue de taille $(M \times N \times 3)$ est convertie en image couleur de taille $(M \times N)$.

Lors du déchiffrement, l'observateur étape par étape (4.46) est considéré afin d'assurer la synchronisation du système de Hénon modifié d'ordre fractionnaire et la reconstruction des clés $\hat{K}_1$ et $\hat{K}_2$. Ainsi, le déchiffrement de l'image chiffrée est effectué de la même manière que pour le chiffrement de l'image originale en utilisant les mêmes clés secrètes. De cette manière, l'image originale est reconstruite.

4.3.2.1 Résultats de simulation et analyse de sécurité

Dans cette partie, nous considérons l'image de Lena en couleur de taille 128×128. Les paramètres et les ordres non entiers du système (4.35) sont pris : $a = 1.6$, $b = 0.1$, $\alpha_1 = 0.97$, $\alpha_2 = 0.94$ et $\alpha_3 = 0.91$. Les nouvelles clés du système (5.13) sont choisies : $c = 0.1$, $d = 0.1$, $e = 0.1$, $f = 0.1$ et $g = 0.1$. Dans ce qui suit, nous allons tester notre schéma par rapport au différentes analyses de sécurité.

- Analyse statistique

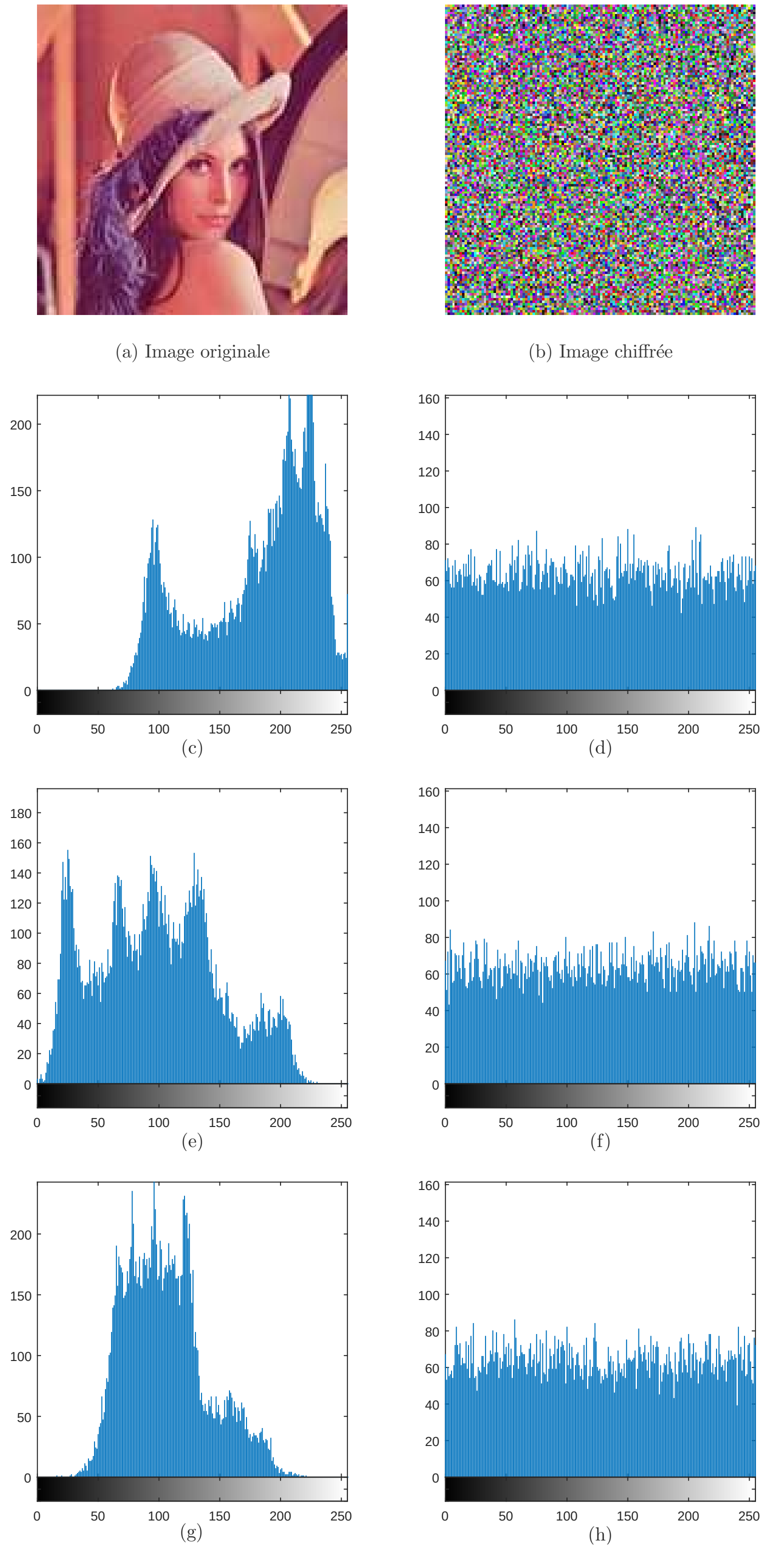
L'analyse statistique de l'algorithme de chiffrement proposé est montrée par les tests d'histogrammes, les corrélations des pixels adjacents ainsi que le test de χ^2 (*chi-square test*).

- Analyse par histogramme

Un système cryptographique de haut niveau de sécurité doit reproduire des images cryptées avec une distribution uniforme des pixels dans chaque canal de couleur, afin de cacher la répartition de l'image originale. Dans le but d'étudier la distribution des valeurs des pixels d'une image couleur, nous allons utiliser l'outil d'analyse visuelle qui correspond à l'histogramme des trois composantes couleurs, dans lequel les fréquences des valeurs des pixels sont tracées séparément pour chaque canal de couleur.
Dans la figure 5.19(a), est présentée l'image clair (Lena) et dans la figure 5.19(b), est montrée l'image chiffrée. Sur la figure 5.19(c, e et g), sont montrés les histogrammes des canaux rouge, vert et bleu de l'image claire et sur la figure 5.19(d, f et h), les histogrammes des canaux rouge, vert et bleu de l'image chiffrée, respectivement. A partir de la figure 5.19, nous pouvons voir que l'image chiffrée est complètement différente de l'image originale et est presque uniformément répartie, ce qui signifie que la méthode de chiffrement proposée résiste à l'analyse par histogramme. Afin de confirmer l'uniformité des histogrammes de l'image chiffrée, nous avons employé le test de χ^2 (voir l'équation (2.55)), avec un niveau de signification de $\alpha = 0.05$, et nous avons obtenu $\chi^2 = 254.0417$. Le résultat obtenu confirme le bon chiffrement de l'image de Lena.

- Corrélation des pixels adjacents

Il est évident qu'il existe une forte corrélation entre les pixels adjacents de l'image originale, il est donc nécessaire de réduire cette corrélation afin d'éviter l'attaque par analyse statistique. Pour tester la corrélation entre les pixels (horizontalement, verticalement ou diagonalement) adjacents, nous avons choisi de manière aléatoire 3000 paires de pixels séparément dans les directions horizontale, verticale et diagonale, et avons calculé les co-



(a) Image originale (b) Image chiffrée

(c) (d) (e) (f) (g) (h)

FIGURE 5.19: L'image de Lena (couleur) et son image chiffrée ainsi que ses histogrammes. Image originale (a) et image chiffrée (b). Composantes rouge (c), verte (e), bleue (g) de l'image originale. Composantes rouge (d), verte (f), bleue (h) de l'image chiffrée.

	Direction	Image originale	Image chiffrée
Image de Lena	Horizontale	0.9360	-0.0068
	Verticale	0.9697	$1.5543e-04$
	Diagonale	0.9118	-0.0055

TABLE 5.9: Coefficients de corrélation des pixels adjacents dans les trois directions.

	Image originale	Image cryptée
Composante rouge	7.2622	7.9889
Composante verte	7.5477	7.9900
Composante bleue	7.0089	7.9874

TABLE 5.10: Entropie d'information des images originale et chiffrée.

efficients de corrélation de chaque paire par la formule (2.56). Le Tableau 5.9 présente les coefficients de corrélation des pixels adjacents de l'image de Lena.

La figure 5.20 montre la distributions des corrélations des pixels adjacents des images originale et chiffrée. Les résultats montrent qu'il existe une forte corrélation entre les pixels de l'image originale, tandis que celles de l'image chiffrée sont très faibles.

- Entropie d'information

Nous avons calculé l'entropie de l'image de Lena (originale et chiffrée) en utilisant l'équation (2.60). Nous pouvons voir que les entropies de l'image claire sont relativement petites, par contre celles de l'image cryptée sont très proches de la valeur 8 ; elles sont présentées par le Tableau 5.10.

