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

UNIVERSITE MOULOUD MAMMERI DE TIZI-OUZOU

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

Mémoire de Fin d'Etudes de MASTER PROFESSIONNEL

Domaine : **Sciences et Technologies**
Filière : **Automatique**
Spécialité : **Automatique industrielle .**

Présenté par
Siham Oukidja
Kahina Ould slimane

O

Thème

Conception d'un crypto-système basé sur la synchronisation de système chaotique :application au cryptage d'image

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

M Nadia DJEGHALI
PROFESSEUR ,UMMTO , Président

M Ahcene HAMOUDI
MCB , UMMTO, Encadrant

M Sarah KASSIM
MCB ,UMMTO, Examinateur

M Sadia ALKAMA
MCB , UMMTO, Examinateur

Table des matières

Table des figures

Liste des tableaux

Symboles et Notations

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

$I^k f(t)$:	$(k \in \mathbb{N})$, L'intégration répétée k fois de la fonction $f(t)$
$I^\alpha f(t)$:	$(\alpha \in \mathbb{R})$, L'intégration non entière d'ordre α de la fonction $f(t)$
${}_{t_0}^{RL}D_t^\alpha f(t)$:	Dérivée d'ordre α de la fonction $f(t)$ selon la définition de Riemann-Liouville
${}_{t_0}^{C}D_t^\alpha f(t)$:	Dérivée d'ordre α de la fonction $f(t)$ selon la définition de Caputo
D^α :	Opérateur de dérivation d'ordre non entier α
Γ :	Fonction Gamma d'Euler
$\mathcal{P}_\alpha(t)$:	Facteur d'oubli
$\binom{\alpha}{j}$:	$(\alpha \in \mathbb{R}_+)$, désigne le binôme de Newton généralisé à des ordres réels
$D^\alpha f(kh)$:	désigne la valeur de la $\alpha^{ème}$ dérivée de $f(t)$ à l'instant kh
E_α :	Fonction Mittag-Leffler
$D^\alpha x$:	$(x \in \mathbb{R}^n)$, tous les éléments du vecteur $x(t)$ sont dérivés au même ordre α
$D^{(\alpha)}(x)$:	$(\alpha \in \mathbb{R}_+^n,\ x \in \mathbb{R}^n)$, le $i^{ème}$ élément du vecteur $x(t)$ est dérivé à la $i^{ème}$ composante du vecteur α
$\mathcal{L}$:	Transformée de Laplace
$\mathcal{L}^{-1}$:	Transformée de Laplace inverse.

LTI :	Linear Time Invariant
LTV :	Linear Time variant
$SISO$:	Single Input, Single Output
$BIBS$:	Bounded Input, Bounded State
LMI :	Linear Matrix Inequality
UIO :	Unknown Input Observer
TS :	Takagi-Sugeno
STA :	Super-Twisting Algorithm

Introduction Générale

De nos jours, la sécurisation de transmission de l'information est un sujet de recherche pour lequel il y a actuellement un fort regain d'intérêt, notamment pour deux raisons. D'une part, c'est une conséquence du formidable développement des télécommunications via le support réseau, notamment l'internet [**?**, **?**]. D'autre part, la sécurité est également apparue naturellement à la suite de la vulgarisation des échanges d'informations confidentielles. En effet, la notion de confidentialité s'est largement étendue du champ qui ne concernait initialement que la diplomatie, l'armée et les gouvernements. Cette confidentialité est devenue nécessaire à chaque individu à travers la banalisation des échanges d'informations sur les grands réseaux de communication comme l'internet. Les échanges d'informations privées concernent, par exemple, les transactions financières suite à des achats électroniques, la transmission de données médicales confidentielles ou, plus simplement, la correspondance électronique entre individus. Par conséquent, le chiffrement de message, de parole ou d'image est devenu un défi de plus en plus sérieux et urgent.

Bien que l'efficacité des algorithmes de chiffrement classique [**?**, **?**, **?**] soit reconnue, leur temps de calcul est long, ce qui conduit à une diminution du débit des messages transmis. Le développement constant des techniques de cryptanalyse, provoqué par la puissance croissante des ordinateurs disponibles [**?**], réduit le niveau de confidentialité de ces algorithmes. Ces failles ont poussé la recherche vers le développement de nouveaux systèmes. L'utilisation du chaos était l'une des alternatives proposées. Récemment, de plus en plus d'attention a été accordée à l'utilisation de la théorie du chaos pour développer de nouveaux schémas de chiffrement. Les propriétés des systèmes chaotiques, qui sont des systèmes déterministes au comportement complexe et imprévisible, très sensibles aux conditions initiales et aux variations paramétriques, motivent l'utilisation du chaos dans les applications de communication sécurisée. En effet, depuis le travail pionnier de Pecora et Carrol [**?**], qui ont démontré la possibilité de synchroniser deux systèmes chaotiques avec des conditions initiales différentes, l'utilisation des systèmes chaotiques dans une

communication sécurisée a révolutionné les méthodes de cryptage traditionnelles. Dans les cryptosystèmes basés sur le chaos, le message secret est masqué par le signal d'aspect aléatoire généré par le système chaotique entraînant (émetteur ou maître) conduisant à un signal inintelligible qui est transmis par le canal public au système chaotique de réponse (récepteur ou esclave). La récupération du message d'origine est possible si l'émetteur et le récepteur sont synchronisés.

Le phénomène de synchronisation peut être décrit comme étant un processus d'ajustement des rythmes des événements répétitifs par l'intermédiaire des faibles interactions. Huygens a observé ce phénomène pour la première fois en 1673 en étudiant un système de deux pendules couplés [**?**]. Depuis le constat de Huygens, la synchronisation des systèmes dynamiques a trouvé des applications en théorie et en pratique, et plusieurs types de synchronisation ont été distingués, notamment l'auto-synchronisation, qui se manifeste par des interactions internes entre les systèmes considérés et la synchronisation commandée, qui nécessite une intervention externe pour forcer deux systèmes ou plus à se synchroniser [**?**]. La synchronisation maître-esclave appartient à la catégorie de la synchronisation par commande, dans laquelle un système dominant (le système maître) impose son rythme à un second système (le système esclave). Ainsi, plusieurs méthodes de synchronisation à base de commande ont été proposés dans la littérature et ce dans le cas des systèmes chaotiques d'ordre entier [**?**, **?**, **?**].

Par ailleurs, avec le développement du calcul d'ordre fractionnaire [**?**, **?**], l'attention a été portée à l'utilisation des systèmes chaotiques d'ordre fractionnaire dans la conception des schémas de communication sécurisée ce qui augmente grandement la sécurité. En effet, les ordres de dérivations sont considérés comme des paramètres supplémentaires de la clé de sécurité. Il est pratiquement impossible pour un intrus d'identifier les ordres fractionnaires à partir des mesures observées, ce qui améliore le niveau de sécurité. Plusieurs méthodes de synchronisation des systèmes chaotiques d'ordre fractionnaire et leur application à la transmission sécurisée de données sont développées dans la littérature [**?**, **?**].

En 1997, Nijmeijer et Mareels [**?**] ont démontré que la synchronisation de deux systèmes chaotiques est un problème de conception d'observateurs où le système esclave est conçu à base d'un observateur d'état pour le système maître. Le problème de l'estimation d'état et de la synthèse d'observateurs pour les systèmes dynamiques a été étudié depuis les années 1960 et est encore un domaine très actif aujourd'hui. En effet, de nombreuses applications, telles que la détection de défauts, la commande, l'identification et la synchronisation des systèmes dynamiques, nécessitent

une estimation d'état. Il s'agit de concevoir un système dynamique appelé observateur dont le but est de reconstruire les états du système en utilisant uniquement des informations partielles, telles que les signaux d'entrée et de sortie.

Dans ce contexte, diverses stratégies de synthèse d'observateurs pour différentes classes des systèmes linéaires et non linéaires ont été développées, telles que les systèmes Lipschitziens, les systèmes satisfaisant les propriétés du secteur et de restriction de pente, les systèmes ayant des formes particulières telle que la forme canonique observable et pour lesquelles plusieurs types d'observateurs linéaires et non linéaires ont été proposés tels que l'observateur de Luenberger [**?**, **?**], le filtre de Kalman [**?**], l'observateur à grand gain [**?**,**?**], l'observateur de Thau [**?**], l'observateur d'Arcak [**?**], etc.

Ces observateurs ont été utilisés et mis en œuvre avec succès dans des conditions idéales. Cependant, dans la pratique, on est fréquemment confronté à des situations dans lesquelles ces stratégies ne parviennent pas à estimer avec précision l'état du système. Il s'agit de contraintes et d'incertitudes imposées par l'environnement extérieur et les imperfections des circuits électroniques, qui se manifestent par des incertitudes paramétriques, des perturbations, des dynamiques non modélisées, des entrées inconnues, des défauts, des bruits de mesure, des retards, etc. Ces imperfections sont particulièrement courantes dans le contexte de la synchronisation maître-esclave et ses applications dans les systèmes de communication, où elles sont souvent négligées ou seulement analysées et quantifiées.

Afin d'améliorer les performances d'un observateur d'état dans de telles circonstances, les chercheurs ont développé des stratégies plus avancées qui tiennent compte des considérations pratiques : les stratégies robustes et adaptatives ont ainsi vu le jour.

Par conséquent, les observateurs à entrées inconnues [**?**, **?**] ont été développés dans le but d'estimer l'état du système tout en découplant les entrées inconnues ; les observateurs à modes glissants [**?**, **?**, **?**] basés sur la théorie de la commande à structure variable sont des observateurs robustes qui permettent l'estimation simultanée de l'état et de l'entrée inconnue ; et les observateurs adaptatifs [**?**, **?**, **?**] ont été développés dans le but de reconstruire simultanément les états et les paramètres inconnus.

Indéniablement, les observateurs à modes glissants sont une solution simple aux problèmes cités ci-dessus. Cependant, la présence des termes discontinus induisent le phénomène de chattering (réticence ou broutement) qui se traduit par de fortes oscillations à des hautes fréquences.

Néanmoins, le recours aux modes glissants d'ordre supérieur permet de conserver les avantages du mode glissant d'ordre un (convergence en temps fini, précision et la robustesse vis à vis des incertitudes) tout en réduisant le phénomène de chattering [**?**].

Par ailleurs, le problème de la conception d'observateurs non linéaires, en présence d'un retard affectant la sortie, a pris de l'ampleur ces dernières années. Les techniques d'immersion et d'invariance ont été étudiées pour concevoir des observateurs pour des systèmes non linéaires lorsque la sortie est soumise à un retard constant [**?**]. Un observateur à grand gain sous mesures retardées est développé dans [**?**]. Un observateur pour les systèmes non linéaires Lipschitziens soumis à un retard variable dans le temps est proposé dans [**?**]. Le premier travail traitant de la conception d'observateurs non linéaires à sortie retardée est présenté dans [**?**], pour une classe de systèmes uniformément observables. Les auteurs proposent un "observateur en chaîne" composé d'observateurs successifs en cascade. Chaque observateur considère qu'il y a eu un retard à chaque instant retardé. Cette idée a été étendue dans [**?**, **?**, **?**]. La conception d'observateur-prédicteur en cascade est une approche efficace pour compenser le problème du retard dans les systèmes non linéaires [**?**, **?**, **?**]. Cette approche se compose de deux étapes. Dans la première étape, un observateur est conçu pour estimer l'état retardé. L'observateur est alimenté par les mesures retardées pour obtenir l'estimation de l'état retardé. Cet observateur fonctionne comme dans une situation de retard libre. Dans la deuxième étape, le prédicteur est utilisé pour compensé le retard.

