RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE

MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR

ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITÉ DE JIJEL

FACULTÉ DES SCIENCES ET DE LA TECHNOLOGIE

DÉPARTEMENT D'ELECTRONIQUE

Thèse

Présentée pour obtenir le diplôme de Doctorat en Sciences en Electronique

Elaboration de nouvelles approches de transmission sécurisée et cryptage par chaos

Par: Abdelkader SENOUCI

Soutenu le : .../.../2014

Président :	Mr. K. KEMIH	MCA	Université de Jijel
Rapporteur :	Mr. A. BOUKABOU	Pr.	Université de Jijel
Examinateurs :	Mr. M. HAMADOUCHE	MCA	Université de Boumerdes
	Mr. D. BOUDJEHEM	MCA	Université de Guelma
Invité :	Mr. R. REMMOUCHE	MCB	Université de Jijel

بسم الله الرحمن الرحيم

وَمَا أُوتِيتُمْ مِنَ الْعِلْمِ إِلاَّ قَلِيلاً (85)

سورة الإسراء

وَقُلْ رَبِّ زِدْنِي عِلْماً (114)

سورة طه

A ma grand-mère,

A mes parents, mes frères & sœurs,

A ma femme & mes enfants.

. . . A tous mes amis.

Acknowledgements

Cette thèse n'aurait pas été achevée sans l'aide et précieux conseils de mon encadreur, **Professeur Abdelkrim Boukabou**. Sa culture scientifique, sa disponibilité et sa simplicité sont autant d'éléments qui ont favorisé le développement de cette thèse. Je tiens à lui exprimer ma profonde gratitude pour m'avoir accepté en thèse. Il m'a toujours encouragé et soutenu durant toutes ces années de préparation de cette thèse. Ses nombreux conseils, orientations et ses très vastes connaissances des sujets abordés m'ont permis d'acquérir des connaissances complémentaires.

Je tiens à exprimer ma profonde gratitude à tous ceux qui m'ont apporté leur soutien, leur amitié ou leur expérience tout au long de ce travail de thèse.

Je suis très reconnaissant au **Professeur Ahmed Bouridane** et au **Professeur Krishna Busawon** pour leur aide et leur accueil au sein du laboratoire à l'université de Northumbria, Newcastle au Royaume Uni.

Je remercie chaleureusement les membres de Jury qui m'ont fait l'honneur d'évaluer ce modeste travail de thèse. Je remercie chaleureusement **Mr. K. Kemih**, MCA à l'Université de Jijel de m'avoir fait l'honneur de présider ma soutenance. Mes vives remerciements vont également à **Mr. M. Hamadouche**, MCA à l'Université de Boumerdes et à **Mr. D. Boudjehem,** MCA à l'Université de Guelma d'avoir accepté d'agrémenter ce travail avec leurs remarques et conseils. Mes chaleureux remerciements s'adressent aussi à **Mr. R. Remmouche**, MCB à l'Université de Jijel d'avoir ornementé cette soutenance par sa présence.

Sommaire

Table des figures

Liste des tableaux

Abbreviations

AES	**A**dvanced **E**ncryption **S**tandard
ASCII	American **S**tandard **C**ode for **I**nformation **I**nterchange
CBC	**C**ipher **B**lock **C**haining
CFB	**C**ipher **F**eed**B**ack
CSK	**C**haotic **S**hift **K**eying
DCSK	Differential **C**haotic **S**hift **K**eying
ECB	**E**lectronic **C**ode **B**ook
FIPS	**F**ederal Information **P**rocessing **S**tandard
FPGA	Field **P**rogrammable **G**ate **A**rray
ICSS	**I**ndirect **I**nstitute of **C**oupled **S**ynchronization **S**cheme
LMI	**L**inear **M**atrix **I**nequality
NIST	**N**ational **I**nstitute of **S**tandards and **T**echnology
NPCR	**N**umber of **P**ixels **C**hange **R**ate
OFB	**O**utput **F**eed**B**ack
OGY	**O**tt **G**rebogi **Y**orke
PRNG	**P**seudo **R**andom **N**umber **G**enerator
RK4	**R**unge Kutta d'ordre **4**
S-Box	**S**ubstitution **B**ox
TS	**T**akagie **S**ugeno
UACI	**U**nified **A**verage **C**hanging **I**ntensity
XOR	**E**xclusive **OR**

Chapitre 0

Introduction Générale

0.1 Introduction

Avec l'évolution des communications en termes de nombre d'utilisateurs et de la nature d'informations à transmettre, la sécurisation de la chaîne de transmission devient de plus en plus nécessaire. Pour cela, actuellement tout système de télécommunication performant nécessite un système de cryptage robuste afin de se protéger envers diverses attaques possibles.

Longtemps restreinte aux usages diplomatiques et militaires, la cryptographie est maintenant une discipline scientifique à part entière, dont l'objet est l'étude des méthodes permettant d'assurer les services d'intégrité, d'authenticité et de confidentialité dans les systèmes d'information et de communication. La cryptographie a depuis des siècles été une histoire de conflits entre deux camps, un cherchant à cacher l'information et un autre essayant de découvrir le secret. L'ancienne cryptographie utilisait différentes techniques pour receler une information secrète. Certains remplaçaient des mots par des nombres, d'autres faisaient des substitutions et/ou des permutations des lettres et des mots pour rendre intelligible le message transmis. La cryptographie, aussi ancienne que les télécommunications, a connu un essor plus grand récemment. La cryptographie moderne cherche à transformer de façon mathématique et algorithmique un message clair en un autre chiffré, qui semble aléatoire. Plus l'inversion de la transformation est difficile, plus la sécurité est élevée. On peut classer la cryptographie selon plusieurs critères (type de la clé, type de données, ...) Selon le type de la clé, on distingue trois algorithmes. Dans la cryptographie symétrique (ou à clé secrète), les clés de chiffrement (au niveau de l'expéditeur) et de déchiffrement (au niveau du destinataire) sont identiques : c'est la clé secrète, qui doit être connue des tiers communicants et d'eux seuls. Le chiffrement symétrique est très rapide et facile à mettre en œuvre. Toutefois, il 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 hybride combine la cryptographie symétrique et la cryptographie asymétrique. Elle utilise la rapidité de l'algorithme symétrique et la sécurité de l'asymétrique et permet aussi d'éviter l'inconvénient lié à la distribution des clés. Selon le type de données, deux types de chiffrement sont connus, le chiffrement par bloc et le chiffrement par flot. Un système de chiffrement est dit par bloc s'il divise le texte clair en blocs de taille (généralement 128 bits) et chiffre un bloc à la fois. Un système de chiffrement est dit par flot (ou en continu) s'il traite le texte clair bit par bit.

Ces dernières années, avec le développement des communications modernes, le débit des télécommunications n'a cessé de s'accroître. Par ailleurs, les systèmes de communications basés sur les méthodes de cryptage citées ci-dessus souffrent du problème du débit faible causé par leur lenteur d'exécution des algorithmes de chiffrement. C'est pour cette raison que de nouveaux systèmes 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 et la cryptographie chaotique à laquelle, on s'intéresse dans le présent travail. Les systèmes chaotiques sont régis par des lois déterministes mais, ils sont imprévisibles à long terme. 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 qui a énoncé la naissance de cette théorie [1].

Au cours des dernières décennies, les nombreuses études menées sur les systèmes chaotiques ont montré que, hormis leur comportement aléatoire, ils possèdent des propriétés attrayantes et que le chaos apparait 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 protagonistes. Bien que ce comportement apériodique parait 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 connait 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. La synchronisation entre deux systèmes dynamiques chaotiques est nécessaire pour récupérer l'information transmise, mais elle n'est pas toujours facile à réaliser.

La synchronisation des systèmes chaotiques a été introduite en 1990 suite aux travaux de Pecorra et Carroll [2]. Cette technique permet de reconstruire les états de l'émetteur à partir du signal transmis par une réalisation à l'aide des circuits analogiques. Différentes approches ont été proposées pour améliorer ce processus et réduire l'erreur entre les états de l'émetteur et ceux restaurés au niveau du récepteur.

0.2 Motivations

Les travaux de recherche portés dans cette thèse ont été motivés par le besoin d'élaborer de nouvelles approches de transmission sécurisée et de concevoir un système cryptographique basé sur le chaos efficace et robuste en vue de son implémentation dans des applications de communications sécurisées. Les principaux résultats attendus sont l'élaboration d'une méthode de cryptage d'images ou de données impliquant deux entités. L'influence du bruit de canal dans le système de communication composé d'émetteur et de récepteur est considérée dans cette étude. Un autre volet a été aussi abordé ; il consiste à contrôler des systèmes chaotiques et hyperchaotiques et exploiter par la suite ce contrôleur afin de synchroniser ces systèmes.

0.3 Contributions scientifiques de la thèse

La principale contribution scientifique de cette thèse consiste à fournir des outils pour le contrôle et la synchronisation des systèmes chaotiques et hyperchaotiques et aussi pour la conception d'un système de communication sécurisée basée sur les systèmes chaotiques. Il relève des défis générés par la conception de systèmes cryptographiques en utilisant les propriétés intrinsèques des systèmes chaotiques, ainsi que les techniques usuelles de la cryptographie classique.

0.3.1 Publication

Cette thèse est basée sur des travaux présentés dans les publications suivantes :

0.3.2 Publications internationales

- A. Senouci, and A. Boukabou, Predictive control and synchronization of chaotic and hyperchaotic systems based on a T-S fuzzy model, Mathematics and Computers in Simulation , 2014, 105, 62 - 78 ;
- A. Senouci, A. Boukabou, K. Busawon, A. Bouridane, A. Ouslimani, Robust chaotic communication based on indirect coupling synchronization, Circuits, Systems & Signal Processing., 2014, 1-26.

0.3.3 Conférences internationales

- $WoSSPA'$2011 .A. Senouci, and A. Boukabou,Chaotic Cryptography Using External Key, Workshop on Systems, Signal Processing and their Applications "7th WoSSPA", 09-11 Mai 2011, Corne d'or, Tipaza, Algérie ;
- $ICCE$ 2014 A. Senouci, I. Benkhaddra, A. Boukabou and K. Busawon, Implementation and Evaluation of an Hyperchaos-based PRNG, The 2014 IEEE Fifth International Conference on Communications and Electronics (ICCE 2014), July 30th – August 1st, 2014, Vietnam ;
- ICM 2014 A. Senouci, I. Benkhaddra, A. Boukabou, A. Bouridane, A. Ouslimani, Implementation and Evaluation of a New Unified Hyperchaos-based PRNG, 26th International Conference on Microelectronics (ICM 2014), December 14-17, 2014, Qatar (soumis).

0.3.4 Conférences Nationales

- DAT'2011 A. Senouci, and A. Boukabou, Secure Advanced Discrete Chaotic Image Encryption, DAT'2011, 21-23 Février 2011, CNA/Alger, Algérie ;
- CGE'07 A. Senouci, and A. Boukabou, Cryptosystème Chaotique Adapté au Cryptage des Images, CGE'07, 12-13 avril 2011, EMP/Alger, Algérie ;
- DAT'2014 A. Senouci, I. Benkhaddra and M. Khiati, Embedded hyper-chaotic Lorenz random number generator for secure communications, DAT'2014, 17-19 Février 2014, CNA/Alger, Algérie.

0.4 Organisation de la thèse

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

Le premier chapitre traite de la théorie du chaos et donne un état de l'art. L'étude approfondie de cette théorie est loin d'être l'objectif de notre travail, mais on donne une description des caractéristiques essentielles communes à tous les systèmes chaotiques et en plus, une investigation d'un ensemble d'outils nécessaires à l'étude de ces systèmes. On termine ce chapitre par une constatation sur l'intérêt du chaos dans les systèmes de communication.

Dans le deuxième chapitre, une nouvelle méthode de cryptage basée-chaos en utilisant plusieurs fonctions chaotiques itératives unidimensionnelles est introduite. Cette méthode de cryptage représente une amélioration significative en termes d'efficacité et de sécurité. Le système de chiffrement proposé produit en plus une image chiffrée ayant une distribution plate. Dans la phase de cryptage, les pixels sont chiffrées en utilisant un module de chiffrement basé sur une rétroaction itérative avec un mécanisme dépendant des entrées de données pour mélanger les paramètres de chiffrement en cours avec des informations préalablement cryptées. Des résultats expérimentaux sont donnés pour démontrer l'efficacité du système proposé. Dans nos résultats expérimentaux, des images en couleur sont évaluées. Une analyse de sécurité de la méthode de chiffrement proposée est décrite.

Le troisième chapitre est dédié à la proposition d'une approche de communication chaotique selon un système de synchronisation par couplage indirect en cryptant des signaux de forte puissance. Le schéma proposé est soigneusement conçu de sorte que le signal crypté ne détériore pas la synchronisation, contrairement aux méthodes traditionnelles de communication. Le problème de synchronisation est résolu en utilisant le contrôleur basé sur observateur. Les avantages de cette approche sont les suivants : une méthodologie générale de conception d'observateur à rétroaction approprié pour la synchronisation ; une flexibilité dans le choix des signaux chaotiques d'entrées et de sorties pour le générateur de clés de chiffrement ; et l'amélioration des caractéristiques fréquentielles du message transmis. Les simulations montrent que la synchronisation entre l'émetteur et le récepteur est plus robuste pour différentes valeurs d'amplitude, de fréquence et de formes du signal d'information, même en présence de perturbations externes.

Le quatrième chapitre présente une conception basée sur un modèle flou pour le contrôle et la synchronisation des systèmes chaotiques et hyperchaotiques. Dans ce cadre, les systèmes chaotiques et hyperchaotiques sont exactement reproduits en se basant sur le modèle flou de Takagi-Sugeno (TS). Ensuite, les contrôleurs flous pour le contrôle et la synchronisation sont conçus en utilisant la méthode prédictive et des nouveaux critères sont dérivés. Enfin, des simulations numériques sont présentées pour illustrer l'efficacité et la faisabilité des résultats théoriques.

Finalement, une conclusion incluant des perspectives pour le travail de cette thèse sont présentées dans le dernier chapitre.

Chapitre 1

Généralités et état de l'art

C'est après un demi-siècle de désintéressement à la faveur des progrès en mathématiques et en informatique, qu'est née, au cours des années 1960, la science du chaos que nous nous apprêtons à étudier, et qui est devenue une discipline à part entière vers 1975. Ainsi, nous nous intéresserons, dans ce chapitre, principalement à l'état de l'art et à quelques notions de base concernant le chaos et les systèmes chaotiques.

1.1 Introduction

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 électriques, de la mécanique, et d'autres systèmes. Au XVIII^{ème} siècle, Isaac Newton exprima de 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 écriva en 1814 dans l'introduction de son ≪Essai philosophique sur les probabilités≫ [3], ≪*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 connaissions 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. 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. La théorie du chaos est définie comme une étude des systèmes dynamiques non-linéaires complexes ou des systèmes complexes exprimés par des récurrences et des algorithmes mathématiques et qui sont dynamiques non constants et non périodiques. Elle inclut l'étude qualitative et quantitative d'un comportement instable non périodique des systèmes dynamiques non linéaires déterministes. Selon le philosophe Daniel Parrochia [4], la théorie du chaos constitue une des trois grandes révolutions scientifiques du XX^{ème} siècle et correspond à un changement de paradigme comparable à ceux qu'entraînèrent la théorie de la relativité et la mécanique quantique. Poincaré fut l'un des premiers à entrevoir la théorie du chaos [5], 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 [1], elle a trouvé de nombreuses applications dans les domaines physiques, biologiques, chimiques et économiques [6]. C'est donc au cours des années soixante-dix que la théorie du chaos a pris son essor. Il apparait que T. Li et J. A. Yorke étaient les premiers auteurs qui, en 1975, ont introduit le terme de ≪chaos≫ et plus précisément le ≪chaos déterministe≫ dans leur article ≪Period Three Implies Chaos≫ [7] et depuis lors, 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.

Dans les années qui ont suivi, à cause des résultats théoriques, de la puissance incrémentale des ordinateurs, et des techniques expérimentales de plus en plus raffinées, il est devenu vraisemblable que ce phénomène est abondant dans la nature et a beaucoup de conséquences et de ramifications dans de nombreux domaines scientifiques. Actuellement la théorie du chaos a émergé beaucoup plus dans l'électronique et plus particulièrement dans la cryptographie et les communications sécurisées.

1.2 Histoire de la théorie du chaos

La théorie du Chaos a vu le jour dans les travaux d'Henri Poincaré à la fin du XIX^{ème} siècle et c'est dans les années soixante qu'elle fut redécouverte, après la publication d'un article qui allait révolutionner le monde des sciences [5]. Nous allons présenter dans cette section quelques effets marquant l'évolution de la théorie du chaos et qui sont

liés à quelques notions caractérisant le chaos. En 1964 Sharkovsky a établi les lois les plus générales de la coexistence de cycles de périodes différentes dans les transformations ponctuelles à une dimension. Le 29 décembre 1972, Lorenz intitula ≪The Butterfy Effect : l'effet papillon≫ dans sa conférence [8] au $139^{ème}$ meeting de l'American Association for the Advancement of Science : The Butterfly Effect Predictability : Does the Flap of a Butterfly's Wings in Brazil Set off a Tornado in Texas ? En 1973, le mathématicien Benoît Mandelbrot a écrit un article concernant de nouvelles formes d'aspect aléatoire dans les sciences (les fractales), il a constaté aussi que l'attracteur de Lorenz est une forme fractale [9]. Les fractales, du latin fractus, ≪brisé≫ sont des formes géométriques obtenues par fragmentation régulière à l'infini d'une figure donnée. On parle aussi ≪d'objets fractals≫ ou de ≪géométries fractales≫. Le terme de ≪chaos≫ a été utilisé pour la première fois en 1975 par T. Li et J. A. Yorke [7] et depuis ce temps, ce mot a été largement utilisé. D'autre part, en 1975, le mathématicien et physicien Mitchell Feigenbaum a découvert deux nombres réels appelés nombres de Feigenbaum ou constantes de Feigenbaum [10], exprimant des rapports apparaissant dans les diagrammes de bifurcation de la théorie du chaos. En 1976, en modélisant des interactions de populations en biologie, Robert May a montré qu'un système non linéaire, présentant un modèle très simple d'évolution du nombre d'individus d'une population, peut présenter un comportement complexe et chaotique [11]. Ce modèle appelé ≪application logistique≫ par référence à ≪l'équation logistique≫ a été introduit par Pierre-François Verhulst en 1846. L'augmentation du paramètre dans la fonction logistique se manifeste par une succession de bifurcations avec doublement de période des cycles produits. En 1979, en essayant de calculer précisément la suite des valeurs auxquelles se produisent les doublements de période, Mitchell Feigenbaum a observé que cette suite convergeait de façon géométrique et a montré que les points de bifurcation à doublement de période tendent vers une limite qui est le seuil de l'apparition du chaos. Il a ainsi découvert que le passage d'un système vers un comportement chaotique est régi par des lois universelles [12]. En 1991, Yves Pomeau et Paul Manneville ont évoqué la notion d'intermittence qui recouvre un phénomène relativement simple : un système devient turbulent lorsqu'il est agité par des fluctuations "anormales"[13]. La dynamique chaotique dans les systèmes électroniques a été un sujet d'intérêt depuis 1981 quand Linsay a montré éxpérimentalement qu'un circuit simple formé d'une résistance linéaire, d'une inductance et d'une diode et excité par une tension sinusoidale était capable de produire un phénomène chaotique [14]. En 1983, Chua et Matsumoto ont conçu le premier circuit électronique chaotique autonome, connu sous l'appelation ≪circuit de Chua≫ [15].

1.2.1 L'impossibilité de prédiction

A la fin du XIX^{ème} siècle, Henri Poincaré a remporté le prix du roi Oscar de Suède et de Norvège en 1889 après avoir présenté une étude de la stabilité du système solaire, une étude sur le «problème des trois corps». Cette étude constitue l'esquisse d'une grande partie de la nouvelle mathématique qu'il créa au fil des ans à travers des ouvrages qui sont considérés aujourd'hui comme des références : «Les Méthodes nouvelles de la Mécanique céleste» ; trois volumes parus entre 1892 et 1899 [16]. Poincaré a démontré dans son étude que toute prédiction à long terme est impossible, comme il affirmait dans son livre [5] dans le chapitre sur le Hasard de son ouvrage intitulé «Science et Méthode», publié en 1908 : «*Une cause très petite, qui nous échappe, détermine un effet considérable que nous ne pouvons pas ne pas voir, et alors nous disons que cet effet est dû au hasard. Il peut arriver que de petites différences dans les conditions initiales en engendrent de très grandes dans les phénomènes finaux. Une petite erreur sur les premières produirait une erreur énorme sur les derniers. La prédiction devient impossible et nous avons le phénomène fortuit*». Henri Poincaré disait «*alors même que les lois naturelles n'auraient plus de secret pour nous, nous ne pourrions connaître la situation initiale qu'approximativement*», et selon lequel «*d'infimes incertitudes sur l'état initial d'un système pourraient en engendrer de très grandes sur l'état final*». Il annonçait les recherches modernes sur le phénomène de sensibilité aux conditions initiales, c'était la naissance de la théorie du chaos.

En 1961, Edward Lorenz a découvert la sensibilité aux conditions initiales des systèmes dynamiques et ce en constatant découvert que d'infimes variations dans les conditions initiales conduisaient aux résultats extrêmement changeants et imprédictibles. Il a décrit en 1963 les conséquences de sa découverte dans un article [1] :«*Cela implique, dit-il, que deux états qui ne diffèrent que par d'infimes quantités peuvent évoluer vers deux états totalement différents. Partant de là s'il y la moindre erreur dans l'observation d'un état au temps présent, et de telles erreurs semblent inévitables dans n'importe quel système réel, il se pourrait bien qu'il soit impossible de faire une prédiction valable de ce que deviendra cet état dans un futur lointain*».

1.2.2 La notion d'attracteur étrange

David Ruelle et Floris Takens ont proposé en 1971 une nouvelle théorie relative à la turbulence dans les fluides et ont qualifié les surfaces de forme papillon formant les trajectoires du modèle de Volterra d'«attracteurs étranges» [17].

1.2.3 L'effet papillon

L' «effet papillon » est une locution de Lorenz souvent exprimée à l'aide d'une question : «Un simple battement d'ailes d'un papillon à un bout du monde peut-il déclencher une tornade à l'autre bout du monde ? ». Elle est liée aussi à l'image concernant le phénomène fondamental de sensibilité aux conditions initiales en théorie du chaos.

1.2.4 Les fractales

Un objet fractal est doté d'une propriété dite d'autosimilitude. Ce phénomène est observé dans les systèmes chaotiques : c'est à dire qu'on y observe une invariance par changement d'échelle. Si l'on zoome d'un facteur suffisant sur une partie de la courbe, on retrouve la structure et la topologie de celle-ci à sa taille initiale. Un zoom plus grossissant encore reproduit le phénomène, aussi loin qu'on puisse aller.

1.3 Le chaos : définition et propriétés

1.3.1 Définitions du chaos

Le mot CHAOS prend origine du terme $\ll \chi\alpha o\sigma \gg$, 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.

1.3.2 Définition des systèmes dynamiques

Un systéme dynamique est défini à partir d'un ensemble de variables qui forment le vecteur d'état $X = \{x_i \in \mathbb{R}\}, i = 1, ..., n$, où n représente la dimension du vecteur. 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.

Les systèmes dynamiques sont classés en deux catégories :

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

– Systèmes dynamiques à temps continu

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

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

Si la dynamique du système donnée par l'équation (1.1) 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 :

$$\dot{x}(t) = F(x(t)) \tag{1.2}$$

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

Comme il a été déjà précisé, le système dynamique est dans ce cas représenté par des équations aux différences finies, avec le modèle général suivant :

$$x(k + 1) = G(x(k), k) \tag{1.3}$$

où $G : \mathbb{R}^n \times \mathbb{Z}^+ \to \mathbb{R}^n$ 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 :

$$x(k + 1) = G(x(k)) \tag{1.4}$$

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

1.3.3 Système dynamique non-linéaire

La théorie du chaos traite des systèmes dynamiques déterministes présentant un phénomène fondamental d'instabilité appelé «sensibilité aux conditions initiales», ce qui les rend non prédictibles en pratique sur le «long» terme. Le chaos est défini généralement comme un comportement semblant aléatoire (ou imprévisible) d'un système dynamique régi par des équations déterministes. Le chaos est défini généralement comme un comportement particulier d'un système dynamique déterministe

non-linéaire. Du point de vue mathématique, la notion générale de système dynamique est définie à son tour à partir d'un ensemble de variables qui forment le vecteur d'état. Ce jeu de variables a la propriété de caractériser complètement l'état instantané du système dynamique générique. Conjointement avec l'espace d'état, un système dynamique est défini aussi par une loi d'évolution, généralement désignée par dynamique, qui caractérise l'évolution de l'état du système en temps. La notion de déterminisme provient du fait que le système considéré est complètement caractérisé par son état initial et sa dynamique.

1.3.4 Etats et dynamique d'un système

L'état d'un système est l'ensemble des variables qui, étant connues à l' instant initial, permettent de décrire l'évolution de ce système. L'ensemble de tous les états pouvant être pris par le système s'appelle l'espace des phases. Le processus évolue de manière déterministe si ses états futurs sont caractérisés par la connaissance de ses états présents et passés. Donc, la notion de déterminisme provient du fait que le système est caractérisé par son état initial et sa dynamique. Il faut noter que la non-linéarité est une condition nécessaire, mais pas suffisante pour générer le chaos. Il faut aussi noter que le comportement chaotique observé dans le temps n'est dû, ni à une source extérieure de bruit, ni à un degré infini de liberté, ni à un caractère stochastique, c.-à-d. c'est intrinsèque.

1.3.5 Déterminisme et conditions initiales

Le déterministe signifie qu'un phénomène est régi par des lois. Poincaré a montré que certaines lois non linéaires, telles que les lois de l'attraction universelle de Newton peuvent engendrer des mouvements chaotiques. Donc, le chaos se rattache plutôt à une notion d'imprévisibilité, d'impossibilité de prévoir à long terme. Du fait que l'état final dépend de manière si sensible de l'état initial ou qu'un petit rien peut venir tout modifier ; on ne peut pas prédir l'état final. La connaissance de l'état initial est toujours entachée d'une certaine imprécision, si petite soit-elle. Dans les systèmes dits chaotiques, cette imprécision s'amplifie de manière exponentielle et a pour résultat une non-connaissance de l'état final. On appelle donc chaotiques des phénomènes complexes, dépendant de plusieurs paramètres et caractérisés par une extrême sensibilité aux conditions initiales. Plusieurs systèmes physiques se comportent de manière chaotique. Parmi ces systèmes, on peut citer l'atmosphère, un pendule excité dans un champ magnétique, un robinet qui goutte. . .

1.3.6 Propriétés du Chaos

Nous allons essayer de caractériser le chaos à travers la présentation de quelques propriétés qui lui sont inhérentes.

1.3.6.1 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.

1.3.6.2 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.

1.3.6.3 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.

Cette sensibilité aux conditions initiales est mesurée par ce qu'on appelle le ≪temps caractéristique≫. Il s'agit du délai après lequel une différence dentre les deux points de départ est multipliée par un facteur 10 et devient $10d$.

La Fig.1.1 illustre cet aspect. Elle montre l'évolution de deux systèmes chaotiques régis par les mêmes équations, qui démarrent des mêmes conditions initiales, sauf pour la composante z, qui se diffère entre les deux systèmes de 10^{-8}. Ce qu'on constate est que l'observation du système (en rouge) nous ne renseigne plus sur l'évolution du système (en bleu) après le temps caractéristique T. En plus, malgré que la différence des

conditions initiales se situe au niveau de la composante z seulement, les trajectoires des composantes x ont aussi divergées, ce qui montre la diffusion de l'erreur dans toutes les composantes du système.

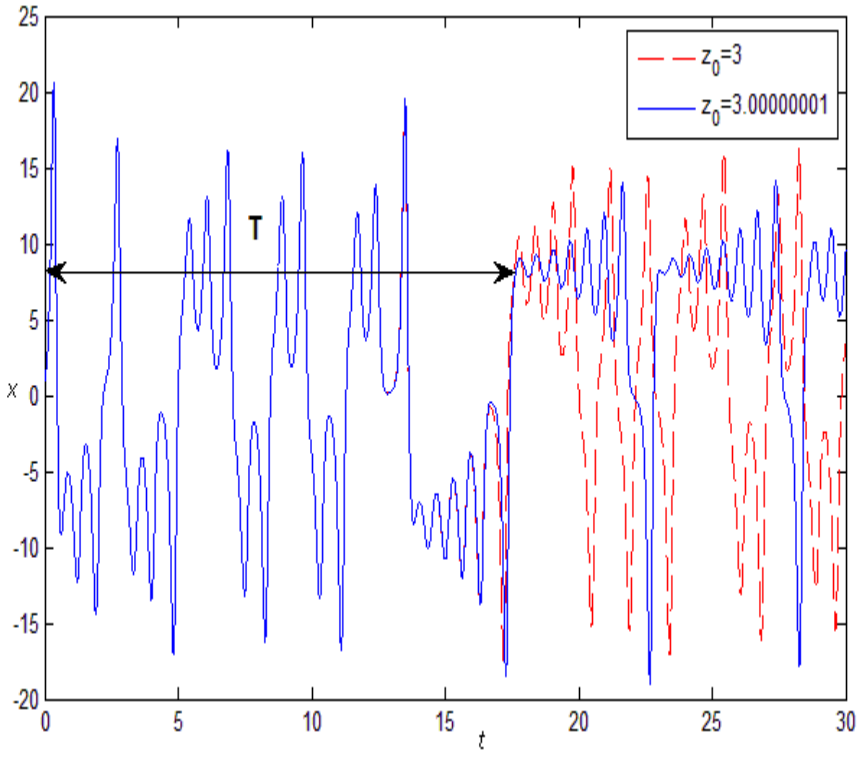


FIGURE 1.1: Sensibilité aux Conditions Initiales.

1.3.6.4 Dynamique complexe

Les systèmes chaotiques ont une dynamique très complexe, mais cette dynamique n'est pas erratique comme dans le cas d'un bruit, mais elle comporte une certaine régularité qui donne naissance à ce qu'on appelle «un attracteur étrange», lorsqu'on analyse le système dans l'espace de phase, comme le montre la Fig. 1.2. 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 à une toute autre suite qui après une courte phase, dessine la même image. D'où qu'on parte, on se retrouve toujours sur l'attracteur, c'est le côté prévisible de l'évolution. Où se retrouve-t-on exactement sur l'attracteur ? Il est

impossible de répondre à la question, c'est le côté imprévisible de l'évolution. À la suite de la découverte d'Edward Lorenz en 1963 de son fameux attracteur à l'allure d'un papillon, plusieurs recherches, principalement en physique, ont permis d'améliorer les connaissances sur les attracteurs étranges.

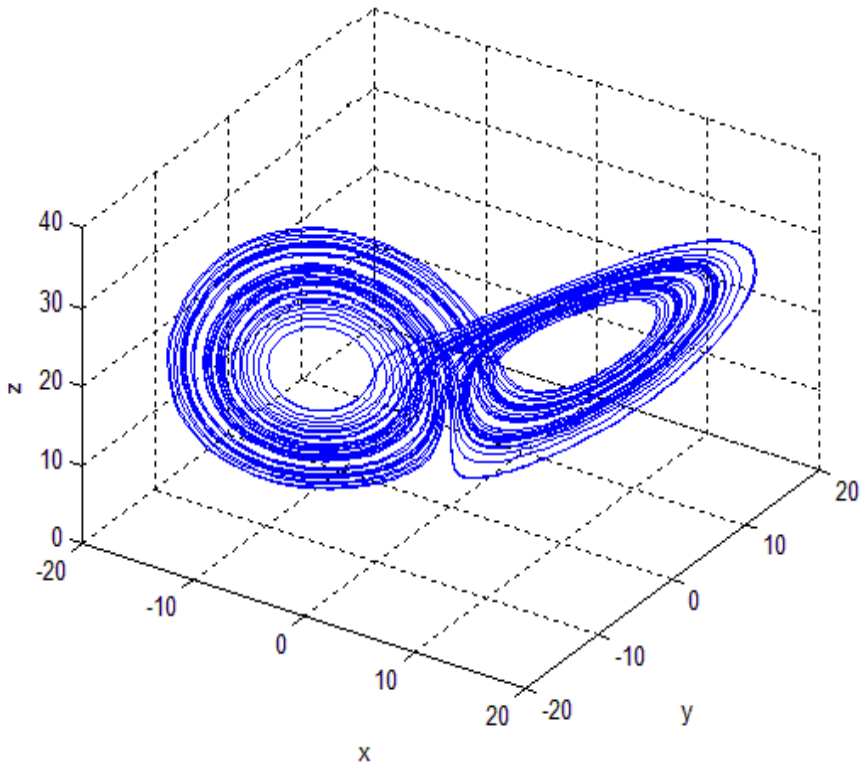


FIGURE 1.2: Attracteur étrange de Lorenz ... un papillon !.

1.3.6.5 Signal apériodique

La forme temporelle des signaux chaotiques présente des trajectoires qui sont ni divergentes, ni convergentes, ni périodiques, elles oscillent continuellement sans périodicité comme le montre la Fig.1.1. Une évaluation de la fonction d'autocorrélation va nous renseigner plus sur cet aspect.

1.3.6.6 Autocorrélation temporelle

L'autocorrélation temporelle est une fonction qui mesure la ressemblance de la variable x, à un instant donné t, avec sa valeur à un instant ultérieur $t + \tau$. Les signaux périodiques (ou quasi-périodiques) gardent leur similitude interne quand le temps s'écoule, ce qui implique que le comportement du système soit prédictible. La fonction d'autocorrélation d'un signal chaotique est présentée sur la Fig.1.3.

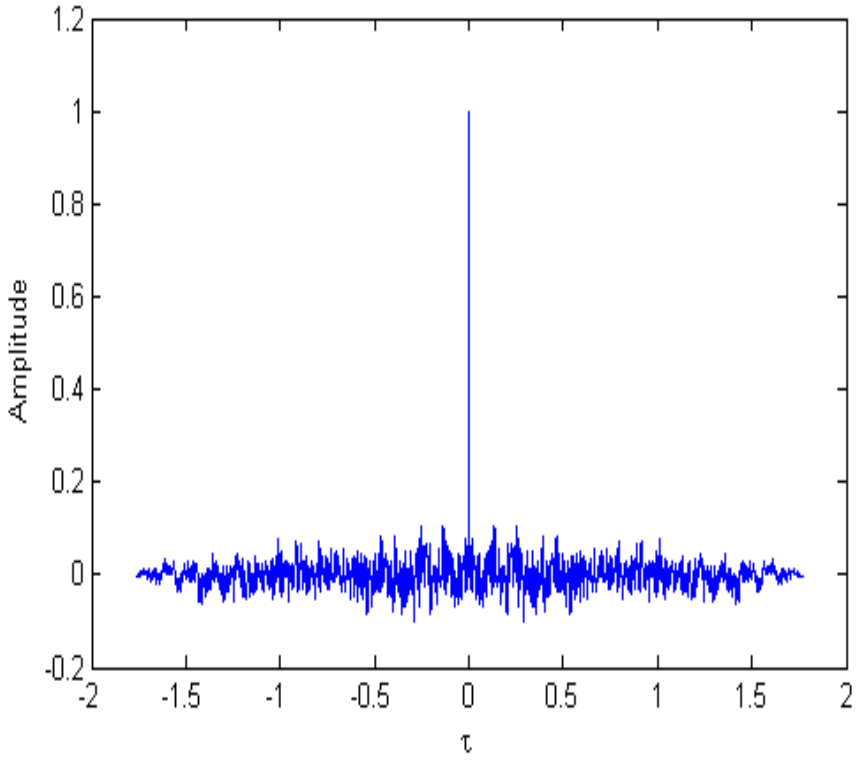


FIGURE 1.3: Fonction d'autocorrélation d'un signal chaotique.

On remarque que la fonction d'autocorrélation est nulle presque partout, sauf à l'origine ou elle présente un pic, cela veut dire que le signal chaotique ne ressemble à aucune de ses versions décalées, ou bien en d'autres mots, le signal chaotique ne contient aucune sorte de répétition.