- Analyse de la sensibilité de la clé

Pour évaluer la sensibilité du schéma proposé à la clé de chiffrement, nous allons considérer deux cas. Premièrement, nous chiffrons l'image claire (Lena) en utilisant deux clés de chiffrement qui diffèrent légèrement au niveau de l'ordre α_1 ($\alpha_1 = \alpha_1 + 10^{-14}$). Nous constatons d'après la figure 5.21, que les images chiffrées (figure 5.21(b) et figure 5.21(c)) sont totalement différentes ; ceci est confirmé par l'image de différence (figure 5.21(e)) entre les deux images chiffrées (figure 5.21(b) et 5.21(c)). Le tableau 5.11 présente

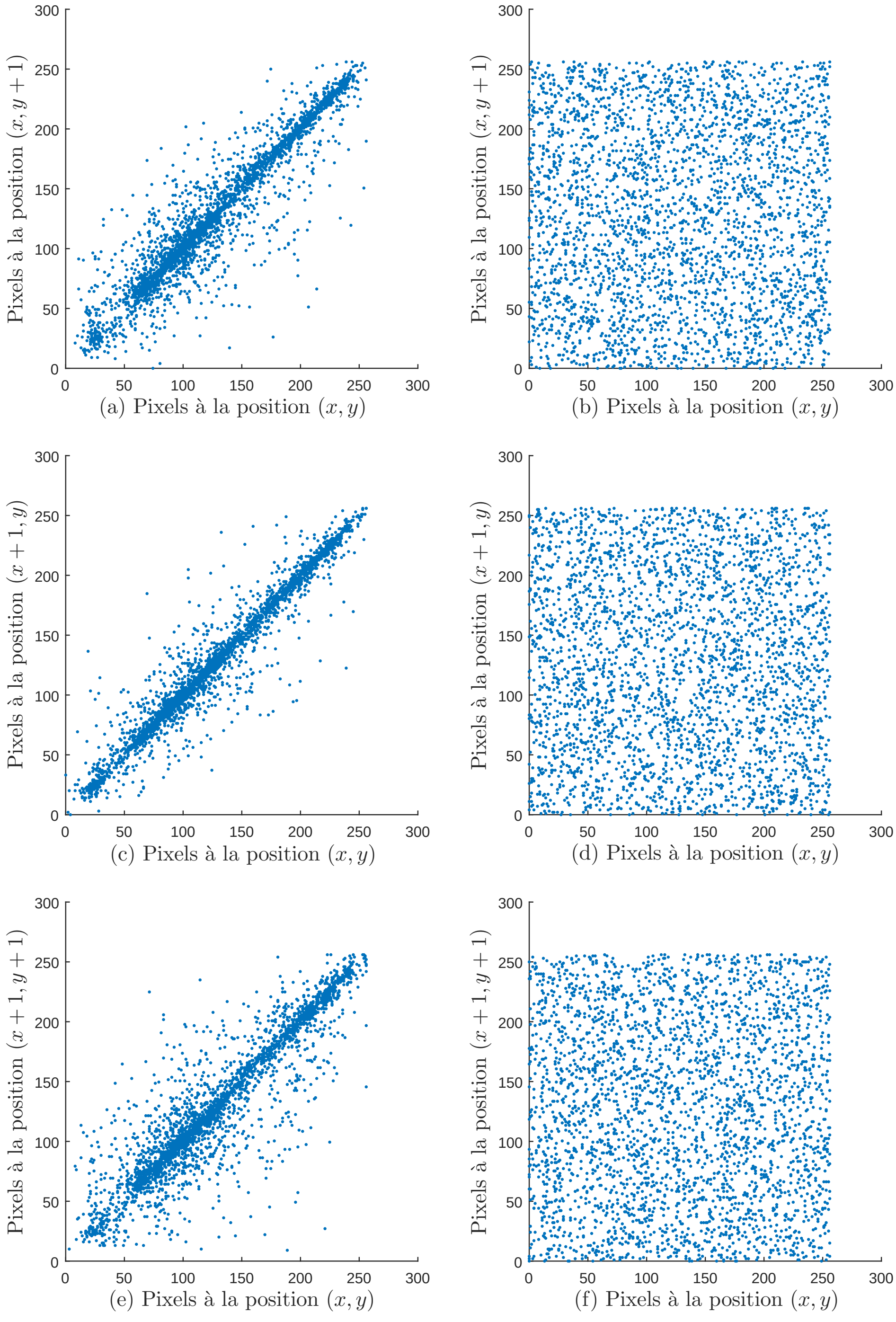


FIGURE 5.20: Distribution de corrélation des pairs de pixels adjacents dans les images originale et chiffrée de Lena (couleur). (a) la corrélation des pixels horizontalement adjacents dans l'image originale, (b) la corrélation des pixels horizontalement adjacents dans l'image chiffrée, (c) la corrélation des pixels verticalement adjacents dans l'image originale, (d) la corrélation des pixels verticalement adjacents dans l'image chiffrée, (e) la corrélation des pixels diagonalement adjacents dans l'image originale, (f) la corrélation des pixels diagonalement adjacents dans l'image chiffrée.

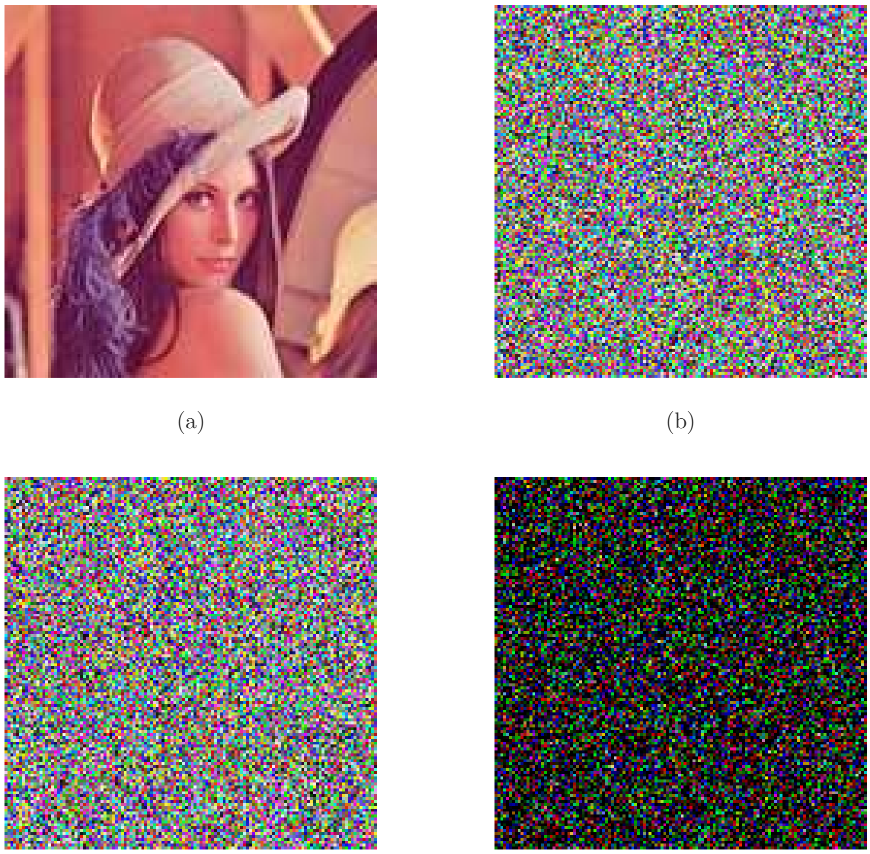


FIGURE 5.21: Sensibilité à la clé de chiffrement. (a) image claire, (b) image chiffrée avec la première clé, (c) image chiffrée avec la deuxième clé, (d) image de différence.

Clé secrète	$NPCR(\%)$	$UACI(\%)$
Paramètre modifié $a + 10^{-13}$	99.5768	33.5198
Ordre fractionnaire modifié $\alpha_1 + 10^{-14}$	99.6440	33.3677
Coefficient modifié $c + 10^{-13}$	99.4466	34.1570

TABLE 5.11: $NPCR$ et $UACI$ de deux images chiffrées par des clés légèrement différentes.

quelques valeurs de $NPCR$ et $UACI$ entre deux images chiffrées par des clés différentes au niveau de quelques paramètres. En deuxième lieu, nous déchiffrons l'image chiffrée en utilisant la clé de chiffrement réelle et avec une autre clé qui diffère de la clé réelle d'un seul paramètre a ($a = a + 10^{-5}$). Les résultats présentés sur la figure 5.22 montrent que dans le premier cas (figure 5.22(c)), nous arrivons à retrouver l'image originale, par contre dans le second cas (figure 5.22(e)), l'image obtenue est erronée. Le $NPCR$ et $UACI$ des images originale et déchiffrée sont obtenues ($NPCR = 99.6257\%$ et $UACI = 30.2920\%$).