La théorie des observateurs non linéaires a joué un rôle fondamental dans le développement des méthodes de synchronisation des systèmes chaotiques d'ordre entier et d'ordre fractionnaire et de leurs applications dans les systèmes de transmission de données sécurisés. Plusieurs observateurs ont été développés dans la littérature, parmi eux, on peut citer l'observateur synergétique [**?**, **?**], l'observateur proportionnel intégral [**?**], l'observateur à mode glissant [**?**, **?**], l'observateur exponentiel non fragile [**?**] et l'observateur adaptatif [**?**, **?**].

Cependant, dans la plupart des méthodes de synchronisation proposées dans la littérature, les moyens de communication sont considérés comme idéaux. En effet, plusieurs contraintes de communication, telles que retard dans le canal de transmission (retard sur la mesure), les incertitudes et les perturbations externes ne sont pas prises en considération. Ces contraintes peuvent dégrader la synchronisation. Ainsi, un retard dû au délai de communication peut altérer la réalisation de la synchronisation. Si la synchronisation entre l'émetteur et le récepteur n'est pas

correctement réalisée, il serait alors impossible de reconstruire le message secret. Par conséquent, il est souhaitable que les méthodes de synchronisation tiennent compte de ces contraintes.

Objectifs de la thèse

L'objectif majeur de cette thèse est d'apporter des réponses aux problèmes rencontrés dans les applications de communication basées sur la synchronisation de systèmes chaotiques soumis à des contraintes de communication (retard, incertitudes paramétriques et perturbations externes), en utilisant des techniques issues de l'automatique, notamment la théorie des observateurs non linéaires. Les résultats attendus se résument comme suit :

- Développement de nouvelles méthodes de synchronisation des systèmes chaotiques d'ordre entier et d'ordre fractionnaire en présence des incertitudes et du retard dans le canal de transmission (retard sur la mesure) en utilisant les observateurs à mode glissant d'ordre supérieur.
- Synthèse d'un prédicteur d'état d'ordre entier et d'ordre fractionnaire permettant d'atténuer et éliminer les effets du retard et ainsi d'obtenir les estimations des états à l'instant présent.
- Synthèse d'une méthode de synchronisation d'un système chaotique de Takagi-Sugeno (TS) à base d'un observateur proportionnel intégral (PI) avec application à la transmission sécurisée d'un message audio.

Chapitre 1

Systèmes chaotiques

1.1 Introduction :

la théorie du chaos s'intéresse aux phénomène qui semble irréguliers et aléatoire mais qui sont régi par des lois déterministe .henri poincaré a été le premier a observe ce lors d'étude consacrées a la stabilité du système solaire.après cella de nombreux chercheur se sont vivement intéressés a la théorie du chaos ,ainsi qu'aux méthodes pour le contrôlé .un phénomène chaotique est défini comme un phénomène qui généralement un comportement particulier et imprévisible d'un système dynamique détermine no linéaire .la théorie du chaos se trouve être utile dans de nombreux domaines tels que système finassiers ...
le chaos présente un certain nombre de caractéristique notamment la sensibilité aux conditions initiales et l'imprévisible ,ce qui rend le système chaotique très intéressants pour cryptage des données .

1.1.1 Les systèmes dynamiques :

En général,un syst ?me dynamique d ?crit des ph ?nom ?nes qui ?voluent au cours du temps. Le terme syst ?me fait r ?f ?rence ? un ensemble de variables d ? ?tat (dont la valeur ?volue au cours du temps) et aux interactions entre ces variables. L ?ensemble des variables d ? ?tat d ?un syst ?me permet de construire un espace math ?matique appel ? espace de phase. Ce dernier, qui est une structure correspondante ? toutes les trajectoires possibles du syst ?me consid ?r ?. ces derniers sont class ?s en deux cat ?gories :

les syst ?mes dynamiques continu :

Un syst ?me dynamique continu d ?signe un syst ?me dont l' ?volution dans le temps est d ?crite de mani ?re continue par des ?quations diff ?rentielle sans interruption ni saut. Les ?tats du syst ?me varient de fa ?on continue sur un intervalle non disjoint, d ?termin ? par les variables d' ?tats et les param ?tres du syst ?me.Ce dernier est d ?crit par un syst ?me d' ?quations diff ?rentielles ordinaires du premier ordre de la forme :

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

Ce qui est une ?criture abr ?g ?e du syst ?me suivant :

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

ou :

- $f : \mathbb{R}^+ \times \mathbb{R}^n \to \mathbb{R}^n$ d ?signe la dynamique du syst ?me.
- $x(t) \in \mathbb{R}^n$ c'est le vecteur d' ?tat de dimension n.
- $t \in \mathbb{R}^+$ designe le temps.

les systemes dynamiques discret :

Un syst ?me dynamique discret est un mod ?le math ?matique qui d ?crit l' ?volution d'un syst ?me au fil du temps, mais avec des pas de temps discrets.

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

o ? :

– $g : \mathbb{Z}^+ \times \mathbb{R}^n \to \mathbb{R}^n$ designe la dynamique du systeme en temps discret.

1.1.2 Les systemes autonomes :

Un syst ?me autonome est un syst ?me dynamique non lin ?aire qui ne d ?pend pas explicitement du temps. Il est donn ? comme suit :

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

Contrairement aux syst ?mes non autonomes, les syst ?mes autonomes ne sont pas influenc ?s par le temps initial. En d'autres termes, dans un syst ?me autonome, n'importe quel moment peut ?tre consid ?r ? comme un point de d ?part, et tout ?tat x(t) du syst ?me peut ?tre consid ?r ? comme un ?tat initial. Cette caract ?ristique signifie que l' ?volution d'un syst ?me autonome est enti ?rement d ?termin ?e par son ?tat actuel, sans n ?cessiter de r ?f ?rence ? un temps sp ?cifique

1.1.3 la th ?orie du chaos :

La th ?orie du chaos fait partie des sciences les plus r ?centes est devenue l'un des domaines les plus avanc ?s dans la recherche contemporaine. La th ?orie du chaos est d ?finie comme une ?tude des syst ?mes dynamiques non lin ?aires complexes et les syst ?mes complexes qui sont exprim ?s par des r ?currences et des algorithmes math ?matiques et qui sont dynamiques (non constants) et non p ?riodique.Elle inclut l' ?tude qualitative et quantitative d'un comportement instable non p ?riodique et al ?atoire des syst ?mes dynamiques non lin ?aires d ?terministes.

1.1.4 Le chaos :

Bien qu'il n'existe pas de d ?finition universelle du chaos adopt ?e dans la litt ?rature, on peut le d ?crire comme un ph ?nom ?ne qui peut se manifester dans les syst ?mes dynamiques d ?terministes non lin ?aires. Ces syst ?mes se caract ?risent par une ?volution qui semble al ?atoire et par un aspect fondamental d'instabilit ? appel ? sensibilit ? aux conditions initiales. Cette sensibilit ? signifie que de petites variations dans les conditions initiales peuvent conduire ? des r ?sultats totalement diff ?rents ? mesure que le syst ?me ?volue dans le temps, ce qui le rend impr ?dictible en pratique ? long terme.

o ? :

- $g : \mathbb{Z}^+ \times \mathbb{R}^n \to \mathbb{R}^n$ **designe la dynamique du systeme en temps discret.**

Pour une meilleure compr ?hension des syst ?mes chaotiques li ?s ? ce ph ?nom ?ne, nous nous appuyons sur plusieurs d ?finitions, propri ?t ?s et domaines d'application. Ces concepts nous aident ? explorer et ? analyser ces syst ?mes qui d ?fient souvent nos intuitions sur la pr ?dictibilit ? et le comportement d ?terministe. Un syst ?me dynamique chaotique inclut les caract ?ristiques, qui lui sont inh ?rentes, pr ?sent ?es comme suit :

1.4.1.1 Non-lin ?arit ? : L'analyse d ?taill ?e des syst ?mes dynamiques non lin ?aires d ?montre de mani ?re ?vidente que la caract ?ristique fondamentale du chaos exclut la possibilit ? d'un syst ?me lin ?aire d' ?tre chaotique.

1.4.1.2 Le d ?terminisme : Le d ?terminisme se r ?f ?re ? la capacit ? de pr ?dire le futur d'un ph ?nom ?ne en se basant sur son ?tat pass ? ou pr ?sent. L'instabilit ? du comportement d'un syst ?me chaotique est directement li ?e ? ses non-lin ?arit ?s. Contrairement aux ph ?nom ?nes al ?atoires o ? il est absolument impossible de pr ?dire la trajectoire d'une particule, un syst ?me chaotique suit des lois fondamentales d ?terministes, ?cartant toute notion de probabilit ?.

1.4.1.3 L'aspect al ?atoire : Tous les ?tats d'un syst ?me chaotique d ?voilent des aspects al ?atoires.

1.4.1.4 Sensibilit ? aux conditions initiales : Une caract ?ristique fondamentale des syst ?mes chaotiques est leur sensibilit ? aux conditions initiales. Cela signifie que deux points de d ?part,

aussi proches soient-ils, auront des ?volutions tellement divergentes qu'il sera impossible d' ?tablir une relation entre leurs trajectoires. M ?me la plus petite erreur ou impr ?cision dans la condition initiale rend impossible la pr ?diction de la trajectoire r ?elle du syst ?me ? tout moment, emp ?chant ainsi toute pr ?diction autre que statique de son ?volution ? long terme. Malgr ? le caract ?re d ?terministe de ces syst ?mes, leur comportement ? long terme reste impr ?visible. Une des propri ?t ?s essentielles du chaos est donc bien cette sensibilit ? aux conditions initiales que l'on peut caract ?riser en mesurant des taux de divergence des trajectoires.

1.4.1.5 Attracteur ?trange : Les attracteurs, fondamentaux en dynamique des syst ?mes, repr ?sentent les ?tats vers lesquels convergent les trajectoires de l'espace des phases d'un syst ?me. Ils d ?peignent les configurations vers lesquelles le syst ?me ?volue, ind ?pendamment de ses conditions initiales. Dans un espace des phases bidimensionnel, les attracteurs peuvent ?tre des points fixes ou des cycles limites.

Pour les attracteurs r ?guliers, caract ?ristiques des syst ?mes non chaotiques, les trajectoires d ?butant ? proximit ? les unes des autres dans l'espace des phases restent continuellement proches. Cette stabilit ? permet de pr ?dire de mani ?re fiable l' ?volution de ces syst ?mes ? partir de conditions initiales pr ?cises.

Cependant, il convient de noter qu'un syst ?me ? deux variables ne peut engendrer naturellement des mouvements chaotiques. L'introduction d'une troisi ?me variable est requise pour que, dans des circonstances appropri ?es, le syst ?me devienne instable. ? l'origine du chaos d ?terministe se trouve l'attracteur ?trange, une structure complexe et fractale.

Ainsi, l'attracteur ?trange occupe une place centrale dans l' ?tude du chaos d ?terministe. Contrairement aux attracteurs r ?guliers permettant une pr ?diction pr ?cise ? partir de conditions initiales connues, les attracteurs ?tranges r ?v ?lent une complexit ? infinie. Les trajectoires convergentes vers un attracteur ?trange semblent chaotiques, mais restent confin ?es dans un espace d ?fini. Cette caract ?ristique implique que de l ?g ?res variations initiales peuvent entra ?ner des divergences exponentielles avec le temps, rendant la pr ?diction ? long terme impossible malgr ? des conditions initiales minutieusement d ?finies.

1.1.5 Identification du chaos :

?tant donn ?e la complexit ? de la r ?solution des syst ?mes chaotiques de mani ?re analytique, des m ?thodes num ?riques sont souvent utilis ?es. Ainsi, dans cette partie, nous abordons quelques techniques qui nous permettent d'identifier l' ?volution du comportement chaotique d'un syst ?me dynamique et ses caract ?ristiques.