Il est à noter que cette fonction d'autocorrélation est très semblable à celle d'un bruit blanc qui est une impulsion de Dirac à l'origine.

1.3.6.7 Spectre étalé

Si on observe suffisamment un signal chaotique, on remarque qu'il présente une forte dynamique, comme le montre la Fig.1.4.

Une analyse du spectre de puissance de ce signal donne le résultat présenté sur la Fig.1.5.

On remarque qu'un signal chaotique possède un spectre étalé s'étendant sur une gamme de fréquences, proche du spectre d'un bruit.

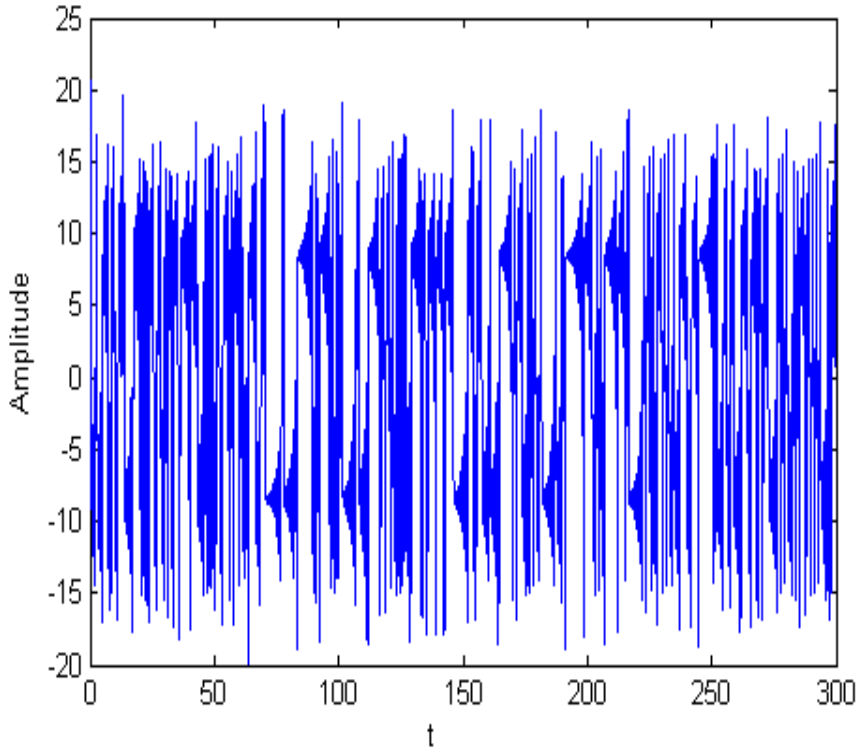


FIGURE 1.4: Dynamique d'un signal chaotique.

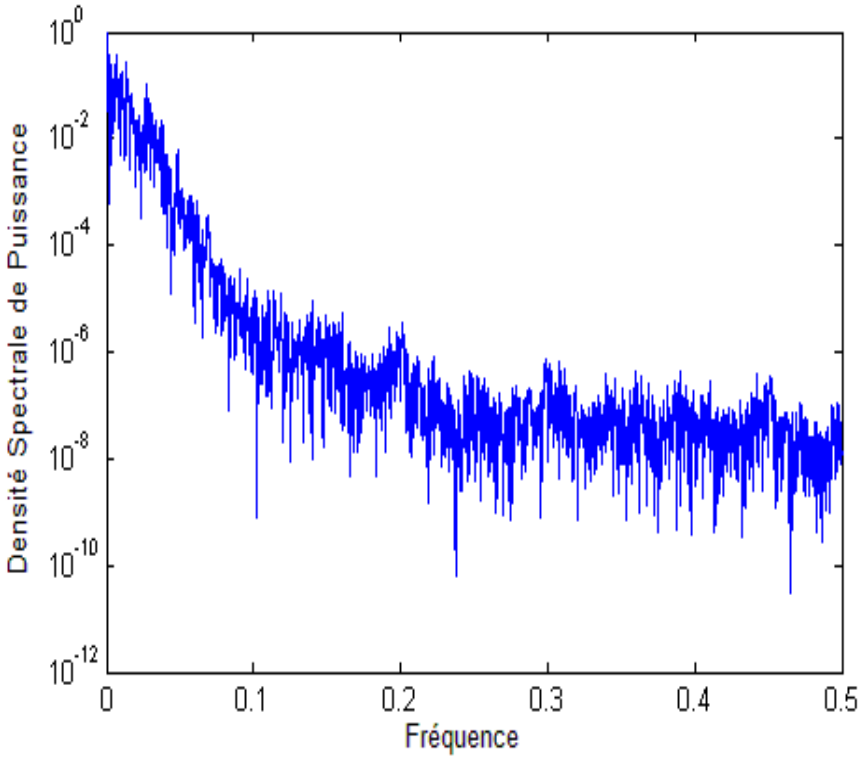


FIGURE 1.5: Spectre de puissance d'un signal chaotique.

1.3.7 Comportement des systèmes dynamiques

A partir d'un état initial $x(0)$ et après un régime transitoire, la trajectoire d'un système dynamique atteint une région limitée de l'espace des phases. Ce comportement asymptotique obtenu pour t(ou k) $\rightarrow \infty$ est une des caractéristiques les plus importantes à étudier pour tout système dynamique. Si dans le cas d'un système linéaire la solution asymptotique est indépendante de la condition initiale et unique, en présence de nonlinéarités il existe une plus grande variété de régimes permanents, parmi lesquelles on trouve, par ordre de complexité : points d'équilibre, solutions périodiques, solutions quasi-périodiques et chaos, respectivement. Il faut préciser que cette fois le comportement développé par un système dynamique particulier est fortement dépendant de la condition initiale choisie.

1.4 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, l'entropie de Kolmogorov ou les exposants de Lyapunov. 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 l'entropie ou les exposants de Lyapunov sont employés pour l'évaluation de l'instabilité propre au phénomène chaotique. Dans la pratique, ces exposants se sont imposés comme des outils performants, même dans le cas de séries temporelles courtes, avec un coût de calcul relativement réduit par rapport à la dimension de corrélation ou l'entropie de Kolmogorov.

A l'heure actuelle, force est de constater que l'aspect numérique revêt une part de plus en plus importante dans l'étude des systèmes dynamiques et, même s'il ne constitue pas une fin en soi, il représente un formidable outil d'investigation et de recherche.

Cette section a pour but de présenter les différents outils qu'on pourra programmer afin de mettre en évidence certains comportements caractéristiques des systèmes dynamiques non-linéaires et, en particulier, les systèmes chaotiques.

1.4.1 L'espace de phase

L'espace des phases est un espace mathématique souvent multidimensionnel, où chaque axe de coordonnées de cet espace correspond à une variable d'état du système dynamique étudié et chaque variable d'état caractérise le système à un instant donné.

Pour chaque instant donné, le système est donc caractérisé par un point de cet espace. A l'instant suivant, il sera caractérisé par un autre point et ainsi de suite.

L'ensemble de toutes les trajectoires de l'équation (1.2) fournit une représentation géométrique complète du comportement dynamique du système sous les conditions spécifiées. En conséquence, il est possible de donner une classification essentiellement complète du comportement du système dans l'espace de phase.

Généralement les équations décrivant un système non linéaire ne peuvent pas être résolues analytiquement, de sorte que, afin de construire la trajectoire exactement, il est nécessaire d'utiliser des méthodes numériques.

Alors en pratique, la construction de l'espace de phase d'un système décrit par l'équation (1.2) est accomplie par intégration numérique avec un pas temporel fini Δt, ce qui va nous ramener au cas discret décrit par l'équation (1.4). Par exemple, la méthode d'intégration d'Euler transforme l'équation (1.2) en :

$$x(t + \Delta t) \approx x(t) + \Delta t.\dot{x}(t)$$

Ainsi, la trajectoire est représentée par une suite de vecteurs $x(t + k\Delta t)$ ou plus simplement x_k. Donc l'espace de phase est construit en marquant les points dont les coordonnées dans l'espace $\mathbb{R}^n$ correspondent aux valeurs des vecteurs d'état. Une simple inspection visuelle peut nous renseigner sur la nature de la trajectoire.

La série de vecteurs x_k sert de base pour calculer des propriétés topologiques de la trajectoire (Exposants de Lyapunov, Dimension...) et en tirer des conclusions sur la nature du système.

1.4.2 La section de Poincaré

Un autre outil important pour l'étude des systèmes chaotiques est la section de Poincaré (voir Fig.1.6) qui permet de transformer un système continu en un système discret en réduisant en même temps la dimension du système d'un degré. L'intersection de la section de Poincaré et la trajectoire du système à n dimensions constitue une série de valeurs à $n - 1$ dimensions, la répétition de l'intersection de la trajectoire avec la section de Poincaré est assurée par le caractère transitif du chaos.

Le comportement du système discrétisé et le système original sont qualitativement équivalents, ce qui motive l'étude des systèmes dynamiques par le biais de la section de Poincaré.

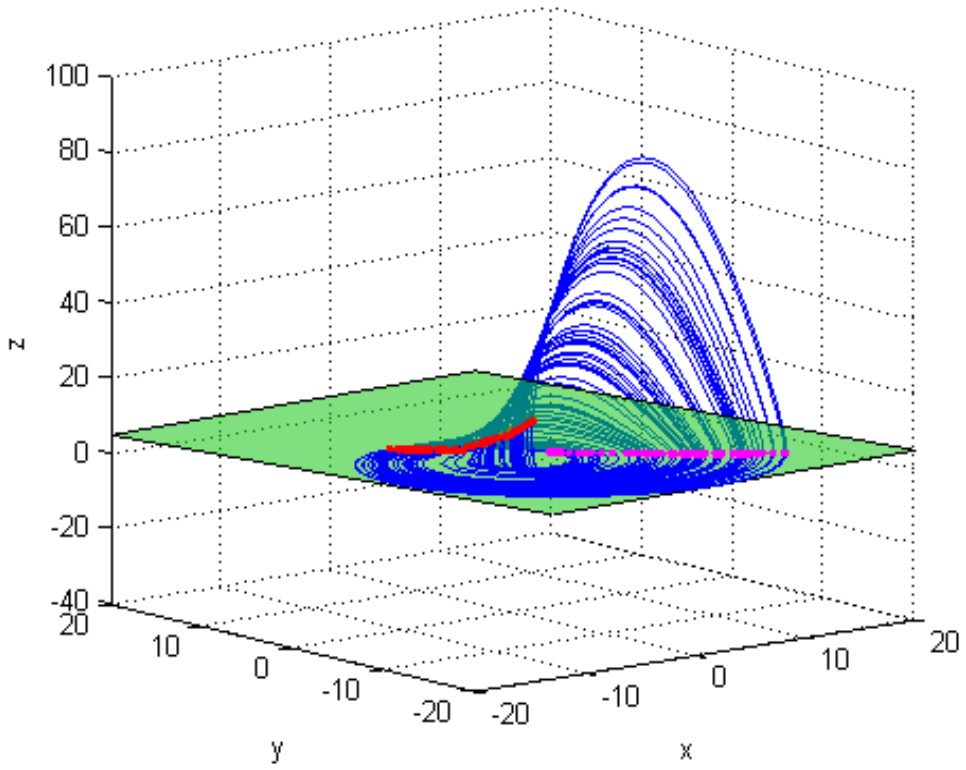


FIGURE 1.6: Section de Poincaré dans l'attracteur tridimensionnel de Rössler.

1.4.3 La dimension de l'attracteur

Les attracteurs des systèmes chaotiques dissipatifs, où les trajectoires éloignées rétrécissent vers l'intérieur d'un méta-cube, ont généralement une géométrie très complexe, d'où l'appellation d'attracteurs étranges comme mentionné précédemment.

Cette étrangeté est traduite par une auto-ressemblance de l'attracteur. En effet, la forme générale de l'attracteur est identique à la forme d'un sous-ensemble de l'attracteur, et identique aussi à la forme d'un sous-ensemble du sous-ensemble, et ainsi de suite. De telles formes géométriques sont appelées fractales.

Cette autosimilarité peut être quantifiée, sous forme d'une dimension, par diverses méthodes, on cite par exemple : la dimension de Kolmogorov ou de capacité, la dimension de corrélation (de Grassberger), la dimension de Lyapunov et la dimension de Hausdorff-Besicovitch. Ces dernières sont des extensions des méthodes de calcul de dimension d'objet non fractal. Ainsi, la dimension calculée d'un point serait égale à zéro, d'une ligne serait égale à 1, d'une surface égale à 2, d'un volume égale à 3, alors que la dimension d'un attracteur étrange est fractionnaire. Selon B. Mandelbrot (1975), un ensemble est fractal si sa dimension de Hausdorff-Besicovitch n'est pas entière.

1.4.4 Le diagramme de bifurcation

Pour un système dynamique donné, la nature de l'attracteur dépend du choix du jeu de paramètres. En général, une faible perturbation de l'un de ceux-ci ne change pas le comportement qualitatif du système, les détails de la forme ou de la position de l'attracteur peuvent se modifier un peu mais c'est tout, on parle alors de comportement générique. Cependant, il y a des valeurs particulières des paramètres pour lesquelles on observe un changement qualitatif des caractéristiques du système : un point fixe stable devient un cycle limite par exemple (voir Fig.1.7), on parle alors de bifurcation.

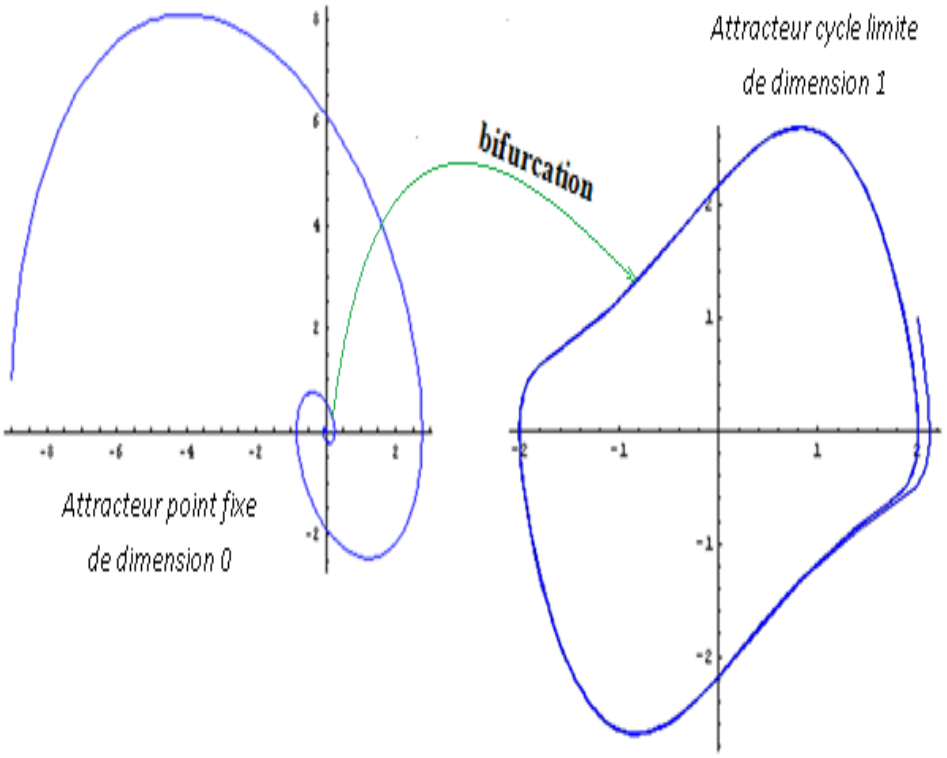


FIGURE 1.7: Changement qualitatif de l'attracteur suite à une variation d'un paramètre.

Donc on peut définir la bifurcation comme étant un changement qualitatif de l'état asymptotique d'un système suite à un changement de la valeur d'un paramètre, et on appelle les valeurs limites du paramètre auxquelles une bifurcation se produit valeurs de bifurcation.

Comme cela a été souligné en 1988 par Glass et Mackey [18], la construction d'un diagramme de bifurcation est un bon moyen pour mettre en lumière une signature du chaos. Le graphe représentant le comportement d'une valeur max associée à chaque point d'un attracteur en fonction d'un des paramètres du modèle permet de mettre en évidence deux types de comportements. Soit l'attracteur est représenté par un nombre fini de

points visités successivement, ce qui va correspondre à un comportement périodique, soit par tout un ensemble de points répartis sur la verticale correspondant à la valeur du paramètre considéré, points visités de façon irrégulière, ce qui permettra de conclure à un attracteur chaotique. La Fig.1.8 montre le diagramme de bifurcation de la fonction Logistique.

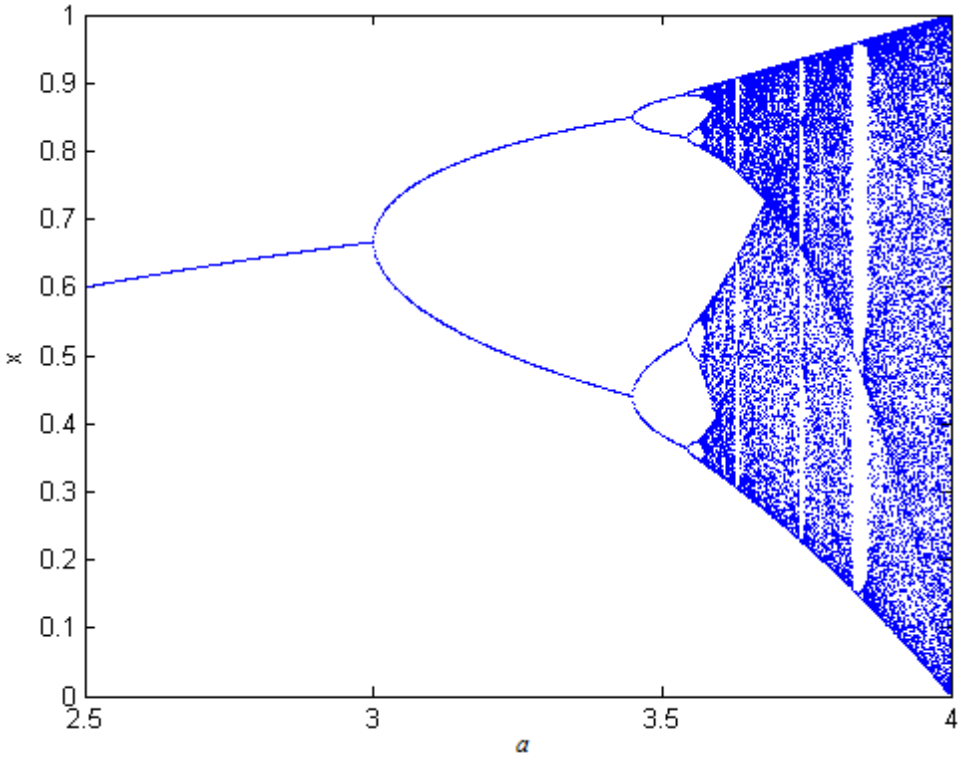


FIGURE 1.8: Diagramme de bifurcation de la fonction Logistique.

De plus, ce type de diagramme met également en évidence l'un des trois scénarii conduisant au chaos, à savoir, la cascade de doublement de périodes.

1.4.5 Les exposants de Lyapunov

Certains systèmes dynamiques sont très sensibles aux petites variations de leurs conditions initiales $x(0)$. Ces variations peuvent rapidement prendre d'énormes proportions. Le mathématicien Alexander Lyapunov a découvert une quantité permettant de mesurer la vitesse à laquelle ces petites variations peuvent s'amplifier. Cette quantité appelée «Exposant de Lyapunov» et qu'on note λ, mesure en fait le degré de sensibilité d'un système dynamique. Ainsi, dans le cas d'un attracteur chaotique, deux trajectoires initialement voisines vont diverger à une vitesse exponentielle quantifiée par l'exposant de Lyapunov. Géométriquement, cela se traduit par le fait que si on choisit un ensemble de conditions initiales situées dans une sphère infiniment petite (de diamètre $\delta(0)$) dans

le bassin d'attraction du système dynamique de dimension n, sous l'effet de la dynamique cette sphère va se déformer pour se transformer en ellipsoïde. Le $i^{ème}$ exposant de Lyapunov se définit alors en fonction de la déformation subie sur la $i^{ème}$ direction comme :

$$\lambda_i = \lim_{t\to\infty} \frac{1}{t} \ln \frac{\delta_i(t)}{\delta_i(0)}, i = 1, ..., n \tag{1.5}$$

L'ensemble $\{\lambda_i\}, i = 1, ..., n$ constitue le spectre de Lyapunov. D'habitude les exposants sont classés par ordre décroissant : $\lambda_i \geq \lambda_{i+1}, i = 1, ..., n$.

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 :

$$\sum_{i=1}^{n} \lambda_i < 0 \tag{1.6}$$

Si le spectre de Lyapunov reste l'une des plus robustes méthodes pour évaluer le comportement dynamique d'un système quelconque, le spectre de fréquence peut donner aussi des indices sur le régime permanent.

Un système sensible à de très petites variations de la condition initiale $x(0)$ aura une quantité positive. La quantité sera négative si de petites variations de $x(0)$ n'ont aucun effet à long terme sur le système. L'exposant de Lyapunov est en fait une mesure du degré de stabilité d'un système.

Pour un attracteur non chaotique, les exposants de Lyapunov sont tous négatifs ou nuls ($\lambda_k \leq 0, \forall t, k$) et leur somme vérifie (1.6). Les attracteurs non chaotiques sont ainsi classés en trois catégories :

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

Un attracteur étrange possedera toujours au moins un exposant de Lyapunov positif avec la propriétée (1.6) vérifiée. De plus, pour un attracteur étrange, un des exposants de Lypunov est toujours nul. Cela signifie que pour respecter la condition (1.6), un attracteur étrange doit avoir au minimum trois exposants de Lyapunov. Donc, un système continu dans le temps doit etre au moins de dimension trois pour produire le chaos.

Régime permanant	**Attracteur**	**Spectre**	**Exposants de Lyapunov**
point d'équilibre	Point	composante continue	$0 > \lambda_1 \geq ... \geq \lambda_n$
périodique	Courbe fermée	fréq. fondamentale + harmoniques entières	$\lambda_1 = 0$ $0 > \lambda_2 \geq ... \geq \lambda_n$
quasi-périodique	Tore	composantes fréquentièlles en rapport irrationnel	$\lambda_1 = ...\lambda_i = 0$ $0 > \lambda_{i+1} \geq ... \geq \lambda_n$
chaotique	Fractale	spectre large	$\lambda_1 > 0$ $0 \geq \lambda_2 \geq ... \geq \lambda_n$

TABLE 1.1: Différents régimes d'un système dynamique non linéaire

Si les exposants de Lyapunov demeurent l'une des plus robustes méthodes pour évaluer le comportement dynamique d'un système quelconque, le spectre de fréquence peut donner aussi des indices sur le régime permanent.

Les divers critères permettant de caractériser la dynamique d'un système quelconque sont regroupés dans le tableau 1.1.

1.5 Contrôle des systèmes chaotiques

Les effets chaotiques dans les circuits électroniques ont été constatés pour la première fois par Van der Pol en 1927 [19]. Van der Pol et al. ont remarqué que à certaines fréquences, un bruit irrégulier a été toujours observé. Pour supprimer ces effets indesirables, il est nécessaire de contrôler de tels systèmes. Parmi les méthodes de contrôle des systèmes chaotiques, on peut citer le contrôle en boucle ouverte, contrôle linéaire et non-linéaire, contrôle adaptatif, la linéarisation du Map de Poincaré (Méthode OGY), méthode de contrôle par retour d'état (Méthode de Pyragas), etc. La première tentative de controler le chaos est née de l'idée de perturber certains paramètres du système à controler. Cette idée est apparue en 1989 et peut être consultée dans l'article de Pettini [20], où il a souligné qu'une variation relative appropriée de paramètres peut être en mesure de réduire ou de supprimer le chaos. Pettini a considéré l'oscillateur Duffing-Holmes pour montrer que le chaos peut en effet être réduit ou éliminé dans un système dissipatif. Dans la même année, Hübler a publié un premier article sur le contrôle adaptatif des systèmes chaotiques [21]. En 1990, Ott, Grebogi et Yorke ont publié le premier article sur le contrôle du chaos et ont développé l'algorithme OGY [22]. Ils ont montré qu'une telle dynamique complexe pouvait être stabilisée par une méthode simple et efficace. En modélisant le système discret de Hénon, ils ont démontré qu'une perturbations suffisamment petite des paramètres du système peut transformer une trajectoire chaotique en une trajectoire périodique et vice versa. Plusieurs algorithmes ont

été dérivés de cette méthode. En 1990, Ditto a confirmé expérimentalement la méthode OGY dans une publication ultérieure [23]. En 1992, dans [24], Rajasekar et Lakshmanan ont montré que le comportement du système de Bonhoeffer-Van der Pol peut être mis en mouvement régulier en ajoutant un bruit gaussien.

Un système chaotique peut être contrôlé soit par perturbation d'un des paramètres du système, ou par stabilisation d'une des orbites périodiques instables du système en appliquant une méthode de contrôle par retour d'état. Pyragas a proposé une méthode basée sur l'injection des états retardés dans l'entrée du système. Dans cette méthode, l'entrée du contrôle est basée sur la différence entre un état retardé et l'état courant. La loi de contrôle appliquée au système est donnée par :

$$u(k) = K\left(x\left(k-T\right) - x\left(k\right)\right) \tag{1.7}$$

où K est le gain de contrôle.

Plusieurs autres méthodes bsées sur celle de Pyragas ont été développées. La loi de commande proposée par Yamamoto et al est de la forme suivante :

$$u(k) = K\left(\hat{x}\left(k+1\right) - x\left(k\right)\right) \tag{1.8}$$

D'autres méthodes plus récentes sont citées dans le chapitre 4 [25], [26].

1.6 Synchronisation du chaos

En 1990, Pecora et Caroll ont affirmé que deux systèmes chaotiques peuvent être synchronisés, en envoyant seulement une partie de l'information de l'espace d'état d'un système vers l'autre [2]. Ils ont montré qu'il était possible de synchroniser deux systèmes chaotiques, même si leurs conditions initiales sont totalement différentes. Dans les systèmes de communication, la synchronisation est une clé très importante pour une transmission réussie. La synchronisation classique employée dans les systèmes de télécommunication cherche à reproduire juste le signal périodique de la porteuse. Par contre, la synchronisation chaotique au niveau du récepteur cherche à dupliquer le signal chaotique envoyé de l'émetteur. Cela veut dire que deux signaux chaotiques seront dits synchronisés s'ils sont asymptotiquement identiques lorsque le temps t tend vers l'infini.

Diverses stratégies de synchronisation ont été proposées et étudiées sur la base de modèles simples ou de circuits électroniques générateurs de chaos. Certaines méthodes ont supposé que l'émetteur et le récepteur sont identiques, d'autres ont considéré le cas le plus réaliste où il existe effectivement une différence entre les systèmes maître et

esclave. Ils ont mis ainsi un accent particulier sur l'effet des incertitudes des paramètres des deux systèmes. Parmi les approches proposées dans la littérature pour synchroniser les systèmes chaotiques identiques, non identiques, incertains, etc., nous pouvons citer les méthodes de synchronisation basées sur le contrôle non linéaire, le contrôle adaptatif, le contrôle par mode glissant, le contrôle actif, le contrôle backstepping, le contrôle à retour d'état, etc.

A ce jour, différentes formes de synchronisation ont été explorées. Parmi ces formes, on trouve les méthodes à synchronisation complète, les méthodes à synchronisation généralisée, les méthodes à synchronisation de phase, la synchronisation Lag, la synchronisation projective, etc.

1.6.1 La synchronisation complète

Dans la synchronisation complète, nous avons une coïncidence complète entre les variables d'états des deux systèmes synchronisés. Les méthodes à synchronisation complète sont typiquement associées avec la synchronisation des systèmes identiques (un exemple est le système de Pecora et Carroll).

Soit un système maître défini par les équations suivantes :

$$\dot{x} = f(t, x), y = h(x), x \in \mathbb{R}^n, h : \mathbb{R}^n \to \mathbb{R}^m \tag{1.9}$$

et un système esclave donné par :

$$\dot{\hat{x}} = \hat{f}(t, \hat{x}, y), \hat{y} = \hat{h}(\hat{x}), \hat{x} \in \mathbb{R}^p, \hat{h} : \mathbb{R}^p \to \mathbb{R}^q \tag{1.10}$$

où $(x, \hat{x})$ sont les états des systèmes et $(y, \hat{y})$ sont les sorties.

Soit φ une fonction continue, qui décrit la relation entre le maître et l'esclave lors de la synchronisation :

$$\hat{y} = \varphi(y), \varphi : \mathbb{R}^m \to \mathbb{R}^q \tag{1.11}$$

La synchronisation est dite complète si $\hat{x}(t) = x(t)$.

Ce qui implique que ; $m = q$ et φ est une identité.

Si $\hat{f} = f$, la relation devient une synchronisation complète identique.

Si $\hat{f} \neq f$ c'est une synchronisation complète non identique. La synchronisation complète est donc une coïncidence complète entre les variables d'état des deux systèmes synchronisés. Les méthodes de synchronisation complète sont typiquement associées avec la synchronisation des systèmes identiques.

1.6.2 La synchronisation généralisée

Les méthodes à synchronisation généralisée sont considérées comme une généralisation des méthodes à synchronisation complète. Elle est utilisée pour synchroniser des systèmes chaotiques typiquement différents.

1.6.3 La synchronisation Lag

Elle est définie pour le cas où $\hat{x}(t) \approx x(t-\tau)$, avec τ est un nombre positif très petit.

1.6.4 La synchronisation anticipée

Comme dans le cas de la synchronisation Lag, la relation entre les variables d'état des systèmes maître et esclave est donnée par :

$$\hat{x}(t) \approx x(t+\tau). \tag{1.12}$$

1.6.5 La synchronisation de phase

Soit φ_1 et φ_2 les phases des systèmes maître et esclave respectivement. La synchronisation de phase est réalisée si pour deux nombres entiers m et n, il existe un nombre positive très petit ε tel que :

$$|m\varphi_1 - n\varphi_2| < \varepsilon \tag{1.13}$$

La synchronisation de phase est différente de celles présentées précédemment. Généralement, lorsque la synchronisation chaotique est obtenue, les exposants de Lyapunov du système esclave sont tous négatifs. Donc, le système esclave est un système non chaotique avec une sortie chaotique. Cependant, dans le cas de la synchronisation de phase, les exposants de Lyapunov peuvent prendre des valeurs positives.

1.6.6 La synchronisation projective

Dans les systèmes couplés partiellement linéaires, deux systèmes identiques peuvent être synchronisés à un facteur d'échelle près. Ce type de synchronisation chaotique est appelé synchronisation projective.

D'autres méthodes plus récentes sont citées dans le chapitre 3.

1.7 Le chaos dans la communication sécurisée

Ces deux dernières décennies ont été marquées par une utilisation massive des systèmes chaotiques pour le cryptage 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. Cependant, Pecora a proposé un exemple, où un système chaotique et un duplicata d'une partie du système sont synchronisés.

A partir des années 1980, deux nouvelles méthodes de cryptographie ont vu le jour : d'abord la cryptographie quantique en 1984 , puis en 1990, la cryptographie chaotique . Les chercheurs Charles Bennett et Gilles Brassard ont réalisé la première expérience de distribution quantique de clés de cryptage en 1989. De leur côté, les chercheurs Louis Pecora et Thomas Carroll, ont mis en évidence en 1990, la synchronisation de deux systèmes chaotiques, ouvrant ainsi la porte à la cryptographie par chaos.

La cryptographie quantique repose sur le principe d'Heisenberg, selon lequel la mesure d'un système quantique perturbe ce système. Il est alors possible de transmettre une clé en étant sûr qu'elle n'a pas été écoutée, et de l'utiliser ensuite avec un chiffrement habituel.

Quant à elle, la cryptographie par chaos permet de crypter 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 bruitée et un déterminisme local.

1.8 Le chaos et la logique floue

Cette thèse traite aussi une classe particulière de modèles non linéaires appelés modèles Takagi-Sugeno (TS). Ces modèles sont issus au départ de la représentation des connaissances et de la recopie du savoir-faire d'un opérateur humain. Même s'ils sont issus de cette approche historique de la logique floue, ils peuvent s'interpréter comme une collection de modèles linéaires interconnectés par des fonctions non linéaires. Les fonctions non linéaires sont dépendantes des variables dites de prémisses. L'espace de ces dernières représente l'espace dans lequel on partitionne le modèle non linéaire. Il ne s'agit pas ici de réaliser des linéarisations autour de points de fonctionnement et de connecter ces modèles linéaires par des fonctions ce qui ne représente qu'une approximation d'un modèle non linéaire. Bien au contraire, il s'agit dans notre contexte de décrire le plus exactement possible un modèle non linéaire ou un système physique. Dans ce dernier cas, on peut s'appuyer sur le fait que ces modèles ont la propriété d'approximation universelle. Il existe alors des techniques d'identification principalement entrée/sortie qui permettent d'obtenir de tels modèles. Le problème le plus délicat restant dans le choix des variables de prémisses qui partitionnent l'espace.

L'approche utilisée dans notre cas se fait sur la base de modèles non linéaires en utilisant l'espace d'état. Dans ce cas, il est possible de mettre une grande partie des modèles non linéaires sous la forme de modèles TS représentant exactement le modèle non linéaire dans un compact de l'espace d'état.

Les lois de commande couramment utilisées sur ce type de modèles sont de type retour d'état non linéaire statique appelé PDC (Parallel Distributed Compensation). Ce type de loi de commande utilise les mêmes fonctions non linéaires permettant d'interpoler les modèles linéaires des modèles TS.

De plus, l'emploi du chaos dans les systèmes de communication peut permettre de renforcer la sécurité de transmission de l'information et réduire la probabilité d'interception. Dans la littérature, de nombreuses études ont été réalisées concernant plusieurs systèmes de transmission. Ces études ont montré que le chaos apparaissait comme une solution prometteuse pour augmenter la performance des systèmes de transmission actuels [27], [28], [29].

1.9 Conclusion

Depuis quelques années, les chercheurs s'intéressent à la possibilité d'utiliser les systèmes chaotiques dans la cryptographie et les transmissions sécurisées. En effet, les

systèmes chaotiques sont déterministes, cependant, les grandeurs chaotiques ont un aspect aléatoire. Par conséquent, il est intéressant d'exploiter ces caractéristiques pour générer des clés aléatoires au sein d'un système de cryptage.

Cependant, les systèmes hyperchaotiques ont un comportement plus complexe et un aspect plus aléatoire que les systèmes chaotiques. De plus, ils ont quatre variables d'état ou plus. C'est pour cette raison, les recherches actuelles sont focalisées sur les systèmes hyperchaotiques et leurs utilisations dans les communications sécurisées.

Après un court historique du chaos, nous avons fourni les moyens d'apprécier et de reconnaitre un comportement chaotique, qualitativement et quantitativement et avons aussi introduit les notions majeures utilisées tout au long de ce manuscrit. Ainsi, nous avons illustré les différentes approches et les célèbres techniques de chiffrement des données transmises basés chaos.

Enfin, nous avons étudié le contrôle et la synchronisation des systèmes chaotiques et hyperchaotiques en exploitant la modélisation floue de type Takagi-Sugeno.

Chapitre 2

Cryptographie chaotique basée sur une clé externe

Dans ce chapitre, une nouvelle méthode de cryptage basée-chaos en utilisant plusieurs fonctions chaotiques itératives unidimensionnelles est introduite. Cette méthode de cryptage représente une amélioration significative en termes d'efficacité et de sécurité. Le système de chiffrement proposé produit en plus une image chiffrée ayant une distribution plate. Dans la phase de cryptage, les pixels sont chiffrées en utilisant un module de chiffrement basé sur une rétroaction itérative avec un mécanisme dépendant des entrées de données pour mettre à jour les paramètres de chiffrement en cours en utilisant les informations préalablement cryptées. Des résultats expérimentaux sont donnés pour démontrer l'efficacité du système proposé. Dans nos résultats expérimentaux, une image en couleur est évaluée. Une analyse de sécurité de la méthode de chiffrement proposée est décrite.