- Analyse de l'espace de la clé

Dans cette partie, nous souhaitons évaluer la sécurité de système proposé en terme d'espace de clés. La taille N de l'espace de clés est déterminée en fonction des paramètres du système (a, b), les ordres fractionnaires (α_1, α_2) et les clés secrètes additionnelles (c, d, e, f, g). Nous supposons que la précision de chaque paramètre est au minimum 10^{-10}, ainsi la taille de l'espace de clés est :

$$N = \prod_{i=1}^{9} = 10^{(10\times 9)} = 10^{90} \gg 2^{100} \tag{5.17}$$

Nous pouvons clairement voir l'espace de clés de la méthode proposée est assez grand. Cela permet à notre système de résister efficacement contre l'attaque exhaustive (ou par force brute).

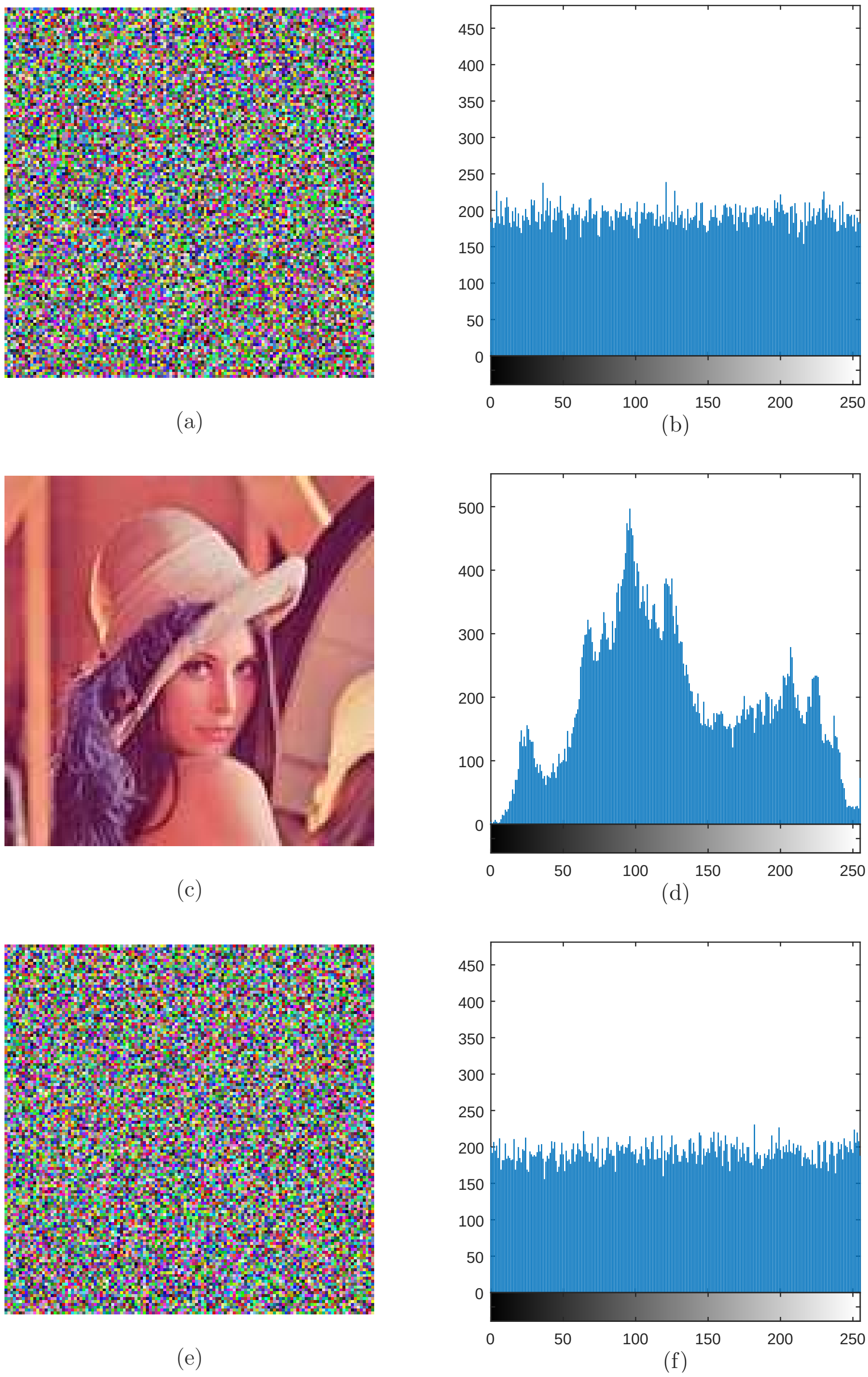


FIGURE 5.22: Sensibilité à la clé de déchiffrement (a) image chiffrée avec la première clé, (c) image déchiffrée avec la première clé, (e) image déchiffrée avec la deuxième clé (f) ainsi que leurs histogrammes correspondants.

5.4 Conclusion

Dans ce chapitre, la synchronisation des systèmes chaotiques à base d'observateur étape par étape est utilisée pour concevoir des méthodes efficaces pour la transmission sécurisée d'images. Dans le premier schéma de chiffrement proposé, les paramètres, les ordres non entiers du système chaotique et les clés secrètes externes sont utilisés pour rendre la relation entre l'image originale et l'image chiffrée plus confuse. En outre, pour rendre le chiffrement plus robuste contre toute attaque, l'image chiffrée est noyée dans la dynamique du système chaotique. La robustesse du système proposé est encore renforcée par la transmission sur un seul canal, ce qui rend le schéma proposé plus efficace. Deux variantes du schéma proposé sont également présentées. Dans le premier schéma, deux systèmes chaotiques couplés sont utilisés, où l'observateur impulsif est employé en plus de l'observateur étape par étape afin de garantir la synchronisation des deux systèmes chaotiques. Un autre schéma de chiffrement d'images couleur est proposé, où l'image originale est permutée puis chiffrée par des clés générées à partir d'un système chaotique. Dans ce cas, l'observateur étape par étape est également utilisé pour assurer la synchronisation avec le système chaotique, et garantir la reconstruction de l'image originale. Les résultats de simulation montrent que les techniques de cryptage d'image proposées possèdent plusieurs caractéristiques intéressantes, telles que la distribution uniforme des pixels des images chiffrées, le niveau de sécurité élevé et l'espace des clés assez grand. De plus, il a été montré que le crypto système présenté possède une extrême sensibilité des images chiffrée/déchiffrée aux petites variations de la clé de chiffrement/déchiffrement.

Chapitre 6

Conclusion Générale

Le travail effectué dans le cadre de cette thèse consiste en l'élaboration d'un nouveau schéma de transmission sécurisée de données basé sur les générateurs de séquences chaotiques d'ordre fractionnaire.

Dans une première étape, nous avons synthétisé un observateur exact étape par étape, pour les systèmes chaotiques discrets d'ordre fractionnaire en vue de l'utiliser dans un schéma de transmission sécurisée de données. Cet observateur est inséré au niveau du récepteur dans le but d'assurer sa synchronisation avec l'émetteur ainsi que la récupération de l'information noyée dans sa dynamique. Pour cela, nous avons étudié la condition d'observabilité des systèmes non linéaire affines en l'entrée discrets d'ordre fractionnaire. En outre, nous avons étudié la condition de recouvrement d'observabilité pour cette catégorie de systèmes.

Afin d'exploiter les résultats obtenus, le système de Hénon modifié d'ordre fractionnaire est considéré comme un premier exemple d'application. Les conditions d'observabilité et de recouvrement ont été vérifiées et, par conséquent, l'observateur exact étape par étape est conçu pour ce système. Par la suite, l'observateur développé est appliqué dans un schéma de communications sécurisées afin de transmettre en sécurité deux types de signaux.

Les résultats de simulation sur la synchronisation des états et du message de l'émetteur avec ceux estimés au niveau du récepteur sont obtenus à l'aide du logiciel Matlab. Les résultats que nous avons obtenus confirment le bon fonctionnement de l'observateur et, bien sûr, le bon choix de son application dans les schémas de transmission sécurisée.

En vue des applications potentielles et de l'importance d'avoir un cryptosystème fiable pour le chiffrement d'image, nous avons proposé dans la deuxième étape, un nouveau schéma de transmission sécurisée robuste basé sur la synchronisation par observateur étape par étape, que nous avons développé dans la première partie. L'efficacité du schéma proposé est démontrée avec succès contre les attaques de cryptanalyse. Les résultats de simulations montrent que la méthode de chiffrement d'images proposée possède plusieurs caractéristiques intéressantes, telles que la distribution uniforme des pixels de l'image chiffrée, la bonne propriété d'entropie d'information, une grande sensibilité à la clé de chiffrement/déchiffrement et l'espace de clés largement grand permettant de résister à l'attaque par force brute.

Dans la troisième partie, nous avons proposé deux variantes du schéma de transmission sécurisée d'images élaboré. Dans la première variante, nous avons réalisé un schéma de transmission hybride basé sur la synchronisation de deux systèmes chaotiques couplés. Au niveau du récepteur, deux types d'observateurs ont été développés, à savoir l'observateur impulsif et l'observateur étape par étape. Une analyse de performance du schéma proposé est effectuée pour montrer l'efficacité de la méthode décrite. Par la suite, nous avons présenté un troisième schéma pour la transmission sécurisée d'images couleur. Dans ce schéma, l'image originale est d'abord permutée, puis cryptée en utilisant deux séquences clés générées à partir du système chaotique d'ordre fractionnaire. Dans ce cas, la synchronisation à base d'observateur étape par étape est effectuée dans le but d'estimer les clés lors du déchiffrement. Nous avons également analysé la robustesse du schéma proposé contre différentes attaques de cryptanalyse.