1.5.1 exposants Lyapunov : L' ?volution d'un flot chaotique est complexe ? comprendre en raison de la divergence rapide des trajectoires sur l'attracteur. C'est pourquoi l'estimation ou la mesure de la vitesse de divergence ou de convergence est souvent entreprise.Alexandre Lyapunov a d ?velopp ? une quantit ? permettant de mesurer la divergence des trajectoires qui sont voisines au d ?part. Cette quantit ? est appel ?e "exposant de Lyapunov" . L'exposant de Lyapunov est utilis ? pour ?valuer le niveau de stabilit ? d'un syst ?me et permet de quantifier la sensibilit ? aux conditions initiales d'un syst ?me chaotique. Le nombre d ?exposants de Lyapunov est ?gal ? la dimension de l ?espace des phases et ils sont g ?n ?ralement index ?s du plus grand au plus petit λ_1 ;λ_2 ;λ_3...

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

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

avec $x_j = f_j(x_0)$

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

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

ou λ est l'exposant de Lyapunov.

Les exposants de Lyapunov sont une g ?n ?ralisation des valeurs propres pour les points fixes et des multiplicateurs caract ?ristiques pour les solutions p ?riodiques. Pour un attracteur non chaotique, tous les exposants de Lyapunov sont inf ?rieurs ou ?gaux ? z ?ro, et leur somme est n ?gative. Un attracteur ?trange poss ?de toujours au moins trois exposants de Lyapunov, parmi lesquels au moins un est positif .Les divers crit ?res permettant de caract ?riser la dynamique d ?un syst ?me non lin ?aire sont regroup ?s dans le tableau ci-dessous :

R ?gime permanent	Attracteur	Exposants de Lyapunov
Point d ? ?quilibre	Point	$0>\lambda_1\geq...\geq\lambda_n$
P ?riodique	Courbe ferm ?e	$\lambda_1=0, \quad 0>\lambda_2\geq...\geq\lambda_n$
Quasi-p ?riodique	Tore	$\lambda_1=...=\lambda_i=0, \quad 0>\lambda_i+1\geq...\geq\lambda_n$
Chaotique	Fractal	$\lambda_1>0, \quad \lambda_2>0\geq...\lambda_n$
Hyperchaotique	Fractal	$\lambda_1>\lambda_2>0, \quad 0>\lambda_3\geq...\geq\lambda_n$

TABLE 1.1: Diff ?rents r ?gimes d ?un syst ?me dynamique non lin ?aire.

1.5.2 L'aspect al ?atoire : Une fa ?on simple de caract ?riser le chaos consiste ? calculer le spectre de puissance, qui repr ?sente la r ?partition de la puissance le long de l ?axe des fr ?quences, de l ? ?volution temporelle d ?une des variables du syst ?me . Tout signal x(t), dans le cas continu (x(k) dans le cas discret), peut en effet ?tre repr ?sent ? comme une superposition de composantes p ?riodiques. Ces derni ?res sont toujours exprim ?es en terme de fonctions ?l ?mentaires sinus et cosinus. La d ?termination des amplitudes relatives de ces composantes constitue l ?objet de l ?analyse spectrale. Le spectre de puissance est simplement la transform ?e de Fourier de la fonction d ?auto corr ?lation.

1.5.3 Bifurcation : La th ?orie des bifurcations est l' ?tude math ?matique des changements qualitatifs ou topologiques de la structure d'un syst ?me dynamique. Une bifurcation se produit lorsqu'il y a un changement quantitatif ou qualitatif dans la solution d'un syst ?me dynamique en modifiant les param ?tres auxquels il d ?pend. Plus pr ?cis ?ment, il s'agit de la disparition ou du changement de stabilit ?, ou de l'apparition de nouvelles solutions. Il existe deux types de bifurcations : locale et globale. Chacune de ces bifurcations est caract ?ris ?e par une forme normale, telles que la bifurcation pli, la bifurcation transcritique, la bifurcation fourche, la bifurcation flip, la bifurcation Neimark-Sacker, la bifurcation n ?ud-col, et la bifurcation doublement de p ?riode. L' ?volution vers le chaos dans les syst ?mes dynamiques peut ?tre observ ?e en ajustant la valeur d'un param ?tre, que ce soit par des ?tudes th ?oriques ou exp ?rimentales. Trois sc ?narios th ?oriques principaux d ?crivent ces transitions vers le chaos :

1.Le doublement de p ?riode : Pour un syst ?me p ?riodique, une augmentation du param ?tre peut entra ?ner un ph ?nom ?ne de doublement de sa p ?riode. Cette p ?riode est ensuite multipli ?e par 2, 4, 8, 16, et ainsi de suite. ? chaque ?tape de doublement, l'augmentation n ?cessaire du param ?tre devient de plus en plus petite. ? partir d'une certaine valeur critique du param ?tre, le syst ?me bascule soudainement dans un comportement chaotique. Lorsque la p ?riode du syst ?me tend vers l'infini, les mouvements deviennent alors compl ?tement chaotiques.

2.L'intermittence vers le chaos : Ce sc ?nario d ?crit un ph ?nom ?ne o ? un mouvement p ?riodique stable est perturb ? par des ?pisodes de turbulence. En augmentant progressivement le param ?tre de contr ?le, ces ?pisodes de turbulence deviennent de plus en plus fr ?quents. ? un certain seuil, la turbulence devient dominante et le syst ?me entre alors dans un ?tat chaotique. Cela peut ?tre illustr ? par des exemples tels que les syst ?mes m ?t ?orologiques, o ? des p ?riodes de calme sont suivies par des temp ?tes de plus en plus fr ?quentes jusqu' ? ce que la turbulence pr ?domine.

3.La quasi-p ?riodicit ? : Dans ce sc ?nario, un syst ?me p ?riodique peut pr ?senter des signes de nouvelles fr ?quences qui ne sont pas rationnellement li ?es ? la premi ?re. Lorsque le param ?tre est ajust ?, une troisi ?me fr ?quence peut appara ?tre, et ainsi de suite. Ces fr ?quences suppl ?mentaires peuvent g ?n ?rer des motifs complexes dans le comportement du syst ?me. ? me-

sure que le param ?tre est modifi ? davantage, le syst ?me finit par entrer dans un ?tat chaotique o ? les mouvements ne suivent plus de sch ?ma p ?riodique pr ?visible.

Ces sc ?narios repr ?sentent des m ?canismes cruciaux pour comprendre comment les syst ?mes dynamiques ?voluent vers le chaos. Ils sont observ ?s dans divers domaines, de la m ?t ?orologie ? la physique des oscillateurs, et sont essentiels pour appr ?hender les fondements du chaos d ?terministe.

1.1.6 Exemple illustrant des syst ?mes chaotique :

Dans la recherche de signaux complexes et non lin ?aires, diff ?rents types de syst ?mes dynamiques sont utilis ?s pour g ?n ?rer des comportements chaotiques. Il est int ?ressant de noter que dans le cas continu, un syst ?me chaotique autonome, c'est- ?-dire sans entr ?e ni retard, doit poss ?der au moins trois ?tats pour exhiber des propri ?t ?s chaotiques. En revanche, dans le domaine discret, m ?me un syst ?me dynamique ? une seule variable d' ?tat peut manifester des comportements chaotiques, comme c'est le cas avec la fonction logistique.

Pour illustrer ces concepts, nous pr ?sentons ci-dessous des exemplesde systemes chaotique en continu et en discret. Ces syst ?mes sont des mod ?les largement ?tudi ?s et utilis ?s pour comprendre et simuler le chaos d ?terministe.

1.6.1 Cas continu :

a.Syst ?me chaotique de Lorenz : Le mod ?le de Lorenz, d ?velopp ? dans les ann ?es 1960, repr ?sente une avanc ?e significative dans la compr ?hension des syst ?mes dynamiques chaotiques, en particulier dans le contexte de la mod ?lisation des ph ?nom ?nes m ?t ?orologiques tels que la convection atmosph ?rique. L'approche de Lorenz ?tait d ?lib ?r ?ment orient ?e vers la compr ?hension plut ?t que vers la pr ?cision pr ?visionnelle. Il a entrepris de simplifier les ?quations m ?t ?orologiques complexes pour obtenir un mod ?le plus accessible, mais qui capture toujours l'essence de la dynamique chaotique des masses d'air. Plut ?t que de s'enliser dans la complexit ? des ?quations de Navier-Stokes, qui d ?crivent les mouvements des fluides avec une grande pr ?cision mais sont difficiles ? r ?soudre, Lorenz a choisi une voie plus abordable. Il a r ?duit ces ?quations ? un syst ?me plus g ?rable d' ?quations diff ?rentielles, d ?sormais connu sous le

nom d' ?quations de Lorenz :

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

avec :

- x,y et z : sont des variables respectivement proportionnelles aux amplitudes du champ de vitesse, et du champ de temp ?rature.
- t : Le temps.
- σ Le coefficient de Prandtl, qui est un nombre sans dimension utilis ? pour caract ?riser la viscosit ? du fluide et le taux de transfert de chaleur par conduction par rapport au transfert de chaleur par convection.
- ρ : Le nombre de Rayleigh, un autre nombre sans dimension qui caract ?rise le gradient de temp ?rature ? travers le fluide.
- β : Un param ?tre qui mesure le rapport des variations de densit ? du fluide ? la temp ?rature. C'est le coefficient de couplage du mod ?le.

On prend :(σ= 10 ;ρ = 28 ;β= 8/3) ; Des valeurs pour lesquelles le syst ?me pr ?sente un comportement chaotique, et pour les conditions initiales suivantes :x0 = 10 ;y0 = 10 ;z0 = 20.

FIGURE 1.1: ?volution dans le temps, pour deux conditions initiales tr ?s proches.

FIGURE 1.2: Aspect al ?atoire des ?tats du syst ?me de Lorenz.

FIGURE 1.3: L'attracteur de Lorenz

FIGURE 1.4: Exposants de Lyapunov du syst ?me de Lorenz

La figure pr ?sente les exposants de Lyapunov du syst ?me de Lorenz o ? $\lambda_1 = 1.50564$, $\lambda_2 = -0.000802294$et $\lambda_3 = -22.5048$.

FIGURE 1.5: Spectre de puissance de la variabe x du syst ?me de Lorenz.

FIGURE 1.6: Diagramme de bifurcation de Lorenz.

b.Syst ?me chaotique de R ?ssler : Syst ?me de R ?ssler a ?t ? propos ? par l ?Allemand Otto R ?ssler,est li ? ? l ? ?tude de l ? ?coulement des fluides ; il d ?coule des ?quations de Navier-Stokes. Les ?quations de ce syst ?me ont ?t ? d ?couvertes ? la suite de travaux en cin ?tique chimique.Les ?quations de ce syst ?me sont les suivantes :

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

o ? :

- x,y,z est le vecteur d' ?tat.
- a,b,c sont les param ?tres du syst ?me de R ?ssler .

Le syst ?me de R ?ssler montre un comportement chaotique pour a= 0.2 , b= 5.7, c= 0.2, avec les conditions initiales x0=0.1 ;y0=0.1 ;z0=0.1.

FIGURE 1.7: Aspect al ?atoire

FIGURE 1.8: ?volution dans le temps, pour deux conditions initiales tr ?s proches(sensibilit ? aux conditions initiales).

FIGURE 1.9: Attracteur de R ?ssler

FIGURE 1.10: Diagramme de bifurcation du syst ?me de R ?ssler.

FIGURE 1.11: Exposants de Lyapunov du syst ?me de Rossler.

La figure pr ?sente les exposants de Lyapunov du syst ?me de Rossler o ? λ_1 =0.039206, λ_2=0.0020676 et λ_3=-9.8911.

1.1.7 Cas discret :

a.Syst ?me de Henon : Le syst ?me chaotique de H ?non est un exemple embl ?matique de la complexit ? que peut pr ?senter un syst ?me dynamique non lin ?aire. Propos ? par Michel H ?non en 1976, ce mod ?le se compose d'un ensemble d' ?quations it ?ratives simples mais produisant des comportements extraordinaires.Les ?quations de Henon sont les suivantes :

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

o ? x et y repr ?sentent les coordonn ?es d'un point dans un espace bidimensionnel, et a et b sont des param ?tres contr ?lant le comportement du syst ?me. Ce mod ?le illustre comment de petites variations dans les conditions initiales peuvent conduire ? des trajectoires compl ?tement diff ?rentes, caract ?risant ainsi le comportement chaotique.