2.1 Introduction

Au cours des dernières années, une attention particulière a été accordée au développement des techniques pour le contrôle, la synchronisation et la communication en utilisant des systèmes dynamiques chaotiques. Plus particulièrement, la communication basée-chaos est un nouvel axe de recherche prometteur pour les communications [30]. Il a évolué à partir de l'étude des systèmes dynamiques chaotiques, non seulement en mathématiques, mais aussi en physique et en génie électrique. Le comportement chaotique est complexe, mais néanmoins on peut l'observer dans des systèmes dynamiques assez simples. Les signaux chaotiques sont irréguliers, apériodiques, 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 tous les domaines [31–38].

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. En général, un cryptosystème doit considérer plusieurs aspects, tels que l'intégrité des données, l'authentification, la confidentialité, la non répudiation et bien d'autres services de sécurité. Pour ces raisons, plusieurs chercheurs essayent de mettre en œuvre d'autres cryptosystèmes. Durant ces dernières décennies, la théorie des systèmes non linéaires a été appliquée à la cryptographie afin d'augmenter le degré de sécurité. Grâce aux propriétés intrinsèques des systèmes chaotiques, telles que leurs sensibilités 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.

L'objectif principal de cryptage de l'image est de développer un crypto-système, qui d'une part convertit une image originale intelligible, dénommée plain-image (ou image claire), en une image apparemment aléatoire sans sens, appelée cipher-image (ou image chiffrée) et d'autre part, permet aussi de récupérer la forme de l'image originale.

Par conséquent, l'utilisation du chaos dans la cryptographie est d'un grand intérêt pour de nombreux domaines, y compris les bases de données militaires de l'image, les opérations et services bancaires par Internet et la protection des canaux de communication afin de préserver les données confidentielles contre les attaques d'ennemis, des espions, des antagonistes, etc. Quelques règles générales sur l'évaluation de la sécurité des systèmes de cryptage basé-chaos peuvent être trouvées dans [37].

En cryptographie classique, il existe plusieurs modes opératoires. Un mode opératoire est la manière de traiter les blocs de texte clair et chiffré au sein d'un algorithme de chiffrement par bloc pour le convertir en un chiffrement par flot. Avec un mode opératoire, le chiffrement accepte des données de taille quelconque. [39] Plusieurs modes existent, certains sont plus vulnérables que d'autres et des modes combinent les concepts d'authentification et de sécurité. On peut citer les modes opératoires les plus connus :

– Dictionnaire de codes (Electronic Code Book, ECB) ;
– Chiffrement par enchaînement des blocs (Cipher Block Chaining, CBC) ;

– Chiffrement à rétroaction (Cipher Feedback, CFB) ;
– Chiffrement à rétroaction de sortie (Output Feedback, OFB).

1. Dictionnaire de codes (Electronic Code Book, ECB) : Il s'agit du mode le plus simple. Le message à chiffrer est subdivisé en plusieurs blocs qui sont chiffrés séparément les uns après les autres. L'inconvénient de cette méthode est que deux blocs avec le même contenu seront chiffrés de la même manière.
2. Chiffrement par enchaînement des blocs (Cipher Block Chaining, CBC) : Dans ce mode, on applique sur chaque bloc une opération 'OU exclusif' (XOR) avec le texte chiffré du bloc précédent avant qu'il soit lui-même crypté. De plus, afin de rendre chaque message unique, un vecteur d'initialisation est utilisé. Le déchiffrement est aussi facile. Un bloc de texte chiffré est déchiffré normalement et est stocké dans le registre de rétroaction. Après que le bloc suivant ait été déchiffré, il est combiné par ou exclusif avec le contenu du registre de rétroaction. Ensuite, le bloc suivant de texte chiffré est stocké dans le registre. Commençant par le chiffrement des données aléatoires comme premier bloc. Ce bloc de données aléatoires est appelé vecteur d'initialisation. Avec l'utilisation d'un vecteur d'initialisation, deux blocs de texte en clair identiques successifs auront deux messages chiffrés différents. Dans ce mode, une seule erreur dans un bloc de texte en clair va affecter le bloc de texte chiffré correspondant et tous les blocs de textes chiffrés qui suivent.
3. Chiffrement à rétroaction (Cipher Feedback, CFB) : Ce mode agit comme un chiffrement par flot. Il génère un flux de clés qui est ensuite appliqué au texte original. L'opération XOR est appliquée entre le bloc de texte clair et le résultat précédent chiffré à nouveau par la fonction de chiffrement. Pour le premier bloc du texte clair, on génère un vecteur d'initialisation. Un vecteur d'initialisation différent doit être utilisé pour chaque message pendant la durée de vie de la clef. Avec le mode CFB, une erreur dans le texte en clair affecte tous les textes chiffrés suivants, tout comme pour le mode CBC.
4. Chiffrement à rétroaction de sortie (Output Feedback, OFB) : Dans ce mode, le flux de clés est obtenu en cryptant le précédent flux de clés. Au départ, un vecteur d'initialisation est généré. Ce bloc est chiffré à plusieurs reprises et chacun des résultats est utilisé successivement dans l'application de l'opération XOR avec un bloc de texte clair. Le vecteur d'initialisation est envoyé tel quel avec le message chiffré. Le mode OFB n'a pas d'amplification d'erreurs. Une erreur d'un seul bit dans le texte chiffré occasionne une erreur d'un seul bit dans le texte en clair récupéré.

En vue des applications potentielles et de l'importance d'avoir un crypto-système basé- chaos fiable pour le chiffrement d'image, nous proposons dans la section suivante un

crypto-système basé-chaos efficace utilisant une rétroaction itérative pour le chiffrement d'image satisfaisant les exigences de transfert d'image sécurisé, en utilisant les critères acceptées par l'industrie. Le résultat est un système amélioré, qui a des caractéristiques similaires au mode de chiffrement CBC (Cipher-Block Chaining), connu de la théorie des algorithmes de chiffrement par bloc ; ici les blocs sont des pixels. Une telle propriété est particulièrement importante pour le chiffrement d'image, car n'importe quel mode ECB (Electronic Code Book), où les pixels identiques sont cryptées à l'identique ne cache pas les contours d'éléments d'une image. L'efficacité de l'algorithme proposé est démontrée avec succès contre les attaques de cryptanalyse.

2.2 L'algorithme de chiffrement d'image proposé

Dans cette application, le cryptosystème basé chaos proposé utilise le principe de chiffrement symétrique par bloc, où une seule clé secrète est partagée entre l'émetteur et le récepteur. A partir de cette clé secrète sont dérivées les conditions initiales, les nombres d'itérations ainsi que les paramètres de contrôle des deux systèmes chaotiques. Dans le but de renforcer la sécurité, les conditions initiales, les nombres d'itérations ainsi que les paramètres de contrôle des deux systèmes chaotiques sont mis à jour après chiffrement (déchiffrement) de chaque pixel de l'image claire (chiffrée). Soit la fonction logistique donnée par :

$$X(k+1) = \lambda X(k)(1 - X(k)) \tag{2.1}$$

où λ représente le paramètre du system et $k = 1, 2, ..., N$.

Lorsque $0 < \lambda < 1$, on peut facilement montrer que toutes les orbites convergent vers le seul point fixe $\bar{X} = 0$. De même, pour $1 < \lambda < 3$, toutes les orbites sont attirées vers le point fixe $\bar{X} = 1 - 1/\lambda$. Pour $3 < \lambda < \lambda_\infty = 3.58$, la fonction logistique présente le phénomène de doublement de périodes. Pour $\lambda_\infty < \lambda < 4$, l'orbite révèle un entrelacement inattendu entre l'ordre et le chaos avec des fenêtres périodiques intercalées entre les nuages de points chaotiques.

Dans ce qui suit, nous présentons les différentes étapes de conception de l'algorithme proposé. Ces étapes sont décrites par l'organigramme de la Fig.2.1.

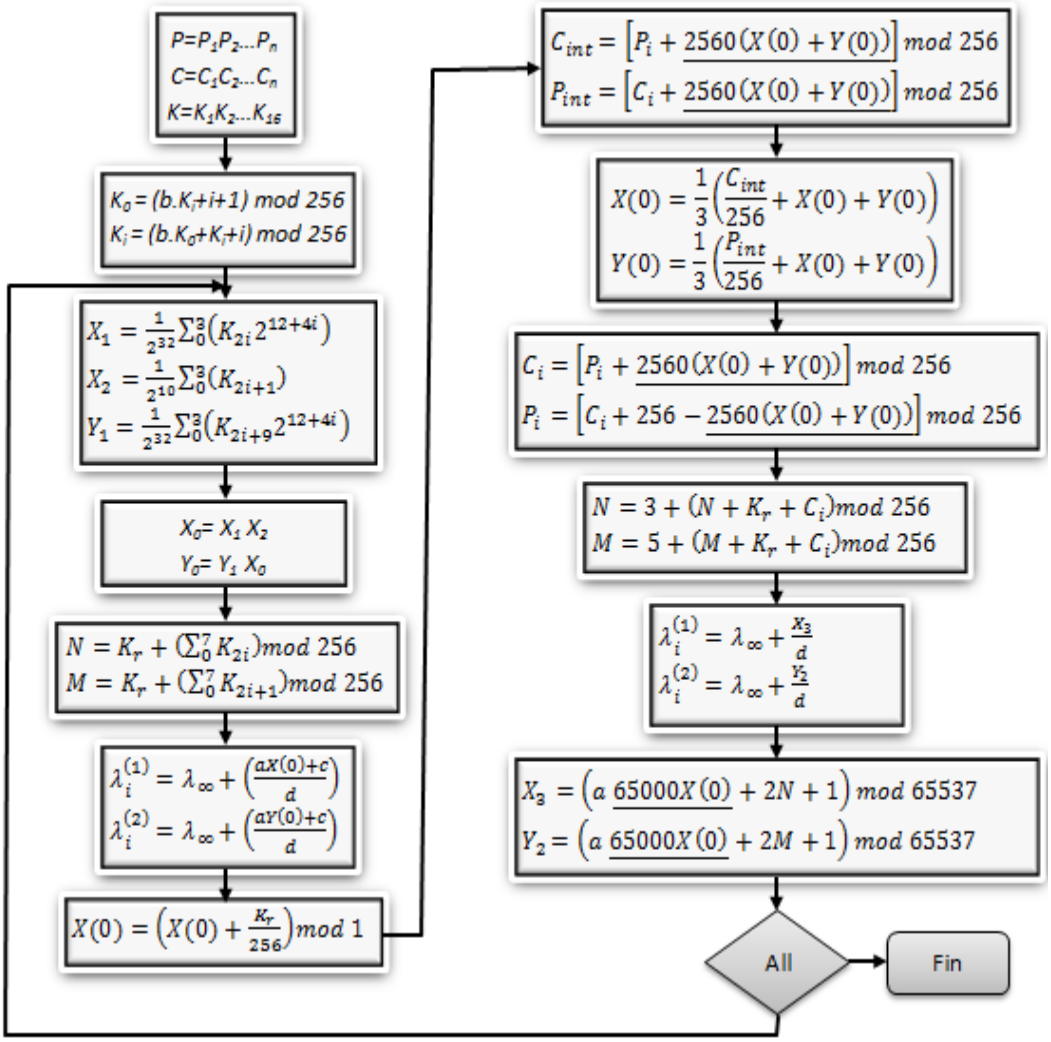


FIGURE 2.1: Organigramme de l'algorithme proposé.

1. Pour les processus de chiffrement et de déchiffrement, nous divisons l'image claire et l'image chiffrée en n blocs de 8 bits comme suit

$$P = P_1P_2P_3...P_n \tag{2.2}$$

$$C = C_1C_2C_3..C_n \tag{2.3}$$

2. Une clé secrète K choisie de 128 bits est divisée en blocs de 8 bits comme montrée ci-après

$$K = K_1K_2K_3K_4...K_{16} \tag{2.4}$$

3. Afin d'éviter les clés faibles, la clé secrète est regénérée comme suit :

$$K_0 = (bK_i + i + 1)mod\ 256; \tag{2.5}$$

$$K_i = (bK_0 + K_i + i) mod\ 256, \tag{2.6}$$

où b est une constante à choisir et K_i représente la valeur ASCII de la $i^{ème}$ clé secrete recalculée avec $i = 1, 2, ...16$.

4. Nous générons un indice r de clé de session aléatoire par la fonction *rand* de $C++$ et la graine de cette fonction est la clé secrète recalculée à l'étape 3.
5. Nous utilisons deux fonctions logistiques X et Y pour les processus de chiffrement/déchiffrement avec les conditions initiales $(X(0), Y(0))$, les nombre d'itérations (M, N) et les paramètres des deux systèmes $(\lambda^{(1)}, \lambda^{(2)})$. A l'aide des équations suivantes :

$$\begin{aligned} X_1 &= \frac{1}{2^{32}} \sum_{i=0}^{3} 2^{12+4i} K_{2i}, \\ X_2 &= \frac{1}{2^{10}} \sum_{i=0}^{3} K_{2i+1}, \\ Y_1 &= \frac{1}{2^{32}} \sum_{i=0}^{3} 2^{12+4i} K_{2i+9}, \end{aligned} \tag{2.7}$$

les conditions initiales $(X(0); Y(0))$ sont calculées comme suit :

$$X(0) = X_1 X_2; Y(0) = Y_1 X(0) \tag{2.8}$$

Les nombres d'itérations (M, N) sont déterminés par :

$$\begin{aligned} M &= K_r + \sum_{i=0}^{7} K_{2i+1} mod\ 256, \\ N &= K_r + \sum_{i=0}^{7} K_{2i} mod\ 256 \end{aligned} \tag{2.9}$$

La condition initiale de la première fonction logistique est mise à jour ainsi :

$$X(0) = \left(X(0) + \frac{K_r}{256} \right) mod\ 1 \tag{2.10}$$

où K_r représente la valeur ASCII d'une clé de session choisie au hasard. En outre, nous posons les conditions suivantes :

– Les conditions initiales $(X(0), Y(0))$ doivent être maintenues dans l'intervalle $[0.1, 0.9]$,
– Si $N < 3$, alors $N = 5 + K_r$ et si $M < 3$, alors $M = 3 + K_r$.

Les valeurs des paramètres des fonctions chaotiques pour le chiffrement (déchiffrement) du $i^{ième}$ bloc de l'image claire (chiffrée) sont déterminées par les équations suivantes :

$$\begin{aligned} \lambda_i^{(1)} &= \lambda + (aX(0) + c)/d, \\ \lambda_i^{(2)} &= \lambda + (aY(0) + c)/d. \end{aligned} \tag{2.11}$$

où $\lambda = 3.58; a = 421; b = 13; c = 987$ et $d = 156039$ pour le chiffrement (déchiffrement) de tous les blocs de l'image claire (chiffrée).

6. Nous générons un indice r de clé de session aléatoire comme dans l'étape 4 et nous choisissons une clé de session $(Kr, 1 \leq r \leq 16)$ au hasard pour modifier les valeurs des graines pour les nombres d'itérations (N, M).
7. La condition initiale de la première fonction logistique est mise à jour ainsi :

$$X(0) = \left(X(0) + \frac{K_r}{256} \right) mod\ 1 \tag{2.12}$$

8. Les valeurs intermédiaires utilisées pour le chiffrement (déchiffrement) de l'image claire (chiffrée) sont déterminées par :

$$C_{int} = \left[P_i + \underline{2560\,(X(0) + Y(0))} \right] mod\ 256; \tag{2.13}$$

$$P_{int} = \left[C_i + \underline{2560\,(X(0) + Y(0))} \right] mod\ 256; \tag{2.14}$$

L'expression soulignée signifie la partie entière de cette expression.

9. La condition initiale de la seconde fonction logistique est mise à jour ainsi :

$$\begin{aligned} X(0) &= \frac{1}{3}\left[\frac{C_{int}}{256} + Y(0) + X(0) \right], \\ Y(0) &= \frac{1}{3}\left[\frac{P_{int}}{256} + Y(0) + X(0) \right] \end{aligned} \tag{2.15}$$

10. Les nouvelles valeurs des conditions initiales sont utilisées pour le chiffrement (déchiffrement) de l'image claire (chiffrée) de la manière suivante :

$$C_i = \left[P_i + \underline{2560\,(X(0) + Y(0))}\right] mod\ 256; \tag{2.16}$$

$$P_i = \left[C_i + 256 - \underline{2560\,(X(0) + Y(0))}\right] mod\ 256; \tag{2.17}$$

11. Les nombres d'itérations (N, M) et les paramètres du système $(\lambda^{(1)}, \lambda^{(2)})$ sont mis à jour comme suit :

$$\begin{aligned} N &= 3 + (N + K_r + C_i) mod\ 256, \\ M &= 5 + (M + K_r + C_i) mod\ 256, \\ \lambda_i^{(1)} &= \lambda + \frac{X_3}{d}, \\ \lambda_i^{(2)} &= \lambda + \frac{Y_2}{d}, \end{aligned} \tag{2.18}$$

où

$$\begin{aligned} X_3 &= \left[\underline{65000aX(0)} + 2N + 1\right] mod\ 65537 \\ Y_2 &= \left[\underline{65000aY(0)} + 2M + 1\right] mod\ 65537 \end{aligned} \tag{2.19}$$

Nous choisissons le prochain bloc de l'image claire (chiffrée) et répétons les étapes 5 à 11 jusqu'à ce que l'image claire (chiffrée) est épuisée. Le processus de déchiffrement est tout à fait semblable à celui du chiffrement. Ainsi on peut récupérer l'image dans sa forme originale si et seulement si la clé secrète est exactement la même.

2.3 Résultats expérimentaux

L'analyse statistique de l'algorithme de chiffrement proposé a montré que ses propriétés de confusion et de diffusion lui permettent de résister aux attaques statistiques. Ceci est montré par les tests d'histogrammes de l'image chiffrée, les corrélations des pixels adjacents de l'image chiffrée, l'entropie de l'image chiffrée, le NPCR (Number of Pixels Change Rate), ainsi que l'UACI (Unified Average Changing Intensity).

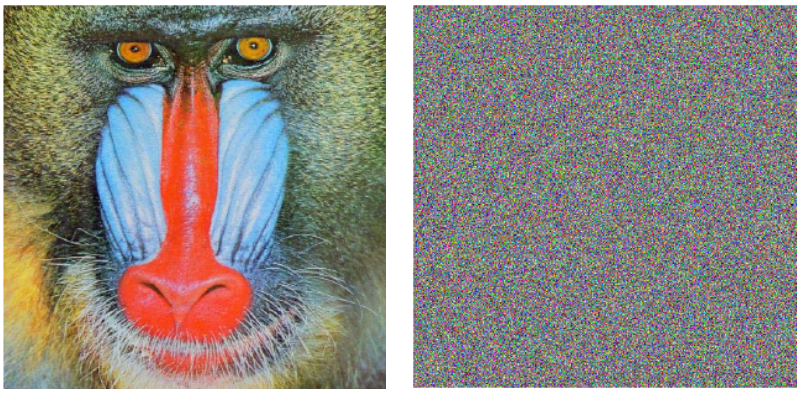
2.3.1 Analyse par histogramme

Un système cryptographique de haut niveau de sécurité doit produire des images cryptées avec une distribution uniforme des pixels dans chaque canal de couleur, afin de cacher la répartition de la plain-image.

L'outil d'analyse visuelle le plus souvent utilisé pour étudier la distribution des valeurs des pixels d'une image en couleur est l'histogramme des trois composantes couleurs, dans lequel les fréquences des valeurs des pixels sont tracées séparément pour chaque canal de couleur.

Dans la Fig.2.2(a), est présentée l'image claire (Baboon) et dans la Fig.2.2(b), est montrée l'image chiffrée. Sur la Fig.2.3(a-c), sont montrés les histogrammes des canaux rouge, bleu et vert de l'image claire et sur la Fig.2.3(d-e), les histogrammes des canaux rouge, bleu et vert de l'image cryptée, respectivement.

Les histogrammes des composantes rouge, vert et bleu de l'image claire (Lena) et de l'image chiffrée sont montrés sur les Fig.2.4(a-c) et Fig.2.4(d-f), respectivement. A partir des Fig.2.4(d-f), nous pouvons voir que l'image cryptée est complètement différente de l'image originale et est presque uniformément répartie, ce qui signifie que la méthode de chiffrement proposée offre une sensibilité haute clé. Donc un attaquant ne peut pas extraire des informations statistiques sur le plain-image ou sur la clé de chiffrement utilisée.



(a) (b)

FIGURE 2.2: Résultats de cryptage de l'image (Baboon). (a) La plain-image choisie. (b) L'image cryptée.

A partir des différentes figures, on peut voir que les histogrammes de l'image chiffrée sont assez uniformes et ils sont très différents de ceux de l'image originale. En outre,

on peut constater que l'algorithme de chiffrement a dissimulé tous les caractères de la plain-image et a rendu plus compliquée la dépendance statistique de la sortie sur l'entrée.

Nous notons que la clé secrète $K = 7D807EB9E1D48ED67B9FB9C5B095FEC0$ (en hexadécimal) a été utilisé pour crypter les images Baboon et Lena.

2.3.2 Sensibilité à la clé

Afin de résister efficacement contre l'attaque exhaustive (ou par force brute), nous devrions avoir un espace de clés aussi grand que possible. Dans notre cas, on a utilisé une clé de taille suffisante (de 128 bits). On pourrait facilement augmenter cette taille.

Pour évaluer la sensibilité du cryptosystème à la clé de chiffrement, on va considérer deux cas. Premièrement, on chiffre l'image claire (Lena) en utilisant deux clés de chiffrement qui diffèrent d'un seul bit ($K_2 = K + 1$). On constate d'après la Fig.2.5(a-d), que les images chiffrées (Fig.2.5(b et c)) sont totalement différentes ; ceci est confirmé par l'image de différence (Fig.2.5(c)) entre les deux images cryptées (Fig.2.5(b et c)). En deuxième lieu, on déchiffre l'image cryptée en utilisant la clé de chiffrement réelle et avec une autre clé qui diffère de la clé réelle d'un seul bit. Les résultats présentés sur la Fig.2.6(a-c) montrent que dans le premier cas Fig.2.6(b), on arrive à retrouver l'image originale, par contre dans le scond cas Fig.2.6(c), l'image obtenue est erronée.

2.3.3 Corrélation entre deux pixels adjacents

Il est évident qu'il existe une forte corrélation entre deux pixels adjacents de l'image claire, il est donc nécessaire de réduire cette coorélation afin d'éviter l'attaque par analyse statistique. Pour tester la corrélation entre deux pixels (verticalement, horizontalement ou diagonalement) adjacents, nous avons choisi de manière aléatoire 1000 paires de pixels séparément dans les directions horizontales, verticales et diagonales, et avons calculé les coefficients de corrélation de chaque paire par la formule suivante :

$$r_{xy} = \frac{cov\,(x, y)}{\sqrt{D\,(x)}\sqrt{D\,(y)}} \tag{2.20}$$

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

et $D\,(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E\,(x))^2\,; E\,(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$

Ici, x et y représentent les valeurs des niveaux de gris de deux pixels adjacents dans l'image.

Test image	Direction	Plain image	Cipher image
Lena	Horiz.	0.9892	-0.0013
	Vert.	0.9943	-0.0044
	Diag.	0.9821	-0.0008
Baboon	Horiz.	0.9645	-0.0021
	Vert.	0.9650	-0.0045
	Diag.	0.9571	0.0024

TABLE 2.1: Coefficients de correlation des pixels adjacents dans les trois directions.

La Fig.2.7(a-f) montre les coefficients de corrélation des images originale et chiffrée. Les résultats montrent qu'il existe une forte corrélation entre deux pixels adjacents de l'image claire (Lena), tandis que celles de l'image cryptée sont très faibles, de sorte que l'effet de chiffrement est évident.

Le Tableau.2.1 présente les coefficients de correlation des pixels adjacents des deux images Lena et Baboon.

2.3.4 Entropie

L'entropie, un concept de la théorie de l'information, est utilisé pour mesurer la quantité d'information. Plus un système est ordonnée, plus est faible l'entropie de l'information ; inversement, plus un système est confus, plus est élevée l'entropie. L'entropie peut être calculée par la formule suivante :

$$H(s) = \sum_{i=0}^{2^L-1} p(s_i) \log_2 \frac{1}{p(s_i)} \tag{2.21}$$

où $p(s_i)$ désigne la probabilité du symbole s_i. Plus l'entropie de l'information est proche de 8, plus l'image est aléatoire d'une certaine manière.

Nous avons pris comme exemple l'image Lena. On pouvait prendre d'autres images, mais on s'est limitée à un seul exemple. Nous pouvons voir que l'entropie de l'image claire est relativement petite 7.271856, par contre celle de l'image cryptée est très proche de 8 ; elle est égale à 7.999202.

Le Tableau.2.3 montre l'entropie des images claires et cryptées et le Tableau 3 montre les informations relatives au NPCR et UACI des images cryptées.

Test image	Plain image	Cipher image
Lena	7.44556	7.99920
Baboon	7.21163	7.99965

TABLE 2.2: Entropies.

2.3.5 Sensibilité à la Plain-image

Pour tester l'influence du changement d'un pixel sur la plaine image chiffrée par l'algorithme proposé, deux mesures communes peuvent être utilisées : NPCR (Number of Pixels Change Rate (NPCR) et UACI (Unified Average Changing Intensity).

Considérons deux images chiffrées C_1 et C_2, dont les images claires correspondantes ont seulement un pixel de différence. Soient $C_1(i,j)$ et $C_2(i,j)$ les valeurs des pixels (i,j) en C_1 et C_2 respectivement. Définissons une matrice bipolaire D, avec la même taille que les images C_1 et C_2. Alors,

$$D\left(i,j\right) = \begin{cases} 1, & if \quad C_1(i,j) \neq C_2(i,j) \\ 0, & otherwise \end{cases} \tag{2.22}$$

Tout d'abord, le NPCR mesure le pourcentage de nombres de pixels différents entre la plain-image et la cipher-image donné par :

$$NPCR = \frac{100}{wh} \sum_{i,j} D\left(i,j\right) \tag{2.23}$$

où w et h sont la largeur et la hauteur de l'image cryptée.

En second lieu, l'UAC (en %) est défini comme suit :

$$UACI = \frac{100}{wh} \sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255} \tag{2.24}$$

qui mesure l'intensité moyenne des différences entre les deux images.

Le NPCR et UACI sont obtenus en utilisant l'algorithme de chiffrement proposé. Les résultats ($NPCR = 99.60$ et $UACI = 33.40$) prouvent que le système de cryptage est très sensible à l'égard de petits changements dans la plain-image. En outre, le taux de l'influence du à une modification d'un seul pixel est très grand. En général, ces résultats obtenus pour NPCR et UACI montrent que l'image cryptée par l'algorithme proposé est très sensible aux petites variations de l'image claire.

Test image	**NPCR** (%)	**UACI** (%)
Lena	99.62043	33.49491
Baboon	99.61280	33.48139

TABLE 2.3: Le NPCR et UACI des images cryptées.

Le Tableau.2.3 montre les informations relatives au NPCR et UACI des images cryptées.

2.4 Conclusion

Dans ce chapitre, certaines propriétés intrinsèques des systèmes chaotiques sont utilisées pour concevoir une méthode efficace pour le chiffrement d'image. Dans le schéma de chiffrement proposé, une clé secrète externe de 128 bits et deux fonctions logistiques chaotiques sont utilisées pour rendre plus confuse la relation entre l'image chiffrée et l'image claire. En outre, pour rendre le chiffrement plus robuste contre toute attaque, le nombre d'itérations et les paramètres des fonctions logistiques sont modifiés après le cryptage de chaque pixel de la plain-image. La robustesse du système proposé est de plus renforcée par un mécanisme de rétroaction, ce qui rend le chiffrement de chaque pixel clair dépendant de la clé et de la valeur du pixel chiffré précédemment. Les résultats expérimentaux montrent que la technique de cryptage d'image proposée possède plusieurs caractéristiques intéressantes, telles que la distribution uniforme des pixels de l'image cryptée, le niveau de sécurité élevé et l'espace des clés assez grand. Il a été montré aussi l'extrême sensibilité de l'image cryptée aux infimes changements de l'image à chiffrer, ainsi qu'aux petites variations de la clé de chiffrement.

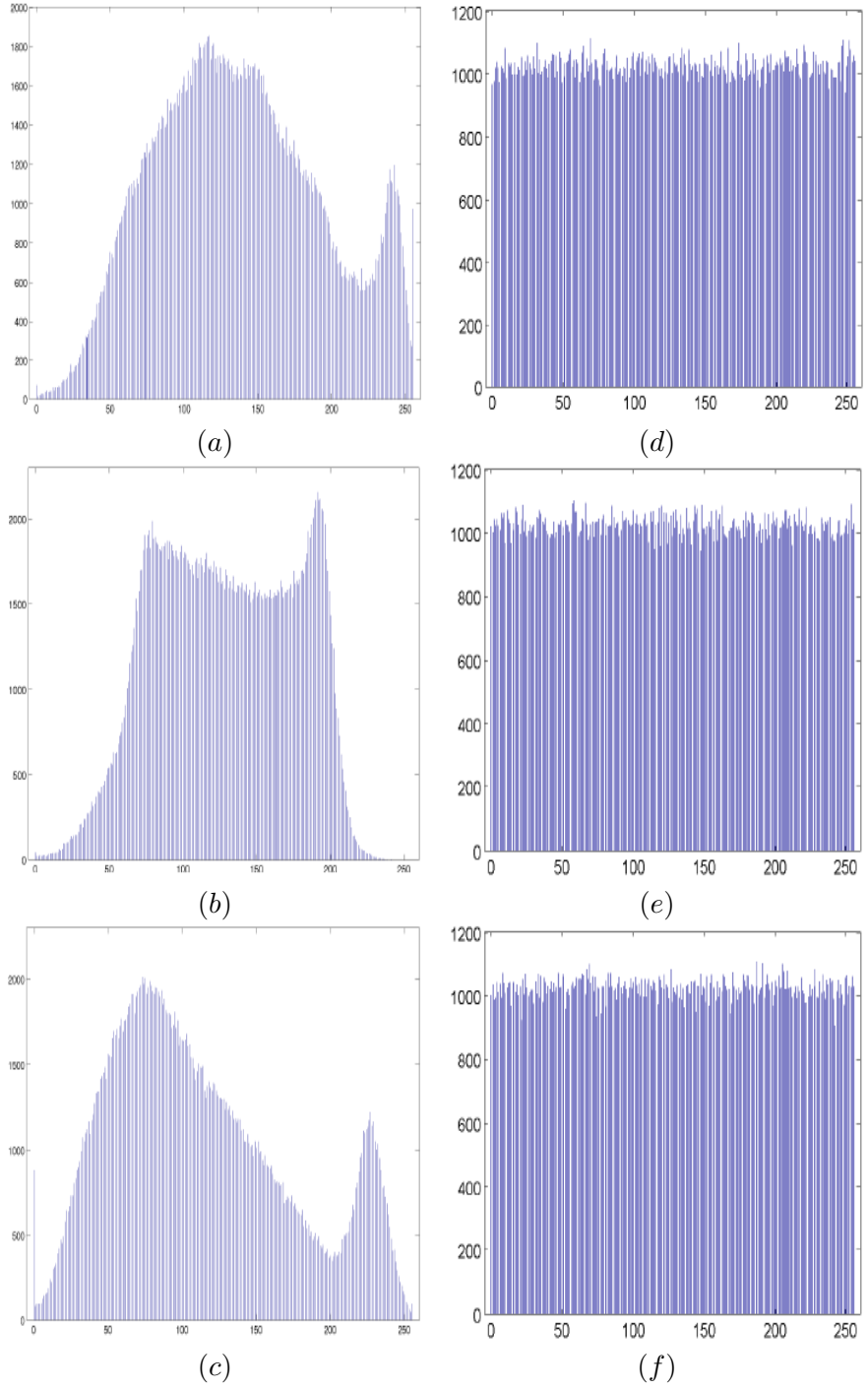


FIGURE 2.3: Histogrammes de l'image claire (Baboon) et l'image cryptée. Composantes rouge (a), verte (b), bleue (c) de l'image claire. Composantes rouge (d), verte (e), bleue (f) de l'image cryptée.

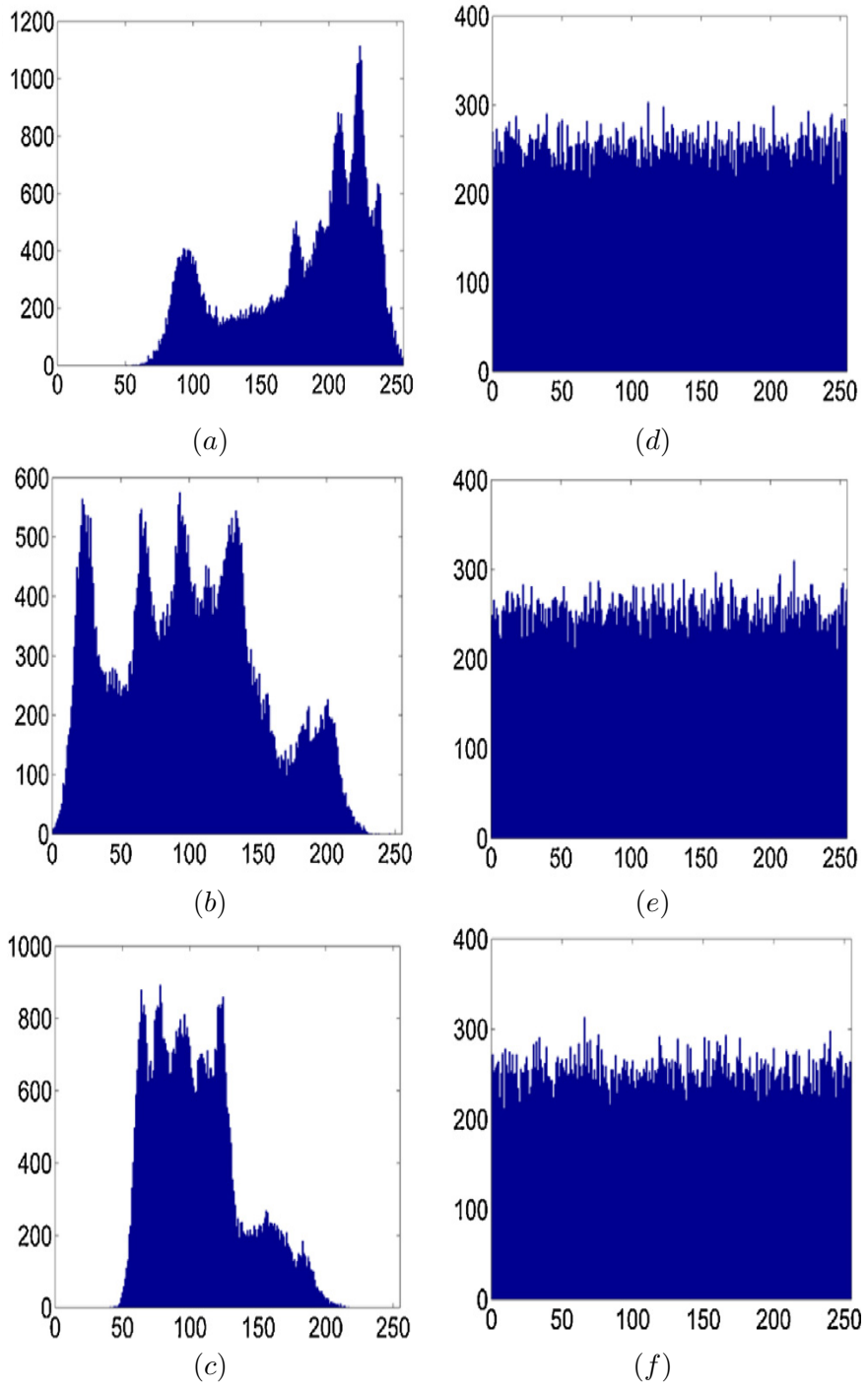
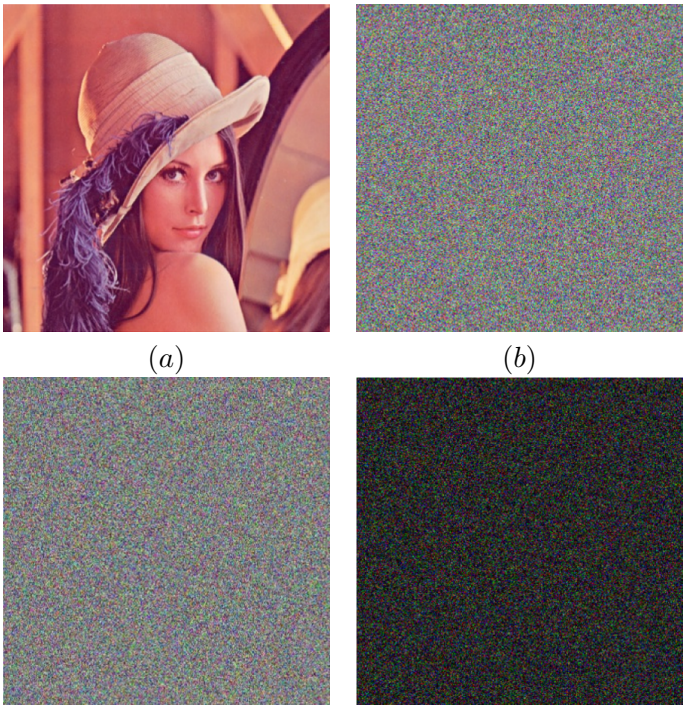


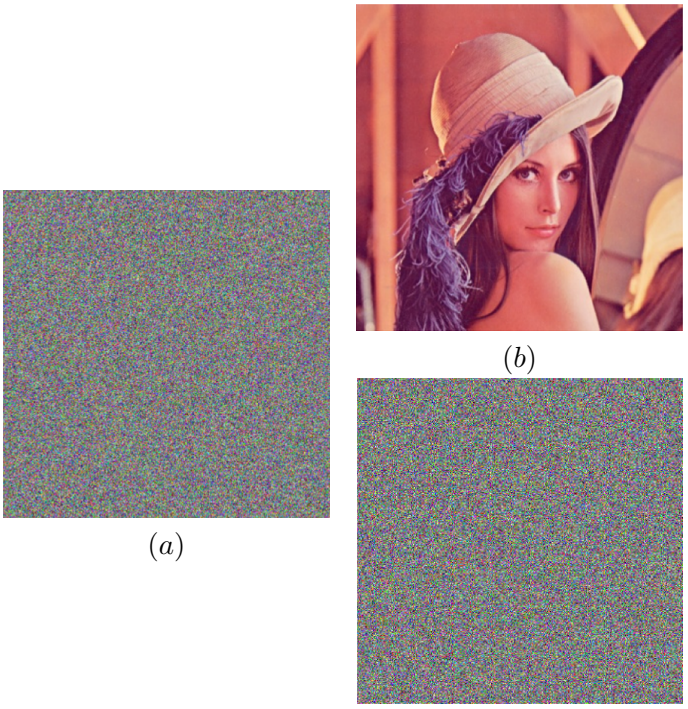
FIGURE 2.4: Histogrammes de l'image claire (Lena) et l'image cryptée. Composantes rouge (a), verte (b), bleue (c) de l'image claire. Composantes rouge (d), verte (e), bleue (f) de l'image cryptée.