En perspective, nous envisageons une suite aux travaux présentés dans cette thèse, qui sont entre autre :

1. Une validation expérimentale des schémas présentés.

2. Amélioration des performances des schémas proposés (diminution du temps d'exécution, considération du bruit de canal).

3. Développement de nouvelles approches de synchronisation à base d'observateurs

pour les systèmes chaotiques d'ordre fractionnaire.

4. Application des nouvelles approches dans les schémas de transmission sécurisée de données, images, vidéos et sons.
5. Cryptanalyse pour les crypto-systèmes à base du chaos fractionnaire.

Bibliographie

[1] W. Stallings, *Cryptography and Network Security*, 5th edn. Prentice-Hall, Englewood Cliffs, 2011.

[2] A. J. Menezes, P. C. Oorschot, S. A. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL : CRC Press. 1996.

[3] D. Kahn, *La Guerre des codes secrets, des hiéroglyphes à l'ordinateur*, InterEditions, 1980.

[4] S. Singh, *The science of secrecy from ancient Egypt to quantum cryptography*, Anchor Books, 1999.

[5] Data Encryption Standard, *Federal Information Processing Standards Publication* (FIPS PUB) 46, National Bureau of Standards, Washington, DC , 1977.

[6] Standard ANS X9.52 de l'ANSI, 1993.

[7] W. Diffie, M.E. Hellman, *New directions in cryptography*, IEEE transactions on information theory, Vol. IT-22, No. 6, pp. 644-654, 1976.

[8] R.L. Rivest, A. Shamir, L. Adleman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, Communications of the ACM, Vol. 21, pp. 120-126, 1978.

[9] H. C. Williams, *A modification of the RSA public-key encryption procedure*, IEEE Transactions on Information Theory, 26, pp. 726-729, 1980.

[10] T. Kean, A. Duncan, *DES key breaking, encryption and decryption on the XC6216*, IEEE Symposium on FPGAs for Custom Computing Machines, 15-17, pp. 310-311, 1998.

[11] M. J. Wiener, *Cryptanalysis of short RSA secret exponents*, IEEE Transactions Information Theory, 36, pp. 553-558, 1990.

[12] C. Bennett, G. Brassard. *Quantum Cryptography : Public Key Distribution and Coin Tossing*, IEEE Conf. on Computers, Systems and Signal Processing, Bangalore, India, pp. 175, 1984.

[13] A. K. Ekert, *Quantum cryptography based on Bell's theorem*, Phys. Rev. Lett. 67, 661, 1991.

[14] M.S. Baptista, *Cryptography with chaos*, Physics Letters A, 240, pp. 50-54, 1998.

[15] L. Kocarev, *Chaos-based cryptography : A brief overview*, IEEE Circuits and Systems Magazine, 1, pp. 6-21, 2001.

[16] G. Jakimoski, L. Kocarev, *Chaos and cryptography : block encryption ciphers based on on chaotic maps*, Circuits and systems I : Fundamental Theory and Application, IEEE Transactions on, 48(2), pp. 163-169, 2001.

[17] G. Alvarez and S. Li, *Some Basic Cryptographic requirements for chaos-based cryptosystems*, International Journal of Bifurcation and Chaos, 16, pp. 2129- 2151, 2006.

[18] W. Perruquetti, J.-P. Barbot, *Chaos in Automatic Control*, CRC Press, Boca Raton, 2006.

[19] J. Daemen, V. Rijmen, *The Design of Rijndael : AES-The Advanced Encryption Standard*, Springer, Berlin, 2002.

[20] E.N. Lorenz, *Deterministic Nonperiodic Flow*, J. Atmos. Sci., 20(2), pp. 130-141, 1963.

[21] L.M. Pecora, T.L. Carroll, *Synchronization in chaotic systems*, Phys. Rev. Lett. 64, pp. 821-824, 1990.

[22] H. Nijmeijer, I.M.Y. Mareels, *An Observer Looks at Synchronization*, IEEE Trans. on Circuits Systems. I. Fundam. Theory Appl. 44(10), 882-890, 1997.

[23] A.A. Kilbas, H.M. Srivastava, J.J. Trujillo, *Theory and applications of fractionnal differential equations*, Elsevier, North-Holland, 2006.

[24] K.B. Oldham, J. Spanier, *The fractional calculus.* Academic Press. New-York, 1974.

[25] K.S. Miller, B. Ross, *Fractional difference calculus, in : Proceedings of the International Symposium on Univalent Functions*, Fractional Calculus and Their Applications, Nihon University, Koriyama, Ellis Horwood Ser. Math. Appl., Horwood, Chichester, pp. 139-152, 1989.

[26] C.A. Monje, Y.Q. Chen, B.M. Vinagre, D. Xue, V. Feliu, *Fractional-order Systems and Controls : Fundamentals and Applications*, Springer, Berlin, 2010.

[27] H. Zhu, S. Zhou, J. Zhang, *Chaos synchronization of the fractional order chen's systems*, Chaos, Solitons and Fractals, 39(4), pp. 1595-1603, 2009.

[28] G.C. Wu, D. Baleanu, *Chaos synchronization of the discrete fractional logistic map*, Signal Processing, 102, pp. 96-99, 2014.

[29] C. Li, J. Zhang, *Synchronization of a fractional-ordre chaotic system using finite-time input-to-state stability*, International Journal of Systems Science, 47(10), pp. 2440-2448, 2016.

[30] I. Podlubny, *Geometric and physical interpretation of fractional integration and fractional differentiation*, Fract. Calc. Appl. Anal. 5, pp. 367-386, 2002.

[31] 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*, Communications in Nonlinear Science and Numerical Simulation, 14, pp. 863-879, 2009.

[32] R. Martínez-Guerra, C. A. Pérez-Pinacho, G. C. Gómez-Cortés, *Synchronization of Integral and Fractional Order Chaotic Systems : A Differential Algebraic and Differential Geometric Approach With Selected Applications in Real-Time*, Springer, 2015.

[33] A. T. Azar, S. Vaidyanathan, A. Ouannas, *Fractional Order Control and Synchronization of Chaotic Systems*, Springer, 2017.

[34] J. Sabatier, O. Agrawal, J.A.T. Machado, *Advances in Fractional Calculus : Theoretical Developments and Applications in Physic and Engineering*, Springer, Berlin, 2007.

[35] J. Zhao, S. Wang, Y. Chang, X. Li,*A novel image encryption scheme based on an improper fractional-order chaotic system*. Nonlinear Dyn. 80, 1721-1729, 2015.

[36] Y.Q. Wang, S.B. Zhou, *Image encryption algorithm based on fractional-order Chen chaotic system*. J. Comput. Appl. 33(4), 1043-1046, 2013.

[37] S. Guermah, M. Bettayeb, S. Djennoune, *Controllability and the Observability of Linear Discrete-time Fractional-order Systems*, International Journal of Applied Mathematics and Computer Science, 18, pp. 213-222, 2008.

[38] F. M. Atici, S. Senguel, *Modeling with fractional difference equations*, J. Math. Anal. Appl, 369, pp. 1-9, 2010.

[39] G.C. Wu, D. Baleanu, *Discrete fractional logistic map and its chaos*, Nonlinear Dyn, 75, pp. 283-287, 2014.

[40] G.C. Wu, D. Baleanu, S.D. Zeng, *Discrete chaos in fractional sine and standard maps*, Phys. Lett. A, 378, pp. 484-487, 2014.

[41] Y. Liu, *Discrete Chaos in Fractional Henon Maps*, International Journal of Nonlinear Science, 18(3), pp. 170-175, 2014.

[42] H. Hamiche, S. Kassim, S. Djennoune, S. Guermah, M. Lahdir, M. Bettayeb, *Secure data transmission scheme based on fractional-order discrete chaotic system* , International Conference on Control, Engineering and Information Technology (CEIT'2015). Tlemcen, Algeria, 2015.

[43] 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, pp. 2473-2489, 2017.

[44] S. Kassim, O. Megherbi, H. Hamiche, S. Djennoune, M. Lahdir, M. Bettayeb, *Secure image transmission scheme using hybrid encryption methods*, International Conference on Automatic Control.Telecommunications and Signals (ICATS'2015). Annaba, Algeria, 2015.

[45] S. Kassim, H. Hamiche, S. Djennoune, O. Megherbi, M. Bettayeb, *A novel robust image transmission scheme based on fractional-order discrete chaotic systems*, Inter-

national Workshop on cryptography and its applications (IWCA'16). Oran, Algeria, 2016.