FIGURE 1.12: Aspect al ?atoire.

FIGURE 1.13: Sensibilit ? aux conditions initiales de l ? ?tat x du syst ?me de H ?non.

FIGURE 1.14: Attracteur de Henon.

FIGURE 1.15: Diagramme de bifurcation du syst ?me de H ?non.

FIGURE 1.16: Exposants de Lyapunov du syst ?me de H ?non.

La figure pr ?sente les exposants de Lyapunov du syst ?me de Rossler o ? λ_1 =0.42311, λ_2=-1.6271.

FIGURE 1.17: Spectre de puissance de la variable x du syst ?me de H ?non.

1.2 Conclusion :

En conclusion de ce chapitre d ?di ? aux syst ?mes chaotiques, il est clair que leur ?tude nous r ?v ?le une dynamique complexe, o ? l'apparent d ?sordre cache des r ?gles d ?terministes. Leur sensibilit ? aux conditions initiales peut engendrer des trajectoires divergentes et impr ?visibles, remettant en question nos notions de stabilit ? et de pr ?dictibilit ?. L'importance de comprendre ces syst ?mes va au-del ? de la th ?orie, puisqu'ils trouvent des applications dans divers domaines, de la physique ? la biologie en passant par l' ?conomie. Cette ?tude a ?galement conduit au d ?veloppement de nouvelles m ?thodes math ?matiques et informatiques pour les mod ?liser, ouvrant ainsi de nouvelles perspectives de recherche et d'innovation. En fin de compte, les syst ?mes chaotiques nous rappellent que m ?me dans le chaos, il existe un ordre sous-jacent ? d ?couvrir, stimulant ainsi notre curiosit ? intellectuelle et alimentant notre qu ?te de comprendre la complexit ? qui r ?git le monde qui nous entoure.

Chapitre 2

synchronisation des systèmes chaotiques

2.1 Introduction

L'application du chaos à la transmission numérique suscite un intérêt croissant dans la littérature depuis les travaux de Pecora et Carroll sur la synchronisation chaotique. Ils ont démontré que, bien que les systèmes chaotiques soient extrêmement sensibles aux conditions initiales, deux systèmes dynamiques identiques configurés en maître et esclave peuvent se synchroniser parfaitement sans bruit. Cette synchronisation est possible grâce au caractère déterministe du chaos, bien que les trajectoires chaotiques ressemblent à des signaux aléatoires. Les recherches sur l'utilisation du chaos pour la transmission, observées au cours de la dernière décennie, sont principalement motivées par des préoccupations liées à la sécurité de l'information.

En effet, en servant de clé de chiffrement, le code chaotique offre une faible probabilité de détection des symboles d'information et constitue également un moyen potentiel de minimiser l'interruption du signal. Parmi les avantages des systèmes de transmission chaotiques, on cite souvent un meilleur partage des canaux et une moindre complexité matérielle dans un environnement à accès multiple (CDMA), car les circuits traditionnels d'acquisition et de suivi des missions peuvent théoriquement être supprimés. La transmission chaotique d'informations sous forme numérique peut être réalisée par le principe de commutation (Chaos Shift Keying) : les deux systèmes chaotiques A et B codent respectivement les bits 0 et 1 au niveau de l'émetteur. Lors de la réception, le signal pilote les deux systèmes esclaves A et B, et les symboles transmis

peuvent être détectés en comparant les erreurs de synchronisation des deux systèmes maître et esclave.

Pecora et Carroll ont montré que deux trajectoires chaotiques peuvent être synchronisées (la distance entre elles tend asymptotiquement vers zéro). Cependant, en pratique, ce résultat n'est pas totalement correct en raison du bruit de canal. Seules des erreurs de synchronisation limitées sont à prévoir. Recevoir le signal avec un taux d'erreur acceptable devient un véritable défi en présence de trajets multiples et/ou de non-stationnarité des canaux, comme c'est le cas avec les communications sans fil. Les méthodes de synchronisation généralisées sont exprimées comme une relation fonctionnelle entre deux systèmes chaotiques couplés. Ces méthodes sont considérées comme des généralisations de méthodes entièrement synchronisées pour synchroniser des systèmes chaotiques généralement différents.

La synchronisation a été développée comme une solution au problème de synthèse de l'observateur. Ce type de problème est classique dans le domaine de l'automatique, et de nombreux résultats liés au contrôle du chaos sont utilisés. Plus récemment, des approches innovantes ont exploré les systèmes discrets et hybrides, soit en tant que systèmes à synchroniser, soit dans le cadre d'une méthode de synchronisation. Enfin, nous avons trouvé une proposition de méthode efficace pour quantifier la synchronisation, autrement dit, une méthode pour évaluer la qualité et la sensibilité des méthodes de synchronisation.

2.1.1 Définition :

La synchronisation se caractérise par deux systèmes se comportant de la même manière au même moment. Cela signifie que chaque système évolue en suivant le comportement de l'autre.

2.1.2 Méthodes de synchronisation chaotique :

Il existe plusieurs méthodes de synchronisation chaotique. Ci-dessous, nous présentons les méthodes les plus performantes et les plus couramment utilisées.

2.3.1 Synchronisation par répartition du système :

Certains systèmes chaotiques possèdent la propriété d'auto-synchronisation, c'est-à-dire qu'ils peuvent être décomposés en deux sous-systèmes, l'un maître, l'autre esclave. Ces sous-systèmes

FIGURE 2.1: Principe de Pecora et Carroll.

peuvent se synchroniser sous l'effet d'un couplage avec un signal commun. Dans le schéma de synchronisation proposé par Pecora et Carroll, un système chaotique est représenté par :

$$\dot{x} = (f(x)) \tag{2.1}$$

Avec $y = h(x)$, une sortie scalaire est décomposée en deux sous-systèmes dont les états sont x_1 et x_2 respectivement :

$$\dot{x1} = f1(x1, x2) \tag{2.2}$$

$$\dot{x2} = f2(x2, y) \tag{2.3}$$

Le système est partitionné de façon à ce que les exposants de Lyapunov conditionnels du sous-système soient négatifs. Si tous les exposants de Lyapunov conditionnels sont négatifs, alors la trajectoire $x_2(t)$ est asymptotiquement stable. Cela signifie que les états de plusieurs copies du sous-système se synchroniseront à l'aide du même signal $y(t)$.
En particulier, on considère le système décrit par :

$$\dot{x2} = f2(x2, y) \tag{2.4}$$

Si les exposants de Lyapunov conditionnels de ce système sont tous négatifs et si $x_2(0)$ est suffisamment proche de $x_2(0)$, alors l'état x_2 converge asymptotiquement vers x_2, c'est-à-dire :

$$\lim_{t\to\infty} (kx^2(t) - x^2(t)) = 0$$

2.3.2 Synchronisation par boucle fermée

On l'appelle aussi « méthode de synchronisation par contre-réaction ». Elle consiste à utiliser l'erreur entre l'émetteur et le récepteur pour corriger le comportement du récepteur afin de réaliser la synchronisation.

Supposons les deux systèmes suivants :
Émetteur :

FIGURE 2.2: La synchronisation par la boucle fermée.

FIGURE 2.3: Synchronisation impulsive.

$$\begin{aligned} \dot{x} &= f(x) \\ y &= h(x) \end{aligned} \tag{2.5}$$

Récepteur :

$$\begin{aligned} \dot{\hat{x}} &= f(\hat{x}) + g(y - \hat{y}) \\ \hat{y} &= h(\hat{x}) \end{aligned} \tag{2.6}$$

Avec g étant une fonction de l'erreur entre y et $\hat{y}$, g est choisie afin de garantir la synchronisation entre l'émetteur et le récepteur. Ce type de récepteur peut être considéré comme la conception d'un observateur. La figure suivante illustre la synchronisation par la boucle fermée.

2.3.3 Synchronisation impulsive :

Dans les schémas de transmission classiques, l'un des états du système dynamique est généralement transmis au récepteur pour réaliser la synchronisation. Toutefois, afin de réduire la redondance du signal transmis, une méthode appelée synchronisation impulsive a été proposée. Cette technique consiste à diviser le signal de transmission en de courts intervalles, ou impulsions.

Le signal de sortie du système maître est transmis au système esclave sous forme d'impulsions à des instants discrets prédéfinis. À ces instants, les variables d'état subissent un saut et un changement d'état. Son schéma est illustré par cette figure :

2.3.4 Synchronisation par inversion du système :

Jusqu'à présent, toutes les approches mentionnées visent à synchroniser uniquement les états du système, sans aborder l'estimation des entrées inconnues du système. Cependant, la capacité à estimer ces entrées inconnues est évidemment essentielle dans le contexte de la transmission

FIGURE 2.4: Synchronisation par l'inversion du système.

chaotique de données, car ces entrées inconnues correspondent généralement au message confidentiel.

$x \in \mathbb{R}^n$ est le vecteur des états du système d'ordre n, tandis que R^m est le vecteur des entrées inconnues d'ordre m. Les fonctions $f : \mathbb{R}^n \to \mathbb{R}^n \times \mathbb{R}^n$, $h : \mathbb{R}^n \to \mathbb{R}^p$, et $g : \mathbb{R}^n \to \mathbb{R}^{n \times m}$ sont des fonctions vectorielles analytiques.

Le vecteur d'entrée du récepteur correspond au vecteur de sortie de l'émetteur. Il est donc essentiel de concevoir le récepteur de manière à ce que son vecteur de sortie converge au moins asymptotiquement vers le vecteur d'entrée de l'émetteur.

2.3.5 Synchronisation généralisée

La synchronisation généralisée est une extension du concept de synchronisation identique. Les systèmes sont considérés comme synchronisés, au sens généralisé, s'il existe une transformation M telle que :

$$\lim_{t \to \infty} \|k x_0(t) - M x(t)\| = 0$$

indépendamment des conditions initiales.

Si la fonction M est inversible, alors $M^{-1}(x_0)$ fournit une estimation de l'état x. Cependant, si cette transformation n'est pas inversible, il devient impossible d'estimer x. Cela représente un inconvénient majeur pour certaines techniques de communication, qui utilisent l'état de l'émetteur pour déchiffrer le message transmis.

2.3.6 Synchronisation retardée :

L'état du système esclave converge vers l'état décalé dans le temps du système maître, c'est-à-dire :

$$\lim_{t \to 0} k\, x_0(t) - x(t - \tau) = 0$$

où τ est un retard positif.

FIGURE 2.5: Principe de la synchronisation à base d'observateur.

FIGURE 2.6: Principe d'un observateur.

2.3.7 Synchronisation projective :

L'état du système récepteur se synchronise avec un multiple de l'état du système émetteur. Il existe donc a et τ tels que :

$$|n\Phi_1 - m\Phi_2| < c$$

où m et n sont des entiers naturels, et c est une constante positive.

Cette notion classique de synchronisation a été étendue aux systèmes chaotiques. Pour définir la phase d'un système chaotique, on peut mentionner l'approche analytique. Un signal analytique $\Psi(t)$ est une fonction complexe définie par :

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

2.3.8 Synchronisation à base d'observateurs

La synchronisation peut également être réalisée en employant un observateur. Le système maître est un système chaotique quelconque, et le système esclave est un observateur d'état correspondant.