(a) (b)

(c) (d)

FIGURE 2.5: Sensibilité à la clé de chiffrement.(a) image claire, (b) image cryptée avec la $1^{ère}$clé, (c) image cryptée avec la $2^{ème}$clé, (d) image de différence.



(b)

(a)

(c)

FIGURE 2.6: Sensibilité à la clé de déchiffrement (a) image chiffrée avec la $1^{ère}$clé, (b) image déchiffrée avec la $1^{ère}$clé, (c) image décryptée avec la $2^{ème}$clé.

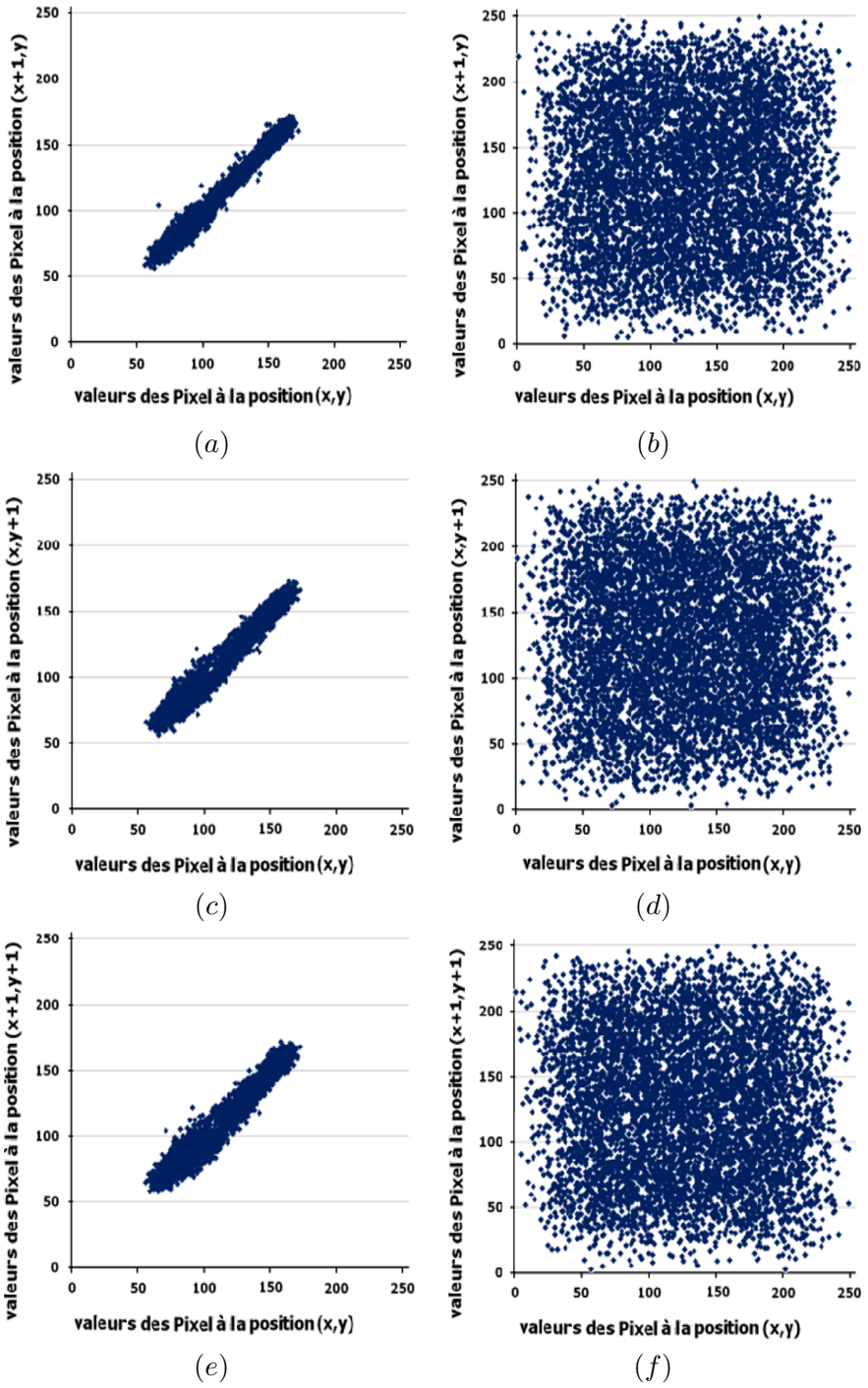


FIGURE 2.7: Corrélation des pixels adjacents de l'image (Lena) claire / cryptée. (a) la corrélation des pixels horizontalement adjacents dans l'image originale, (b) la corrélation de pixels horizontalement adjacents dans l'image chiffrée, (c) la corrélation de pixels verticalement adjacents dans l'image originale, (d) corrélation des pixels verticalement adjacents dans l'image cryptée, (e) corrélation des pixels diagonalement adjacents de l'image originale, (f) corrélation des pixels diagonalement adjacents de l'image cryptée.

Chapitre 3

Communication chaotique robuste basée sur la synchronisation à couplage indirect

Ce chapitre est dédié à la proposition d'une approche de communication chaotique selon un système de synchronisation par couplage indirect en cryptant des signaux de forte puissance. Le schéma proposé est soigneusement conçu de sorte que le signal crypté ne détériore pas la synchronisation, contrairement aux méthodes traditionnelles de communication. Le problème de synchronisation est résolu en utilisant un contrôleur basé sur observateur. Les avantages de cette approche sont les suivants :

- la méthodologie générale de conception d'observateur à rétroaction est appropriée pour la synchronisation ;
- la flexibilité dans le choix des signaux chaotiques pour le générateur de clé du cryptosystème sécurisé ;
- et l'amélioration des caractéristiques fréquentielles du message transmis.

Les simulations montrent que la synchronisation entre l'émetteur et le récepteur est plus robuste pour différentes valeurs d'amplitude du signal d'information, même en présence de perturbations externes.

3.1 Introduction

L'utilisation du chaos pour concevoir des systèmes de communication analogiques et numériques sécurisés a conduit les chercheurs à porter un intérêt de recherche de plus en plus important dans le domaine des communications sécurisées. La plupart des systèmes de communication analogiques par chaos sécurisés 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 le début des années quatre-vingt-dix, plusieurs méthodes de synchronisation chaotique du récepteur avec l'émetteur ont été proposées [2, 40–45], avec des applications pour sécuriser les communications [46–54]. Selon les structures de cryptage utilisées pour crypter le plain-signal, les systèmes de communication analogiques par chaos peuvent être classés en quatre catégories : masquage chaotique, commutation chaotique (aussi appelée modulation par déplacement chaotique : Chaotic Shift Keying - CSK), modulation chaotique, et par approche du système inverse. La plupart des systèmes basés sur ces techniques ont été cassés [52, 55–57]. 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 classiques. Dans [45], un système de communication chaotique est proposé dans lequel un premier état est utilisé en tant que clé de chiffrement en utilisant l'algorithme de chiffrement à n-decalage, et un second état du même système chaotique est utilisé comme signal conducteur pour synchroniser le récepteur. Le signal conducteur est obtenu après avoir masqué le deuxième état chaotique et le message chiffré. Il a été déclaré qu'un espion peut avoir un succès limité en utilisant des techniques de prévision dynamiques non linéaires pour en extraire le message. En plus, afin de fournir une approche systématique pour la synchronisation et la communication, l'utilisation de l'approche basée sur un observateur a été proposée dans [51, 58, 59]. Dans de tels systèmes de communication chaotiques sécurisés, 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 rapide 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 [60], les auteurs ont proposé un système de communication chaotique sécurisé fondé sur un schéma de synchronisation avec couplage indirect (indirect coupled synchronisation scheme - ICSS). L'émetteur chaotique est d'abord utilisé pour générer deux signaux de sortie. Le premier signal de sortie est utilisé à des

fins de modulation tandis que le second signal de sortie est utilisé pour conduire le générateur chaotique des clés, et dont la structure est différente de celle de l'émetteur. Ensuite, la sortie du générateur des clés est utilisée comme clé pour chiffrer le message clair. Le signal crypté résultant est masqué par le premier signal de sortie de l'émetteur. Au niveau du récepteur, lors de la réception du signal de sortie, l'observateur chaotique permet d'obtenir, après synchronisation, une estimation du signal de sortie transmis. Par conséquent, le plain-message peut être récupéré en appliquant la règle de déchiffrement, où les générateurs des clés au niveau de l'émetteur et du récepteur sont couplés indirectement. Comme l'énergie du plain-message doit être beaucoup plus petite que celle du signal de commande, il semble impossible d'éliminer ce défaut de sécurité essentiel sans modifier la structure de l'émetteur. L'inconvénient majeur est que, dans ce cas, le message clair ne peut pas être distingué du bruit de canal et donc, les performances du système sont fortement dégradées par la distorsion d'amplitude et du bruit dans le canal. Il existe donc un réel intérêt à trouver des moyens de surmonter les inconvénients précités.

Dans la présente contribution, qui peut être vue comme une généralisation de l'approche effectuée dans [60], nous étudions l'approche basée sur des observateurs non linéaires généralisés à la fois pour la synchronisation du chaos et la communication sécurisée. Nous introduisons des transformations ordinaires utiles pour établir des conditions suffisantes pour la convergence asymptotique. Afin de clarifier notre contribution, nous mettons en exergue les principales différences par rapport aux travaux de Kharel et al. [60]. Tout d'abord, nous considérons les systèmes chaotiques à sorties multiples et à signaux d'information multiples qui peuvent être injectés d'une façon non linéaire dans le modèle chaotique. Cela signifie que nous élargissons la classe des systèmes non linéaires à prendre en considération. D'autre part, la synchronisation et la communication sécurisée sont traitées simultanément. Par ailleurs, en plus de la synchronisation du chaos, on traite le problème du bruit de canal, et nous y tenons en compte lors de la conception du contrôleur. L'approche proposée est donnée comme suit. Tout d'abord, le signal crypté est réinjecté dans l'émetteur. Ensuite, ce signal crypté est envoyé au récepteur. Lors de la conception d'un récepteur, la synchronisation chaotique, entre l'émetteur et le récepteur couplés et entre les générateurs de clés au niveau de l'émetteur et du récepteur à couplage indirect, est obtenue en calculant les gains de l'observateur [58, 61]. Une fois la synchronisation établie, ce qui signifie que les états internes de l'émetteur et le récepteur sont les mêmes, nous régénérons le même signal crypté en utilisant l'algorithme de chiffrement à n-décalage, puis nous récupérons le signal crypté au niveau du récepteur. En utilisant le théorème de stabilité de Lyapunov et les techniques adaptatives, des conditions suffisantes pour la synchronisation à couplage indirecte pour une communication sécurisée sont atteintes. A travers les simulations numériques présentées, nous avons pu

vérifier l'efficacité du schéma proposé pour sécuriser la transmission de l'information qui possède une remarquable stabilité au bruit. Comme il serait indiqué plus tard, notre schéma illustre une grande résistance au bruit en comparaison avec le schéma initial proposé basé sur la synchronisation à couplage indirecte.

Ce système de communication chaotique proposé présente plusieurs avantages :

1. la synchronisation peut être atteinte simplement en calculant les gains d'observateurs, ce qui peut être résolu par des toolboxes logicielles puissantes ;
2. la flexibilité dans le choix des signaux chaotiques pour le générateur de clés du cryptosystème sécurisé ;
3. les dynamiques de l'émetteur sont commandés par des signaux variables dans le temps, ce qui semble indiquer que l'émetteur est un système non autonome, qui est en général plus compliquée ;
4. et l'amélioration des caractéristiques fréquentielles du signal crypté.

À la lumière de ces avantages, le système de communication chaotique proposé possède une conception efficace, ce qui offre un niveau de sécurité plus élevé. Une étude comparative entre le système de communication proposé et certains systèmes de communication rapportés dans la littérature est réalisée. En effet, il est montré que la synchronisation entre l'émetteur et le récepteur est plus robuste pour différentes valeurs d'amplitude du signal crypté, même en présence de perturbations extérnes.

3.2 Structure de la communication chaotique

Dans les communications chaotiques traditionnelles, est exploitée la synchronisation de l'émetteur-récepteur. De tels types de systèmes de communication chaotique présentent souvent des échecs en matière de sécurité, comme indiqué dans [62]. La structure du cryptosystème chaotique proposé est représentée sur la Fig.3.1.

Le message $m(t)$ à transmettre est le texte en clair, qui est chiffré en utilisant l'algorithme de chiffrement à n-décalage. Le plaintext crypté résulte dans le texte chiffré $\vartheta\left(m\left(t\right), k\left(t\right)\right)$. La récupération du plaintext à partir du texte chiffré est possible gràce à l'utilisation de la fonction de déchiffrement $\hat{\vartheta}(m\left(t\right), \hat{k}\left(t\right))$. Les processus de chiffrement et de déchiffrement utilisent respectivement les générateurs de clés (KG_T) et (KG_R). Le système de communication sécurisé proposé se compose de trois éléments principaux, à savoir l'émetteur, le récepteur et les blocs de chiffrement et de déchiffrement.

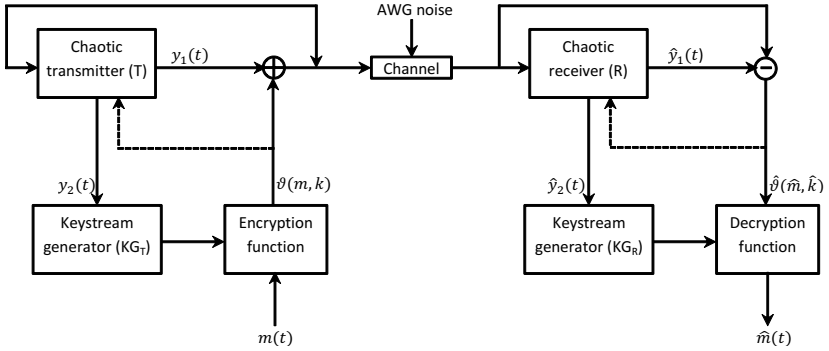


FIGURE 3.1: Schéma du système de communication chaotique proposé.

3.2.1 L'émetteur

L'émetteur chaotique (T) est représenté par

$$(T): \begin{cases} \dot{X}(t) = A(y_d)X(t) + f(t, y_d) + L\vartheta(m(t), k(t)) \\ y_1(t) = C_1 X(t) \\ y_2(t) = C_2 X(t) \\ y_d(t) = y_1(t) + \vartheta(m(t), k(t)) \end{cases} \tag{3.1}$$

où $X(t) \in \mathbb{R}^n$ est le vecteur d'état ; $y_1, y_2 \in \mathbb{R}$ sont les sorties de l'émetteur ; $y_d(t) \in \mathbb{R}$ est le signal de commande servant à synchroniser le récepteur ; C_1, C_2 sont des matrices constantes de dimensions appropriées ; L est la matrice des gains de l'observateur de dimension appropriée ; et $\vartheta(m, k)$ est une fonction de chiffrement qui crypte le message $m(t)$ à l'aide de la clé $k(t)$. Ici, la matrice $A(y_d)$ est une fonction de $y_d(t)$, et $f(t, y_d)$ est une fonction lisse du signal conducteur. Il est supposé que les entrées de $A(y_d)$ sont lisses et bornées et que la paire $(A(y_d), C)$ est de rang-observable pour tous $y_d(t) \in \mathbb{R}$. Le générateur des clés (KG_T) au niveau de l'émetteur utilise un autre système chaotique de la forme suivante

$$(KG_T): \begin{cases} \dot{Z}(t) = FZ(t) + g(t, y_2) \\ k(t) = h(Z(t)) \end{cases} \tag{3.2}$$

où $Z(t) \in \mathbb{R}^m$ est le vecteur d'état ; $k(t) \in \mathbb{R}$ est la sortie du générateur des clés (KG_T); F est une matrice de dimension appropriée ; h est une fonction vectorielle analytique ; et g est une fonction lisse.

Le signal obtenu est transmis à travers le canal de communication (où le bruit est supposé être également observé) vers le récepteur situé de l'autre côté de du canal de communication.

3.2.2 Le récepteur

Le récepteur global (R) est conu de sorte qu'il se synchronise avec l'émetteur chaotique (T). Il est décrit comme suit :

$$(R):\begin{cases}\dot{\hat{X}}(t)=A(y_d)\hat{X}(t)+f(t,y_d)+L(y_d(t)-\hat{y}_1(t))\\ \hat{y}_1(t)=C_1\hat{X}(t)\\ \hat{y}_2(t)=C_2\hat{X}(t)\end{cases} \tag{3.3}$$

où $\hat{X}(t)\in\mathbb{R}^n$ est le vecteur d'état et $\hat{y}_1,\hat{y}_2\in\mathbb{R}$ sont les sorties du récepteur. Le générateur des clés (KG_R) au niveau du récepteur est décrit comme suit :

$$(KG_R):\begin{cases}\dot{\hat{Z}}(t)=F\hat{Z}(t)+g(t,\hat{y}_2)\\ \hat{k}(t)=h(\hat{Z}(t))\end{cases} \tag{3.4}$$

où $\hat{Z}(t)\in\mathbb{R}^m$ est le vecteur d'état, $\hat{k}(t)\in\mathbb{R}$ est la sortie du générateur des clés (KG_R). F, h et g sont définies dans (3.2).

A la sortie du récepteur, le signal émis passe par le soustracteur et le signal récupéré est ainsi détecté.

3.2.3 Processus de chiffrement et de déchiffrement

Le processus de chiffrement consiste à exécuter l'algorithme de chiffrement à n-décalage donné comme suit

$$\vartheta(m(t),k(t))=\underbrace{S(...S(S}_{n}(m(t),\underbrace{k(t)),k(t)),...,k(t)}_{n}) \tag{3.5}$$

où $S(m(t),k(t))$ est une fonction nonlinéaire donnée par

$$S(m(t),k(t))=\begin{cases}m(t)+k(t)+2l & -2l\le m(t)+k(t)<-l\\ m(t)+k(t) & -l\le m(t)+k(t)\le l\\ m(t)+k(t)-2l & l<m(t)+k(t)\le 2l\end{cases} \tag{3.6}$$

avec l étant un paramètre de cryptage choisi de telle sorte que $m(t)$ et $k(t)$ se situent dans l'intervalle $[-l,\ l]$.

Le processus de déchiffrement est basé sur l'algorithme de déchiffrement à n-décalage, où le texte chiffré $\hat{\vartheta}(m(t), \hat{k}(t))$ donné par

$$\hat{\vartheta}(m(t), \hat{k}(t)) = y_d(t) - \hat{y}_1(t) \tag{3.7}$$

Une fois, $\hat{\vartheta}(m(t), \hat{k}(t)) \rightarrow \vartheta(m(t), k(t))$, le plaintext est obtainu en déchiffrant le ciphertext $\hat{\vartheta}(m(t), \hat{k}(t))$ comme suit :

$$\begin{aligned} \hat{m}(t) &= \vartheta^{-1}(\hat{\vartheta}(m(t), \hat{k}(t)), -\hat{k}(t)) \\ &= \underbrace{S(...S(S}_{n}(\hat{\vartheta}(m(t), \hat{k}(t)), \underbrace{-\hat{k}(t)), -\hat{k}(t)), ..., -\hat{k}(t))}_{n} \end{aligned} \tag{3.8}$$

3.3 Synchronisation chaotique

Dans cette section, nous considérons le problème de synchronisation avec la méthode de couplage indirecte proposée dans [60], mais avec la généralisation suivante. Nous considérons les hypothèses suivantes.

Hypothèse 1 : Il existe des matrices symétriques définies positives P_1, P_2; et des constantes positives c_1, c_2 tel que

$$(A(y_d) - LC_1)^T P_1 + P_1 (A(y_d) - LC_1) \leq -c_1 P_1, \quad \forall y_d \in \mathbb{R} \tag{3.9}$$

et

$$F^T P_2 + P_2 F \leq -c_2 P_2 \tag{3.10}$$

Hypothèse 2 : Il existe $M > 0$ tel que $\left\| \frac{\partial g}{\partial y_2} \right\| < M$, où $\|\cdot\|$ est la norme Euclidiène.

Hypothèse 3 : La fonction de sortie $h(\cdot)$ est globalement Lipschitzian.

La condition de stabilité est obtenue en utilisant la méthode de Lyapunov.

Theorem 3.1. *Sous les hypothèses H1–H3, il existe une constante $\mu_1 > 0$ telle que*

$$\left\| \psi(t) - \hat{\psi}(t) \right\| \leq \left\| \psi(0) - \hat{\psi}(0) \right\| \exp(-\mu_1 t), \text{ quelque soit } t \geq 0, \tag{3.11}$$

où $\psi^T(t) = [X(t) \;\; Z(t)]$.

En d'autres termes, le récepteur R et le générateur des clés KG_R au niveau du récepteur, se synchronisent respectivement de façon exponentielle avec l'émetteur T et le générateur des clés KG_T au niveau de l'émetteur.

Démonstration. Définissons le vecteur d'état d'erreur $\tilde{X}(t) = X(t) - \hat{X}(t)$. D'après (3.1) et (3.3) alors la dynamique d'erreurs de $\tilde{X}(t)$ est exprimée ainsi

$$\begin{aligned}
\dot{\tilde{X}}(t) &= A(y_d)\tilde{X}(t) + L\vartheta(m(t), k(t)) - L(y_d - \hat{y}_1(t)) \\
&= A(y_d)\tilde{X}(t) + L\vartheta(m(t), k(t)) - L\left(C_1 X(t) + \vartheta(m(t), k(t)) - C_1\hat{X}(t)\right) \\
&= (A(y_d) - LC_1)\tilde{X}(t)
\end{aligned}$$

Etant donnée une fonction candidat de Lyapunov $V_1(\tilde{X}(t)) = \tilde{X}^T(t) P_1 \tilde{X}(t) > 0$, nous avons

$$\begin{aligned}
\dot{V}_1(\tilde{X}(t)) &= \dot{\tilde{X}}^T(t) P_1 \tilde{X}(t) + \tilde{X}^T(t) P_1 \dot{\tilde{X}}(t) \\
&= \tilde{X}^T(t) (A(y_d) - LC_1)^T P_1 \tilde{X}(t) + \tilde{X}^T(t) P_1 (A(y_d) - LC_1)\tilde{X}(t) \\
&= \tilde{X}^T(t) \left[(A(y_d) - LC_1)^T P_1 + P_1 (A(y_d) - LC_1)\right]\tilde{X}(t)
\end{aligned}$$

Sous réserve de l'hypothèse H1, alors

$$\dot{V}_1(\tilde{X}(t)) \leq -c_1 V_1(\tilde{X}(t)) < 0$$

Maintenant, définissons l'erreur entre les générateurs des clés (KG_T) et (KG_R) telle que $\tilde{Z}(t) = Z(t) - \hat{Z}(t)$. D'après (3.2) et (3.4), alors la dynamique d'erreurs de $\tilde{Z}(t)$ est donnée par

$$\begin{aligned}
\dot{\tilde{Z}}(t) &= F\tilde{Z}(t) + g(t, y_2) - g(t, \hat{y}_2) \\
&= F\tilde{Z}(t) + \frac{\partial g}{\partial y_2}(y_2(t) - \hat{y}_2(t)) \\
&= F\tilde{Z}(t) + \frac{\partial g}{\partial y_2} C_2 \tilde{X}(t)
\end{aligned}$$

Etant donnée une fonction candidat de Lyapunov $V_2(\tilde{Z}(t)) = \tilde{Z}^T(t) P_2 \tilde{Z}(t) > 0$, nous avons

$$\begin{aligned} \dot{V}_2(\tilde{Z}(t)) &= \dot{\tilde{Z}}^T(t) P_2 \tilde{Z}(t) + \tilde{Z}^T(t) P_2 \dot{\tilde{Z}}(t) \\ &= \tilde{Z}^T(t) \left[F^T P_2 + P_2 F\right] \tilde{Z}(t) + 2\frac{\partial g}{\partial y_2} \tilde{Z}^T(t) P_2 C_2 \tilde{X}(t) \end{aligned}$$

Sous réserve des l'hypothèses H1 et H2, alors

$$\dot{V}_2(\tilde{Z}(t)) \leq -c_2 V_2(\tilde{Z}(t)) + 2M \left\| \tilde{Z}^T(t) P_2 C_2 \tilde{X}(t) \right\|$$

Il existe une constante $\theta > 0$ telle que

$$\begin{aligned} 2M \left\| \tilde{Z}^T(t) P_2 C_2 \tilde{X}(t) \right\| &\leq 2\theta \left\| \tilde{X}(t) \right\| \left\| \tilde{Z}(t) \right\| \\ &\leq 2\theta \sqrt{V_1(\tilde{X}(t))} \sqrt{V_2(\tilde{Z}(t))} \end{aligned}$$

En plus, il existe une constante $\xi > 0$ telle que

$$\begin{aligned} 2\theta \sqrt{V_1(\tilde{X}(t))} \sqrt{V_2(\tilde{Z}(t))} &= 2\theta \sqrt{\xi V_1(\tilde{X}(t))} \sqrt{V_2(\tilde{Z}(t))/\xi} \\ &\leq \theta \left(\xi V_1(\tilde{X}(t)) + V_2(\tilde{Z}(t))/\xi\right) \end{aligned}$$

Ainsi,

$$\dot{V}_2(\tilde{Z}(t)) \leq -c_2 V_2(\tilde{Z}(t)) + \theta \left(\xi V_1(\tilde{X}(t)) + V_2(\tilde{Z}(t))/\xi\right)$$

Soit $W^T(t) = \left[\tilde{X}(t) \;\; \tilde{Z}(t)\right]$, alors

$$\dot{\chi}(t) = \begin{pmatrix} A(y_d) - KC_1 & 0 \\ \frac{\partial g}{\partial y_2} C_2 & F \end{pmatrix} \chi(t)$$

Soit une fonction candidat de Lyapunov $V_3(W(t)) = V_1(\tilde{X}(t)) + V_2(\tilde{Z}(t))$, alors, nous avons

$$\begin{aligned}\dot{V}_3(W(t)) &= \dot{V}_1(\tilde{X}(t)) + \dot{V}_2(\tilde{Z}(t)) \\ &\leq -c_1 V_1(\tilde{X}(t)) - c_2 V_2(\tilde{Z}(t)) + \theta\left(\xi V_1(\tilde{X}(t)) + V_2(\tilde{Z}(t))/\xi\right) \\ &\leq -(c_1 - \theta\xi) V_1(\tilde{X}(t)) - (c_2 - \theta/\xi) V_2(\tilde{Z}(t))\end{aligned}$$

En posant $\mu_1 = c_1 - \theta\xi$ et $\mu_2 = c_2 - \theta/\xi$, alors,

$$\begin{aligned}\dot{V}_3(W(t)) &\leq -\mu_1 V_1(\tilde{X}(t)) - \mu_1 V_2(\tilde{Z}(t)) + \mu_1 V_2(\tilde{Z}(t)) - \mu_2 V_2(\tilde{Z}(t)) \\ &\leq -\mu_1 W(\chi(t)) - (\mu_2 - \mu_1) V_2(\tilde{Z}(t))\end{aligned}$$

La dérivée dans le temps $\dot{V}_3(W(t))$ est définie négative pour $\mu_1 > 0$ et $\mu_2 - \mu_1 > 0$. Par conséquent, si θ appartient à l'intervalle $[(-c_0 - \sqrt{c_0^2 + 4\xi^2})/2\xi, (-c_0 + \sqrt{c_0^2 + 4\xi^2})/2\xi]$ avec $c_0 = c_2 - c_1$, alors

$$\dot{V}_3(W(t)) \leq -\mu_1 V_3(W(t))$$

Par suite,

$$\|W(t)\| \leq \|W(0)\| \exp(-\mu_1 t)$$

Cela signifie que $\hat{X}(t)$ et $\hat{Z}(t)$ convergent exponentiellement vers $X(t)$ et $Z(t)$, respectivement. Autrement dit, l'émetteur T et le récepteur R se synchronisent exponentiellement. De même, KG_R converge exponentiellement vers KG_T lorsque le temps $t \to \infty$. Ce qui termine la démonstration. □

Remark 3.2. En application du texte chiffré, nous avons une variété de choix pour la clé sécurisée $k(t)$. Par exemple, l'un des états internes de l'émetteur chaotique peut être utilisé. De plus, les états internes des générateurs des clés ne sont pas accessibles de l'exterieur (ne sont pas publics), ce qui permet d'obtenir une plus grande sécurité.

Remark 3.3. La méthode proposée peut être étendue, le long du travail développé dans [63], à la conception généralisée d'observateur d'ordre réduit de sorte que les exigences de calcul sont réduits. De plus, la méthode proposée peut être élargée pour la mise en œuvre pratique, le long des travaux développés dans [64–66], pour surmonter les limites

en fréquence et d'éliminer les effets négatifs y afférents. D'autre part, il existe de nombreux articles concernant la synchronisation dans les réseaux complexes. En particulier, Serrano-Guerrero et al. [67] ont présenté certains critères de synchronisation basée sur le concept de la synchronisation complète. Le système de communication sécurisée proposé utilisant la synchronisation à couplage indirect dans le présent travail peut également être appliqué pour l'étude de synchronisation et de communication sécurisée dans les réseaux complexes. En effet, la synchronisation à couplage indirecte ne nécessite pas une identité des générateurs chaotiques des deux côtés du canal de communication en raison de l'utilisation du concept de la synchronisation généralisée à la place de la synchronisation complète.

Remark 3.4. Nous notons également que le système de communication sécurisé proposé est valable pour les systèmes hyperchaotiques avec plus d'un exposant de Lyapunov positif.

3.4 Résultats de simulation

Pour vérifier les résultats théoriques, nous effectuons des simulations numériques sur le système de communication sécurisée proposé. Le système chaotique unifié est utilisé pour synchroniser l'émetteur et le récepteur en utilisant un couplage indirect, alors que les générateurs des clés au niveau de l'émetteur et du récepteur sont des systèmes de Chua et choisis pour être couplés indirectement. Ce choix est lié au fait que :

- Les systèmes cités sont largement étudiés dans la littérature,
- La synchronisation remplit les exigences énoncées dans les Sections 3.1 - 3.2 (voir aussi [60]),
- La réalisation pratique de ces générateurs est possible.

3.4.1 Résultats de synchronisation

Dans ce paragraphe, nous expliquons comment concevoir les matrices du contrôleur P_1, P_2 et les constantes c_1, c_2 selon le Theorem 1. L'émetteur (T) et le récepteur (R)

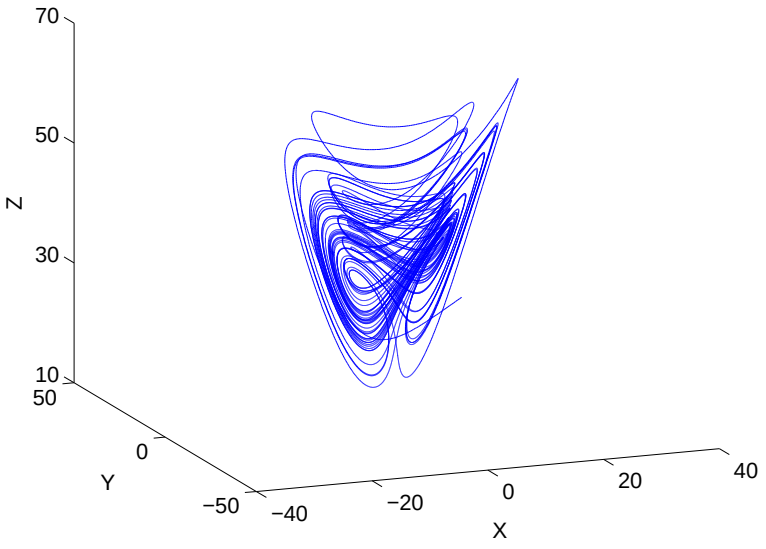


FIGURE 3.2: Portrait de phase du système chaotique unifié.

construits à partir du système chaotique unifié [68] sont donnés par

$$(T) \quad : \quad \begin{cases} \dot{x}_1 = (25\alpha + 10)(x_2 - x_1) + L_1\vartheta(m,k) \\ \dot{x}_2 = (28 - 35\alpha - x_3)\, y_d - (1 - 29\alpha)\, x_2 + L_2\vartheta(m,k) \\ \dot{x}_3 = y_d x_2 - \frac{\alpha+8}{3} x_3 + L_3\vartheta(m,k) \\ y_1 = x_1 \\ y_2 = x_2 \\ y_d = x_1 + \vartheta(m,k) \end{cases} \tag{3.12}$$

$$(R) \quad : \quad \begin{cases} \dot{\hat{x}}_1 = (25\alpha + 10)(\hat{x}_2 - \hat{x}_1) + L_1(y_d - \hat{y}_1) \\ \dot{\hat{x}}_2 = (28 - 35\alpha - \hat{x}_3) y_d - (1 - 29\alpha)\, \hat{x}_2 + L_2(y_d - \hat{y}_1) \\ \dot{\hat{x}}_3 = y_d \hat{x}_2 - \frac{\alpha+8}{3} \hat{x}_3 + L_3(y_d - \hat{y}_1) \\ \hat{y}_1 = \hat{x}_1 \\ \hat{y}_2 = \hat{x}_2 \end{cases} \tag{3.13}$$

où α est le paramètre du système tel que $\alpha \in [0,\ 1]$. Evidemment, le système chaotique unifié devient le système original de Lorenz pour $\alpha = 0$ et devient le système original de Chen pour $\alpha = 1$. Le comportement chaotique du système chaotique unifié pour $\alpha = 0.8$ est montré dans la Fig3.2.