[46] O. Megherbi, S. Kassim, H. Hamiche, S. Djennoune, M. Bettayeb,*A New Robust Hybrid Transmission Scheme based on the Synchronization of Discrete-Time Chaotic Systems*, International Workshop on cryptography and its applications (IWCA'16). Oran, Algeria, 2016.

[47] O. Megherbi, S. Kassim, H. Hamiche, S. Djennoune, M. Bettayeb, J-P. Barbot,*Robust Image Transmission Scheme Based on Coupled Fractional-Order Chaotic Maps*, SIAM Conference on Control and Its Applications (CT17), USA, July 10-14, 2017.

[48] S. Kassim, H. Hamiche, S. Djennoune, M. Bettayeb, *Secure color image transmission scheme based on synchronization of fractional-order discrete-time hyperchaotic systems*, Accepté pour présentation à The International Conference on Fractional Differentiation and its Applications (ICFDA'2018), Amman, The Hashemite Kingdom of Jordan, 16-18 July, 2018.

[49] H. Hamiche, S. Kassim, O. Megherbi, S. Djennoune, M. Bettayeb, *Secure Digital Data Communication Based on Fractional-Order Chaotic Maps*, Advanced Synchronization Control and Bifurcation of Chaotic Fractional-Order Systems, pp. 438-467, Editeur IGI Global, 2018.

[50] E. Alvarez, A. Fernandez, P. Garcia, J. Jimenez, A. Marcano, *New approach to chaotic encryption*, Physics Letters A, 263, pp. 373-375, 1999.

[51] N.K. Pareek, V. Patidar, K.K. Sud, *Discrete chaotic cryptography using external key*, Physics Letters A, 309, pp. 75-82, 2003.

[52] G. Chen, Y. Mao, C.K. Chui, *A symmetric image encryption scheme based on 3d chaotic cat maps*, Chaos, Solitons & Fractals, 21(3), pp. 749-761, 2004.

[53] C.E. Shannon, *A mathematical theory of communication*, The Bell System Technical Journal, Vol. 27, pp. 379 - 423, 623 - 656, 1948.

[54] C.E. Shannon, *Communication theory of secrecy systems*, Bell System Technical Journal, 28, pp. 656-715, 1949.

[55] A. Kerckhoffs, *La cryptographie militaire*, Journal des sciences militaires, Vol. IX, pp. 5 - 38, 161-191, 1883.

[56] L.S, Hill, *Cryptography in an Algebraic Alphabet*, The American Mathematical Monthly, Vol. 36, No. 6, pp. 306-312, 1929.

[57] H. Feistel, *Cryptography and computer privacy*, Scientific American, 228, pp. 15-23, 1973.

[58] H. Feistel, *Block cipher cryptographic system*, U.S. patent, 3, 798,359, 1974.

[59] T. El Gamal, *A public key cryptosystem and a signature based on discrete logarithms*, IEEE Transactions on Information Theory, 31(4), pp. 469-472, 1985.

[60] R.J. McEliece, *A Public-Key Cryptosystem Based on Algebraic Coding Theory*, Jet Propulsion Laboratory DSN Progress Report, pp. 42-44, 1978.

[61] R. Matthews, *On the derivation of a chaotic encryption algorithm*, Cryptologia, 13, pp. 29-41, 1989.

[62] O. Morgul, M. Feki, *A chaotic masking scheme by using synchronized chaotic systems*, Phys Lett A, 251(3), pp. 169-76, 1999.

[63] O. Morgul, E. Solak, *Observer based synchronization of chaotic systems*, Phys. Rev. E. 5, 4803-4811, 1996.

[64] J. -P. Barbot, M. Djemai, T. Boukhobza, *Sliding mode observers, in Sliding mode control in engineering*, Marcel Dekker, pp. 103-130, 2002.

[65] H. J. C. Huiberts, T. Lilge, H. Nijmeijer, *Nonlinear discrete-time synchronisation via extended observers,* International Journal of Bifurcation and Chaos, 11, pp. 1997-2001, 2001.

[66] O. Morgul, *Necessary condition for observer-based chaos synchronization*, Phys. Rev. Lett., 82, pp. 169-176, 1999.

[67] L. Kocarev, Z. Galias, S. Lian, *Intelligent computing based on chaos*, Springer-Verlag, 2009.

[68] H. Hamiche, M. Lahdir, M. Tahanout, S. Djennoune, *Masking digital image using a novel technique based on a transmission chaotic system and SPIHT coding algorithm.* Int. J. Adv. Comput. Sci. Appl. 3(12), pp. 228-234, 2012.

[69] H. Hamiche, S. Guermah, R. Saddaoui, K. Hannoun, M. Laghrouche, S. Djennoune, *Analysis and implementation of a novel robust transmission scheme for private digital communications using Arduino Uno board.* Nonlinear Dyn. 81(4), pp. 1921-1932, 2015.

[70] H. Hamiche, M. Ghanes, J-P. Barbot, K. Kemih, S. Djennoune, *Hybrid dynamical systems for private digital communications.* Int. J. Model. Identif. Control 20, 99-113, 2013.

[71] 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, 2016.

[72] H. Hamiche, M. Ghanes, J-P. Barbot, *Systèmes dynamiques hybrides pour les communications privées.* CIFA, Nancy, France, pp. 6, 2010.

[73] H. Hamiche, *Inversion à Gauche des Systèmes Dynamiques Hybrides Chaotiques. Application à la Transmission Sécurisée de Données*, Thèse de Doctorat en Sciences, Université Mouloud Mammeri de Tizi-Ouzou, Algérie, 2011.

[74] A. Senouci, *Élaboration de nouvelles approches de transmission sécurisée et cryptage par chaos*, Thèse de Doctorat en Sciences, Université de Jijel, Algérie, 2014.

[75] O. Megherbi, *Étude et réalisation d'un système sécurisé à base de systèmes chaotiques*, Mémoire de Magister, Université Mouloud Mammeri de Tizi-Ouzou, Algérie, 2013.

[76] B. Schneier, *The Blowfish Encryption Algorithm*, Dr Dobbs Journal 19, 38, 1994.

[77] J. Fridrich, *Symmetric ciphers based on two-dimensional chaotic maps*, International Journal of Bifurcation and Chaos, 8(06), pp. 1259-1284, 1998.

[78] S. El Assad, M. Farajallah, *A new chaos-based image encryption system*, Signal Processing : Image Communication, 41, pp. 144-157, 2016.

[79] X. Li, G. Zhang, X. Zhang, *Image encryption algorithm with compound chaotic maps*, Journal of Ambient Intelligence and Humanized Computing, 6(5), pp. 563-570, 2015.

[80] P.S. de Laplace, *Essai philosophique sur les probabilités. English ; A philosophical essay on probabilities [microform]*, J. Wiley, 1902.

[81] E. Ott, *Chaos in dynamical systems*, Cambridge University Press, 1993.

[82] S. H. Strogatz, *Non linear dynamics and chaos*, Preseus Books Publishing, LLC, 1994.

[83] T.S. Parker, L.O. Chua, *Practical Numerical Algorithms for Chaotic Systems*, Springer-Verlag, 1989.

[84] R.E. Kalman, *A new approach to linear filtering and prediction problems.* Transactions of the ASME. Journal of Basic Engineering, 82 pp. 35-45, 1960.

[85] D.G. Luenberger, *An introduction to observers.* IEEE Transactions on Automatic Control, 16, pp. 596-602, 1971.

[86] J. P. Gauthier, G. Bonard, *Observation for any u(t) of a classe of nonlinear systems.* IEEE transaction on Automatic control, 1994.

[87] H. Poincaré, *Science et méthode*, Ernest-Flammarion, 1908.

[88] T.Y. Li, J.A. Yorke, *Period three implies chaos.* American Mathematics Montly, 82, pp. 985-992, 1975.

[89] S. Sastry, *Nonlinear systems. Analyse, stability and control*, Springer-Verglas, 1999.

[90] H.K. Khalil, *Nonlinear systems*, 3^{rd} ed, Prentice Hall, Inc, 2002.

[91] F. Kais,*Analyse spectrale des signaux chaotique*, Thèse de Doctorat, Université de Tunis El Manar, 2014.

[92] H. Poincaré, *Mémoire sur les courbes définies par une equation différentielle.* J. Math. 7, 375-422, 1881. (Oeuvre, Gauthier-Villars, Paris, 1890)

[93] M. Hénon, *Numerical study of quadratic area preserving mappings*, Q. Appl. Math. 27, 1969.

[94] T. Yamada, H. Fujisaka, *Stability theory of synchronized motion in coupled oscillator system II.* Prog. Theor. Phys, 70, pp. 1240-1248, 1983.

[95] A. Pikovsky, M. Rosenblum, J. Kurths, *Synchronization, a universal concept in non-linear sciences*. Cambridge University Press, 2001.

[96] S. Boccaletti, J. Kurths, G. Osipov, D.L. Valladares, C.S. Zhou, *The synchronization of chaotic systems*. Phys. Rep. 366, pp. 1-2, 2002.