Pour ce principe, nous disons que l'émetteur et le récepteur se synchronisent si le système $\dot{\hat{x}} = \hat{f}(x, \hat{u})$ défini au niveau du récepteur est un observateur convergent pour le système $\dot{x} = f(x, u)$ (défini au niveau de l'émetteur). Autrement dit, le problème de synchronisation revient à déterminer une fonction $\hat{f}$ telle que :

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

Exemples d'observateurs pour la synchronisation : **Cas Continu** : On peut citer l'observateur de Luenberger, ainsi que l'observateur à entrée inconnue. **Cas Discret** : On peut citer l'observateur retardé étape par étape appelé également *Observateur Dead Beat*. **Définition** : Un observateur est un système dynamique qui permet la reconstruction de l'état d'un système, à partir de ses entrées, de ses sorties, et de la connaissance de son modèle dynamique.

FIGURE 2.7: Schémas de couplage unidirectionnel.

FIGURE 2.8: Schémas de couplage bidirectionnel.

2.1.3 Types de synchronisation

La synchronisation des systèmes chaotiques peut être classée en deux types, en fonction de la manière dont les deux systèmes chaotiques sont couplés.

2.4.1 Synchronisation unidirectionnelle

Dans la synchronisation unidirectionnelle, le couplage entre deux systèmes identiques a et b est réalisé à l'aide d'un élément fonctionnant dans un seul sens.

2.4.2 Synchronisation bidirectionnelle

Dans le couplage bidirectionnel, l'élément de couplage permet l'échange d'énergie dans les deux sens.

2.1.4 Techniques de cryptage par chaos :

Pour introduire les informations transmises de l'émetteur au récepteur dans le chiffrement, on choisit une fonction chaotique. Ensuite, on superpose le signal chaotique au flux de données à transmettre selon l'une des techniques choisies pour le cryptage par chaos. Ces techniques sont présentées ci-dessous :

2.5.1 Cryptage par addition :

La méthode de masquage du chaos est la première solution proposée dans la littérature pour appliquer le chaos à la sécurisation des communications. L'idée est d'additionner le signal d'information $s(t)$ directement au signal chaotique $y(t)$, puis de le récupérer par synchronisation chaotique. L'émetteur et le récepteur utilisent le même système, sauf que le récepteur est contrôlé par le signal d'émission pour la synchronisation. Ceci est illustré dans la figure suivante :

Du fait de la synchronisation chaotique en sortie du système dynamique récepteur, le signal peut être plus proche du signal chaotique d'origine $y(t)$ que de $y(t) + s(t)$. Ainsi, une simple

FIGURE 2.9: Cryptage par addition(masquage additif)

FIGURE 2.10: Cryptage par commutation.

FIGURE 2.11: Cryptage par commutation.

différence permet d'obtenir une approximation $s(t)$ du signal d'information initial. La présence de bruit important dans le canal de communication affecte évidemment fortement les performances du système.

Cryptage par commutation (Chaos Shift Keying - CSK) :

Cette méthode, également connue sous le nom de Chaos Shift Keying en anglais, est utilisée pour transmettre des messages binaires. L'émetteur est constitué de deux systèmes chaotiques, dont l'un envoie sa sortie sur la ligne de transmission pour chaque niveau de message $m(t)$ (0 ou 1). Ainsi, le signal transmis bascule entre deux attracteurs étranges. Le récepteur est également composé de deux systèmes chaotiques identiques à ceux de l'émetteur, et un bloc de comparaison peut enregistrer la valeur du message notée $m_0(t)$. Le schéma suivant illustre cette méthode de chiffrement.

La technique utilise des messages contenant des informations pour moduler les paramètres d'un émetteur chaotique. Le contrôleur adaptatif est responsable du maintien de la synchronisation au niveau du récepteur tout en suivant les modifications des paramètres de modulation. Le schéma correspondant est illustré dans la figure ci-dessous. Au niveau de l'émetteur, le fait qu'un (ou plusieurs) paramètres soient modulés oblige la trajectoire à changer constamment d'attracteur, rendant ainsi le signal émis plus complexe que le signal chaotique normal. Cependant, la manière dont le message est injecté et donc la fonction de modulation paramétrique, ne peut éliminer le caractère chaotique du signal envoyé au récepteur. Il convient de souligner que cette technique tire pleinement parti des propriétés des systèmes chaotiques et n'a pas d'équivalent dans les systèmes de communication traditionnels. Cependant, le chiffrement par modulation s'est avéré vulnérable à certaines attaques.

2.3.4 Cryptage par inclusion :

Cette technique de cryptage, illustrée ci-dessous, consiste à intégrer le message dans la dynamique de l'émetteur. La récupération de l'information se fait principalement par deux techniques : soit en s'appuyant sur des observateurs à entrées inconnues, soit en inversant le système émetteur.

FIGURE 2.12: Cryptage par modulation paramétrique.

Cette méthode présente de nombreux avantages et reste largement utilisée en pratique.

2.2 Conclusion

La synchronisation des systèmes chaotiques représente une avenue prometteuse pour des applications de transmission numérique sécurisée. Les travaux pionniers de Pecora et Carroll ont démontré que malgré la nature imprévisible du chaos, une synchronisation précise entre deux systèmes dynamiques identiques est réalisable. Cette synchronisation, basée sur des mécanismes déterministes, ouvre la voie à des méthodes de transmission robustes et sécurisées, particulièrement cruciales dans un contexte où la sécurité de l'information est primordiale.
L'utilisation du chaos pour le cryptage offre plusieurs avantages, notamment une faible probabilité de détection des symboles d'information et une résilience accrue face aux perturbations du signal. Les différentes techniques de synchronisation chaotique présentées dans ce chapitre offrent un large éventail d'approches pour atteindre cet objectif, de la synchronisation par répartition du système à la synchronisation par inclusion du message dans la dynamique de l'émetteur.
Dans le prochain chapitre, nous aborderons la conception d'un cryptosystème destiné au cryptage d'une image.

Chapitre 3

Une application sur la cryptologie de l'image

3.1 Introduction

De profonds changements ont rapport ? un accroissement significatif des ?changes d'images, induisant ainsi des transformations majeures dans la fa ?on dont les individus vivent, travaillent et communiquent. La s ?curisation de ces ?changes implique n ?cessairement le recours de la cryptographie. Dans la premi ?re partie, nous avons pr ?sent ? une vue d'ensemble des concepts li ?s a la cryptographie, g ?n ?ralement impl ?mentes a l'aide de blocs ou de flux, en introduisant les principes de Kerckhoffs et les mesures des propri ?t ?s de Shannon pour les chiffrements modernes. Compte tenu de la sp ?cificit ?, de la grande capacit ? et de la forte redondance des donn ?es d'image, les algorithmes traditionnels AES et DES ne sont pas adapt ?s pour chiffrer ce type de donn ?es. La deuxi ?me partie ?tait consacr ?e a la recherche et a l'analyse bas ?e sur le cryptogramme chaotique. L'analyse des r ?sultats exp ?rimentaux montre que l'algorithme choisi offre un niveau de fiabilit ? et de s ?curit ? tr ?s satisfaisant, r ?sistant ainsi aux attaques statistiques connues. Ces travaux constituent une preuve solide en faveur de l'utilisation d'algorithmes bas ?s sur le chaos comme alternative pour la s ?curisation des donn ?es d'images. Les images, en tant que moyen de communication universel, permettent a des individus de diff ?rents ages et cultures de se comprendre. Elles repr ?sentent ?galement le moyen le plus efficace de communication, chaque individu ?tant capable d'analyser l'image a sa mani ?re, d'obtenir des impressions et d'extraire des informations pr ?cises. Par cons ?quent, le traitement d'images regroupe un en-

semble de m ?thodes et de techniques visant a am ?liorer facilement et efficacement les aspects visuels des images afin d'en extraire des informations jug ?es pertinentes. Ce chapitre vise a mettre en lumi ?re les concepts li ?s aux images num ?riques ainsi que leurs caract ?ristiques et types afin de pouvoir les s ?curiser (d ?chiffrer). Il se conclut par un exemple de d ?chiffrement d'une image et sa simulation sous Python.

3.1 D ?finition de l'image :

Une image repr ?sente visuellement ou mentalement quelque chose (objet, ?tre vivant et/ou concept), et est obtenue par la transformation d'une sc ?ne r ?elle par un capteur, puis affich ?e sur un ?cran avec une signification pour l'oeil humain. La formation de l'image implique l'utilisation d'un dispositif physique capable de d ?tecter les informations de la sc ?ne et de les coder dans l'image. Cette repr ?sentation visuelle est donn ?e par une mesure physique, qui correspond a la quantit ? d' ?nergie r ?fl ?chie, ?mise ou absorb ?e par l'objet, et qui est mesur ?e par le capteur. En g ?n ?ral, une image est une repr ?sentation partielle de la sc ?ne r ?elle a un instant donn ?, situ ?e dans un espace bidimensionnel et acquise a l'aide de divers syst ?mes de g ?n ?ration d'images tels que des cam ?ras, des scanners, etc. Elle peut ?tre sous forme analogique (comme la photographie, la vid ?o, etc.) ou num ?rique (telles que les images num ?ris ?es dans divers formats, les images compress ?es, etc.). La num ?risation d'une image, ?galement appel ?e digitalisation, est le processus de conversion d'une image analogique (signal analogique) en une image num ?rique ou discr ?te, repr ?sent ?e par une suite de bits, afin de reproduire l'image le plus fid ?lement possible a l'original.

3.2 D ?finition de l'image num ?rique :

Une image num ?rique est une image dont la surface est divis ?e en ?l ?ments de taille fixe appel ?s pixels(cellules), dont chacun est caract ?ris ? par une ?chelle de gris ou un niveau de couleur pris a un emplacement correspondant dans l'image r ?elle, ou de l'int ?rieur de la sc ?ne ou la description des calculs sont repr ?sent ?s .

3.3 Caract ?ristiques de l'image num ?rique :

L'image est un ensemble structur ? d'informations caract ?ris ? par les param ?tres suivants :

3.3.1 Le pixel :

Un pixel, une abr ?viation de "Picture Elements" en anglais, repr ?sente le plus petit point carr ? dans une image et constitue ?galement l'entit ? calculable qui peut int ?grer la structure et la quantification. Comme un bit est la plus petite unit ? d'information g ?rable par un ordinateur, un pixel repr ?sente donc le plus petit ?l ?ment que le mat ?riel et les logiciels d'affichage ou d'impression peuvent traiter. La quantit ? d'informations transmise par chaque pixel marque une subtile distinction entre une image monochrome et une image en couleur. Dans le cas des images monochromes, chaque pixel est cod ? sur un octet, ce qui signifie que la m ?moire n ?cessaire pour afficher une telle image est directement li ?e a sa taille. En revanche, dans une image couleur (RVB), un pixel peut ?tre repr ?sent ? par trois octets : un pour chaque couleur : rouge (R), vert (V) et bleu (B).

3.3.2 Dimension :

La dimension elle correspond a la taille de l'image. Cette derni ?re se pr ?sente sous la forme d'une matrice dont les ?l ?ments sont des valeurs num ?riques repr ?sentant des intensit ?s lumineuses (pixels).le nombre total de pixels dans l'image se fait par la multiplication.

2.3.3 Contour :

Les contours se d ?finissent comme la d ?marcation entre deux pixels ou les niveaux de gris pr ?sentent une variation notable. En termes plus simples, ils marquent la transition entre les diff ?rents objets pr ?sents dans l'image.des nombre de lignes dans cette matrice avec le nombre de colonnes.

3.3.4 R ?solution :

La r ?solution d'une image num ?rique d ?signe la qualit ? des d ?tails reproduits par un ?cran ou une imprimante lors de la cr ?ation d'une image. Pour les ?crans d'ordinateur, la r ?solution est mesur ?e en nombre de pixels par unit ? de longueur, g ?n ?ralement en pouces ou en centim ?tres.

Le terme "r ?solution" est utilis ? pour d ?crire le nombre de pixels affich ?s horizontalement ou verticalement sur un ?cran plus ce nombre est ?lev ?, meilleure est la r ?solution.