Les générateurs des clés au niveau de l'émetteur (KG_T) et du récepteur (KG_R) sont mis en uvre à l'aide du célèbre système de Chua tel que

$$(KG_T) \quad : \quad \begin{cases} \dot{z}_1 = \delta\left(z_2 - z_1 - \varphi\left(y_2\right)\right) \\ \dot{z}_2 = y_2 - z_2 + z_3 \\ \dot{z}_3 = -\beta z_2 - \gamma z_3 \\ k = z_1 \end{cases} \tag{3.14}$$

$$(KG_R) \quad : \quad \begin{cases} \dot{\hat{z}}_1 = \delta\left(\hat{z}_2 - \hat{z}_1 - \varphi\left(\hat{y}_2\right)\right) \\ \dot{\hat{z}}_2 = \hat{y}_2 - \hat{z}_2 + \hat{z}_3 \\ \dot{\hat{z}}_3 = -\beta\hat{z}_2 - \gamma\hat{z}_3 \\ \hat{k} = \hat{z}_1 \end{cases} \tag{3.15}$$

avec la fonction nonlinéaire

$$\varphi\left(y_2\right) = m_1 y_2 + \frac{1}{2}\left(m_0 - m_1\right)\left(\left|y_2 + 1\right| - \left|y_2 - 1\right|\right) \tag{3.16}$$

et les paramètres $\delta = 9.35$, $\beta = 14.79$, $\gamma = 0.016$, $m_0 = -1.13$, $m_1 = -0.722$ afin d'obtenir l'attracteur à double scroll.

Le problème de synchronisation, tel que défini dans (3.9) et (3.10), correspond à

$$\begin{bmatrix} -\left(25\alpha + 10\right) - L_1 & L_2 & L_3 \\ \left(25\alpha + 10\right) & -\left(1 - 29\alpha\right) & y_d \\ 0 & -y_d & -\frac{\alpha+8}{3} \end{bmatrix} P_1 + P_1 \begin{bmatrix} -\left(25\alpha + 10\right) - L_1 & \left(25\alpha + 10\right) & 0 \\ L_2 & -\left(1 - 29\alpha\right) & -y_d \\ L_3 & y_d & -\frac{\alpha+8}{3} \end{bmatrix} \leq -c_1 P_1 \tag{3.17}$$

et

$$\begin{bmatrix} -\delta & 0 & 0 \\ \delta & -1 & -\beta \\ 0 & 1 & -\gamma \end{bmatrix} P_2 + P_2 \begin{bmatrix} -\delta & \delta & 0 \\ 0 & -1 & 1 \\ 0 & -\beta & -\gamma \end{bmatrix} \leq -c_2 P_2 \tag{3.18}$$

respectivement.

En posant $P_1 = diag(p_{11}, p_{12}, p_{13})$, et choisissant $p_{12} = p_{13}$, $L_2 = -\sigma p_{11}/p_{12}$, $L_3 = 0$, alors l'inégalité (3.17) devient

$$\begin{bmatrix} 2\left(25\alpha + 10 + L_1 - 0.5c_1\right)p_{11} & 0 & 0 \\ 0 & 2\left(1 - 29\alpha - 0.5c_1\right)p_{12} & 0 \\ 0 & 0 & \left(2\frac{\alpha+8}{3} - c_1\right)p_{12} \end{bmatrix} > 0 \tag{3.19}$$

qui est satisfaite pour $L_1 > c_1/2 - 25\alpha - 10$ avec $0 < c_1 < 2\left(1 - 29\alpha\right)$.

D'autre part, en posant $P_2 = diag(p_{21}, p_{22}, p_{23})$, et en choisissant $p_{22} = \beta p_{23}$, alors l'inégalité (3.18) devient

$$\begin{bmatrix} \left(2\delta - c_2\right)p_{21} & -\delta p_{21} & 0 \\ -\delta p_{21} & \beta\left(2 - c_2\right)p_{23} & 0 \\ 0 & 0 & \left(2\gamma - c_2\right)p_{23} \end{bmatrix} > 0 \tag{3.20}$$

qui est satisfaite pour $c_2 < 2\gamma$.

Remark 3.5. Il est à noter que ce choix des matrices P_1 et P_2 n'est pas unique, et l'on peut faire d'autres choix afin de satisfaire hypothèse H1.

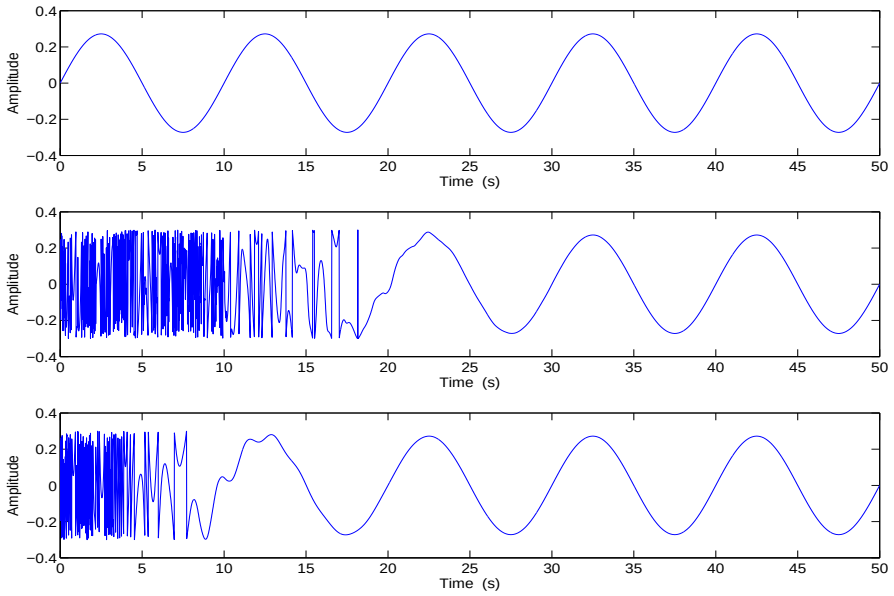
3.4.2 Transmission de l'information

La fonction de chiffrement au niveau de l'émetteur est telle que définie par (3.12). Les gains d'observateur ont été fixés à $L_1 = 0.7$, $L_2 = 0.7$ et $L_3 = 0$. Les conditions initiales de l'émetteur et du générateur des clés dans l'émetteur sont choisies $(x_1(0), x_2(0), x_3(0)) = (1, 2, 3)$ et $(z_1(0), z_2(0), z_3(0)) = (0.05, 0.06, 0.07)$, respectivement. Les conditions initiales du récepteur et du générateur des clés dans le récepteur sont choisies $(\hat{x}_1(0), \hat{x}_2(0), \hat{x}_3(0)) = (10.1, 10.2, 10.3)$ et $(\hat{z}_1(0), \hat{z}_2(0), \hat{z}_3(0)) = (-10.1, -12.2, 3.3)$, respectivement.

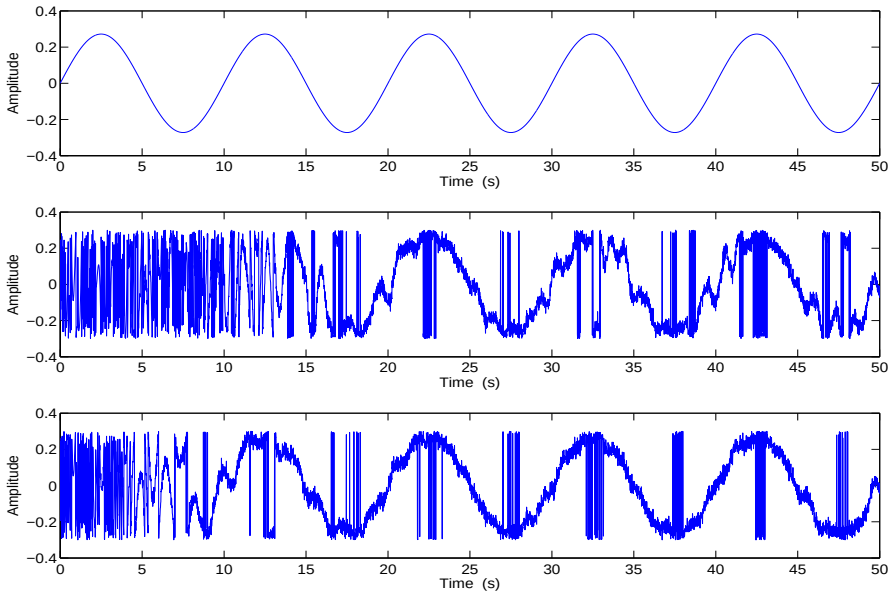
Le schéma de communication proposé a été simulé et comparé avec l'approche de ICSS. Afin de vérifier la robustesse du cryptosystème proposé en présence du bruit, un bruit blan Guaussien WGN (White Gaussian Noise) est ajouté aux états du système de l'émetteur.

Les Fig.3.3 et Fig.3.4 montrent les résultats de simulations où le message à transmettre est un signal sinusoïdal $m(t) = A\sin(2\pi ft)$ avec différentes valeurs d'amplitude.

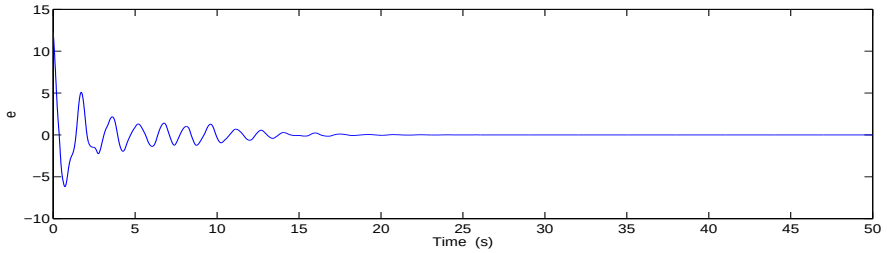
Nous pouvons clairement constater que la récupération des plain-messages en utilisant le schéma de communication sécurisé proposé est réalisée rapidement, en présence

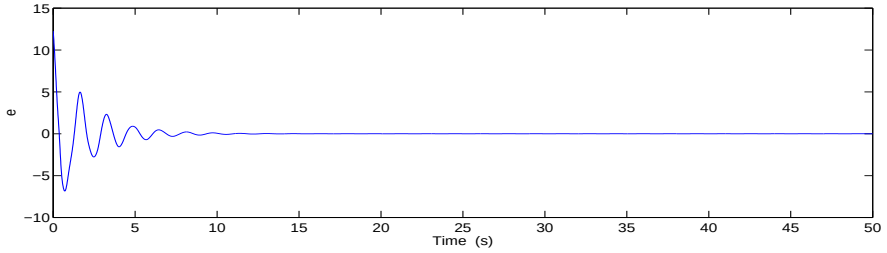


(a)

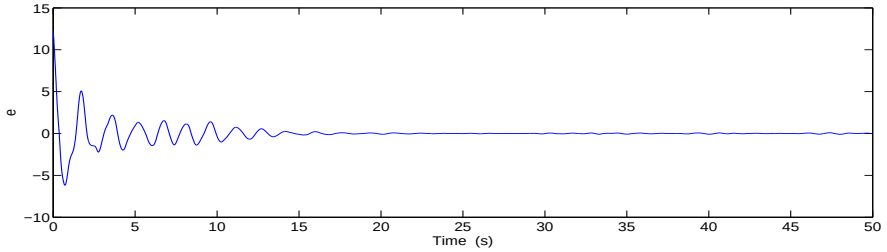


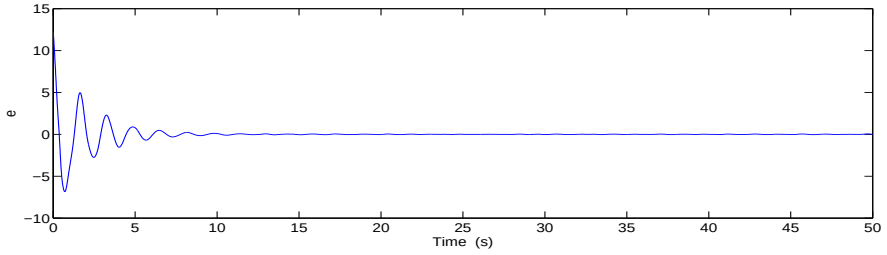
(b)



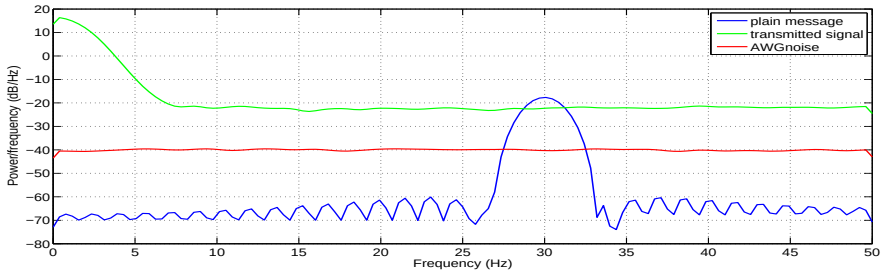


(c)



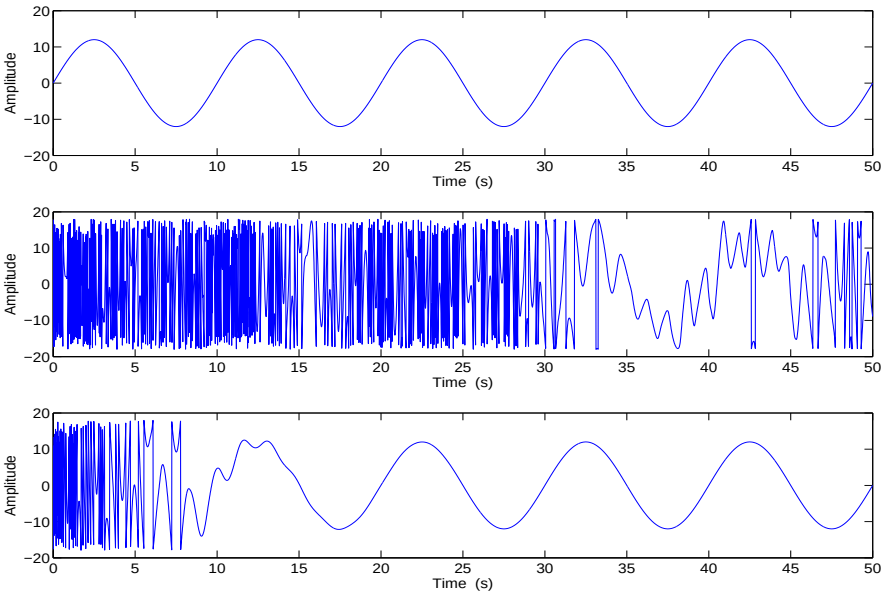


(d)

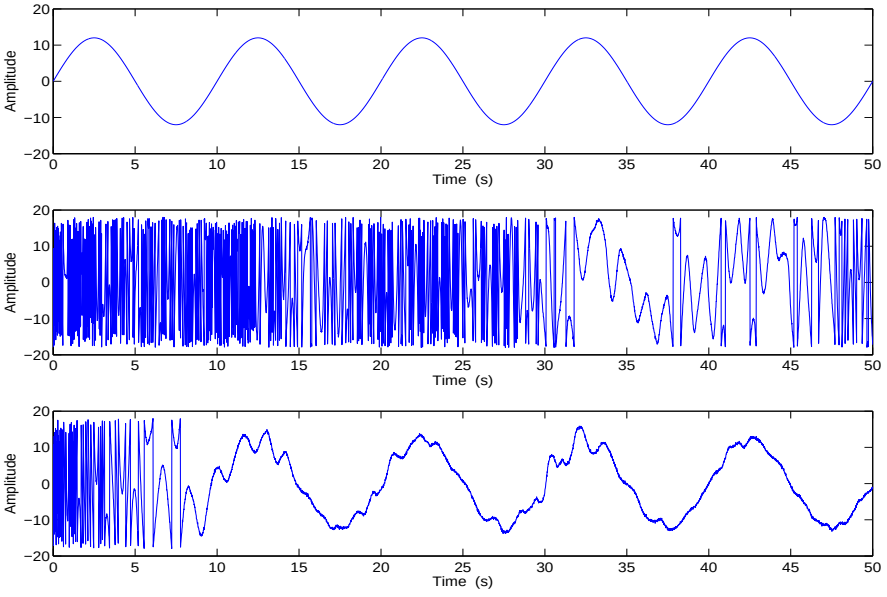


(e)

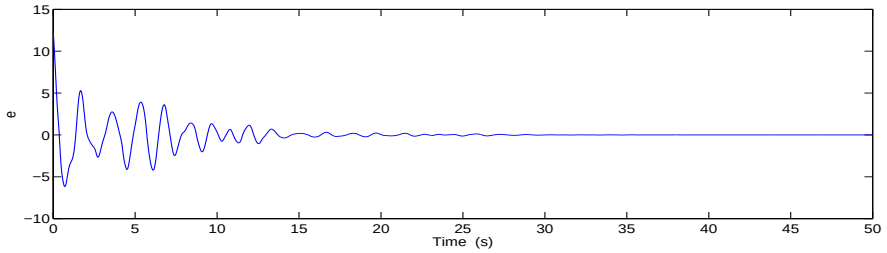
FIGURE 3.3: Communication chaotique robuste basée sur la synchronisation à couplage indirect. (a) Plain message $m(t) = 0.3\sin(60\pi t)$,le message récupéré en utilisant ICSS et le message récupéré en utilisant le système de cryptage proposé. ; (b) plain message, le message récupéré en utilisant ICSS et le message récupéré en utilisant le système de cryptage proposé en présence du WGN ; (c) erreur de synchronisation entre les générateurs des clés ; (d) erreur de synchronisation entre les générateurs des clés en présence du bruit additif ; et (e) densités spectrales de puissance du plain message, du bruit additif et du signal transmis .

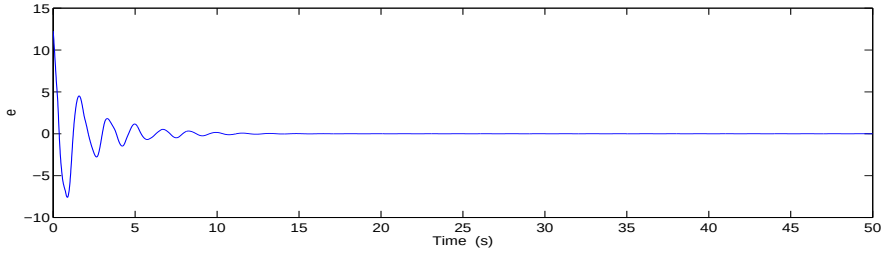


(a)

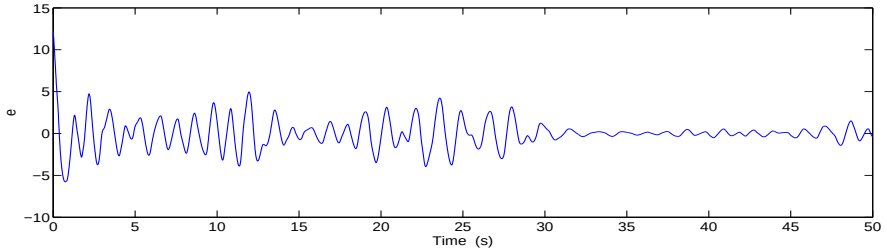


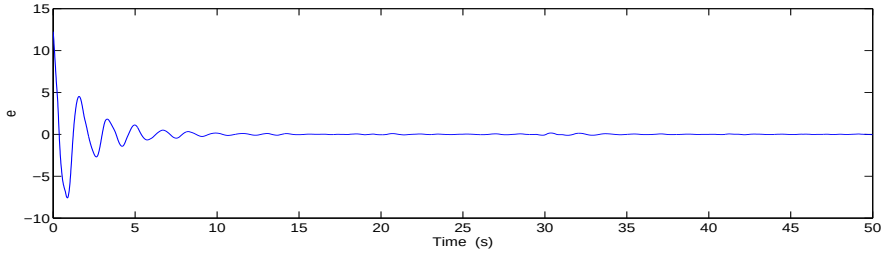
(b)



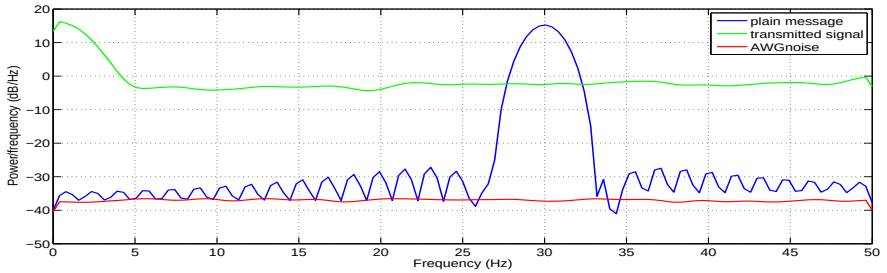


(c)





(d)



(e)

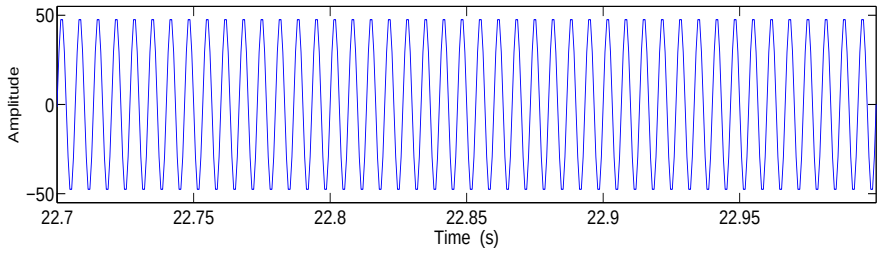
FIGURE 3.4: Communication chaotique robuste basée sur la synchronisation à couplage indirect. (a) Plain message $m(t) = 12\sin(60\pi t)$, le message récupéré en utilisant ICSS et le message récupéré en utilisant le système de cryptage proposé. ; (b) plain message, le message récupéré en utilisant ICSS et le message récupéré en utilisant le système de cryptage proposé en présence du WGN ; (c) erreur de synchronisation entre les générateurs des clés ; (d) erreur de synchronisation entre les générateurs des clés en présence du bruit additif ; et (e) densités spectrales de puissance du plain message, du bruit additif et du signal transmis .

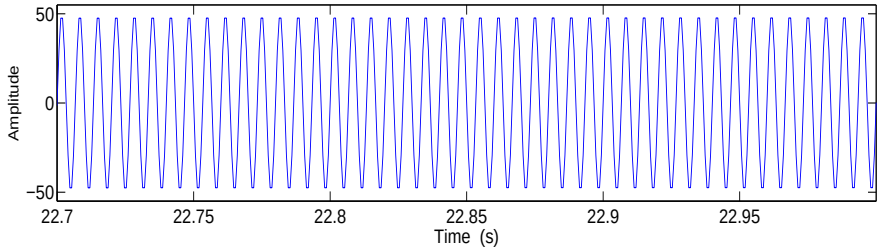
de bruit de canal ou en son absence. En particulier, les Fig.3.4 (a) - (e) montrent que, avec une augmentation de l'amplitude du message clair, la méthode proposée conserve la récupération du plain-message, et elle est plus robuste contre le bruit additif, par contre l'approche de ICSS est fortement affectée. Des simulations pour un niveau plus élevé d'amplitude et de fréquence du plain-message sont représentées dans les Fig.3.5 (a) - (c).

Les Fig.3.6 et Fig.3.7 montrent les résultats de simulations où le message à transmettre est un signal carré d'amplitude $A = 50$, et de fréquence $f = 150Hz$. On a fait varier le rapport cyclique de 0 à 100%. Sur la Fig.3.6 sont montrés les résultats de simulation pour le cas où le rapport cyclique est égal à 20%. On peut remarquer que l'erreur de synchronisation tend rapidement vers zéro. On constate aussi, d'après la densité spéctrale de puissance, qu'on ne peut détecter la fréquence du message clair dans le spectre du message cryptétransmis. De méme, on a varier les temps de montée et de descente du signal carré. Sur la Fig.3.7 sont montrés les résultats de simulation pour le cas où le rapport entre le temps de montée t_r et le temps de decente t_f sont tel que $t_r = t_f = 1/(10f), avec f = 150Hz$. On peut remarquer que l'erreur de synchronisation tend rapidement vers zéro. On constate aussi, d'après la densité spéctrale de puissance, qu'on ne peut détecter la fréquence du message clair dans le spectre du message cryptétransmis.

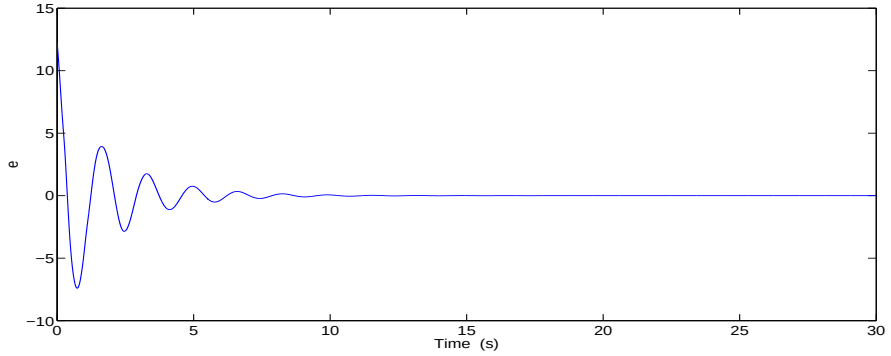
3.5 Analyse des performances

Afin de mesurer l'efficacité du cryptosystème proposé dans une communication sécurisée infectée par le bruit, il est comparé à certains systèmes rapportés dans la littérature en prenant en considération plusieurs critères tels que les exposants de Lyapunov, la robustesse au bruit, les performances en termes de taux d'erreur binaire (BER : bit-error rate), les distorsions non linéaire (ND : nonlinear distortions) et le paramètre de disparité (PM : parameter mismatch). En effet, nous ne pouvions pas considérer tous les systèmes connus jusqu'à à présent, mais nous avons essayé de choisir des systèmes déjà devenus classiques, à savoir le masquage chaotique (CM : chaotic masking) [40], modulation par déplacement chaotique (CSK : chaotic shift keying) [41], la synchronisation complète(CS : complete synchronisation) [69], et certains systèmes plus proches de notre système tels que le CSK amélioré (iCSK : improved CSK) [70], la synchronisation adaptative (AS : adaptive synchronisation) [71] , et ICSS [60].

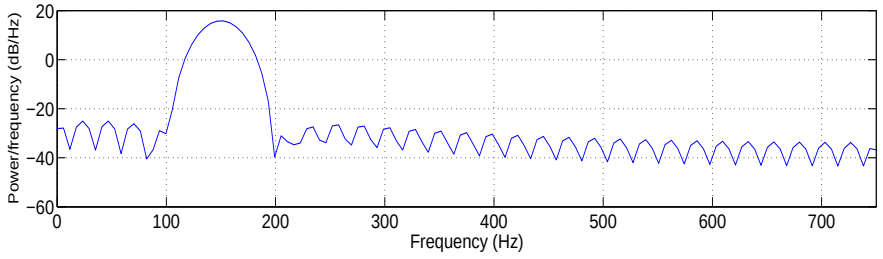


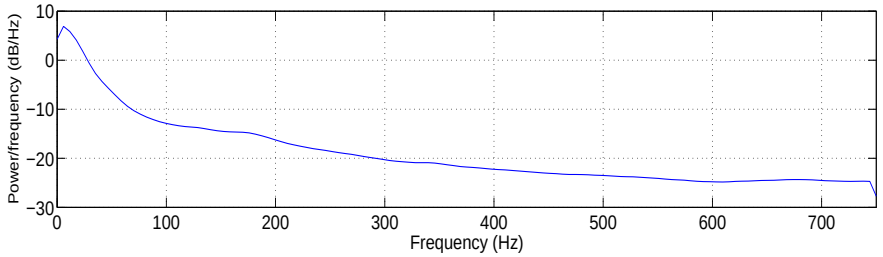


(a)



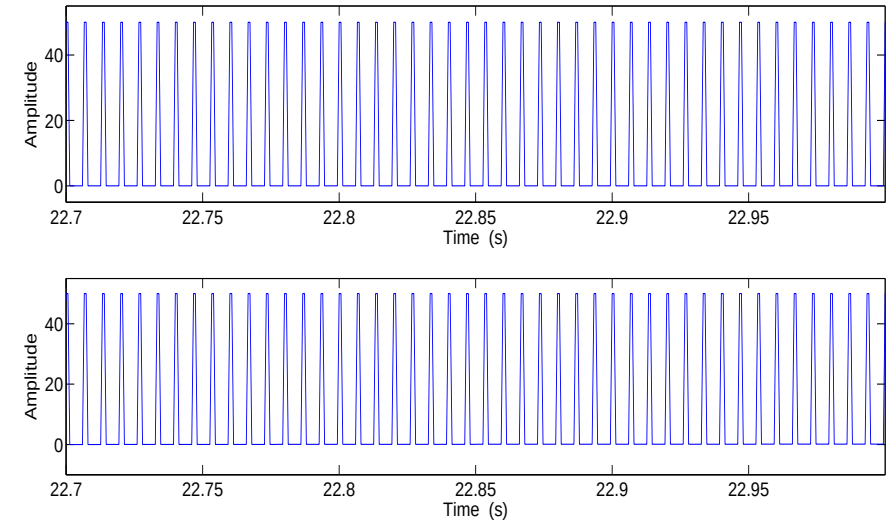
(b)



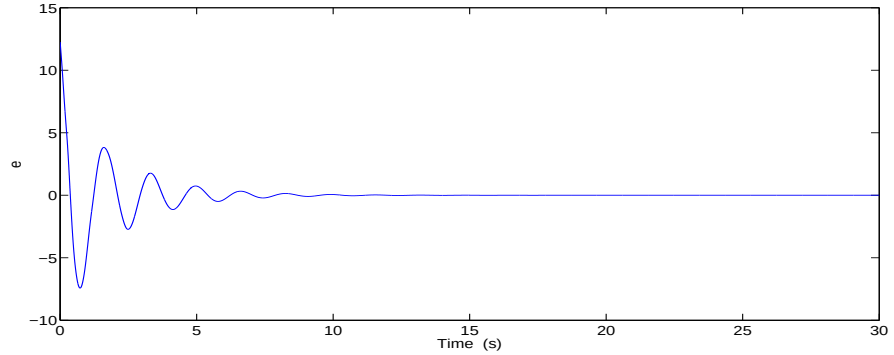


(c)

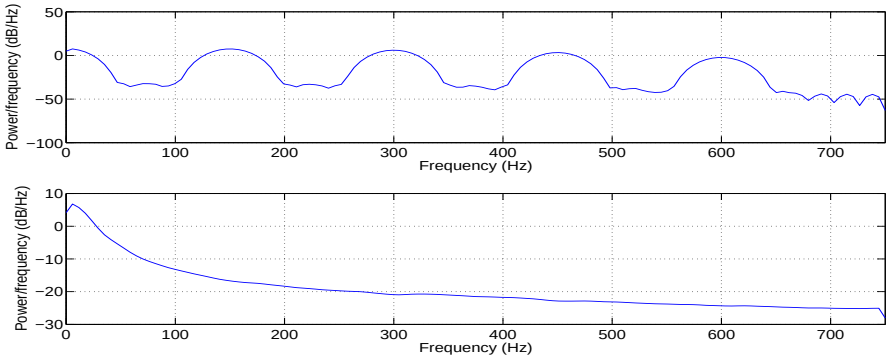
FIGURE 3.5: Communication chaotique robuste basée sur la synchronisation à couplage indirect. (a) Zoom du plain-message $m(t) = 50\sin(300\pi t)$ et du message récupéré ; (b) erreur de synchronisation entre l'émetteur et le récepteur ; et (c) densités spectrales de puissance du plain-message et du message transmis.



(a)

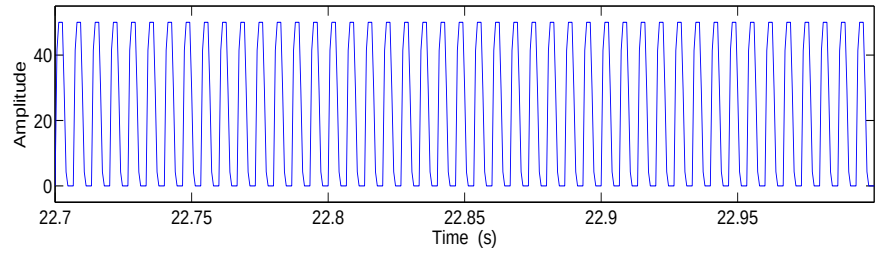


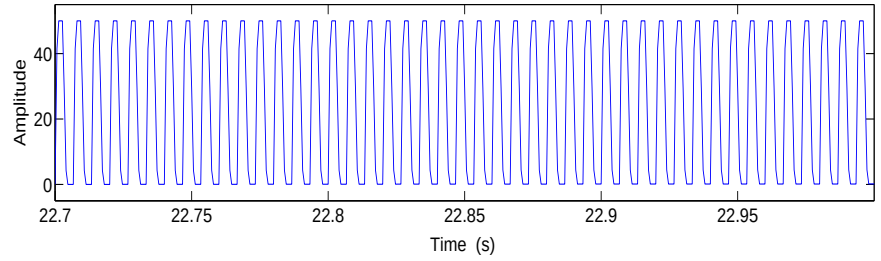
(b)



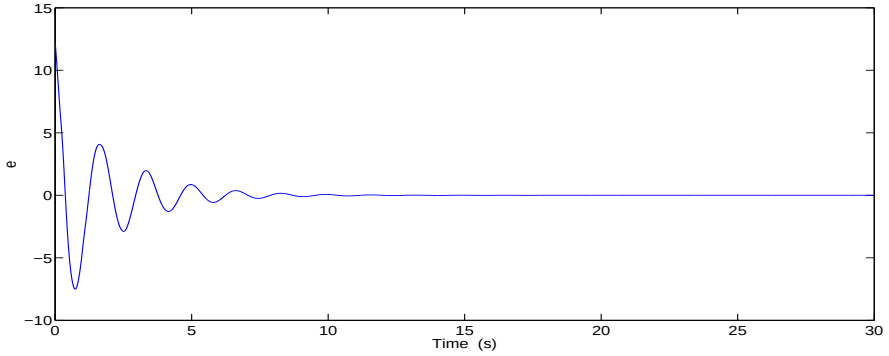
(c)

FIGURE 3.6: Communication chaotique robuste basée sur la synchronisation à couplage indirect. (a) Zoom du plain-message et du message récupéré pour un signal carré d'amplitude $A = 50$, fréquence $f = 150Hz$, et un rapport cyclique de 20%; (b) erreur de synchronisation entre l'émetteur et le récepteur ; et (c) densités spectrales de puissance du plain-message et du message transmis.

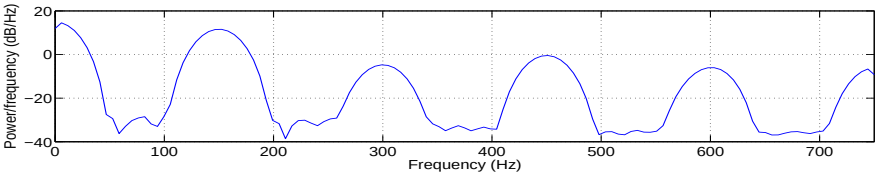


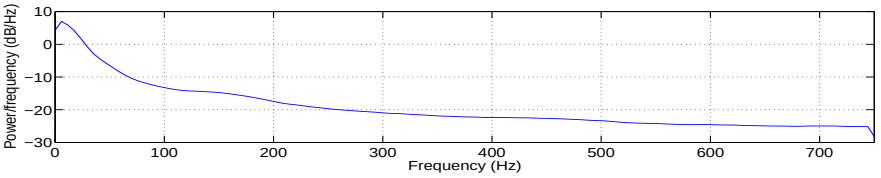


(a)



(b)





(c)

FIGURE 3.7: Communication chaotique robuste basée sur la synchronisation à couplage indirect. (a) Zoom du plain-message et du message récupéré pour un signal carré d'amplitude$A = 50$, fréquence $f = 150Hz$, et un temps de montée différent t_r et temps de descentet_f. Ici, $t_r = 2t_f = 1/(10f)$; (b) erreur de synchronisation entre l'émetteur et le récepteur ; et (c) densités spectrales de puissance du plain-message et du message transmis.