[97] N.F. Rulkov, M.M. Sushchik, L.S. Trimring, H.D.I. Abarbanel, *Generalized synchronization of chaos in biderctionally coupled chaotic systems*. Phys. Rev. E, 51(2), pp. 980-993, 1995.

[98] L.M. Pecora, T.L. Carroll, *Detecting chaotic drive-response geometry in generalized synchronization*. Int. J. of Bifurcation and Chaos (IJBC), 10(4), pp. 875-889, 2000.

[99] M.G. Rosenblum, A.S. Pikovsky, J. Kurths, *Phase synchronization in driven and coupled chaotic oscillators*. IEEE Trans. Circuits Syst. I, 44(10), pp. 874-881, 1997.

[100] O. Morgul, E. Solak, *On the synchronization of chaotic systems by using state observations*. Int. J. Bifurcations Chaos, 7(6), pp. 1307-1322, 1997.

[101] K.M. Cuomo, A.V. Oppenheim, S.H. Strogatz *Synchronization of Lorenz-Based Chaotic Circuits with Applications to Communications*. IEEE Transactions on Circuits and Systems II : Analog and Digital Signal Processing, 40(10), 1993.

[102] R. He, P.G. Vaidya, *Analysis and synthesis of synchronous periodic and chaotic systems*, Phys. Rev. A, 46, pp. 7387-7392, 1992.

[103] T. Kapitaniak, *Synchronization of chaos using continuous control*, Phys. Rev. E, 50, pp. 1642-1644, 1994.

[104] L. Kocarev, U. Parlitz,*General approach for chaotic synchronization with applications to communication*. Phys. Rev. Lett. 74, pp. 5028-5031, 1995.

[105] U. Parlitz, L. Kocarev, T. Stojanovski, H. Preckel, *Encoding messages using chaotic synchronization*, Phys. Rev. E, 53, pp. 4351 - 4361, 1996.

[106] J. Guemez, C. Martín, and M. A. Matias, *Approach to the chaotic synchronized state of some driving methods*, Phys. Rev. E, 55, pp. 124-134, 1997.

[107] T. L. Carroll, L. M. Pecora, *Synchronizing chaotic circuits*, IEEE Transaction on Circuit and Systems-I : Fundamental Theory And Applications, 38, pp. 453-456, 1991.

[108] L. Kocarev and U. Parlitz, *Generalized synchronization, predictability, and equivalence of unidirectionally coupled dynamical systems*, Phys. Rev. Lett., 76, pp. 1816-1819, 1996.

[109] R. Mainieri, J. Rehacek,*Projective synchronization in three chaotic systems*, Physical Review Letters, 82(15), pp. 3042-3045, 1999.

[110] Z. Li, D. Xu, *A secure communication scheme using projective chaos synchronization*, Chaos, Solitons and Fractals, 22, pp. 477-481, 2004.

[111] M.G. Rosenblum, A.S. Pikovsky, J. Kurths, *From Phase to Lag Synchronization in Coupled Chaotic Oscillators*, Phys. Rev. Lett, 78, pp. 4193-4196, 1997.

[112] C. Li, X. Liao, K.-W. Wong,*Chaotic lag synchronization of coupled time-delayed systems and its application in secure communication*, Systems and Control Letters, 7, pp. 133-142, 1986.

[113] M.G. Rosenblum, A.S. Pikovsky, J. Kurths. *Phase synchronization of chaotic oscillators*, Physical Review Letters, 76, pp. 1804-1807, 1996.

[114] T. Yang, L.O. Chua, *Impulsive stabilization for control and synchronization of chaotic systems : Theory and application to secure communications*, IEEE Transactions on Circuits and Systems I, 44(10), pp. 976-988, 1997.

[115] H. Hamiche, M. Ghanes, J.-P. Barbot, K. Kemih, S. Djennoune,*Chaotic synchronisation and secure communication via sliding-mode and impulsive observers*. Int. J. Model. Identif. Control, 20(4), pp. 305-318, 2013.

[116] 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.

[117] A. D. Angeli, R. Genesio, A. Tesi, *Dead-beat chaos synchronization in discrete-time systems*, IEEE Trans. Circ. Syst. I, 42(1), pp. 54-56, 1995.

[118] H. Sira-Ramirez, P. Rouchon, *Exact state reconstructors in the recovery of messages encrypted by the states of nonlinear discrete-time chaotic systems*, International Journal of Bifurcation and Chaos, 12(1), pp. 169-177, 2002.

[119] L. Kocarev, K.S. Halle, K. Eckert, L.O. Chua, U. Parlitz, *Experimental demonstration of secure communications via chaotic synchronisation*, International Journal of Bifurcation and Chaos, 2, pp. 709-713, 1992.

[120] 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, 3, pp. 1619-1627, 1994.

[121] K.M. Short, *Steps toward unmasking secure communications*, International Journal of Bifurcation and Chaos, 4, pp. 959-977, 1994.

[122] G. Perez, H. A. Cerdeira, *Extracting messages masked by chaos*, Phys. Rev. Lett., 74, pp. 1970-1973, 1995.

[123] T. Yang, L. B. Yang, C. M. Yang, *Application of neural networks to unmasking chaotic secure communication*, Physica D, 124, pp. 248-257, 1998.

[124] T. Yang, L. B. Yang, C. M. Yang, *Cryptanalysing chaotic secure communication using return maps*, Physics Letters A, 245, pp. 495-510, 1998.

[125] G. Alvarez, F. Montoya, M. Romena, G. Pastor, *Breaking two secure communication systems based on chaotic masking*, Circuits and System II : Express Briefs, IEEE Transaction on, 51(10), pp. 505-506, 2004.

[126] M. Itoh, H. Murakami, L. O. Chua, *Communication systems via chaotic modulations*, IEICE Transaction Fundamentals, E77-A, pp. 1000-1006, 1994.

[127] K. S. Halle, C. W. Wu, M. Itoh, L. O. Chua, *Spread spectrum communication through modulation of chaos in Chua's circuit*, International Journal of Bifurcation and Chaos, 3, pp. 469-477, 1993.

[128] J. Y. Chen, K. W. Wong, L. M. Cheng, J. W. Shuai, *A secure communcation scheme based on the phase synchronization of chaotic systems*, Chaos, 13, pp. 508-514, 2003.

[129] T. Yang, L. O. Chua, *Secure Communication via parameter modulation*, IEEE Transaction on Circuit and Systems-I : Fundamental Theory And Applications, 43, pp. 817-819, 1996.

[130] T. Yang, L. B. Yang, C. M. Yang, *Breaking chaotic secure communication using a spectrogram*, Physics Letters A, 247, pp. 105-111, 1998.

[131] K. M. Short, *Unmasking a modulated chaotic communications scheme*, International Journal of Bifurcation and Chaos, 6, pp. 367-375, 1996.

[132] G. Alvarez, F. Montoya, M. Romena, G. Pastor, *Breaking parameter modulated chaotic secure communication systems*, Chaos Solitons and Fractals, 21, pp. 783-787, 2004.

[133] H. Dedieu, M. P. Kennedy, M. Hasler, *Chaos shift keying : modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits*, IEEE Transaction on Circuit and Systems-II, 40, pp. 634-642, 1993.

[134] U. Parlitz, *Transmission of digital signals by chaotic synchronization*, International Journal of Bifurcation and Chaos, 2, pp. 973-977, 1992.

[135] T. L. Carroll, L. M. Pecora, *Using multiple attractor chaotic systems for communication*, Chaos, 9, pp. 445-451, 1999.

[136] G. Kolumban, M. P. Kennedy, L. O. Chua, *The Role of Synchronization in Digital Communications Using Chaos-part II : Chaotic Modulation and Chaotic Synchronization*, IEEE Transactions on Circuits and Systems-I : Fundamental Theory and Applications, 45, pp. 1129-1140, 1998.

[137] T. Yang, L. B. Yang, C. M. Yang, *Breaking chaotic swithing using generalized synchronization : examples*, IEEE Transactions on Circuits and Systems - I : Fundamental thoery and applications, 45, pp. 1062-1067, 1998.

[138] S. Li, G. Chen, G. Alvarez, *Return-map cryptanalysis revisited*, International Journal of Bifurcation and Chaos, 16, pp. 1557-1568, 2006.

[139] M. L'Hernault, J.-P. Barbot, A. Ouslimani, *Feasibility of analog realization of a Sliding-Mode Observer : Application to Data Transmission*, IEEE Transactions on Circuits and Systems I : Regular Papers, 55, pp. 614-624, 2008.

[140] H. Zhou, X. Ling, *Problems with the chaotic inverse system encryption approach*, IEEE Trans. Circuits Syst. I, 44, pp. 268-271, 1997.

[141] S. Diop, M. Fliess, "On nonlinear observability," in Proc. 1st Europ. Control Conf., Hermes, pp. 152-157, 1991.

[142] J.-P. Barbot, M. Fliess, T. Floquet, *An algebraic framework for the design of nonlinear observers with unknown inputs*, in 46th IEEE Conference on Decision and Control, New Orleans, LA 2007, pp. 384-389, 2007.