3.3.5 Luminance :

C'est le degr ? de luminosit ? des points de l'image. Elle est d ?finie aussi comme ?tant le quotient de l'intensit ? lumineuse d'une surface par l'aire apparente de cette surface. Une meilleure luminance(brillance) est caract ?ris ?e par :

* Des images lumineuses (brillantes).

* Un bon contraste donc pour l'avoir il faut ?viter les images ou la gamme de contraste tend vers le blanc ou le noir car ces images entrainent des pertes de d ?tails dans les zones sombres ou lumineuses.

* L'absence de parasites.

3.3.6 contraste :

le constate c'est l'opposition apparente entre deux zones d'une image, plus pr ?cis ?ment entre les zones sombres et claires de cette image.Le contraste est d ?fini en fonction de la luminosit ? de deux zones de l'image.

3.3.7 Voisinage :

Le voisinage dans une image d ?signe les pixels qui entourent un pixel donn ? dans un espace bidimensionnel. Ces pixels voisins peuvent ?tre situ ?s au diff ?rentes distances et directions par rapport au pixel central, selon la d ?finition sp ?cifique du voisinage utilis ?e dans le contexte de traitement d'images.

3.4 types d'images num ?riques :

Il existe trois types d'images : binaire, en niveau de gris et couleur qu'on citera ci-dessous :

3.4.1 Image binaire :

Une image binaire est une structure en forme de matrice rectangulaire ou les nuances de gris sont restreintes a deux valeurs : 0 et 1. Dans ce contexte, le 0 repr ?sente le noir absolu tandis que le 1 repr ?sente le blanc. Cette repr ?sentation utilise seulement un bit pour encoder chaque niveau de gris.

3.4.2 Image en niveaux de gris :

Le niveau de gris est la valeur d'intensit ? lumineuse d'un point avec un nombre limit ? de couches interm ?diaires, les pixels peuvent prendre des valeurs allant du noir au blanc.Ainsi, pour repr ?senter une image en niveaux de gris, nous pouvons attribuer ? chaque pixel de l'image une valeur qui correspond ? la quantit ? de lumi ?re envoy ?e. Par exemple,la valeur peut ?tre comprise entre 0 et 255. Ainsi, chaque pixel n'est plus repr ?sent ? par des bits, mais par des octets.

3.4.3 image couleur :

Ces images couleurs sont en g ?n ?ral cod ?es par les trois couleurs fondamentales(principales) tel que le rouge, vert et le bleu, on parle alors d'images RVB. Chaque couleur contient donc trois plans de couleurs le rouge, vert et bleu (RVB). Chaque plan est cod ? comme une image en niveau de gris avec des valeurs allant de 0 ? 225).

3.4.4 Application de cryptage sur une image :

L'application de cryptage sur une image consiste a utiliser des techniques de cryptographie pour rendre une image illisible sans la cl ? de d ?chiffrement appropri ?e. Ce processus peut impliquer diff ?rentes m ?thodes, telles que le chiffrement de l'image enti ?re ou de parties sp ?cifiques de l'image . L'objectif principal est de s ?curiser l'image contre l'acc ?s non autoris ?, en garantissant que seules les personnes disposant de la cl ? appropri ?e peuvent la visualiser ou la modifier. voici une explication par rapport a notre programme :

1.Chargement de l'image et pr ?traitement :

- L'image "Lena.jpg" est charg ?e et convertie en niveau de gris avec la fonction "imread" et "rgb2gray".
- L'image est ensuite dimensionn ?e en un vecteur colonne avec 'img(:)'.

- La taille de l'image est stock ?e dans les variables 'row' et 'col'.
- Calcul du nombre total de pixels s.

2.G ?n ?ration de la carte de Lozi : :

- Une carte de Lozi est utilis ?e pour g ?n ?rer une s ?quence de nombres pseudo-al ?atoires. Ces nombres sont utilis ?s comme cl ? de chiffrement.
- La carte de Lozi est d ?finie par les ?quations it ?ratives de 'z1' et 'z2'.
- Les valeurs de k sont calcul ?es en fonction de 'z1' et 'z2'.
- La cl ? est g ?n ?r ?e ? partir de 'k' et de 'ktemp'
- It ?rations de la carte de Lozi pour g ?n ?rer une s ?quence 'w'.
- Tri de la s ?quence 'w' et permutation des pixels de l'image en fonction de ce tri.

3.Chiffrement avec la carte de Lozi : :

- G ?n ?ration d'une cl ? de chiffrement 'key' ? partir de la s ?quence 'w'.
- Utilisation de la fonction 'bitxor()' pour chiffrer les pixels de l'image avec la cl ?.

4.Chiffrement avec le syst ?me de Henon :

- Initialisation des param ?tres du syst ?me de Henon ('a', 'b') et des conditions initiales ('x1(1)', 'x2(1)', 'x3(1)').
- G ?n ?ration des it ?rations du syst ?me de Henon pour chiffrer davantage les pixels de l'image.

5.D ?chiffrement avec le syst ?me de Henon :

- Utilisation des it ?rations inverses du syst ?me de Henon pour retrouver les pixels originaux de l'image.

6.Calcul et comparaison de l'entropie :

- Calcul de l'entropie de l'image originale ('enO'), de l'image chiffr ?e ('enC') et de l'image d ?chiffr ?e ('enD').
- Comparaison des valeurs d'entropie pour ?valuer la qualit ? du chiffrement.

7.Calcul du NPCR (Nombre de Pixels Chang ?s Ratio) :

- Calcul du pourcentage de pixels diff ?rents entre l'image originale et l'image chiffr ?e.

– Le NPCR mesure la sensibilit ? du chiffrement aux modifications de l'image.

8.Affichage des histogrammes :

– Affichage des histogrammes des niveaux de gris de l'image originale, de l'image chiffr ?e et de l'image d ?chiffr ?e pour comparer leurs distributions

9.Calcul de la corr ?lation des pixels :

– Calcul de la corr ?lation entre les pixels de l'image originale et de l'image chiffr ?e dans diff ?rentes directions (horizontale, verticale, diagonale).

– Affichage des r ?sultats sous forme de graphiques pour visualiser la corr ?lation.

Ce programme combine les syst ?mes dynamiques et les techniques de chiffrement pour s ?curiser l'image et utilise des mesures telles que l'entropie, le NPCR et la corr ?lation des pixels pour ?valuer l'efficacit ? du chiffrement.

3.5 Analyses et r ?sultats :

FIGURE 3.1: plan de phase Z1 versus $\hat{Z}1$

FIGURE 3.2: plan de phase Z2 versus $\hat{Z}2$

D'apr ?s la figure 1 et 2 on remarque que les ?tats du syst ?me de Lozi et les ?tats de l'observateur sont synchronis ?es. exemple : quand X1 = 0 $\hat{x}1 = 0$ est cela veut dire qu'ils sont synchronis ?.

FIGURE 3.3: plan de phase X1 versus $\hat{X}1$

FIGURE 3.4: plan de phase X2 versus $\hat{X}2$

FIGURE 3.5: plan de phase X3 versus $\hat{X}3$

D'apr ?s la figure 3,4 et5 on remarque que les ?tats du syst ?me de Henon et les ?tats de l'observateur sont synchronis ?es.

FIGURE 3.6: L'image original.

cette figure repr ?sente l'image original c'est celle la qu'on va crypter.

FIGURE 3.7: L'image crypter.

Cette figure illustre la r ?ussite de cryptage,en effet on a aucune information relative a l'image original sur l'image crypter.

FIGURE 3.8: L'image d ?crypter.

Cette figure illustre l'image qu'on a r ?ussi a d ?crypter.

FIGURE 3.9: L'histogramme de l'image original,Crypter et d ?crypter.

L'histogramme est une repr ?sentation visuelle des zones de lumi ?res d'une image,cette figure repr ?sente l'histogramme de l'image original,Crypter et d ?crypter. on remarque dans la premi ?re marge les pixels de l'image original n'ont pas de valeur entre [20 25] et entre [225 250] ce qui illustre la r ?partition des pixels sur l'image. la 1 ?re figure illustre l'histogramme de l'image original. la 2 ?me figure la distribution uniforme de pixel de l'image crypter. La 3 ?me figure l'histogramme d ?crypter est semblable pour celui de l'image original ce qui indique le cryptage est r ?ussi car on trouve les deux histogrammes de l'image original est d ?crypter qui se ressemble tend dit que l'autre image crypter a une distribution uniforme. Par exemple le nombre de pixel revient a chaque fois dans limage crypter, alors que dans les deux autres y'a des pixels qui n'existe pas.

FIGURE 3.10: La corr ?lation de l'image entre les pixels.

	image crypt ?	image d ?crypt ?
horizontal	0.9722	-0.005
vertical	0.9858	-0.0014
diagonal	0.9593	-0.0027

Cette figure repr ?sente la corr ?lation des images original quelques soit horizontal,vertical et diagonal sont toutes proche d'une droite le tableau illustre ses r ?sultats. Par contre les images crypter ont le coefficients de corr ?lation tr ?s faible ce qui illustre une partie d'efficacit ? de cryptage propos ?. La figure le d ?montre ainsi que les r ?sultats des coefficient obtenus dans le tableau.

Conclusion :

Cette application de cryptologie de l'image illustre la mani ?re dont les avanc ?es dans le domaine de la cryptographie peuvent ?tre appliqu ?es ? la s ?curit ? des donn ?es visuelles. En utilisant des techniques sophistiqu ?es telles que les syst ?mes dynamiques et les m ?thodes de chiffrement, cette application offre une solution robuste pour prot ?ger les images contre les acc ?s non autoris ?s et les alt ?rations malveillantes.

En s ?curisant les donn ?es visuelles, cette application r ?pond ? un besoin croissant de confidentialit ? et de s ?curit ? dans divers domaines, notamment la communication s ?curis ?e, le stockage de donn ?es sensibles, et la protection de la vie priv ?e des individus. Elle d ?montre ?galement l'importance de consid ?rer la s ?curit ? des images comme une composante essentielle de la s ?curit ? de l'information globale.

La mise en ?uvre de mesures d' ?valuation de la qualit ? du chiffrement, telles que l'analyse de l'entropie, du NPCR et de la corr ?lation des pixels, renforce la confiance dans l'efficacit ? du syst ?me de s ?curit ?. Ces mesures permettent de garantir que les images chiffr ?es restent s ?curis ?es et que toute tentative de compromission puisse ?tre d ?tect ?e et contr ?e efficacement.

En r ?sum ?, cette application de cryptologie de l'image offre une solution puissante pour s ?curiser les donn ?es visuelles dans un monde num ?rique en constante ?volution. Elle d ?montre l'importance de la recherche continue dans le domaine de la cryptographie pour relever les d ?fis de s ?curit ? croissants auxquels nous sommes confront ?s dans notre soci ?t ? hautement connect ?e.

Chapitre 4

Application sous Raspberry

4.1 Introduction

Ce chapitre présente l'application de crypto-systèmes basés sur des systèmes chaotiques pour le chiffrement d'image à l'aide de la carte Raspberry Pi. En tirant parti de ses capacités de traitement et de sa flexibilité, nous démontrons comment cette plateforme accessible et polyvalente peut implémenter des solutions de chiffrement robustes. L'objectif est de protéger efficacement les données visuelles sensibles, mettant en lumière le potentiel du Raspberry Pi en tant que solution économique et performante pour la sécurité numérique.

4.2 Composants

4.2.1 Carte Raspberry Pi 3 :

La Raspberry Pi 3 est un micro-ordinateur compact et puissant, idéal pour une variété de projets électroniques et informatiques. Dotée d'un processeur quad-core ARM Cortex-A53 cadencé à 1,2 GHz, elle offre des performances robustes pour les tâches quotidiennes et les applications avancées. Elle dispose également de 1 Go de RAM, de ports USB, d'une sortie HDMI, d'un port Ethernet et de la connectivité sans fil intégrée (Wi-Fi et Bluetooth), ce qui la rend extrêmement polyvalente.