Paramètre α	Exposant de Lyapunov Positif
0	0.82
0.1	1.13
0.2	1.39
0.3	1.57
0.4	1.91
0.5	2.03
0.6	2.07
0.7	2.28
0.8	2.38
0.9	1.96
1.0	1.94

TABLE 3.1: Exposant de Lyapunov Positif pour le système chaotique unifié.

3.5.1 Exposant de Lyapunov

Les exposants de Lyapunov se réfèrent à des taux exponentiels moyens de divergence ou de convergence des trajectoires proches dans l'espace des phases. Pour déterminer le $i^{ème}$ exposant de Lyapunov, on devrait trouver la longue sensibilité dans le temps du flux $X(t)$ par rapport à la condition initiale $X(0)$ dans la direction $p_i(t)$, qui est donnée par

$$\lambda_i = \lim_{t\to\infty} \frac{1}{t} \ln \|p_i(t)\|, \tag{3.21}$$

où l'axe $p_i(t) = X(t)p_i(0)$ pour $i = 1, 2, \ldots, n$ et $p_i(0)$ désigne une base orthogonale de R^n. Il est à rappeler que plus les exposants positifs de Lyapunov de l'oscillateur chaotique sont plus élevés, plus il est imprédictible et par conséquent le système de communication basé sur cet oscillateur est plus sûr. C'est une condition nécessaire, mais non suffisante. Dans un travail récent, Carbajal-Gómez et al. [72] ont proposé un algorithme d'évolution différentielle pour optimiser l'exposant positif de Lyapunov dans un oscillateur chaotique multi-scroll sur la base de séries de fonctions non linéaires saturées. L'exposant de positif Lyapunov est optimisé de deux à neuf scrolls en balayant les différents coefficients de l'oscillateur chaotique. Dans ce travail, le calcul de l'exposant de Lyapunov est effectué en utilisant l'algorithme proposé dans [73] où le système chaotique unifié est décrit par un seul paramètre. Les résultats sont résumés dans le tableau 3.1. On peut voir que la plus grande valeur de l'exposant de Lyapunov positif peut être garantie lorsque $\alpha = 0.8$.

Système de communication sécurisé	Energie moyenne AE [dB]
CM	56.48
CSK	30.76
CS	39.52
iCSK	32.68
AS	22.13
ICSS	31.47
Notre système proposé	18.75

TABLE 3.2: Les valeurs de l'énergie moyenne pour les différents systèmes de communication chaotiques.

3.5.2 Robustesse au bruit

Pour quantifier la robustesse du système de communication proposé en présence du bruit, nous estimons l'énergie moyenne (AE : average energy) de l'impulsion chaotique par bit d'information transmis E_b par rapport à la densité spectrale de bruit N_0 donnée par [74] :

$$AE = \frac{E_b}{N_0} \text{ [dB]} \tag{3.22}$$

où l'énergie par bit E_b est donnée comme suit

$$E_b = P_{signal} \times T \tag{3.23}$$

pour lequel P_{signal} est la puissance de signal transmis sans bruit et (T) est le temps écoulé pour la transmission d'un bit d'information. D'autre part, la densité spectrale du bruit N_0 est définie par

$$N_0 = P_{noise}/\Delta f \tag{3.24}$$

pour lequel P_{noise} est la puissance du bruit dans le canal de communication et $\Delta f = f_u - f_l$, avec f_u et f_l sont les limites supérieure et inférieure de la fréquence du signal, respectivement.

Les valeurs de l'énergie moyenne pour les différents systèmes de communication sécurisés et pour notre système proposé sont présentées dans la Table .

A partir du tableau , on peut observer que notre système proposé présente une robustesse remarquable contre le bruit additif, même si l'intensité du bruit dépasse considérablement celle du signal émis.

3.5.3 Performances en termes du taux d'erreur binaire

Ensuite, nous considérons la dépendance du taux d'erreur binaire (BER : bit error rate) de la valeur moyenne d'énergie des systèmes de communication sécurisés précités. Le BER entre le message émis et le message reçu est calculé par l'équation suivante%

$$\mathrm{BER} = \frac{nombre\ de\ bits\ errones}{nombre\ total\ de\ bits} \times 100\% \tag{3.25}$$

Dans la Fig.3.8 nous évaluons numériquement les performances des schémas mentionnés en termes de BER en tant que fonction de l'énergie moyenne. La densité spectrale de puissance de bruit blanc dans le canal est $N_0/2$. Comme attendu, il ressort clairement que le système proposé est celui qui a la meilleure performance parmi eux. Il en est ainsi essentiellement parce que l'énergie par symbole est maintenue constante dans ce système. Il est à noter qu'aucune information concernant la dynamique du système chaotique n'est utilisée dans sa démodulation. Ces performances seraient pratiquement les mêmes dans le cas où des séquences aléatoires ont été utilisées au lieu de celles chaotiques.

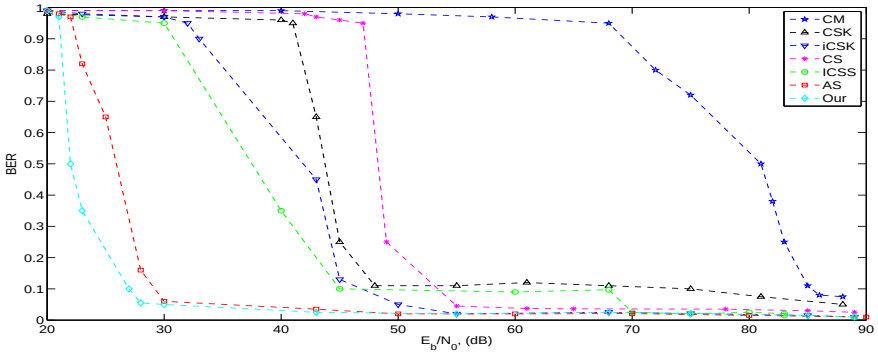


FIGURE 3.8: Performances BER pour différents systèmes de communication sécurisés.

3.5.4 Robustesse aux distorsions non linéaires et au paramètre de disparité

Les distorsions non linéaires (ND) caractérisent le niveau maximal de distorsions non linéaires pour lesquels un système de communication sécurisé reste efficace. Plus cette

Système de communication sécurisé	Distorsions Non-linéaires (ND) en dB	Paramètre de disparité (PM) in %
CM	1.03	0.3
CSK	23.3	2.0
CS	4.83	0.5
iCSK	18.6	0.1
AS	24.15	3.1
ICSS	8.49	0.6
Notre système proposé	10.52	2.3

TABLE 3.3: Robustesse aux distorsions non linéaires et au paramètre de disparité.

valeur est grande, plus le signal serait distordu, donc plus serait le niveau maximal des distorsions non linéaires jusqu'où les méthodes de transmission sécurisée de l'information resteraient efficaces [74]. Pour estimer l'influence des distorsions non-linéaires dans le canal de communication, la caractéristique quantitative suivante est introduite :

$$ND = 10\log_{10}\frac{P_x}{P_y}\ [\text{dB}] \tag{3.26}$$

où P_x et P_y sont les puissances des signaux $x(t)$ et $y(t)$, respectivement, telles que

$$P_x = \int_0^T x^2(t)dt, \quad P_y = \int_0^T y^2(t)dt \tag{3.27}$$

Une autre caractéristique importante pour évaluer un système de communication sécurisé est sa robustesse au paramètre de disparité (PM). Ceci est réalisé en remplaçant le paramètre α par $\alpha \pm \Delta\alpha$ dans l'un des générateurs identiques où $\Delta\alpha$ représente la valeur du PM.

Les résultats de l'influence des distorsions non linéaires et du paramètre de disparité dans le canal de communication sur l'efficacité des systèmes de communication sécurisés susmentionnés sont présentées dans le tableau 3.3. D'après les résultats obtenus, nous pouvons voir que notre système proposé reste efficace pour le niveau maximal des distorsions non linéaires correspondant à $ND = 10.52$ dB et qu'il est capable de fonctionner si les valeurs des paramètres de contrôle sont désaccordés jusqu'à $\Delta\alpha = 0.023$.

Il est nécessaire de mentionner que l'algorithme AS [71] possède une remarquable robustesse aux distorsions non linéaires et au paramètre de disparité. Cela est dû au fait que les systèmes hyperchaotiques possèdent des exposants de Lyapunov positifs plus élevés que les systèmes chaotiques.

3.6 Discussions

Dans la section précédente, nous avons analysé et comparé les performances de notre système de communication sécurisé proposé avec six autres systèmes de communication sécurisés. Pour expliquer ces performances, nous devrions se référer aux discussions suivantes. Comme il a été mentionné ci-dessus, la plupart des systèmes de communication sécurisés dans le tableau 3.5.2 sont basées sur le concept de la synchronisation complète des oscillateurs chaotiques, ce qui nécessite des générateurs chaotiques identiques à l'émission et à la réception. Dans ce cas, les paramètres utilisés dans l'émetteur peuvent être estimés à partir du signal d'émission et par conséquent, le signal d'information peut être extrait facilement. Nous notons que le système ICSS, ainsi que le notre, sont basés sur le concept de la synchronisation généralisée pour la création du signal composé qui sera transmis par le canal de communication, et ne nécessitent pas des générateurs chaotiques identiques aux deux extrimités du canal de communication. Autre caractéristique importante est que le générateur des clés n'est pas semblable à lui-même avec n'importe quelle quantité de décalage de temps, car il est généré à l'aide des générateurs chaotiques, et, par conséquent, il est dans la nature chaotique. Par conséquent, même si le signal crypté est connu, l'extraction du message ne sera pas possible sans la connaissance de la séquence clé. De plus, nous avons établi et prouvé un théorème, qui résume les propriétés du système de communication chaotique proposé. Les résultats théoriques montrent que l'émetteur et le récepteur se synchronisent de manière exponentielle l'un avec l'autre. De même, le générateur de clés au niveau du récepteur converge de façon exponentielle vers le générateur de clé dans l'émetteur. L'examen des résultats de simulations numériques montre que, avec une augmentation de l'amplitude de plain-message, notre méthode proposée préserve encore la récupération de plain-message, et elle est plus robuste contre le bruit de canal, par contre le système ICSS est fortement affecté. A partir des différents résultats, on a montré que les messages de texte en clair sont récupérés avec succès par le récepteur en utilisant un canal bruité avec un rapport signal sur bruit SNR de 40 dB. Avant de poursuivre les discussions sur les résultats obtenus, nous constatons que le système de communication sécurisé proposé peut être étendu aux systèmes de communication numériques. Par exemple, quand la modulation d'amplitude d'impulsion (pulse-amplitude modulation) est utilisée pour transmettre des bits numériques, alors, après avoir récupéré le signal modulé corrompu, on peut facilement le faire passer à travers un filtre adapté, puis un détecteur de seuil est inséré pour récupérer les bits numériques avec précision.

Il faut cependant garder à l'esprit, que dans de nombreuses applications, il est peut être plus approprié de caractériser les performances d'un système de communication par la dépendance du BER sur le SNR. Les résultats de simulation montrent également que

notre système pourrait réaliser un BER réussi. Evidemment, notre analyse de BER a révélé qu'il devient rapidement égal à 1 pour les différents systèmes de communication sécurisés, à l'exception du schéma AS et de notre approche. Il est à signaler que notre système est plus performant que le schéma AS de 5 à 6 dB.

D'autres aspects essentiels pour les systèmes de communications sécurisés sont leur robustesse aux distorsions non linéaires (ND) et le paramètre de disparité (PM). Nous avons vu que, pour atteindre plus de robustesse, des valeurs élevées de ND et PM sont nécessaires. Il ya, cependant, un autre point à discuter dans le cadre de ces deux caractéristiques. Il est nécessaire de souligner que les caractéristiques quantitatives de l'efficacité de notre système sont obtenues pour les systèmes chaotiques à couplage indirect et à distribution gaussienne du bruit dans le canal de communication. Nous notons que l'utilisation des systèmes hyperchaotiques possédant des exposants de Lyapunov positifs plus élevés que les systèmes chaotiques devrait entraîner des variations meilleures des caractéristiques considérées.

3.7 Conclusion

Dans ce chapitre, nous avons proposé une conception flexible pour un système de cryptage chaotique fondé sur un schéma de synchronisation à couplage indirect où les signaux cryptés sont de forte puissance. Puisque le système de chiffrement est conçu en utilisant la synchronisation émetteur-récepteur chaotique, les gains sont obtenus en résolvant un contrôleur basé-observateur. De plus, nous avons montré que la synchronisation des systèmes chaotiques est possible par l'intermédiaire d'une seule entrée de contrôle en mesurant une seule variable. Notre loi de commande est une rétroaction proportionnelle simple qui est activé après un certain laps de temps. Par rapport à certains systèmes de communication sécurisée, ce schéma proposé offre un niveau de sécurité plus élevé, conserve la récupération du message clair, et montre la robustesse contre le bruit additif. Par ailleurs, il ne nécessite pas une identité des générateurs chaotiques des deux extrémités de la voie de communication en raison de l'utilisation du concept de synchronisation généralisée au lieu de la synchronisation complète. Par conséquent, il est assez simple pour une réalisation pratique. Enfin, les simulations numériques confirment les résultats théoriques.

Dans les travaux futurs, nous envisageons de traiter le problème de la synchronisation à couplage indirect en utilisant des systèmes hyperchaotiques.

Chapitre 4

Controle et synchronisation des systèmes chaotiques et hyperchaotiques

Ce chapitre présente la conception basée sur un modèle flou pour le contrôle et la synchronisation des systèmes chaotiques et hyperchaotiques. Dans ce contexte, les systèmes chaotiques et hyperchaotiques sont exactement reproduits sur la base d'un modèle flou de Takagi-Sugeno (TS). Ensuite, en utilisant la méthode prédictive, les côntroleurs flous pour le contrôle et la synchronisation sont conçus et quelques critères nouveaux et utiles sont dérivées. Enfin, des simulations numériques sont présentées pour illustrer l'efficacité et la faisabilité des résultats théoriques.

4.1 Introduction

Le chaos, comme phénomène non linéaire très intéressant, a été largement étudié en sciences et en ingénierie. Des chercheurs ont récemment démontré que le chaos peut s'avérer utile dans des applications pratiques telles que les lasers, la biologie, l'économie, les réactions chimiques et les communications sécurisées. Toutefois, pour tirer pleinement parti du chaos, il convient de le contrôler. Plusieurs stratégies visant à contrôler le chaos ont été proposées et étudiées avec l'objectif de stabilisation des points d'équilibre ou orbites périodiques intégrés dans des attracteurs chaotiques. Il est à noter que la

stabilisation des points d'équilibre instables est principalement utilisée dans les applications d'ingénierie, qui présente de nombreux avantages comme la la stabilité garantie et robuste, la poursuite précise de cible, et une forte capacité de rejet du bruit. Par exemple, l'équilibre stable peut être utile pour faire des prédictions.

L'extrême sensibilité aux conditions initiales est la principale caractéristique du comportement chaotique. Cela signifie que deux trajectoires qui sont initialisées très proches l'une de l'autre se séparent (divergent) de façon exponentielle dans le temps. En raison de ce comportement type, connu sous l'appellation «effet papillon», le temps de prédiction à long terme d'une trajectoire chaotique sur la base de mesures à précision finie est impossible. Cependant, cette caractéristique implique également qu'une trajectoire chaotique est extrêmement sensible à l'effet des perturbations. Juste une petite perturbation appliquée à un moment donné est suffisante pour changer l'évolution future de la trajectoire et de diriger sa route vers d'autres régions de l'ensemble invariant chaotique [75]. Autre caractéristique essentielle du système chaotique est qu'il contient une orbite dense sur l'ensemble invariant qui est une trajectoire chaotique qui passe de manière récurrente infiniment proche à n'importe quel point de cet ensemble. Une troisième caractéristique est que l'ensemble invariant chaotique contient un nombre infini d'orbites périodiques instables de toutes les périodes, qui coexistent avec le mouvement chaotique. Ces orbites sont instables au sens où un petit écart par rapport à l'orbite périodique croît rapidement et exponentiellement dans le temps, et le système se déplace rapidement de l'orbite périodique vers une trajectoire chaotique. La combinaison de ces trois caractéristiques rend les systèmes chaotiques comme l'un des systèmes les plus flexibles qui peuvent être trouvés dans la nature. C'est précisément ces caractéristiques qui sont exploitées pour le contrôle du chaos.

Depuis les travaux pionniers de Ott, Grebogi et York [22], le contrôle du chaos a émergé comme un nouveau sujet très intéressant à étudier, et de nombreuses théories et méthodes ont été développées, telles que la méthode de rétroaction à délai [76], la méthode de commande adaptative [77, 78], la méthode de rétroaction proportionnelle occasionnelle [79], la méthode de contrôle impulsif [80], la méthode d'ordre supérieur [81], la méthode de commande prédictive [82, 83], le contrôle généralisé par l'approche non linéaire d'ordre supérieur [84], etc. Parmi celles-ci, la commande prédictive est particulièrement intéressante en raison de sa simplicité de configuration et de mise en œuvre. En raison de ses avantages, la commande prédictive a été appliquée avec succès à la stabilisation de divers systèmes chaotiques [85–87] et à la synchronisation des systèmes chaotiques satellites [44]. De tous les résultats obtenus, la stabilisation et la synchronisation des systèmes chaotiques sont réalisées avec des performances très satisfaisantes.

D'autre part, il existe en fait une large littérature démontrant la possibilité de modélisation, de contrôle et de synchronisation des systèmes chaotiques à l'aide des modèles flous et de quelques méthodes et techniques efficaces de commande floue. Tanaka et al. ont étudié la commande floue et la synchronisation des systèmes chaotiques sur la base du modèle flou de Takagi-Sugeno (TS) et des inégalités matricielles linéaires (LMI) [88]. Des versions similaires ont été proposées pour le contrôle et la synchronisation des systèmes chaotiques d'ordre élevé et des systèmes chaotiques avec incertitudes sur les paramètres [89–92]. Wang et al. ont étudié la synchronisation asymptotique des systèmes chaotiques basée sur le modèle flou TS et le contrôle impulsif [93]. Hu et al. ont étudié la stabilité asymptotique uniforme et la synchronisation des systèmes chaotiques basés sur le modèle flou TS et une approche de contrôle impulsif général [94]. Boukabou et al. ont étudié la stabilité asymptotique des systèmes chaotiques discrets inconnus et incertains basés sur les contrôleurs TS flou prédictifs [95–97]. Toutefois, le contrôle et la synchronisation des systèmes chaotiques basés sur le modèle flou TS et la commande prédictive n'ont pas été antérieurement étudiés dans la littérature.

Motivés par ces discussions, nous nous intéressons dans ce chapitre au contrôle et à la synchronisation des systèmes chaotiques et hyperchaotiques représentés par le modèle flou TS en utilisant la méthode de commande prédictive. La principale contribution du présent chapitre réside dans trois aspects. Tout d'abord, les systèmes chaotiques et hyperchaotiques sont exactement représentés par le modèle flou TS. Deuxièmement, de nouveaux critères de contrôle prédictif flous sont proposés pour le contrôle et la synchronisation du modèle flou TS obtenu. Troisièmement, les simulations numériques sont présentés pour vérifier les résultats. Afin de démontrer l'efficacité de l'approche proposée, l'une des principales contributions de cet article est de présenter les résultats numériques sur les systèmes chaotiques de haute dimension pour traiter le problème de la transmission de l'information, en présence des bruits extérnes.

Le reste du chapitre est organisé comme suit : Dans la section 2, le concept de la commande prédictive est présenté. La section 3 introduit le modèle flou TS, la commande floue et la synchronisation floue en se basant sur la méthode de commande prédictive. La stabilité et la synchronisation des systèmes de Lorenz et de Rössler sont décrits dans la section 4. Des simulations numériques sont effectuées pour démontrer les résultats théoriques. Enfin, des conclusions sont données dans la section 5.

4.2 Aperçu sur la méthode de commande prédictive

Soit le système chaotique donné par l'équation différentielle ordinaire suivante

$$\dot{X}(t) = f(X(t)), \tag{4.1}$$

où X est le vecteur d'état, et f est une fonction non linéaire. Nous supposons que le système chaotique admet un point d'équilibre instable X_f.

La façon la plus simple pour formuler la loi de commande prédictive est de faire usage du fait que les dynamiques de tout système non linéaire lisse sont approximativement linéaires dans un petit voisinage du point d'équilibre X_f. Ainsi, par linéarisation du système (4.1) autour de X_f, on obtient

$$\delta\dot{X}(t) = A\delta X(t), \tag{4.2}$$

où $\delta\dot{X}(t) = \dot{X}(t) - X_f$, $\delta X(t) = X(t) - X_f$, and $A = \partial f/\partial X$ est la matrice jacobienne évaluée au point d'équilibre X_f avec au moins une valeur propre positive.

Afin de stabiliser le système chaotique (4.1) sur son point d'équilibre instable X_f, l'entrée de commande $u(t)$ est ajoutée comme suit

$$\dot{X}(t) = f(X(t)) + \mu(t). \tag{4.3}$$

L'entrée de commande $\mu(t)$ se compose de la différence entre l'état incontrôlée prédite et l' état contrôlé actuel, multipliée par le gain K. Le système chaotique contrôlé (4.3) peut se réécrire en

$$\dot{X}(t) = f(X(t)) + K(AX(t) - X(t)), \tag{4.4}$$

où K sera déterminée bientôt.

La linéarisation du système chaotique contrôlé (4.4) donne

$$\delta\dot{X}(t) = [A + K(A - I)]\,\delta X(t), \tag{4.5}$$

où I est la matrice identité.

Lemma 4.1. *L'équilibre du système chaotique (4.3) avec contrôle prédictif $\mu(t)$ est asymptotiquement stable s'il existe un gain de rétroaction K tel que [95].*

$$|A + K(A - I)| < I. \tag{4.6}$$

Remark 4.2. Le gain K existe si et seulement si $\det(A - I) \neq 0$. Le voisinage du point d'équilibre instable est déterminé par $|X(t) - X(t-1)| < \varepsilon$ pour un petit nombre positif ε.

4.3 Systèmes de contrôle et de synchronisation prédictifs flous

Dans cette section, nous introduisons la conception basée sur un modèle flou pour stabiliser et synchroniser les systèmes chaotiques et hyperchaotiques. Le point clé est de choisir des gains de commande floue qui garantissent que la trajectoire chaotique converge vers une cible désirée. Cette stratégie garantit que le système chaotique entre dans le domaine attrayant rapidement, réduit le temps de convergence et conduit à une entrée de contrôle pratique.

Pour le système chaotique (4.1), la modélisation floue TS se compose d'un ensemble de règles si-alors (IF-THEN). Le $i^{ème}$ plant du modèle flou est donné par

$$\begin{aligned} R^i: \quad & \text{IF} \quad z_1(t) \text{ is } M_{i1} \text{ and} \ldots \text{and } z_p(t) \text{ is } M_{ip} \\ & \text{THEN} \quad \dot{X}(t) = A_i X(t) + b_i, \quad i = 1, \ldots, r, \end{aligned} \tag{4.7}$$

où R^i $(i = 1, \ldots, r)$ désigne la $i^{ème}$ règle floue, r est le nombre de règles floues, $z_1(t), ..., z_p(t)$ sont les variables de prémisse qui consistent en des états du système, $M_{ij}(j = 1, \ldots, p)$ sont les ensembles flous, et A_i, b_i sont des matrices de système avec des dimensions appropriées.

En utilisant le fuzzifier, la sortie finale du modèle flou chaotique TS est inférée comme suit

$$\dot{X}(t) = \sum_{i=1}^{r} h_i(z(t)) \{A_i X(t) + b_i\}, \tag{4.8}$$

où $z(t) = [z_1(t), z_2(t), ..., z_p(t)]$, et

$$h_i\left(z(t)\right) = \frac{w_i\left(z(t)\right)}{\sum_{l=1}^{r} w_l\left(z(t)\right)}, \text{ avec } w_i\left(z(t)\right) = \prod_{j=1}^{p} M_{ij}\left(z_j(t)\right),$$

pour tout t, où $M_{ij}\left(z_j(t)\right)$ désigne le degré d'appartenance de $z_j(t)$ dans M_{ij}. $h_i\left(z(t)\right)$ sont considérés comme le poids normalisé des règles IF-THEN, qui satisfont $\sum_{i=1}^{r} h_i\left(z\left(t\right)\right) = 1$ et $0 \leq h_i\left(z\left(t\right)\right) \leq 1$ pour tout $t \in \mathbb{R}^+$.

Pour contrôler le système chaotique (4.3), nous introduisons le modèle de commande floue TS comme suit :

$$\begin{array}{lll} R^i: & \text{IF} & z_1(t) \text{ is } M_{i1} \text{ and} \ldots \text{and } z_p(t) \text{ is } M_{ip} \\ & \text{THEN} & \dot{X}\left(t\right) = A_i X\left(t\right) + b_i + \mu_i(t), \quad i = 1, \ldots, r, \end{array} \tag{4.9}$$

où r, A_i, b_i, $z_i(t)$ et M_{ij} sont définis dans (4.7) et $\mu_i(t)$ désigne l'entrée de contrôle.

De même que pour (4.7), la sortie finale du système de contrôle flou TS (4.9) est inférée par

$$\dot{X}\left(t\right) = \sum_{i=1}^{r} h_i\left(z\left(t\right)\right)\left\{A_i X\left(t\right) + b_i + \mu_i(t)\right\}. \tag{4.10}$$

où $h_i\left(z\left(t\right)\right)$ est défini dans (4.3).

Pour poursuivre l'étude, le résultat suivant est nécessaire

Lemma 4.3. *L'équilibre du système de contrôle flou TS (4.9) avec $\mu(t)$ est globalement asymptotiquement stable si [88].*

$$A_i^T P + P A_i < 0, \quad i = 1, \ldots, r, \tag{4.11}$$

où P est une matrice commune.

4.3.1 Système de contrôle prédictif flou

L'objectif du contrôle est de stabiliser le modèle flou chaotique sur les différents points d'équilibre instable. Le modèle flou chaotique sous la loi de contrôle est de la forme

$$\dot{X}\left(t\right) = \sum_{i=1}^{r} h_i\left(z\left(t\right)\right)\left\{A_i X\left(t\right) + b_i + \mu_i^c(t)\right\}. \tag{4.12}$$

Se basant sur le concept du contrôle prédictif, nous concevons le côntroleur prédictif flou suivant pour le processus de stabilisation.

$$\mu_i^c(t) = K_i^c \left[A_i X\left(t\right) - X\left(t\right)\right], \quad i = 1, \ldots, r, \tag{4.13}$$

où K_i^c sont les matrices des gains de contrôle local à concevoir.

En substituant l'équation (4.13) dans l'équation (4.12), on obtient le modèle flou TS contrôlé suivant

$$\begin{aligned} \dot{X}\left(t\right) &= \sum_{i=1}^{r} h_i\left(z\left(t\right)\right)\left\{A_i X\left(t\right) + b_i + K_i^c\left[A_i X\left(t\right) - X\left(t\right)\right]\right\}, \\ &= \sum_{i=1}^{r} h_i\left(z\left(t\right)\right)\left\{\left[A_i + K_i^c\left(A_i - I\right)\right] X\left(t\right) + b_i\right\}. \end{aligned} \tag{4.14}$$

Des lemme 4.1 et lemme 4.3, on obtient le lemme suivant :

Lemma 4.4. *L'équilibre du système de contrôle flou TS (4.14) est globalement asymptotiquement stable si la condition suivante est vérifée*

$$F_i^T P + P F_i < 0, \quad i = 1, \ldots, r, \tag{4.15}$$

où $F_i = A_i + K_i^c\left(A_i - I\right)$.

Remark 4.5. Le contrôleur flou basé sur un modèle, utilisant le modèle flou TS, emploie la notion de compensation distribuée parallèle. La stabilité du système de commande à logique floue est garantie par une matrice symétrique positive commune, qui satisfait les inégalités matricielles linéaires (LMI). Puisque le modèle flou de Takagi-Sugeno décrit le système chaotique avec une précision approchée satisfaisante sur une vaste région, la loi de contrôle basée sur un modèle flou fait le domaine d'attraction plus large qu'elle ne l'est avec LQR (Linear-quadratic regulator).

Remark 4.6. Il est intéressant de noter que l'approche de commande prédictive floue proposée peut stabiliser les points d'équilibre instables des systèmes chaotiques et hyperchaotiques bien connus tels que de Duffing, de Lorenz, de Rössler et bien d'autres, appelées oscillateurs auto-excités. Dans ces attracteurs, en partant d'un point de collecteurinstable dans un petit voisinage d'équilibre instable, la trajectoire atteint un attracteur

après un processus transitoire. Au cours des dernières années, un autre type d'oscillations périodiques et chaotiques, appelées oscillations cachées et attracteurs cachés a été découverts [98–100]. Dans ces attracteurs, les bassins d'attraction ne se croisent pas avec des petits voisinages d'équilibres. Les attracteurs cachés sont des attracteurs chaotiques sans aucun point d'équilibre ou avec des équilibres stables seulement. Ainsi, les systèmes chaotiques n'affichent pas nécessairement un point d'équilibre instable coexistant.

4.3.2 Schéma de synchronisation prédictive floue

L'idée de synchronisation du chaos consiste à conduire la trajectoire d'un système chaotique (esclave) vers la trajectoire d'un autre système chaotique (maître), peu importe la façon dont les deux systèmes sont initialisées.

Nous considérons que le modèle flou TS (4.3) comme système maître, et nous définissons le modèle flou TS suivant en tant que système esclave

$$\begin{array}{lll} R^i: & \text{IF} & z_1(t) \text{ is } M_{i1} \text{ and} \ldots \text{and } z_p(t) \text{ is } M_{ip} \\ & \text{THEN} & \dot{Y}(t) = A_i Y(t) + b_i, \quad i = 1, \ldots, r, \end{array} \tag{4.16}$$

La sortie finale du système esclave est inférée comme suit

$$\dot{Y}(t) = \sum_{i=1}^{r} h_i(z(t)) \{A_i Y(t) + b_i\}. \tag{4.17}$$

On définit également l'erreur de synchronisation $E(t) = Y(t) - X(t)$. Alors, la dynamique de l'erreur de synchronisation est donnée par

$$\dot{E}(t) = \dot{Y}(t) - \dot{X}(t) = \sum_{i=1}^{r} h_i(z(t)) \{A_i E(t)\}. \tag{4.18}$$

Bien entendu, le problème de synchronisation est converti en problème de stabilité pour la solution zéro du système (4.18). Le but de la synchronisation est de stabiliser l'erreur dynamique (4.18) sur l'origine lorsque $t \to \infty$. Ainsi, l'erreur du système flou TS (4.18) est sous la loi de contrôle prédictif

$$\dot{E}(t) = \sum_{i=1}^{r} h_i(z(t)) \{A_i E(t) + \mu_i^s(t).\} \tag{4.19}$$

Pour la synchronisation, nous concevons la commande prédictive floue suivante

$$\mu_i^s(t) = K_i^s \left[A_i E\left(t\right) - E\left(t\right)\right]. \tag{4.20}$$

En insérant l'équation (4.20) dans l'équation. (4.19), on obtient

$$\dot{E}\left(t\right) = \sum_{i=1}^{r} h_i\left(z\left(t\right)\right) \left\{\left[A_i + K_i^s\left(A_i - I\right)\right] E\left(t\right)\right\}. \tag{4.21}$$

où les gains de synchronisation K_i^s $(i = 1, \ldots, r)$ sont à déterminer.

Lemma 4.7. *L'équilibre du système de contrôle flou TS (4.19) est globalement asymptotiquement stable si la condition suivante est vérifiée*

$$G_i^T P + P G_i < 0, \quad i = 1, \ldots, r, \tag{4.22}$$

où $G_i = A_i + K_i^s\left(A_i - I\right)$.

Remark 4.8. Dans le lemme 4.7, le schéma de synchronisation maître - esclave peut être considéré comme à couplage unidirectionnel. De toute évidence, pour les systèmes chaotiques à couplage bidirectionnel, la même forme de la loi de couplage dynamique peut également stabiliser l'état synchronisé.

Remark 4.9. Le contrôle flou TS proposé appliqué à la synchronisation des oscillateurs couplés consiste à des résultats adaptés empruntés à la commande robuste et à la théorie des observateurs. Cependant, alors que les travaux antérieurs sont adaptés pour les systèmes linéaires par morceaux, la méthode proposée ici est beaucoup plus générale, car elle est basée sur la modélisation floue TS. Un autre aspect qui distingue la méthode proposée des autres schémas de synchronisation se reposant aussi sur la modélisation TS floue et les LMIs est la souplesse imposée sur les conditions LMI.

Remark 4.10. Les solutions obtenues en termes de gains de commande pour la stabilisation et la synchronisation peuvent être formulées comme des problèmes d'optimisation LMIs de (4.15) and (4.22), et ils sont résolus en utilisant une technique d'optimisation basée sur le calcul évolutif [88, 89, 95].

Remark 4.11. Il est à noter que les contrôleurs conçus dans ce chapitre sont valables non seulement pour les systèmes chaotiques, mais aussi pour les systèmes hyperchaotiques.

Les systèmes hyperchaotiques sont pris en considération ici parce qu'ils sont plus difficiles que les systèmes chaotiques.

4.4 Résultats de simulation

Dans cette section, nous allons donner les résultats des simulations pour le contrôle et la synchronisation des systèmes chaotiques basés sur les modèles flous TS. Les mêmes procédures sont appliqués aux systèmes de Lorenz et de Rössler. Par ailleurs, les systèmes hyperchaotiques de Lorenz sont étudiés pour illustrer l'efficacité et la faisabilité des résultats théoriques, et aussi pour considérer l'effet des bruits externes.

4.4.1 Système chaotique de Lorenz

Le système de Lorenz est donné par les équations différentielles suivantes

$$\begin{cases} \dot{x}_1 = a(x_2 - x_1), \\ \dot{x}_2 = (b - x_3)x_1 - x_2, \\ \dot{x}_3 = x_1 x_2 - cx_3, \end{cases} \tag{4.23}$$

Ici, les paramètres $a, b,$ and c prennent les valeurs $a = 10$, $b = 28$, $c = 8/3$, ce qui correspond à un comportement chaotique. Le système d'équations différentielles (4.23) possède trois points d'équilibre $E_0(0, 0, 0)$, $E_1(8.485, 8.485, 27)$, et $E_{-1}(-8.485, -8.485, 27)$. Le système de Lorenz est représenté exactement par le modèle flou TS avec les deux règles floues IF-THEN suivantes

$$\begin{aligned} R^1: &\quad \text{IF } x_1(t) \text{ is } M_1 \text{ THEN } \dot{X}(t) = A_1 X(t) + b_1, \\ R^2: &\quad \text{IF } x_1(t) \text{ is } M_2 \text{ THEN } \dot{X}(t) = A_2 X(t) + b_2, \end{aligned} \tag{4.24}$$

où x_1 est la variable de prémisse avec $x_1 \in [-d,\ d]$ and $d > 0$.

Ici, $A_1 = \begin{bmatrix} -a & a & 0 \\ b & -1 & -d \\ 0 & d & -c \end{bmatrix}$, $A_2 = \begin{bmatrix} -a & a & 0 \\ b & -1 & d \\ 0 & -d & -c \end{bmatrix}$, $b_1 = b_2 = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$, $M_1 = \frac{1}{2}(1 + x_1/d)$, $M_2 = \frac{1}{2}(1 - x_1/d)$, $d = 30$. La sortie finale du modèle flou Lorenz TS est inférée comme suit :

$$\dot{X}(t) = \sum_{i=1}^{2} M_i(x_1) \{A_i X(t)\}, \tag{4.25}$$

La Fig.4.1 montre le modèle flou TS du système chaotique de Lorenz.