[143] H. Hamiche, *Inversion à Gauche des Systèmes Dynamiques Hybrides Chaotiques. Application à la Transmission Sécurisée de Données*, Thèse de Doctorat, UMMTO, 2013.

[144] R. W. Brockett, M. D. Mesarovic, *The reproducibility of multivariable systems*, J. Math. Anal. Appl., 11, pp. 548-563, 1965.

[145] M. K. Sain, J. L. Massey, *Invertibility of linear time-invariant dynamical systems*, IEEE Trans. Automat. Control, 14, pp. 141-149, 1969.

[146] L. M. Silverman, *Inversion of multivariable linear systems*, IEEE Trans. Automat. Control, vol. 14, pp. 270-276, 1969.

[147] D. Kahn, *The Codebreakers : The comprehensive history of secret communication from ancient times to the internet*, Simon and Schuster, 1996.

[148] M. S. Lewis-Beck, *Data analysis : An introduction.* 103. Sage, 1995.

[149] S. Manabe, *The non-Integer Integral and its Application to Control Systems*, ETJ of Japan, 6(3/4), pp. 83-87, 1961.

[150] B. Mandelbrot, *The fractal geometry of nature*, Freeman, San Fransisco, 1982.

[151] A. Oustaloup, *La dérivation non entière, théorie, synthèse et applications*, Hermès Edition, Paris, 1995.

[152] G. Montseny, *Diffusive representetion of pseudo-differential time-operators*, in Proc. Fractional Differential Systems :Methods and Applications, 5, pp. 159-175, 1998.

[153] N. Heymans, *Implementation of fractional calculus using hierarchical models : application to the terminal transition of a complex polymer*, in the Proc. of DETC 2003/VIB 48396 ASME, Chicago, USA, 2003.

[154] T.T. Hartley, C.F. Lorenzo, *Dynamics and Control of Initialized Fractional-Order Systems*, Nonlinear Dynamics, 29 pp. 201-233, 2002.

[155] A. Dzielinski, D. Sierociuk, *Adaptive Feedback Control of Fractional Order Discrete State-Space Systems*, Proc of the 2005 International Conference on Computational Intelligence for Modelling, Control and Automation, and International Conference on Intelligent Agents, Web Technologies and Internet Commerce (CIMCA-IAWTIC'05), Vienna, Austria, pp. 524-529, 2005.

[156] Y. Zhang, D. Xue, *Wireless Communications, Networking and Mobile Computing*, WiCom 2007.

[157] Y. Xu, H. Wang, Y. Li, B. Pei, *Image encryption based on synchronisation of fractional chaotic systems*, Commun. Nonlinear Sci. Numer. Simul. 19, pp. 3735-3744, 2014.

[158] I. Podlubny, *Fractional Differential Equations : Mathematics in Science and Engineering*. Academic Press, 1999.

[159] T.T. Hartley, C.F. Lorenzo, H.K. Qammer, *Chaos in a fractional order Chua's system*, IEEE Trans. Circ. Syst-I : Fund. Theor. Appl., 42(8), pp. 485-490, 1995.

[160] G.M Mittag-Leffler, *Sur la nouvelle fonction* $E_\alpha(x)$, C. R. Académie des sciences, Paris Series II, 137, pp. 554-558, 1903.

[161] P. Humbert, *Quelques resultats relatifs à la fonction de Mittag-Leffler*, C. R. Académie des sciences, Paris, 236, pp. 1467-1468, 1953.

[162] R.P. Argarwal, *A propos d'une note de M. Pierre Humbert*, C. R. Académie des Sciences, Paris, 236, pp. 2031-2032, 1953.

[163] S.G. Samko, A.A. Kilbas, O.I. Marichev, *Fractional Integrals and Derivatives*, Gordon and Breach Science Publishers, 1993.

[164] M. Caputo, *Linear models of dissipation whose q is almost frequency independent.* Geophysical journal of the royal astronomical society. 2(13), pp. 529-539, 1967.

[165] A.K. Grunwald, *Ueber begrenzte derivationen und deren anwendung.* Z. Angew. Math. Phys. 12, pp. 441-480, 1867.

[166] K.S. Miller, B. Ross, *An introduction to the fractional calculus and fractional differential equations.* A Wiley Interscience Publication, 1974.

[167] H.F. Raynaud, A. Zergainoh, *State-space representation for fractional-order controllers.* Automatica, 36, pp. 1017-1021, 2000.

[168] R. Hotzel, M. Fliess, *On linear system with fractional derivation : introductory theory and examples.* Mathematics and Computers in Simulation, 45, pp. 385-395, 1998.

[169] L. Dorcak, I. Petras, I. Kostial, *Modeling and analysis of fractional-order regulated systems in the state-space.* Proc. of ICCC'2000, Slovak Republic, pp. 185-188, 2000.

[170] J. Sabatier, O. Cois, A. Oustaloup, *Commande de systèmes non entiers par placement de pôles.* Deuxième Conférence Internationale Francophone D'Automatique, CIFA, France, 2002.

[171] 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.

[172] D. Sierociuk, A. Dzielinski, *Fractional Kalman filter algorithm for the states, parameters and order of fractional system estimation*, Int. J. Appl. Math. Comput. Sci., 16(1), pp. 129-140, 2006.

[173] D. Mozyrska, E. Pawluszewicz, *Observability of linear q-difference fractional order systems with finite initial memory*, Bull. Pol. Acad. Sci. Tech. Sci., 58(4), pp. 601-605, 2010.

[174] F. Atici, P. Eloe, *A transform method in discrete fractional calculus*, Int. J. Difference Equ., 2(2), pp. 165-176, 2007.

[175] A. Dzielinski, D. Sierociuk, *Reachability, controllability and observability of the fractional order discrete state-space System*, IEEE/IFAC International Conference on the Methods and Models in Automation and Robotics, MMAR'2007, Szczecin, Poland, 2007.

[176] G.A. Anastassiou, *Nabla discrete fractional calculus and nabla inequalities*. Mathematical and Computer Modeling, 51, pp. 562-571, 2010.

[177] T. Abdeljawad, *On Riemann and Caputo fractional differences*, Comput. Math. Appl, 62, pp. 1602-1611, 2011.

[178] M. T. Holm, *The Laplace transform in discrete fractional calculus*, Comput. Math. Appl. 62, pp. 1591-1601, 2011.

[179] F. M. Atici, P. W. Eloe, *Initial value problems in discrete fractional calculus*, Proc. Am. Math. Soc, 137, pp. 981-989, 2009.

[180] R.A.C. Ferreira, D.F.M. Torres, *Fractional h-difference equations arising from the calculus of variations*, Applicable Analysis and Discrete Mathematics, 2011.

[181] M. D. Ortigueira, F. J. Coito, J. J. Trujillo, *A new look into the discrete-time fractional calculus : derivatives and exponentials*, in : proceedings of the 6th Workshop on Fractional Differentiation and Its Applications, WTC, Grenoble, France, 2013.

[182] M. D. Ortigueira, *Introduction to fractional linear systems. Part2 : Discrete-time case*, IEE Proc. on Vision, Image and Signal Processing, 147, pp. 71-78, 2000.

[183] S. Guermah, S. Djennoune, M. Bettayeb, *Discrete-Time Fractional-Order Systems : Modeling and Stability Issues*, Advances in Discrete Time Systems, InTech publications, pp. 183-212, 2012.

[184] I. Podlubny, *Numerical solution of ordinary fractional differential equations by the fractional difference method*, in : S. Elaydi, I. Gyori, G. Ladas, (eds), Advances in difference equations, Gordon and Breach, Amsterdam, pp. 507-516, 1997.

[185] B. Kuttner, *On differences of fractional order*, Proceeding of the London Mathematical Society, 3, pp. 453-466, 1957.

[186] J.B. Diaz, T.J. Osler, *Differences of Fractional Order*, American Mathematical Society, 28, pp. 185-202, 1974.

[187] G.A. Anastassiou, *Discrete fractional calculus and inequalities*, arXiv :0911.3370v1 [math.CA], 2009.

[188] R. Mansouri, M. Bettayeb, S. Djennoune, *State Space fractional Model Approximation by taking account of the initial conditions*. Submited to the third International Conference on Modeling and Simulation ICMSAO'09. January 20-22, Sharjah, UAE, 2009.

[189] C.F. Lorenzo, T.T. Hartley. *Initialization of fractional differential equations : Theory and application*. Proccedings of the ASME 2007 International Design Engeneering Technical Conferences, DETC2007-34814., Las Vegas, USA, 2007.

[190] C.F. Lorenzo, T.T. Hartley, *Initialization of fractional-Order operators and fractional differential equations*. ASME Journal of Computational and Nonlinear Dynamics. April 2008, Vol. 3 /021101-pp1-9.

[191] J-C. Trigeassou, N. Maamri, *State space modeling of fractional differential equations and the initial condition problem*, In Systems, Signals and Devices, 2009. SSD'09. 6th International Multi-Conference on, pp. 1-7, March 2009.