4.2.2 Carte mémoire :

Une carte mémoire est un dispositif électronique portable utilisé pour stocker des données dans divers appareils. Elle existe sous différents formats comme SD, microSD, CompactFlash, et Memory Stick, et permet de stocker des photos, vidéos et documents. Insérée dans des emplacements dédiés sur les appareils compatibles, elle étend la capacité de stockage et facilite le transfert de données.

4.2.3 Cable USB type A/B :

Un câble de connexion avec un connecteur de type A à une extrémité et un connecteur de type B à l'autre. Il est couramment utilisé pour connecter des périphériques tels que les imprimantes, les scanners ou les appareils photo à un ordinateur. Ce câble permet la transmission de données entre les périphériques et l'ordinateur de manière rapide et fiable.

4.3 Programmer avec Raspberry :

Programmer avec le Raspberry Pi et Python constitue une fusion puissante propice à la réalisation de projets électroniques et informatiques captivants. Le Raspberry Pi, nano-ordinateur à la fois abordable et polyvalent, s'associe harmonieusement à Python, langage de programmation réputé pour sa puissance. En exploitant Python sur le Raspberry Pi, il devient envisageable de commander des capteurs, des actionneurs et divers composants matériels, tout en développant des applications IoT, des robots ou encore des systèmes dynamiques.

4.3.1 Introduction des bibliothèque :

Pour installé la bibliothèque opencv :

•pour commencer ,on démarre la recherche sur google en tapant la phrase (pypi.org)

•la fenêtre d'accueil de python s'affiche

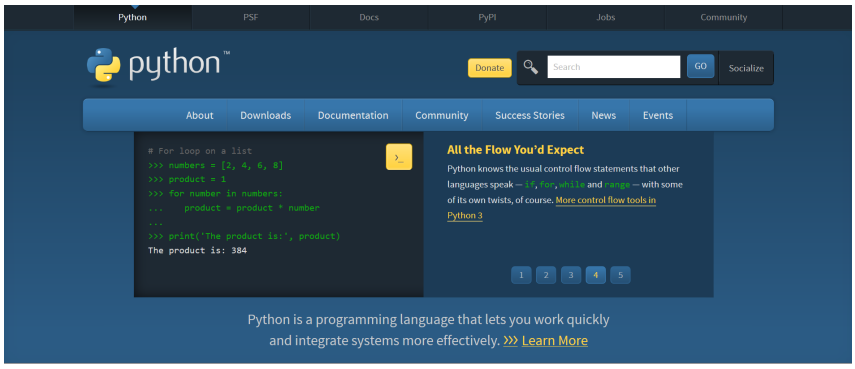


FIGURE 4.1: choisir la version

•Ensuite lancez la recherche (opencv).

•Il affiche plusieurs version en choisi la plus récente.

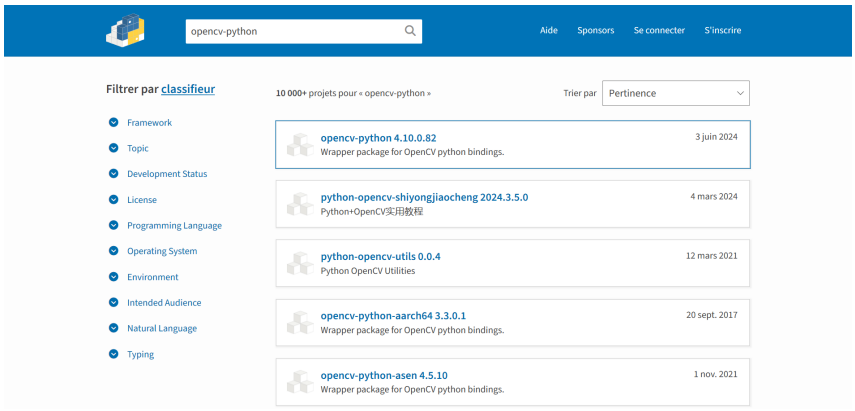


FIGURE 4.2: choisir la version

•Lorsque vous cliquez sur la version la plus récente de python ,il vous propose une liste de clé.ces clé sont généralement des clé d'installation ou d'activation pour la version choisie .

•Choisissent la clé suivante (pip installe opencv-contrib-python).

•Puis ouvrir un fichier texte sur le bureau et copié la clé sélectionné .

•une fois vous avez trouvé l'emplacement de IDLE ,en cliquant sur "AppData) , puis "programme" , puis "python", et enfin "python.12" .

•Après avoir trouvé le chemin d'accès ,il suffit de le copier et de le coller dans un fichier texte .

•Ouvrir la commande-cmd.pngs et changé le répertoire en tapant "cd" ,laissé de l'espace puis collé le chemins d'accès en appuyant sur entrée .en suite collé la clé ET en appuyer sur entré pour lancé l'installation .

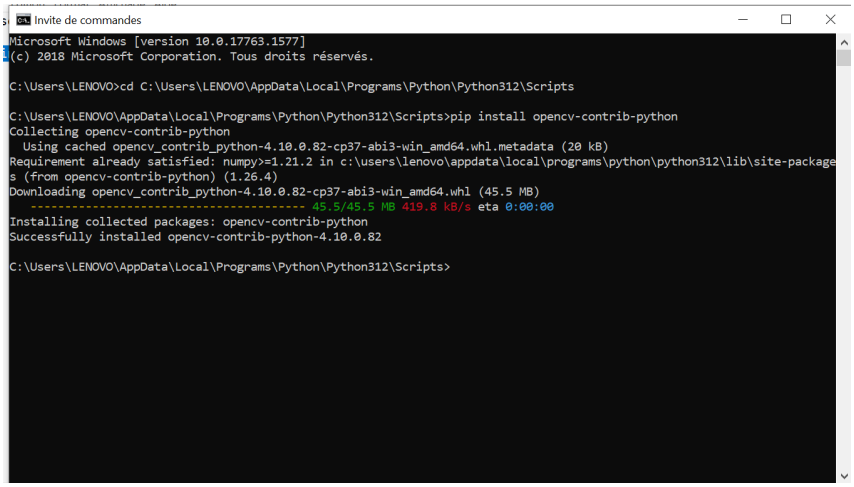


FIGURE 4.3: installation de opencv

•Une fois l'installation et terminé ,ouvrir "IDLE" et importe la bibliothèque "opencv" en appuyant la ligne de code suivant "import cv2".

4.3.2 fonctionnement d'une carte Raspberry

•insert la carte mémoire dans l'ordinateur portable et créé un fichier "SHH" et l'enregistrai dans la carte mémoire , puis éjecté .

•insert la carte mémoire dans la carte Raspberry ,puis cliqué sur la barre de recherche "putty" pour ce connecté a la carte

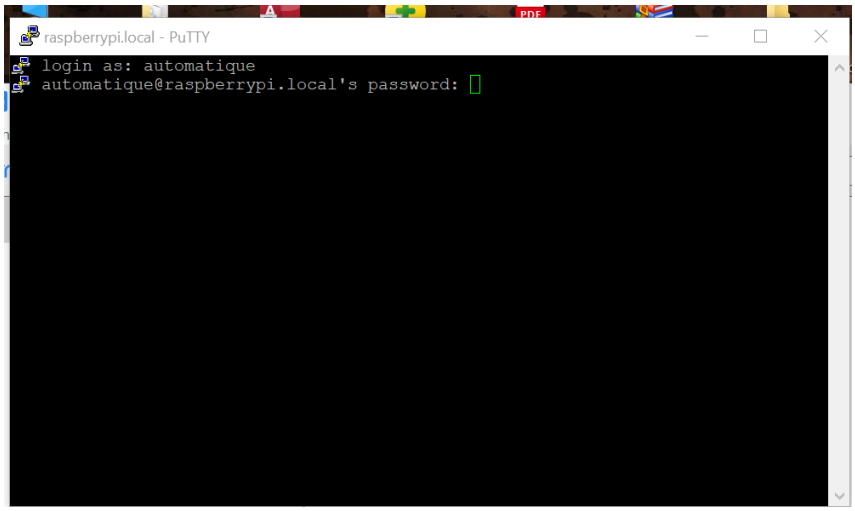


FIGURE 4.4: connecte a la carte

•puis ouvrir la fenêtre "realVNC viewer" ,il affiche sur l'écran "putty configuration" ,et dans HOST Name écrire "raspberrypi.local" et sélectionné le "SHH" dans "conection type ",puis cliqué sur "open".

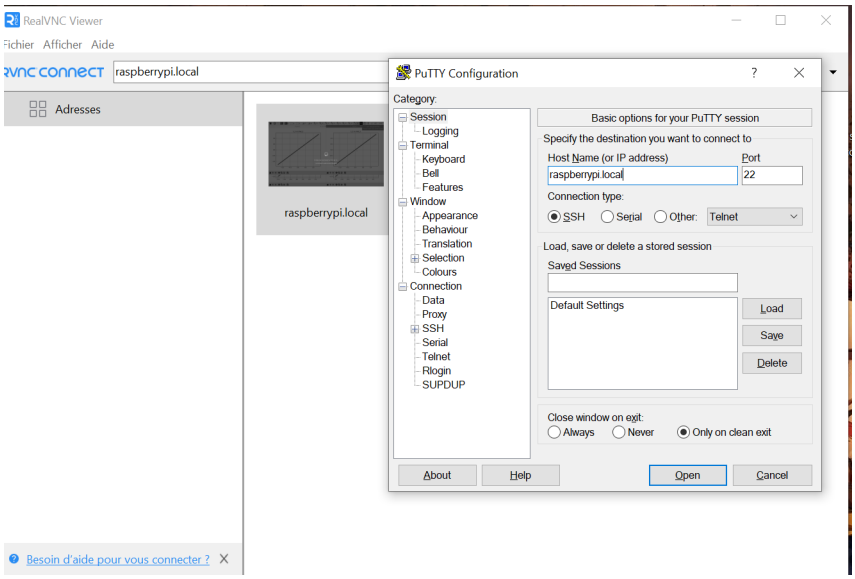


FIGURE 4.5: connecte aux cerveaux

•avec un double clique sur "raspberrypi.local", s'affiche la fenêtre "authentification" pour introduire "nome d'utilisateur "et "le mot de passe ".

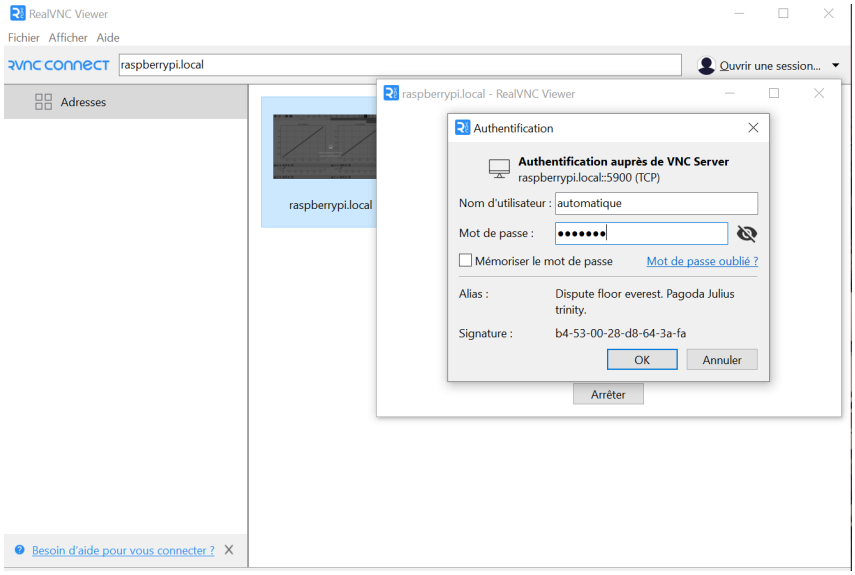


FIGURE 4.6: connexion aux Raspberry

•l'interface de carte Raspberry s'affiche .