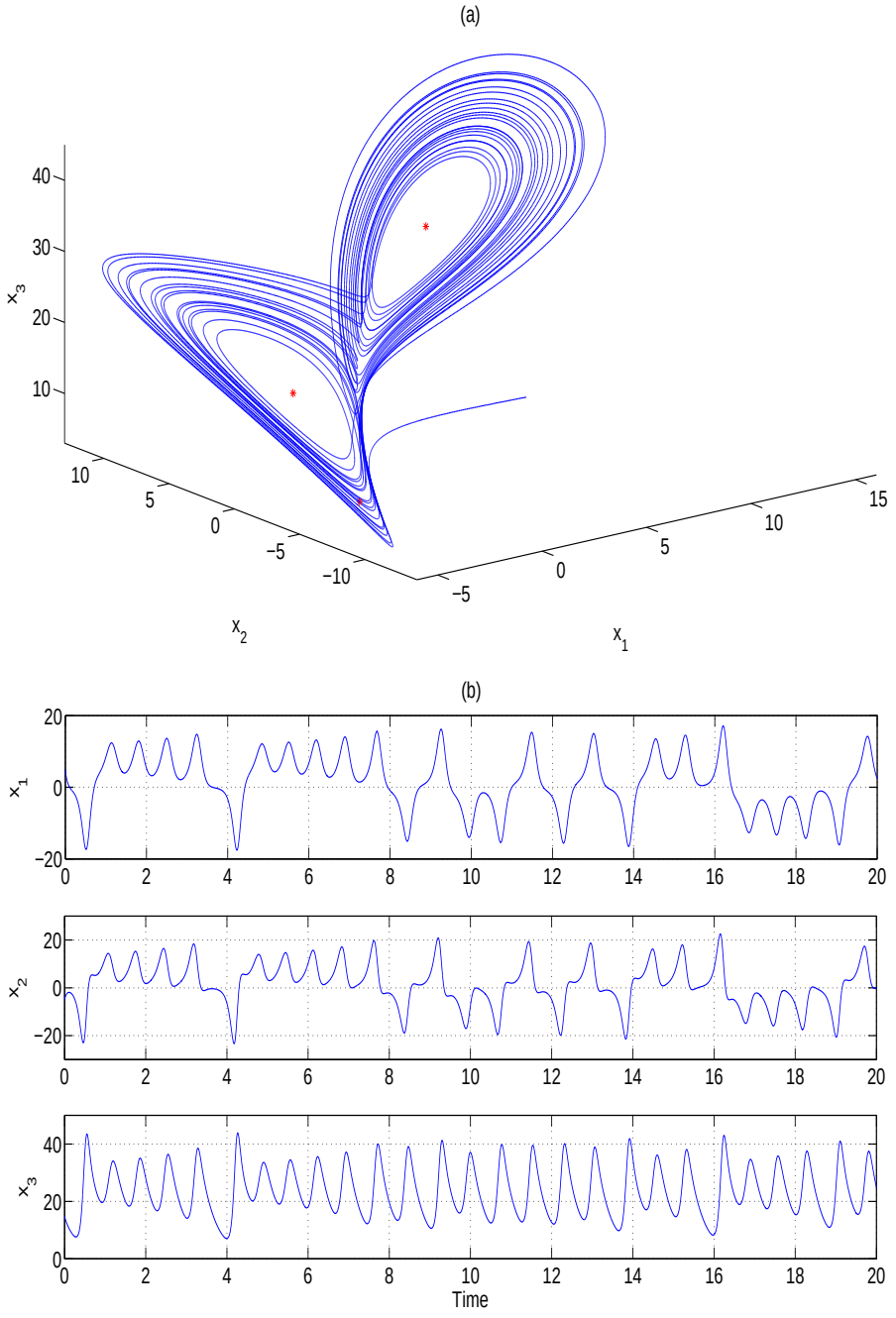


FIGURE 4.1: Le modèle T-S flou de Lorenz . (a) l'espace de phase ; (b) l'evolution des variables d'état.

Une fois le modèle flou TS du système de Lorenz est obtenu, nous pouvons appliquer les lois de contrôle flou prédictif (4.13) et (4.20) pour les processus de contrôle et de synchronisation, respectivement.

Tout d'abord, nous considérons la commande prédictive du modèle flou TS de Lorenz. Les gains de contrôle K_i^c $(i = 1, 2)$ sont choisis pour le point d'équilibre E_0 tel que

$$\begin{aligned} K_1^c &= \begin{bmatrix} -1.007 & 0.011 & -0.058 \\ 0.030 & -1.113 & -0.064 \\ 0.162 & 0.064 & -1.200 \end{bmatrix}, \\ K_2^c &= \begin{bmatrix} -1.007 & 0.011 & 0.058 \\ 0.030 & -1.113 & 0.064 \\ -0.162 & -0.064 & -1.200 \end{bmatrix}, \end{aligned} \tag{4.26}$$

et pour les points d'équilibre E_{-1}, E_1 tels que

$$\begin{aligned} K_1^c &= \begin{bmatrix} -0.892 & 0.011 & -0.058 \\ 0.030 & -0.998 & -0.064 \\ 0.162 & 0.064 & -1.085 \end{bmatrix}, \\ K_2^c &= \begin{bmatrix} -0.892 & 0.011 & 0.058 \\ 0.030 & -0.998 & 0.064 \\ -0.162 & -0.064 & -1.085 \end{bmatrix}, \end{aligned} \tag{4.27}$$

Les résultats de simulation pour stabiliser les différents points d'équilibre sont présentés dans la Fig.4.2.

Il est observé à partir des Figs.4.2 (a)-(c) que le modèle TS flou de Lorenz (4.25) est asymptotiquement stabilisée sur le point d'équilibre instable désirée selon le gain de contrôle de rétroaction appliqué K_i^c $(i = 1, 2)$.

En deuxième lieu, nous considérons la synchronisation entre deux systèmes flous de Lorenz. Les conditions initiales pour les systèmes maître et esclave sont$X(0) = (-10, -10, 10)^T$, $Y(0) = (10, 10, -10)^T$. Les gains de synchronisation K_i^s $(i = 1, 2)$ sont comme suit

$$\begin{aligned} K_1^s &= \begin{bmatrix} 9.801 & 0.222 & -3.723 \\ 0.801 & -0.777 & -3.723 \\ 10.044 & 3.523 & -4.360 \end{bmatrix}, \\ K_2^s &= \begin{bmatrix} 9.801 & 0.222 & 3.523 \\ 0.801 & -0.777 & 3.523 \\ -10.044 & -3.523 & -4.360 \end{bmatrix}. \end{aligned} \tag{4.28}$$

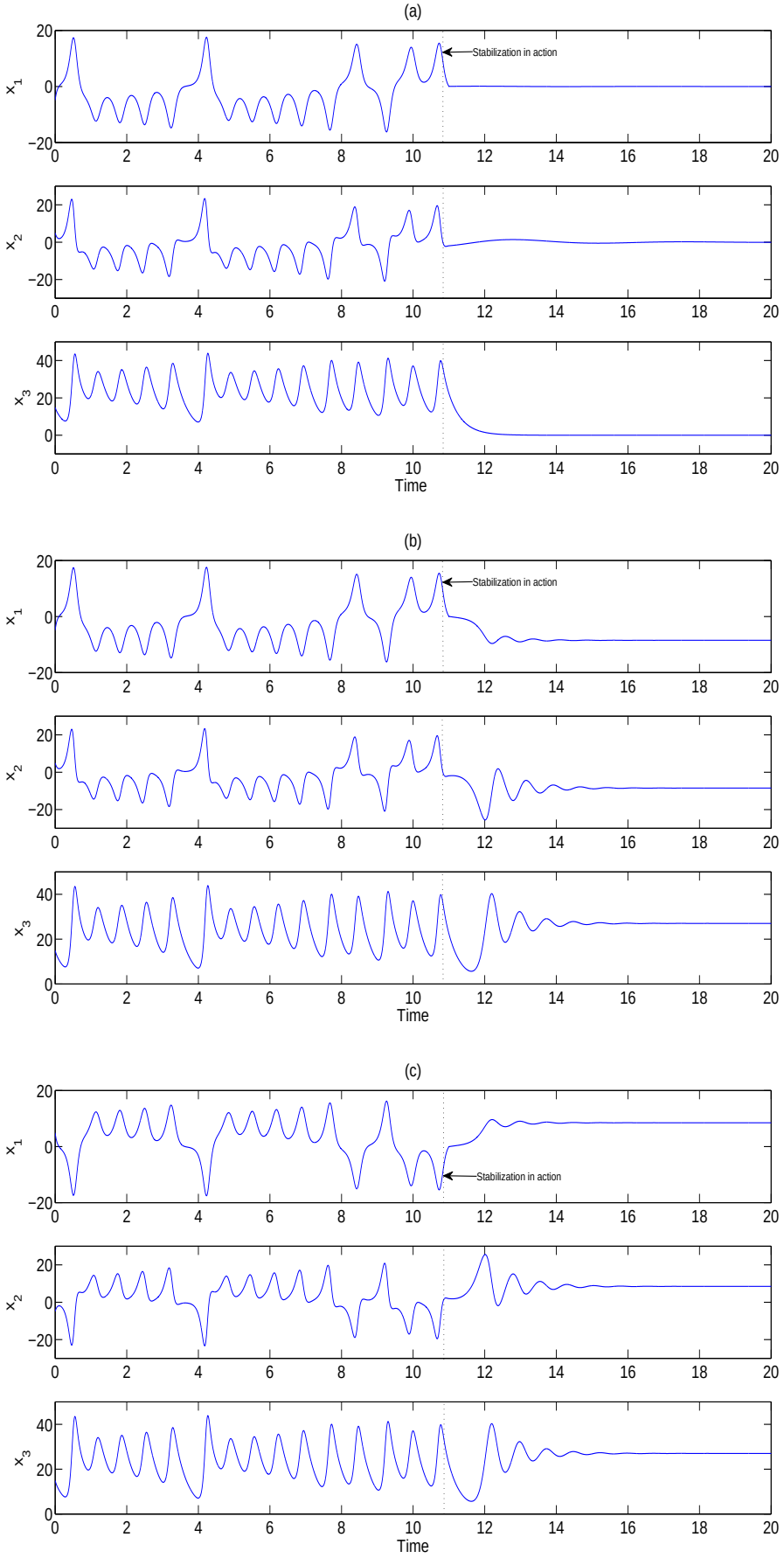


FIGURE 4.2: Stabilisation du système flou T-S de Lorenz . (a) Stabilisation sur $E_{0.}$ (b) Stabilisation sur E_{-1}. (c) Stabilisation sur E_1.

Les réponses temporelles des erreurs de synchronisation sont représentées sur la Fig.4.3. Il est montré que les erreurs de synchronisation oscillent irrégulièrement lorsque le contrôleur n'est pas activé, et lorsque la synchronisation TS floue prédictive est en action à t = 10, les erreurs de synchronisation tendent vers zéro et la synchronisation est réalisée.

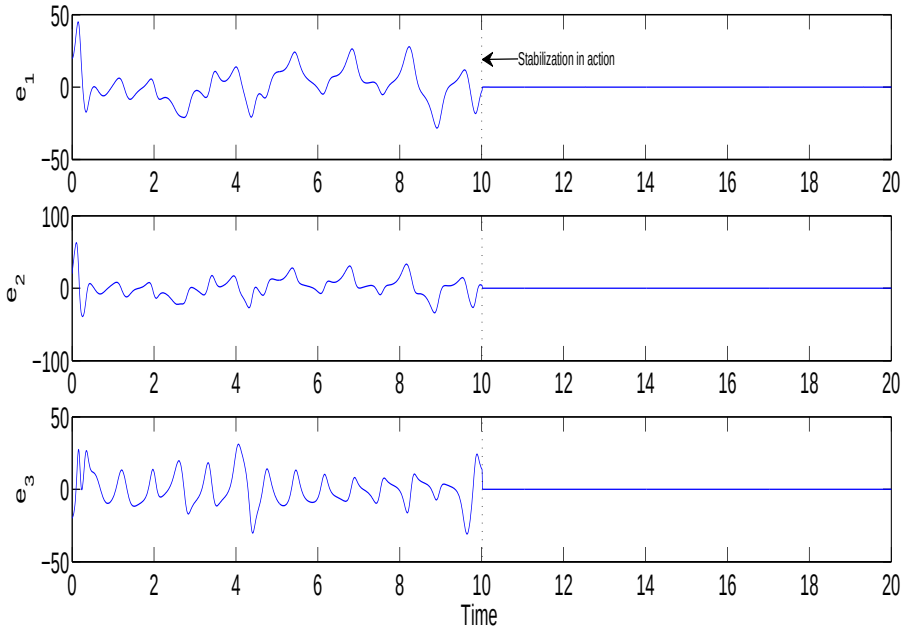


FIGURE 4.3: L'erreur de synchronisation des systèmes maître et esclave flous de Lorenz.

4.4.2 Système chaotique de Rössler

Le système de Rössler est décrit par les équations différentielles suivantes

$$\begin{cases} \dot{x} = -x_2 - x_3, \\ \dot{x}_2 = x_1 + a x_2, \\ \dot{x}_3 = b + (x_1 - c)\, x_3, \end{cases} \tag{4.29}$$

est chaotique pour les valeurs des paramètres du système $a = 0.2$, $b = 0.2$ et $c = 5$.

Le système de Rössler (4.29) possède deux points d'équilibre $E_1\,(0.008, -0.040, 0.040)$, $E_2\,(4.992, -24.960, 24.960)$.

Le modèle flou TS du système de Rössler est dérivé de la même manière que le système de Lorenz. Ici,

$$A_1 = \begin{bmatrix} 0 & -1 & -1 \\ 1 & a & 0 \\ 0 & 0 & d-c \end{bmatrix}, A_2 = \begin{bmatrix} 0 & -1 & -1 \\ 1 & a & 0 \\ 0 & 0 & -d-c \end{bmatrix}, b_1 = b_2 = \begin{bmatrix} 0 \\ 0 \\ b \end{bmatrix},$$

$$M_1 = 0.5\,(1 + x_1/d)\,, \quad M_2 = 0.5\,(1 - x_1/d)\,,\ d = 10.5.$$

La sortie finale du modèle flou de Rössler TS est donnée par

$$\dot{X}\,(t) = \sum_{i=1}^{2} M_i(x_1)\,\{A_i X\,(t)\}\,. \tag{4.30}$$

La Fig.4.4 illustre le modèle flou TS du système chaotique de Rössler.

Tout d'abord, le modèle flou de Rössler TS est stabilisé sur les deux points d'équilibre E_1 et E_2 pour les gains de contrôle

$$\begin{aligned} K_1^c &= \begin{bmatrix} -0.2555 & -0.5556 & 0.0988 \\ 0.5556 & -0.1443 & 0.1235 \\ 0 & 0 & -0.9221 \end{bmatrix}, \\ K_2^c &= \begin{bmatrix} -0.2555 & -0.5556 & -0.0269 \\ 0.5556 & -0.1443 & -0.0337 \\ 0 & 0 & -0.6393 \end{bmatrix}, \end{aligned} \tag{4.31}$$

et

$$\begin{aligned} K_1^c &= \begin{bmatrix} -21.05 & -100 & -3.6364 \\ 100 & -1.05 & 18.1818 \\ 0 & 0 & -19.2318 \end{bmatrix}, \\ K_2^c &= \begin{bmatrix} -21.05 & -100 & 1.2903 \\ 100 & -1.05 & -6.4516 \\ 0 & 0 & 5.4016 \end{bmatrix}. \end{aligned} \tag{4.32}$$

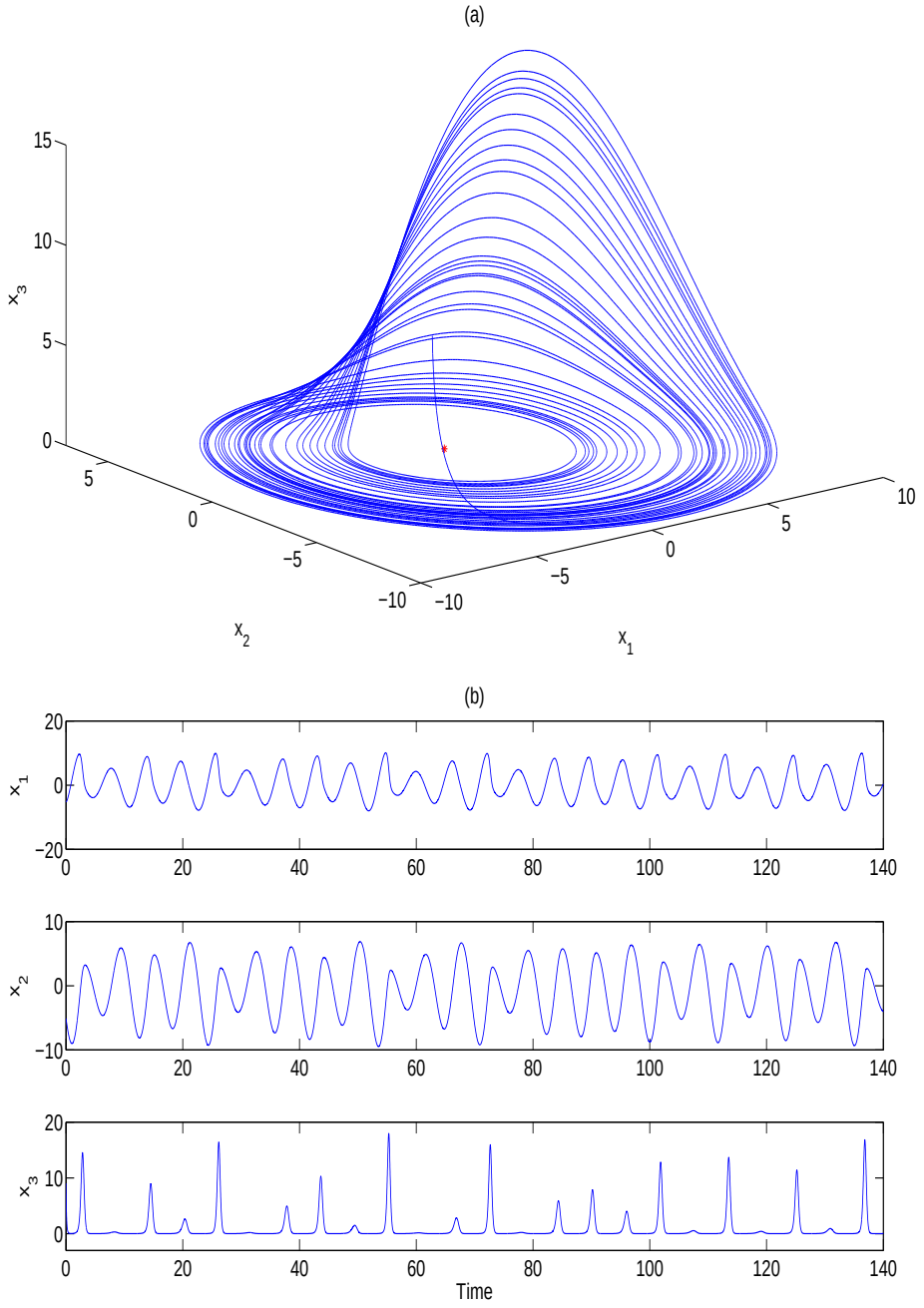


FIGURE 4.4: Le modèle flou de Rössler T-S. (a) l'espace de phase (b) ; l'évolution temporelle des variables d'état.

respectivement. Les résultats de simulation pour la stabilisation de E_1 et E_2 sont présentés dans la Fig.4.5. Il est montré que le modèle TS flou de Rössler (4.30) est stabilisé sur le point d'équilibre instable désiré selon le gain de commande de rétroaction appliqué K_i^c $(i = 1, 2)$.

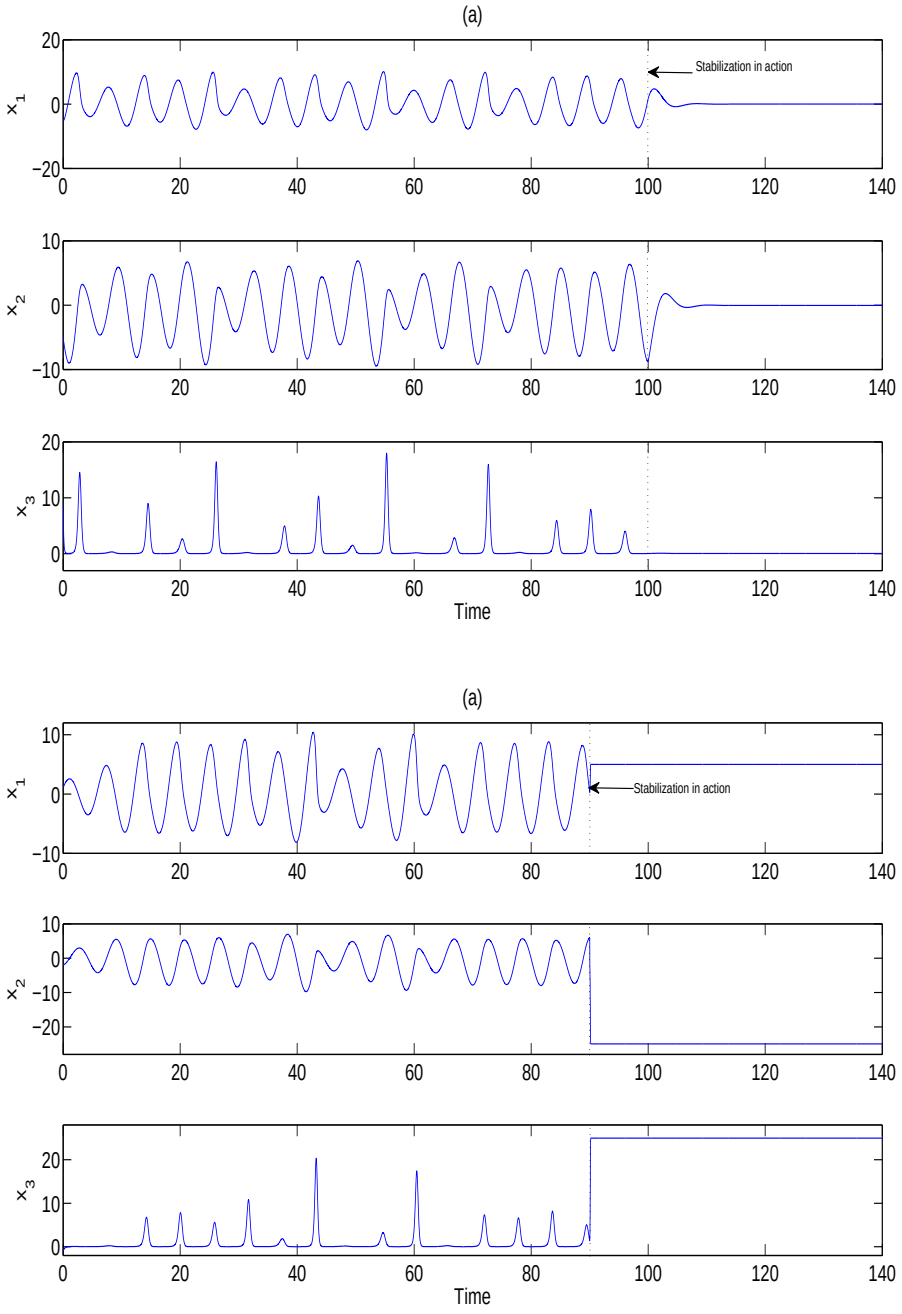


FIGURE 4.5: Stabilisation du système flou T-S de Rössler. (a) Stabilisation sur E_1. (b) Stabilisation sur E_2.

En second lieu, la synchronisation entre les systèmes maître et esclave flous de Rössler avec les conditions initiales $X(0) = (5, -5, 10)^T$, $Y(0) = (-5, 5, 10)^T$, est atteinte pour les gains de synchronisation suivants :

$$K_1^s = \begin{bmatrix} -21.1 & -100.1 & -3.7364 \\ 99.9 & -1.1 & 18.0818 \\ -0.1 & -0.1 & -19.2818 \end{bmatrix},$$
$$K_2^s = \begin{bmatrix} -21.1 & -100.1 & 1.1903 \\ 99.9 & -1.1 & -6.5516 \\ -0.1 & -0.1 & 5.3516 \end{bmatrix}. \tag{4.33}$$

L'erreur de synchronisation est représentée sur la Fig.4.6. Il est montré que les erreurs de synchronisation oscillent irrégulièrement lorsque le contrôleur est hors tension, et lorsque la synchronisation TS floue prédictive est en action à t = 30, les erreurs de synchronisation tendent vers zéro et la synchronisation est assurée.

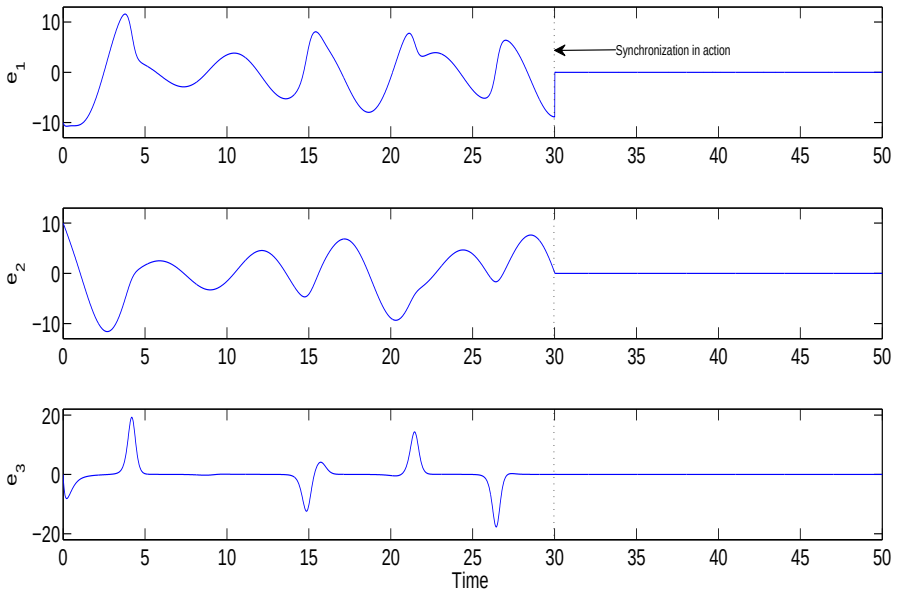


FIGURE 4.6: L'erreur de synchronisation les systèmes maître et esclave flous de Rössler.

4.4.3 Systèm hyperchaotique de Lorenz

Un système chaotique, avec plus d'un exposant de Lyapunov positif est généralement considéré comme un système hyperchaotique [101–104]. Dans ce paragraphe, nous

présentons la conception basée sur un modèle flou pour le contrôle et la synchronisation du système hyperchaotique de Lorenz [105]. Par ailleurs, il est également montré que cette méthode de contrôle peut rejeter les perturbations externes constantes.

Le système hyperchaotique de Lorenz donné par les équations différentielles suivantes

$$\begin{cases} \dot{x}_1 = \sigma(x_2 - x_1), \\ \dot{x}_2 = (r - x_3)x_1 + ax_2 + x_4, \\ \dot{x}_3 = x_1x_2 - bx_3, \\ \dot{x}_4 = -\gamma x_1 \end{cases} \tag{4.34}$$

présente un comportement hyperchaotique pour les valeurs des paramètres du système $\sigma = 35$, $a = 12$, $b = 3$, $r = 7$ and $\gamma = 10$. Pour ces paramètres, l'attracteur est hyperchaotique avec les exposants de Lyapunov suivants : $+0.28$, $+0.24$, 0.00 et -14.24, et avec une dimension fractale telle que $D_L = 3.04$. Le système hyperchaotique de Lorenz (4.34) possède seulement l'origine $E_0\,(0, 0, 0, 0)$ comme point d'équilibrium instable.

Le modèle flou TS du système hyperchaotique de Lorenz est établi comme suit

$$\begin{aligned} A_1 &= \begin{bmatrix} -\sigma & \sigma & 0 & 0 \\ r & a & -d & 1 \\ 0 & d & -b & 0 \\ -\gamma & 0 & 0 & 0 \end{bmatrix}, \; A_2 = \begin{bmatrix} -\sigma & \sigma & 0 & 0 \\ r & a & d & 1 \\ 0 & -d & -b & 0 \\ -\gamma & 0 & 0 & 0 \end{bmatrix}, \; b_1 = b_2 = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \\ M_1 &= \frac{1}{2}\left(1 + \frac{x_1}{d}\right), \; M_2 = \frac{1}{2}\left(1 - \frac{x_1}{d}\right), \; d = 40. \end{aligned}$$

La sortie finale du modèle TS flou hyperchaotique de Lorenz est donnée par

$$\dot{X}\,(t) = \sum_{i=1}^{2} M_i(x_1)\left\{A_i X\,(t)\right\}. \tag{4.35}$$

La Fig.4.7 montre le modèle TS flou du système hyperchaotique de Lorenz.

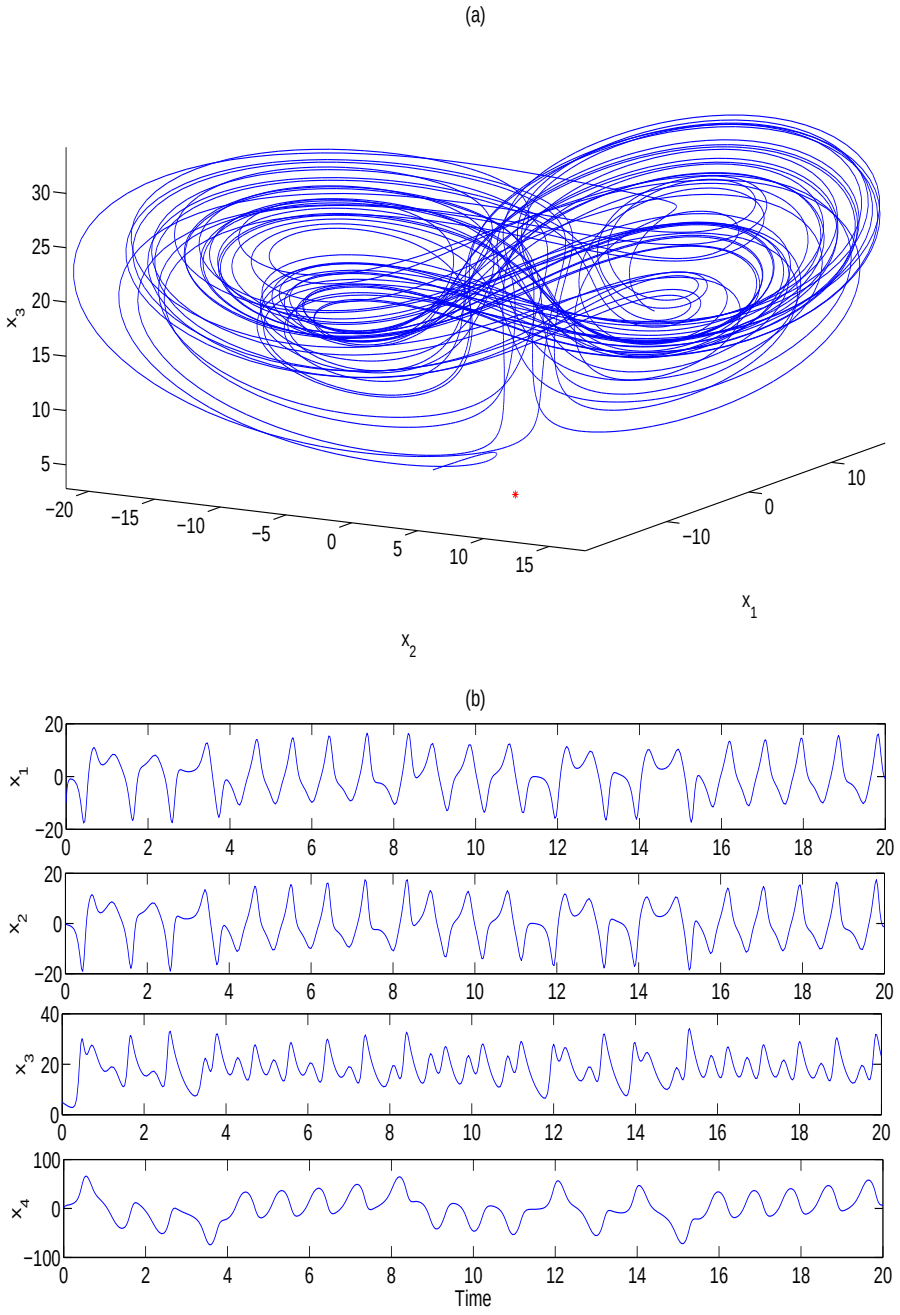


FIGURE 4.7: Le modèle TS flou du système hyperchaotique de Lorenz. (a) Espace des phases (b). Evolution temporelle des variables d'état.

Tout d'abord, le modèle TS flou hyperchaotique de Lorenz est stabilisé sur le point d'équilibre E_0 pour les gains de contrôle calculés par LMIs tels que

$$K_1^c = \begin{bmatrix} -0.647 & 0.020 & -0.273 & -0.597 \\ 0.020 & -1.312 & 0.038 & -0.067 \\ -0.273 & 0.038 & -1.080 & 0.547 \\ -0.597 & -0.067 & 0.547 & 0.140 \end{bmatrix},$$

$$K_2^c = \begin{bmatrix} -0.647 & 0.020 & 0.273 & -0.597 \\ 0.020 & -1.312 & -0.038 & -0.067 \\ 0.273 & -0.038 & -1.080 & -0.547 \\ -0.597 & -0.067 & -0.547 & 0.140 \end{bmatrix}, \tag{4.36}$$

respectivement. Le résultat de simulation du processus de stabilisation est représentée sur la Fig.4.8.

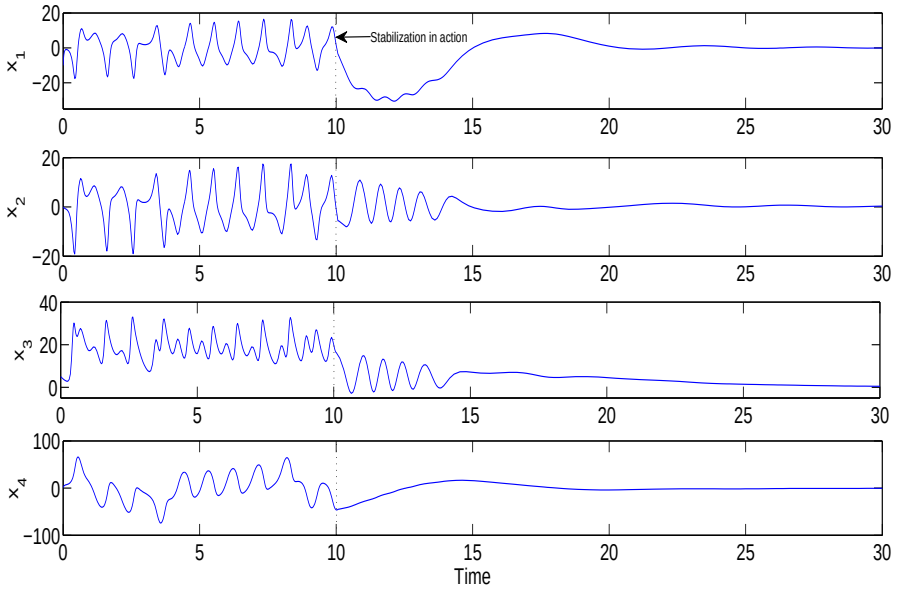


FIGURE 4.8: Stabilisation du modèle TS flou hyperchaotique de Lorenz sur E_0.

Pour montrer la robustesse du contrôleur flou proposé, nous supposons que le système hyperchaotique de Lorenz est soumis à un bruit additif aléatoire uniformément distribué avec une puissance de $0,5$ ajouté au signal $x_1(t)$. Le résultat numérique donné sur la Fig.4.9 montre que l'on peut stabiliser avec succès le modèle TS flou hyperchaotique de Lorenz par le contrôleur flou proposé, et il est également assez robuste en présence de bruit additif.