[192] J.C. Trigeassou, N. Maamri, *Initial conditions and initialization of linear fractional differential equations*, Signal Processing, 91, pp. 427-436, 2011.

[193] J. Sabatier M. Merveillaut, R. Malti, A. Oustaloup, *On a representation of fractional order systems : Interests for the initial condition problem*, Inproc IFAC workshop on fractional differentiation and its applications, Ankara, Turquie, 2008.

[194] K.J. Aström, B. Wittenmark, *Computer-controlled systems, Theory and design*, 2nd edition, Prentice Hall, Englewoods Cliffs, New Jersey, 1990.

[195] D. Matignon, *Stability results on fractional differential equations with application to control processing*. In Computation Engineering in System Applications, pp. 963-968, 1996

[196] D. Matignon, B. D'Andréa-Novel, *Some results on controllability and observability of finite-dimensional fractional differential systems*. In IMACS, IEEE-SMC Proceedings Conference, France, pp. 952-956, 1996.

[197] D. Matignon, *Stability properties for generalized fractional differential systems*. In Proc. of the colloquium FDS'98 : Fractional differential systems : Models, Methods and Applications, 5, pp. 145-158, 1998.

[198] M. Bettayeb, S. Djennoune, *A note on the controllability and the observability of fractional dynamical systems*, Proceedings of the 2nd IFAC Workshop on Fractional Differentiation and its Applications (FDA'06), Portugal, 506-511, 2006.

[199] A. Dzielinski, D. Sierociuk, *Observers for discrete fractional order Systems*, Proceedings of th 2nd IFAC Workshop on Fractional Differentiation and its Application (FDA'06), Porto, Portugal, 2007.

[200] C. Li, J. Yan, *The synchronization of three fractional differential systems*, Chaos, Solitons and Fractals, 32, pp. 751-757, 2007.

[201] I. Petras, *Fractional-Order Nonlinear Systems : Modeling, Analysis and Simulation*,Springer Science and Business Media, 2011.

[202] S.T. Mohammad, H. Mohammad, *Synchronization of chaotic fractional-order systems via active sliding mode controller* Physica A. 387, 1, pp. 57-70, 2008.

[203] A. Boulkroune, A. Bouzeriba, T. Bouden et al., *Fuzzy adaptive synchronization of uncertain fractional-order chaotic systems*, In : Advances in Chaos Theory and Intelligent Control, Studies in Computational Intelligence, Berlin, Heidelberg : Springer, 636, pp. 681-697, 2016.

[204] D. Lia, X. Zhangb, *Impulsive synchronization of fractional order chaotic systems with time-delay*, Neurocomputing 216(C), pp. 39-44, 2016.

[205] R. Li, W. Chen, *Lyapunov-based fractional-order controller design to synchronize a class of fractional-order chaotic systems*, Nonlinear Dynamics, 76(1), pp. 785-795, 2014.

[206] M. Pourgholi, E.A. Boroujeni, *An iterative LMI-based reduced-order observer design for fractional-order chaos synchronization*, Circuits, Systems, and Signal Processing 35(6), pp. 1855-1870, 2016.

[207] M. Bettayeb, U.M. Al-Saggaf, S. Djennoune, *Single channel secure communication scheme based on synchronization of fractional-order chaotic Chua's systems*, Transactions of the Institute of Measurement and Control, 2017. DOI : 10.1177/0142331217729425.

[208] J. Chen, L. Jiao, J. Wu, X. Wang, *Projective synchronization with different scale factors in a driven-response complex network and its application in image encryption*, Nonlinear Anal. Real World Appl., 11, pp. 3045-3058, 2010.

[209] Z. Ping, C. Xue-Feng, Z. Nian-Ying, *Generalized synchronization between different fractional-order chaotic systems*, Commun. Theor. Phys., 50, pp. 931, 2008.

[210] G. Peng, Y. Jiang, F. Chen, *Generalized projective synchronization of fractional order chaotic systems*, Phys. A, 387, pp. 3738-3746, 2008.

[211] L.P. Chen, Y. Chai, R.C. Wu, *Lag projective synchronization in fractional-order chaotic (hyper-chaotic) systems*, Physics Letters A, 375(35), pp. 2099-2110, 2011.

[212] P. Zhou, W. Zhu, *Function projective synchronization for fractional-order chaotic systems*, Nonlinear Anal. Real World Appl., 12, pp. 811-816, 2011.

[213] S. Wang, Y.G. Yu, *Generalized projective synchronization of fractional order chaotic systems with different dimensions*, Chinese Physics Letters, 29(2), Article ID 020505, 3 pages, 2012.

[214] H. Taghvafard, G.C. Erjaee *Phase and anti-phase synchronization of fractional order chaotic systems via active control*, Commun. Nonlinear Sci. Numer. Simul., 16, pp. 4479-4486, 2011.

[215] F. Chen, L. Xia, C-G. Li, *Wavelet Phase Synchronization of Fractional-Order Chaotic Systems*, Chinese Physics Letters, 29(7), 2012.

[216] H. Zhu, Z. He, S. Zhou, *Lag synchronization of the fractional-order system via nonlinear observer*, Int.J.Mod.Phys. B 25, 3951, 2011.

[217] A. Mohammadzadeh, S. Ghaemi, O. Kaynak, et al.*Robust* H_∞ *based synchronization of the fractional-order chaotic systems by using new self-evolving nonsingleton type-2 fuzzy neural networks*, IEEE Transactions on Fuzzy Systems, 24(6), pp. 1544-1554, 2016.

[218] A.T. Parker, K.M. Short, *Reconstructing the keystream from a chaotic encryption scheme*, Circuits and System I : Fundamental Theory and Applications, IEEE Transaction on, 48(5), pp. 624-630, 2001.

[219] S. Li, G. Alvarez, G. Chen, *Breaking a chaos-based secure communication scheme designed by an improved modulation method*, Chaos, Solitons and Fractals, 25(1), pp. 109-120, 2005.

[220] S. Li, G. Alvarez, G. Chen, X. Mou, *Breaking a chaos-noise-based secure communication scheme*, Chaos : An Interdisciplinary Journal of Nonlinear Science, 15(1), 2005.

[221] W. D. Grossman, *Observers for discrete-time nonlinear systems*, New Jersey's Science and Technology University, 1999.

[222] H. Nijmeijer, A.J. van der Schaft, *Nonlinear Dynamical Control Systems*, Springer, New York, 1990.

[223] M.D. Mora, A. Germani, C. Manes, *Design of State Observers from a Drift-Observability Property*, IEEE Transactions on Automatic Control, 45(8), 2000.

[224] P. Brunovski, *A classification of linear controllable systems*, Kybernetika (Praha), 3, pp. 173-187, 1970.

[225] A. Wolf, J.B. Swift, H.L. Swinney, J.A. Vastano, *Determining Lyapunov exponents from a time series*, Physica 16D, pp. 285-317, 1985.

Résumé :
Dans ce travail de thèse, nous avons élaboré une nouvelle approche de transmission sécurisée basée sur des générateurs de séquences chaotiques d'ordre fractionnaire. Les principaux résultats obtenus sont, en premier lieu, le développement d'une nouvelle méthode de synchronisation des systèmes chaotiques discrets d'ordre fractionnaire basée sur l'observateur exact retardé étape par étape. La synthèse de l'observateur dépend de deux conditions : la condition d'observabilité pour récupérer les états du système ; la condition de recouvrement de l'observabilité ("observability matching condition") pour récupérer les états du système et l'information noyée dans le système (inversibilité à gauche du système). Ces deux conditions sont étudiées pour cette catégorie de systèmes. Par la suite, un nouveau schéma de transmission sécurisée efficace et robuste ainsi que quelques variantes ont été élaborés en utilisant la synchronisation par observateurs développée. Des résultats de simulation sont également présentés pour mettre en évidence les performances de notre méthode. Ces résultats montrent que les systèmes proposés peuvent résister à différents types d'attaques et qu'ils présentent de bonnes performances.

Mots-clés : Communication sécurisée, Systèmes chaotiques, Système d'ordre fractionnaire, Observabilité, Inversion à gauche, Observateur non linéaire discret, Synchronisation chaotique, Cryptage d'images, Robustesse.

Abstract :
In this thesis work, we have developed a new secure transmission approach based on fractional-order chaotic sequence generators. The main results obtained are, firstly, the development of a new method of synchronization of fractional chaotic discrete systems based on the exact observer delayed step by step. The observer's synthesis depends on two conditions : the condition of observability to recover the states of the system ; the condition of observability matching ("observability matching condition") to recover the states of the system and the information embedded in the system (left invertibility). These two conditions are studied for this category of systems. Subsequently, a new efficient and robust secure transmission scheme as well as some variants were developed using the developed observer-based synchronization. Simulation results are also presented to highlight the performance of our method. These results show that the proposed systems can resist different types of attacks and have good performance.

Keywords : Secure communication, Chaotic systems, Fractional-order systems, Observability, Left invertibility, Nonlinear discrete observer, Chaotic synchronization, Image encryption, Robustness.