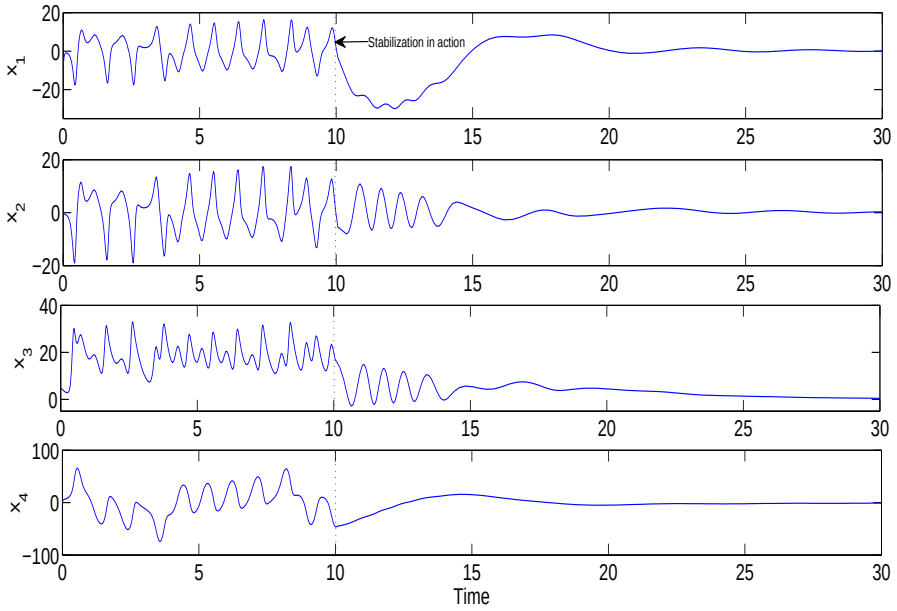


FIGURE 4.9: Stabilisation du modèle TS flou hyperchaotique de Lorenz sur E_0 quand un bruit blanc additif d'amplitude 0,5 est ajouté à la variable dynamique $x_1(t)$.

Dans la simulation numérique suivante, nous prenons les conditions initiales sur les systèmes maître et esclave respectivement telle que $X(0) = (-1,\ 10,\ 5,\ -30)^T$, $Y(0) = (1,\ -10,\ -2.5,\ 30)^T$. Les gains du contrôleur sont choisis tels que $K_1^s = K_1^c$ et $K_2^s = K_2^c$. La Fig.4.10 montre l'évolution du vecteur d'erreur. On peut voir que lorsque la synchronisation TS floue prédictive est en action à $t = 10$, les erreurs de synchronisation tendent vers zéro et la synchronisation est atteinte.

4.5 Conclusion

Dans ce chapitre, ont été étudiées la stabilité et la synchronisation des systèmes chaotiques et hyperchaotiques basées sur le modèle flou TS. Grâce à l'utilisation conjointe du modèle flou TS et du contrôle prédictif, nous avons proposé des conditions floues nouvelles et moins conservatives qui conduisent à la stabilité asymptotique globale et la synchronisation des systèmes chaotiques. La stabilité du système de contrôle flou est garantie par une matrice symétrique positive commune, qui satisfait les inégalités matricielles linéaires (LMIs). Le contrôleur TS flou prédictif est soigneusement choisi, et le temps pour obtenir une stabilisation et une synchronisation peut être ajustée en sélectionnant différents gains du contrôleur. Deux exemples des systèmes chaotiques et un exemple de système hyperchaotique sont utilisés pour illustrer la validité de cette technique, et des

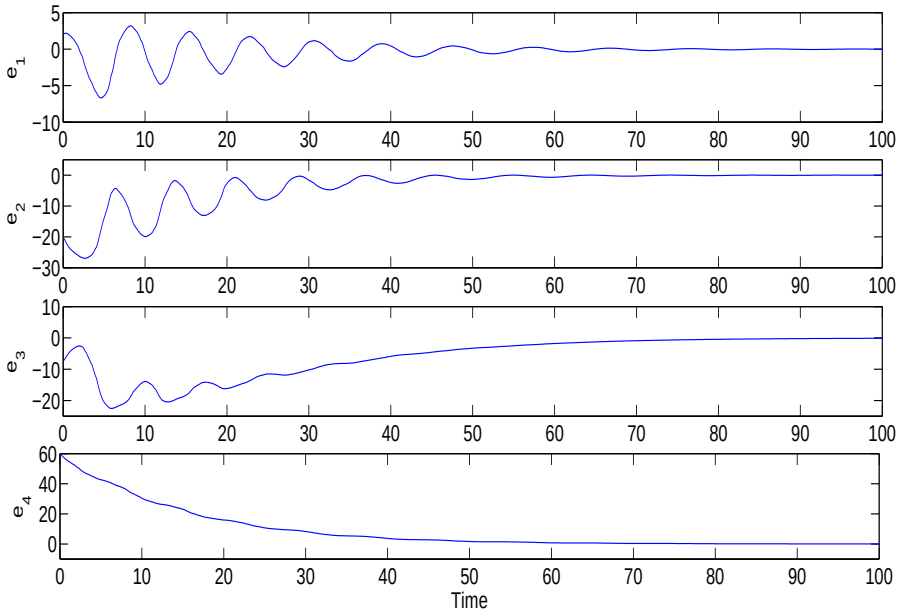


FIGURE 4.10: Les réponses temporelles des erreurs de synchronisation entre deux modèles TS flous hyperchaotiques de Lorenz.

simulations numériques sont également données pour montrer l'efficacité de la méthode proposée. Par ailleurs, il est également montré que cette méthode de contrôle peut rejeter les perturbations externes constantes. Le résultats du présent chapitre font apparaitre l'avantage d'application de la théorie moderne du contrôle à rétroaction et flou pour des problèmes de stabilisation et de synchronisation des systèmes chaotiques de haute dimension. Le principal inconvénient de ce système prédictif flou proposé est que les états du système peuvent ne pas atteindre les objectifs désirés qu'après une longue période d'attente. Toutefois, cela peut être minimisé par l'élargissement du domaine d'attraction flou, à condition qu'il répond aux exigences de stabilité.

En conclusion, la méthode de commande prédictive floue est une alternative efficace pour le contrôle et la synchronisation des systèmes chaotiques et même pour les systèmes dynamiques hyperchaotiques. En particulier, c'est un excellent choix pour de nombreuses applications du monde réel tels que les systèmes biologiques (dynamique du rythme cardiaque), les systèmes micro-électro-mécaniques, et de nombreux autres systèmes lorsqu'aucun modèle mathématique précis n'est disponible. Par ailleurs, cette méthode présente des avantages tels que la faible consommation d'énergie et la simplicité d'emploi du chaos afin d'éliminer les incertitudes du système et la perturbation externe. D'après les résultats obtenus, les performances de la commande prédictive floue proposée pour les processus de stabilisation et de synchronisation confirme l'applicabilité de l'algorithme proposé.

Chapitre 5

Conclusions & Perspectives

Dans ce document ont été présentés quelques aspects aidant à élaborer de nouvelles approches de transmission sécurisée et à concevoir un système cryptographique efficace et robuste basé sur le chaos en vue de son implémentation dans des applications de communications sécurisées. Les contributions apportées peuvent être classées en trois catégories principales :

- Proposition d'une nouvelle méthode de cryptage basée-chaos en utilisant plusieurs fonctions chaotiques itératives unidimensionnelles avec l'utilisation de cl'e de cryptage externe ;
- Développement d'une approche de communication chaotique selon un système de synchronisation par couplage indirect en cryptant des signaux de forte puissance ;
- Conception de contrôleurs flous, en utilisant la méthode prédictive, basée sur un modèle flou pour le contrôle et la synchronisation des systèmes chaotiques et hyperchaotiques.

On présente par la suite pour chaque point évoqué ci-dessus les aspects importants qui caractérisent l'originalité de chaque méthode ainsi que les perspectives de nouveaux résultats.

En vue des applications potentielles et de l'importance d'avoir un cryptosystème fiable pour le chiffrement d'image, nous avons proposé dans le chapitre 2, un cryptosystème basé-chaos efficace utilisant une rétroaction itérative pour le chiffrement d'image satisfaisant les exigences de transfert d'image sécurisé. Pour les cryptosystèmes par bloc, tel que le DES ou l'AES, à cause de la présence de forte corrélation entre les pixels adjacents des images, si aucun mode opératoire supplémentaire n'est utilisé, l'image cryptée présentera toujours des corrélations. Le système de cryptage basé-chaos proposé est un

système amélioré, qui a des caractéristiques similaires à celles d'un système cryptographique par bloc utilisant le mode de chiffrement CBC (Cipher-Block Chaining), connu de la théorie des algorithmes de chiffrement par bloc. Une telle propriété est particulièrement importante pour le chiffrement d'image, car n'importe quel mode ECB (Electronic Code Book), où les pixels identiques sont cryptées à l'identique ne cache pas les contours d'éléments d'une image. L'efficacité de l'algorithme proposé est démontrée avec succès contre les attaques de cryptanalyse. Les résultats expérimentaux montrent que la technique de cryptage d'image proposée possède plusieurs caractéristiques intéressantes, telles que la distribution uniforme des pixels de l'image cryptée, le niveau de sécurité élevé et l'espace des clés assez grand afin de résister aux attaques par force brute. Il a été montré aussi l'extrême sensibilité de l'image cryptée aux infimes changements de l'image à chiffrer, ainsi qu'aux petites variations de la clé de chiffrement afin d'être robuste envers les cryptanalyse linéaire et différentielle. Ceci a été montré par les valeurs des NPCR et UACI.

Plusieurs solutions ont été proposées et 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 décroit très rapide 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 transmis pour construire la dynamique de l'émetteur. Pour y remédier à ce désagrément, une approche récente basée sur un schéma de synchronisation avec couplage indirect a été proposée. Comme l'énergie du plain-message doit être beaucoup plus petite que celle du signal de commande, il semble impossible d'éliminer ce défaut de sécurité essentiel sans modifier la structure de l'émetteur. L'inconvénient majeur est que, dans ce cas, le message clair ne peut pas être distingué du bruit de canal et donc, les performances du système sont fortement dégradées par la distorsion d'amplitude et du bruit dans le canal. Il existe donc un réel intérêt à trouver des moyens de surmonter ces inconvénients.

Dans le souci de résoudre ce problème, le chapitre 3 est dédié à la proposition d'une approche de communication chaotique selon un système de synchronisation par couplage indirect en cryptant des signaux de forte puissance. Le schéma proposé est soigneusement conçu de sorte que le signal crypté ne détériore pas la synchronisation, contrairement aux méthodes traditionnelles de communication. Le problème de synchronisation est résolu en utilisant un contrôleur basé sur observateur.

Le système de communication chaotique proposé présente plusieurs avantages :

– la synchronisation peut être atteinte simplement en calculant les gains d'observateurs ;

– la flexibilité dans le choix des signaux chaotiques pour le générateur de clés du cryptosystème sécurisé ;
– les dynamiques de l'émetteur sont commandés par des signaux variables dans le temps, ce qui semble indiquer que l'émetteur est un système non autonome, qui est en général plus compliquée ;
– et l'amélioration des caractéristiques fréquentielles du signal crypté.

A la lumière de ces avantages, le système de communication chaotique proposé possède une conception efficace, ce qui offre un niveau de sécurité plus élevé. Une étude comparative entre le système de communication proposé et certains systèmes de communication rapportés dans la littérature est réalisée. En effet, il est montré que la synchronisation entre l'émetteur et le récepteur est plus robuste pour différentes valeurs d'amplitude du signal crypté, même en présence de perturbations externes. De plus, nous avons montré que la synchronisation des systèmes chaotiques est possible par l'intermédiaire d'une seule entrée de contrôle en mesurant une seule variable.

Le chapitre 4 présente la conception basée sur un modèle flou pour le contrôle et la synchronisation des systèmes chaotiques et hyperchaotiques. Dans ce contexte, les systèmes chaotiques et hyperchaotiques sont exactement reproduits sur la base d'un modèle flou de Takagi-Sugeno (TS). Ensuite, en utilisant la méthode prédictive, les contrôleurs flous pour le contrôle et la synchronisation sont conçus et quelques critères nouveaux et utiles sont dérivés. La principale contribution de ce chapitre réside dans la proposition de nouveaux critères de contrôle prédictif flous pour le contrôle et la synchronisation du modèle flou TS obtenu. Aussi et afin de démontrer l'efficacité de l'approche proposée, l'une des principales contributions de cet article est de présenter les résultats numériques sur les systèmes chaotiques de haute dimension pour traiter le problème de la transmission de l'information, en présence des bruits externes. Grâce à l'utilisation conjointe du modèle ou TS et du contrôle prédictif, nous avons proposé des conditions floues nouvelles et moins conservatives qui conduisent à la stabilité asymptotique globale et à la synchronisation des systèmes chaotiques. La stabilité du système de contrôle flou est garantie par une matrice symétrique positive commune, qui satisfait les inégalités matricielles linéaires (LMIs). Le contrôleur TS flou prédictif est soigneusement choisi, et le temps pour obtenir une stabilisation et une synchronisation peut être ajusté en sélectionnant différents gains du contrôleur. Deux exemples des systèmes chaotiques et un exemple de système hyperchaotique sont utilisés pour illustrer la validité de cette technique, et des simulations numériques sont également données pour montrer l'efficacité de la méthode proposée. Par ailleurs, il est également montré que cette méthode de contrôle peut rejeter les perturbations externes constantes. Les résultats font apparaitre l'avantage d'application de la théorie moderne du contrôle à rétroaction et flou pour des problèmes de

stabilisation et de synchronisation des systèmes chaotiques de haute dimension. Le principal inconvénient de ce système prédictif flou proposé est que les états du système peuvent ne pas atteindre les objectifs désirés qu'après une longue période d'attente. Toutefois, cela peut être minimisé par l'élargissement du domaine d'attraction ou, à condition qu'il réponde aux exigences de stabilité. La méthode de commande prédictive floue est une alternative efficace pour le contrôle et la synchronisation des systèmes chaotiques et même pour les systèmes dynamiques hyperchaotiques. En particulier, c'est un excellent choix pour de nombreuses applications du monde réel tels que les systèmes biologiques (dynamique du rythme cardiaque), les systèmes micro-électro-mécaniques, et de nombreux autres systèmes lorsqu'aucun modèle mathématique précis n'est disponible. Par ailleurs, cette méthode présente des avantages tels que la faible consommation d'énergie et la simplicité d'emploi du chaos afin d'éliminer les incertitudes du système et la perturbation externe. D'après les résultats obtenus, les performances de la commande prédictive floue proposée pour les processus de stabilisation et de synchronisation confirme l'applicabilité de l'algorithme proposé.

En perspective, on se propose de réaliser une communication sécurisée englobant tous les aspects évoqués dans ce manuscrit. On propose d'implémenter un cryptosystème basé sur le couplage indirect où la synchronisation est basée sur un contrôleur flou prédictif TS. On projette de faire une réalisation pratique dans la bande des hyperfréquences avec des systèmes hyperchaotiques.

Bibliographie

[1] E. N. Lorenz. Deterministic Nonperiodic Flow. *J. Atmos. Sci.*, 20(2) :130–141, March 1963.

[2] L. M. Pecora and T. L. Carroll. Synchronization in chaotic systems. *Phys. Rev. Lett.*, 64 :821–824, Feb 1990.

[3] P. S. de Laplace. *Essai philosophique sur les probabilités. English ; A philosophical essay on probabilities [microform].* J. Wiley, 1902.

[4] D. Parrochia. Les grandes révolutions scientifiques du XXe siècle. *Paris, Presses Universitaires de France*, 1997.

[5] H. Poincaré. *Science et méthode.* Bibliothèque de philosophie scientifique. E. Flammarion, 1908.

[6] M. Faggini and A. Parziale. The Failure of Economic Theory. Lessons from Chaos Theory. *The American Mathematical Monthly*, 3(1) :1–10, December 2012. ISSN 00029890.

[7] T. Y. Li and J. A. Yorke. Period Three Implies Chaos. *The American Mathematical Monthly*, 82(10) :985–992, December 1975. ISSN 00029890.

[8] E. N. Lorenz. Predictability : Does the flap of a butterfly's wings in brazil set off a tornado in texas ? *The 139th Annual Meeting of the American Association for the Advancement of Science*, 1972.

[9] B. Mandelbrot. Formes nouvelles du hasard dans les sciences. *Économie appliquée*, 26 :307–319, 1973.

[10] M. J. Feigenbaum. The universal metric properties of nonlinear transformations. *J. Stat. Phys.*, 21 :669–706, 1979.

[11] R. M. May. Simple mathematical models with very complicated dynamics. *Nature*, 261(5560) :459–467, jun 1976.

[12] M. J. Feigenbaum. Universal behaviour in nonlinear systems. *Los Alamos Science*, 1980.

[13] P. Manneville. Structures dissipatives chaos et turbulence. *Paris, Commissariat à l'énergie atomique*, 1991.

[14] P. S. Linsay. Period doubling and chaotic behaviour in a driven anharmonic oscillator. *Phys. Rev. Lett.*, 47 :1349–1352, 1981.

[15] L. O. Chua. Chua's circuit 10 years later. *International Journal of Circuit Theory and Applications*, 22 :279–305, 1994.

[16] H. Poincaré and R. Magini. Les méthodes nouvelles de la mécanique céleste. *Il Nuovo Cimento Series 4*, 10(1) :128–130, 1899. ISSN 0029-6341.

[17] D. Ruelle and F. Takens. On the nature of turbulence. *Communications in Mathematical Physics*, 20(3) :167–192, 1971.

[18] L. Glass and M. Mackey. From clocks to chaos : The rhythms of life. *Princeton Univ. Press, Princeton*, 1988.

[19] B. Van Der Pol and J. Van Der Mark. Frequency demultiplication. *Nature*, 120 : 363–364, 1927.

[20] M. Pettini. Controlling chaos through parametric excitations. In Ricardo Lima, Ludwig Streit, and Rui Vilela Mendes, editors, *Dynamics and Stochastic Processes Theory and Applications*, volume 355 of *Lecture Notes in Physics*, pages 242–250. Springer Berlin Heidelberg, 1990. ISBN 978-3-540-52347-5.

[21] A. Hubler. Adaptive control of chaotic systems. *Helv. Phys. Acta*, 62 :343–347, 1989.

[22] E. Ott, C. Grebogi, and J. A. Yorke. Controlling chaos. *Phys. Rev. Lett.*, 64 : 1196–1199, Mar 1990.

[23] W. L. Ditto, S. N. Rauseo, and M. L. Spano. Experimental control of chaos. *Phys. Rev. Lett.*, 65 :3211–3214, Dec 1990.

[24] S. Rajasekar and M. Lakshmanan. Controlling of chaos in bonhoder-van der pol oscillator. *Int. J. of Bifur. Chaos*, 2 :201–204, 1992.

[25] A. Senouci and A. Boukabou. Predictive control and synchronization of chaotic and hyperchaotic systems based on a ts fuzzy model. *Mathematics and Computers in Simulation*, 105(0) :62 – 78, 2014. ISSN 0378-4754.

[26] K. Kemih, H. Bouraoui, M. Ghanes, R. Remmouche, and A. Senouci. Passivity-based control of the new hyperchaotic system. *Int. J. Modelling, Identif. Control*, 17(3) :206–211, 2012.

[27] A. Senouci, A. Boukabou, K. Busawon, A. Bouridane, and A. Ouslimani. Robust chaotic communication based on indirect coupling synchronization. *Circuits, Systems, and Signal Processing*, pages 1–26, 2014. ISSN 0278-081X.

[28] A Senouci and A Boukabou. Chaotic cryptography using external key. In *Systems, Signal Processing and their Applications (WOSSPA), 2011 7th International Workshop on*, pages 267–270, May 2011. doi : 10.1109/WOSSPA.2011.5931469.

[29] A. Senouci, I. Benkhaddra, and M. Khiati. Embedded hyper-chaotic lorenz random number generator for secure communications. Febriary 2014.

[30] L. Kocarev, K. S. Halle, K. Eckert, L. O. Chua, and U. Parlitz. Experimental demonstration of secure communications via chaotic synchronization. *Int. J. of Bifurc. and Chaos*, 02(03) :709–713, 1992.

[31] M. S. Baptista. Cryptography with chaos. *Physics Letters A*, 240 :50 – 54, 1998. ISSN 0375-9601.

[32] E. Alvarez, A. Fernández, P. Garcia, J. Jimenez, and A. Marcano. New approach to chaotic encryption. *Physics Letters A*, 263 :373 – 375, 1999. ISSN 0375-9601.

[33] G. Jakimoski and L. Kocarev. Chaos and cryptography : block encryption ciphers based on chaotic maps. *Circuits and Systems I : Fundamental Theory and Applications, IEEE Transactions on*, 48(2) :163–169, 2001. ISSN 1057-7122.

[34] N. K. Pareek, V. Patidar, and K. K. Sud. Discrete chaotic cryptography using external key. *Physics Letters A*, 309 :75 – 82, 2003. ISSN 0375-9601.

[35] G. Chen, Y. Mao, and C. K. Chui. A symmetric image encryption scheme based on 3D chaotic cat maps. *Chaos, Solitons & Fractals*, 21(3) :749 – 761, 2004. ISSN 0960-0779.

[36] N. K. Pareek, V. Patidar, and K. K. Sud. Cryptography using multiple one-dimensional chaotic maps. *Communications in Nonlinear Science and Numerical Simulation*, 10(7) :715 – 723, 2005. ISSN 1007-5704.

[37] G. Alvarez and S. Li. Some basic cryptographic requirements for chaos-based cryptosystems. *International Journal of Bifurcation and Chaos*, 16(08) :2129–2151, 2006.

[38] K. W. Wong, B. S. H. Kwok, and W. S. Law. A fast image encryption scheme based on chaotic standard map. *Physics Letters A*, 372(15) :2645 – 2652, 2008. ISSN 0375-9601.

[39] A. J. Menezes, S. A. Vanstone, and P. C. V. Oorschot. *Handbook of Applied Cryptography*. CRC Press, Inc., Boca Raton, FL, USA, 1st edition, 1996. ISBN 0849385237.

[40] K. M. Cuomo, A. V. Oppenheim, and S. H. Strogatz. Synchronization of lorenz-based chaotic circuits with applications to communications. *Circuits and Systems II : Analog and Digital Signal Processing, IEEE Transactions on*, 40(10) :626–633, Oct 1993. ISSN 1057-7130.

[41] H. Dedieu, M. P. Kennedy, and M. Hasler. Chaos shift keying : modulation and demodulation of a chaotic carrier using self-synchronizing chua's circuits. *Circuits and Systems II : Analog and Digital Signal Processing, IEEE Transactions on*, 40 (10) :634 –642, oct 1993. ISSN 1057-7130.

[42] O. Morgul and M. Feki. A chaotic masking scheme by using synchronized chaotic systems. *Physics Letters A*, 251(3) :169 – 176, 1999. ISSN 0375-9601.

[43] M. G. Rosemblum, A. S. Pikovsky, and J. Kurths. Synchronization in chaotic systems. *Phys. Rev. Lett.*, 76 :1804–1807, 1996.

[44] D. Sadaoui, A. Boukabou, N. Merabtine, and M. Benslama. Predictive synchronization of chaotic satellites systems. *Expert Systems with Applications*, 38(7) :9041 – 9045, 2011. ISSN 0957-4174.

[45] T. Yang, C. W. Wu, and L. O. Chua. Cryptography based on chaotic systems. *Circuits and Systems I : Fundamental Theory and Applications, IEEE Transactions on*, 44(5) :469–472, May 1997. ISSN 1057-7122.

[46] J. F. Chang, T. L. Liao, J. J. Yan, and H. C. Chen. Implementation of synchronized chaotic l systems and its application in secure communication using pso-based pi controller. *Circuits, Systems and Signal Processing*, 29(3) :527–538, 2010. ISSN 0278-081X.

[47] U. Feldmann, M. Hasler, and W. Schwarz. Communication by chaotic signals : the inverse system approach. *International Journal of Circuit Theory and Applications*, 24(5) :551–579, 1996. ISSN 1097-007X.

[48] G. Kaddoum, A. J. Lawrance, P. Charge, and D. Roviras. Chaos communication performance : Theory and computation. *Circuits, Systems, and Signal Processing*, 30(1) :185–208, 2011. ISSN 0278-081X.

[49] G. Kolumban, K. Gabor, J. Zoltan, and M. P. Kennedy. Fm-dcsk : A robust modulation scheme for chaotic communications. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 81(9) :1798–1802, 1998.

[50] O. M. Kwon, J. Park, and S. M. Lee. Secure communication based on chaotic synchronization via interval-time-varying delay feedback control. *Nonlinear Dynamics*, 63(1-2) :239–252, 2011. ISSN 0924-090X.

[51] T. L. Liao and N. S. Huang. An observer-based approach for chaotic synchronization with applications to secure communications. *Circuits and Systems I : Fundamental Theory and Applications, IEEE Transactions on*, 46(9) :1144–1150, Sep 1999. ISSN 1057-7122.

[52] A. T. Parker and K. M. Short. Reconstructing the keystream from a chaotic encryption scheme. *Circuits and Systems I : Fundamental Theory and Applications, IEEE Transactions on*, 48(5) :624–630, 2001. ISSN 1057-7122.

[53] N. F. Reddell, E. M. Bollt, and T. B. Welch. A dual-synchrony chaotic communication scheme. *Circuits, Systems and Signal Processing*, 24(5) :557–570, 2005. ISSN 0278-081X.

[54] C. W. Wu and L. O. Chua. A simple way to synchronize chaotic systems with applications to secure communication systems. *Int. J. Bifur. Chaos*, 3 :1619 – 1627, 1994.

[55] G. Alvarez, F. Montoya, M. Romera, and G. Pastor. Breaking two secure communication systems based on chaotic masking. *Circuits and Systems II : Express Briefs, IEEE Transactions on*, 51(10) :505 – 506, oct. 2004. ISSN 1549-7747.

[56] S. Li, G. Alvarez, and G. Chen. Breaking a chaos-based secure communication scheme designed by an improved modulation method. *Chaos, Solitons & Fractals*, 25(1) :109 – 120, 2005. ISSN 0960-0779.

[57] S. Li, G. Alvarez, G. Chen, and X. Mou. Breaking a chaos-noise-based secure communication scheme. *Chaos : An Interdisciplinary Journal of Nonlinear Science*, 15(1) :013703, 2005.

[58] N. Barhoumi, F. Msahli, M. Djemai, and K. Busawon. Observer design for some classes of uniformly observable nonlinear hybrid systems. *Nonlinear Analysis : Hybrid Systems*, 6(4) :917 – 929, 2012. ISSN 1751-570X.

[59] M. Boutayeb, M. Darouach, and H. Rafaralahy. Generalized state-space observers for chaotic synchronization and secure communication. *Circuits and Systems I :*

Fundamental Theory and Applications, IEEE Transactions on, 49(3) :345–349, Mar 2002. ISSN 1057-7122.

[60] R. Kharel, K. Busawon, and Z. Ghassemlooy. Secure communication based on indirect coupled synchronization. In Hermann Kaindl, editor, *Proceedings of the The Seventh International Conference on Systems (ICONS 2012)*, pages 184–189. IARIA, USA, February 2012. The Seventh International Conference on Systems, 29 February 5 March, 2012, Saint Gilles, Reunion Island.

[61] K. Busawon, R. Kharel, and Z. Ghassemlooy. A new chaos-based communication scheme using observers. In *Communication Systems, Networks and Digital Signal Processing, 2008. CNSDSP 2008. 6th International Symposium on*, pages 16–20, July 2008.

[62] P. Stavroulakis. *Chaos Applications in Telecommunications*. CRC Taylor & Francis, 2006. ISBN 9780849338281.

[63] A. Abdullah. Synchronization and secure communication of uncertain chaotic systems based on full-order and reduced-order output-affine observers. *Applied Mathematics and Computation*, 219(19) :10000 – 10011, 2013. ISSN 0096-3003.

[64] R. Trejo-Guerra, E. Tlelo-Cuautle, C. Cruz-Hernández, and C. Sánchez-López. Chaotic communication system using chua's oscillators realized with CCII+S. *Int. J. Bifurcation and Chaos*, 19(12) :4217–4226, 2009.

[65] R. Trejo-Guerra, E. Tlelo-Cuautle, J. M. Jiménez-Fuentes, C. Sánchez-Lopez, J. M. Munoz-Pacheco, G. Espinosa-Flores-Verdad, and J. M. Rocha-Perez. Integrated circuit generating 3- and 5-scroll attractors. *Communications in Nonlinear Science and Numerical Simulation*, 17(11) :4328 – 4335, 2012. ISSN 1007-5704.

[66] A. Sharma, P. R. Sharma, and M. D. Shrimali. Amplitude death in nonlinear oscillators with indirect coupling. *Physics Letters A*, 376(18) :1562 – 1566, 2012. ISSN 0375-9601.

[67] H. Serrano-Guerrero, C. Cruz-Hernandez, R. M. Lopez-Gutierrez, L. Cardoza-Avendano, and R. A. Chavez-Perez. Chaotic synchronization in nearest-neighbor coupled networks of 3d cnns. *J. App. Resear. Technology*, 11 :26 – 41, 2013.

[68] J. Lu and G. Chen. A new chaotic attractor coined. *Int. J. Bifurcation and Chaos*, 12(3) :659–661, 2002.

[69] J. R. Terry and G. D. VanWiggeren. Chaotic communication using generalized synchronization. *Chaos, Solitons & Fractals*, 12 :145–152, 2001.

[70] A. A. Zaher. Digital communication using a novel combination of chaotic shift keying and duffing oscillators. *Int. J. Innov. Comput. Informat. Control*, 9 :1865–1879, 2013.

[71] N. Smaoui, A. Karouma, and M. Zribi. Adaptive synchronization of hyperchaotic chen system with application to secure communication. *Int. J. Innov. Comput. Informat. Control*, 9 :1127 – 1144, 2013.

[72] V. H. Carbajal-Gomez, E. Tlelo-Cuautle, and F. V. Fernández. Optimizing the positive lyapunov exponent in multi-scroll chaotic oscillators with differential evolution algorithm. *Applied Mathematics and Computation*, 219(15) :8163 – 8168, 2013. ISSN 0096-3003.

[73] A. Wolf, J. B. Swift, H. L. Swinney, and J. A. Vastano. Determining lyapunov exponents from a time series. *Physica D : Nonlinear Phenomena*, 16(3) :285 – 317, 1985. ISSN 0167-2789.

[74] J. G. Proakis and M. Salehi. *Digital Communications*. McGraw-Hill. McGraw-Hill Higher Education, 4th edition, 2012.

[75] E. Scholl and H. G. Schuster. *Handbook of Chaos Control*. WILEY-VCH Verlag GmbH & Co. KGaA, Weinheim, Germany, 2nd edition, 2008. ISBN 978-3-527-40605-0.

[76] K. Pyragas. Continuous control of chaos by self-controlling feedback. *Physics Letters A*, 170(6) :421 – 428, 1992. ISSN 0375-9601.

[77] M. di Bernardo. An adaptive approach to the control and synchronization of continuous-time chaotic systems. *Int. J. Bifurcation and Chaos*, 6 :557–568, 1996.

[78] A. Loria and A. Zavala-Rio. Adaptive tracking control of chaotic systems with applications to synchronization. *Circuits and Systems I : Fundamental Theory and Applications, IEEE Transactions on*, 54 :2019–2029, 2007.

[79] N. Inaba and T. Nitanai. OPF chaos control in a circuit containing a feedback voltage pulse generator. *Circuits and Systems I : Fundamental Theory and Applications, IEEE Transactions on*, 45 :473–480, 1998.

[80] X. Z. Liu. Impulsive stabilization and control of chaotic system. *Nonlinear Analalysis*, 47 :1081–1092, 2001.

[81] A. Boukabou and N. Mansouri. Controlling chaos in higher-order dynamical systems. *Int. J. Bifurcation and Chaos*, 14(11) :4019–4025, 2004.

[82] A. Boukabou, A. Chebbah, and N. Mansouri. Predictive control of continuous chaotic systems. *Int. J. Bifurcation and Chaos*, 18(2) :587–592, 2008.

[83] T. Ushio and S. Yamamoto. Prediction-based control of chaos. *Physics Letters A*, 264(1) :30 – 35, 1999. ISSN 0375-9601.

[84] A. Boukabou and N. Mekircha. Generalized chaos control and synchronization by nonlinear high-order approach. *Mathematics and Computers in Simulation*, 82 : 2268–2281, 2012.

[85] A. Boukabou, B. Sayoud, H. Boumaiza, and N. Mansouri. Control of n-scroll chua's circuit. *Int. J. Bifurcation and Chaos*, 19(11) :3813–3822, 2009.

[86] T. Hino, S. Yamamoto, and T. Ushio. Discrete-time systems using prediction-based feedback control. *Int. J. Bifurcation and Chaos*, 12 :439–446, 2002.

[87] E. Liz and D. Franco. Global stabilization of fixed points using predictive control. *Chaos*, 20 :023124-9, 2010.

[88] K. Tanaka, T. Ikeda, and H. O. Wang. A unified approach to controlling chaos via an LMI-based fuzzy control system design. *Circuits and Systems I : Fundamental Theory and Applications, IEEE Transactions on*, 45(10) :1021–1040, 1998. ISSN 1057-7122.

[89] L. Udawatta, K. Watanabe, K. Kiguchi, and K. Izumi. Fuzzy-chaos hybrid controller for controlling of nonlinear systems. *Fuzzy Systems, IEEE Transactions on*, 10 (3) :401–411, 2002. ISSN 1063-6706.

[90] Y. W. Wang, Z. H. Guan, and H. O. Wang. LMI-based fuzzy stability and synchronization of chen's system. *Physics Letters A*, 320 :154 – 159, 2003. ISSN 0375-9601.

[91] H. Zhang, X. Liao, and J. Yu. Fuzzy modeling and synchronization of hyperchaotic systems. *Chaos, Solitons & Fractals*, 26(3) :835 – 843, 2005. ISSN 0960-0779.

[92] X. Zhang, A. Khadra, D. Yang, and D. Li. Unified impulsive fuzzy-model-based controllers for chaotic systems with parameter uncertainties via LMI. *Communications in Nonlinear Science and Numerical Simulation*, 15(1) :105 – 114, 2010. ISSN 1007-5704.

[93] Y. W. Wang, Z. H. Guan, and H. O. Wang. Impulsive synchronization for takagi-sugeno fuzzy model and its application to continuous chaotic system. *Physics Letters A*, 339 :325–332, 2005.

[94] C. Hu H. Jiang and Z. Teng. General impulsive control of chaotic systems based on a ts fuzzy model. *Fuzzy Sets and Systems*, 174 :66–82, 2011.

[95] A. Boukabou and N. Mansouri. Fuzzy predictive controller for unknown chaotic systems. *Int. J. Bifurcation and Chaos*, 17 :2141–2148, 2007.

[96] A. Boukabou and N. Mansouri. T-s fuzzy control of uncertain chaotic vibration. *Shock and Vibration*, 19 :379–389, 2012.

[97] N. Mekircha, A. Boukabou, and N. Mansouri. Fuzzy control of original upos of unknown discrete chaotic systems. *Applied Mathematical Modelling*, 36 :5135–5142, 2012.

[98] S. Jafari, J. C. Sprott, and S. M. R. H. Golpayegani. Elementary quadratic chaotic flows with no equilibria. *Physics Letters A*, 377(9) :699 – 702, 2013.

[99] G. A. Leonov, N. V. Kuznetsov, and V. I. Vagaitsev. Hidden attractor in smooth chua systems. *Physica D*, 241 :1482–1486, 2012.

[100] G. A. Leonov and N. V. Kuznetsov. Hidden attractors in dynamical systems. *International Journal of Bifurcation and Chaos*, 23 :1330002, 2013.

[101] G. Baier, J. S. Thomsen, and E. Mosekilde. Chaotic hierarchy in a model of competing populations. *Journal of Theoretical Biology*, 165 :593–607, 1993.

[102] H. Killory, O. E. Rössler, and J. L. Hudson. Higher chaos in four variable chemical reaction model. *Physics Letters A*, 122 :341–345, 1987.

[103] O. E. Rossler. An equation for hyperchaos. *Physics Letters A*, 71 :155–157, 1979.

[104] O. E. Rossler and Z. Naturforsch. The chaotic hierarchy. *Physics Letters A*, 38 : 788–801, 1983.

[105] R. Barboza. Dynamics of a hyperchaotic lorenz system. *International Journal of Bifurcation and Chaos*, 17 :4285–4294, 2007.