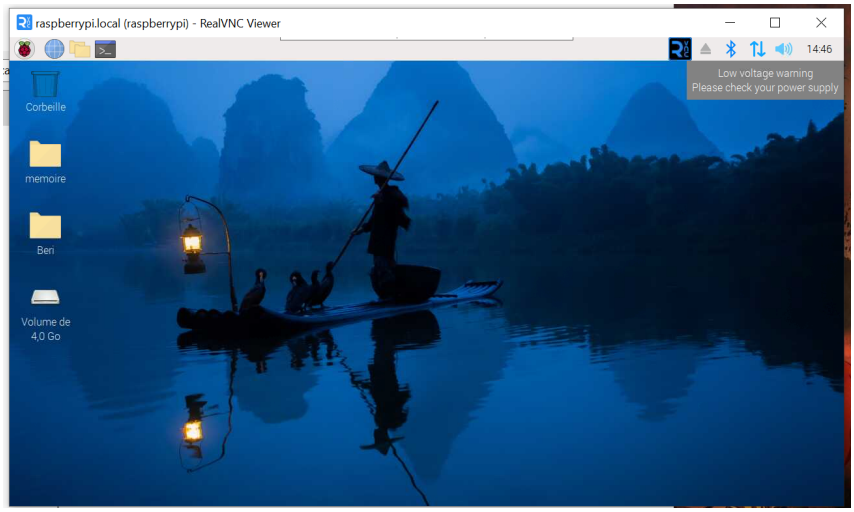


FIGURE 4.7: l'interface de Raspberry

•un clique dorit sur le logo "Raspberry" ,il afiche plusieurs proposition , cliqué sur "IDLE" puis fichier, puis sélectionné le fichier dans vous avez enregistré le programme ,puis cliqué sur "run"

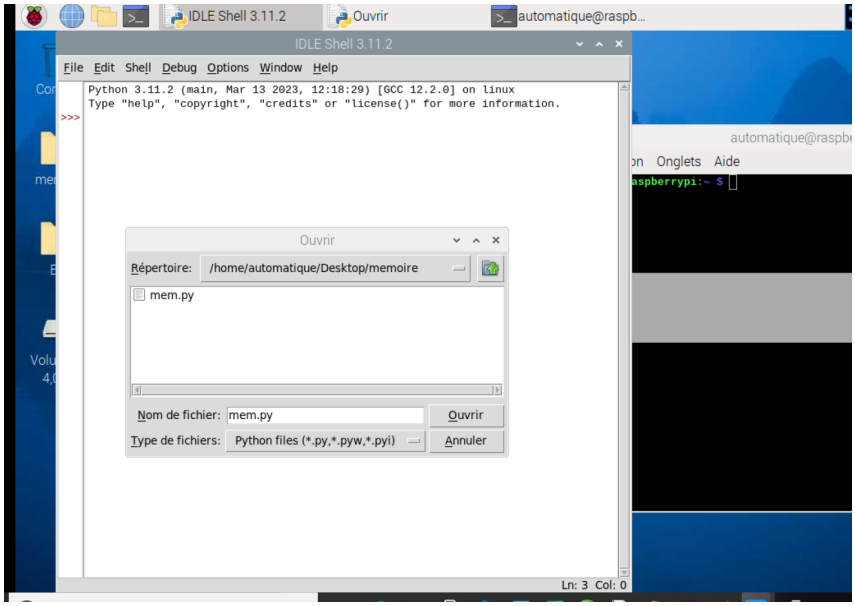


FIGURE 4.8: ouvrir IDLE sur Raspberry

4.3.3 les résultat obtenu :

•Pour faire appelle a l'image utilisé nommé image original sur python on utilise :

img = cv2.imread('Lena.jpg')

e = img-gray.flatten()

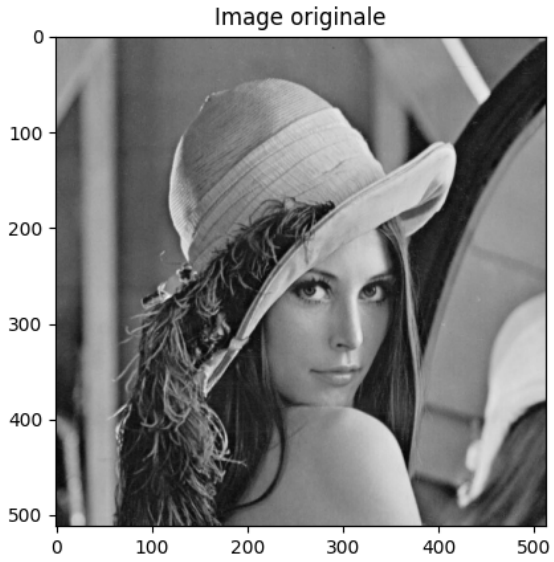


FIGURE 4.9: image original

•Pour affiché l'image crypté on a utilisé :

himg = (timg * 255).astype(np.uint8) .

himg = himg.reshape((row, col))

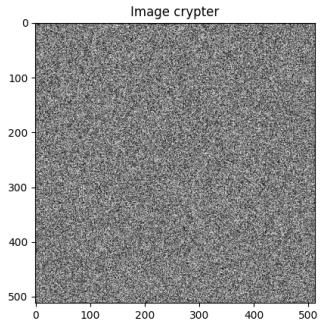


FIGURE 4.10: image cripte

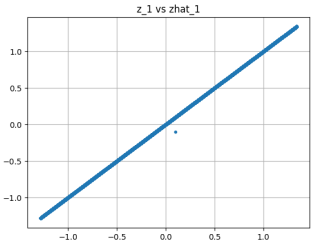
•Pour affiché l'image décrypté en utilise :

timg = timg[sorted-indices-inv]

timg = timg.reshape((row, col))

FIGURE 4.11: image décrypté

•Pour le systéme de lozi



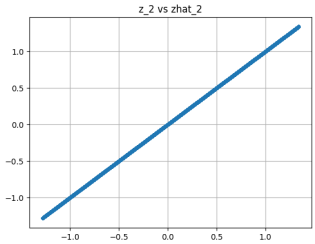
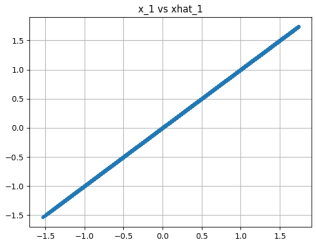
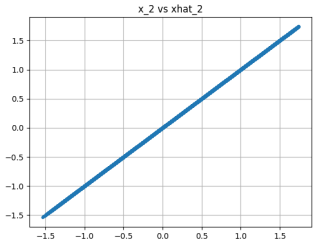


FIGURE 4.12: z1 vs zhat1 FIGURE 4.13: z2 vs zhat2

•Pour le systéme de hanon





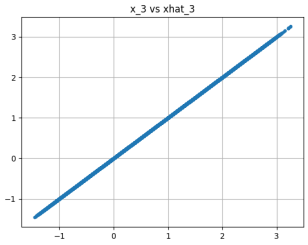


FIGURE 4.14: x1 vs xhat1 FIGURE 4.15: x2 vs xhat2 FIGURE 4.16: x3 vs xhat3

4.3.4 conclution :

L'application du cryptage d'images utilisant le Raspberry Pi, . Nous avons démontré comment ce micro-ordinateur doté de capacité de traitement avancée et d'une drande , flexibilité, peut être configuré pour implémenter des solutions de sécurité robustes et efficaces. La protection des données visuelles sensibles via le Raspberry Pi met en lumière son potentiel en tant qu'outil abordable et performant pour les projets de sécurité numérique. Cette approche illustre non seulement la viabilité technique du Raspberry Pi, mais également son rôle crucial dans l'innovation et l'accessibilité des technologies de cryptage, enrichies par nos recherches approfondies.

Conclusion Générale

L'objectif de ce mémoire est d'étudier en profondeur les systèmes chaotiques, en explorant leurs fondements théoriques, leurs propriétés dynamiques et leurs applications pratiques. Il vise à comprendre comment les systèmes chaotiques peuvent être théoriquement modélisés, synchronisés pour des applications sécurisées comme la cryptographie d'image, et implémentés sur des plateformes physiques comme la Raspberry Pi pour démontrer leur faisabilité technologique.

Dans le premier chapitre, les bases ont été posées en introduisant les concepts fondamentaux des systèmes dynamiques non linéaires. Nous avons exploré la représentation mathématique des systèmes dynamiques continus et discrets, ainsi que leurs propriétés distinctives telles que la non-linéarité, la sensibilité aux conditions initiales et la présence d'attracteurs étranges, comme ceux observés dans les systèmes de Lorenz et de Hénon.

Dans le deuxième chapitre, nous nous sommes concentrés sur la synchronisation des systèmes chaotiques, une exploration essentielle pour comprendre comment ces systèmes peuvent être contrôlés et exploités. Nous avons examiné diverses méthodes de synchronisation, de la synchronisation par répartition à la synchronisation par inversion du système, mettant en évidence leur utilisation dans des applications telles que la cryptographie et la sécurisation des communications.

Dans le troisième chapitre, nous avons exploré une application spécifique des systèmes chaotiques dans la cryptologie de l'image. En utilisant les propriétés chaotiques pour crypter et sécuriser les données visuelles, nous avons illustré comment ces concepts peuvent être appliqués pour protéger l'intégrité et la confidentialité des informations numériques.

Enfin, dans le quatrième chapitre, nous avons présenté une application pratique en utilisant

une carte Raspberry Pi 3 pour expérimenter avec les systèmes chaotiques dans un environnement physique. Nous avons exploré les composants de base de la carte Raspberry Pi 3 et démontré comment les concepts théoriques peuvent être implémentés et testés dans des projets concrets tel que le cryptage d'image.

En perspective, ce travail ouvre une voie prometteuses pour la recherche et les applications des systèmes chaotiques, pour la transmission de données entre deux carte Raspberry Pi.

Biblioghraphique

[1] Lorenz, E. N. (1963). Deterministic Nonperiodic Flow. *Journal of the Atmospheric Sciences, 20*(2), 130-141.

[2] Ott, E., Grebogi, C., & Yorke, J. A. (1990). Controlling Chaos. *Physical Review Letters, 64*(11), 1196-1199.

[3] Pecora, L. M., & Carroll, T. L. (1990). Synchronization in Chaotic Systems. *Physical Review Letters, 64*(8), 821-824.

[4] Li, C., & Chen, G. (2014). Cryptanalysis and Improvement of a Chaos-Based Image Encryption Algorithm. *Nonlinear Dynamics, 77*(4), 1289-1298.

[5] Li, X., Mou, X., Lian, S., & Liu, H. (2012). A New Chaos-Based Image Encryption Algorithm with Bit-Level Permutation. *Information Sciences, 193*, 69-83.

[6] Kocarev, L., & Parlitz, U. (1995). General Approach for Chaotic Synchronization with Applications to Communication. *Physical Review Letters, 74*(25), 5028-5031.

[7] Yang, Y., Xiao, D., & Lian, S. (2014). Chaos-Based Image Encryption Algorithm Resistant to Differential Cryptanalysis. *Signal Processing, 94*, 403-412

[8] T. Hamaizia,« Systèmes dynamiques et chaos »,Thèse Doctorat,l'Université de Constantine 1 ,2013.

[9] -H.HAMICHE,«Inversion à Gauche des Systèmes Dynamiques Hybrides Chaotiques. Application à la Transmission Sécurisée de Données »,Thèse Doctorat,Université Mouloud Mammeri Tizi Ouzou,2011.

[10] - N.E.Lorenz « The essence of chaos » University of Washington Press, 1993. N. Witkowski

[11] _H.Zhang « Chaos synchronization and its application to secure communication » Thèse de doctorat, Université de Waterloo, Canada, 2010.

[12] -Tidjani Menacer,« Synchronisation des systèmes dynamiques chaotiques à dérivées fractionnaires »,Thèse Doctorat,Université Constantinne1,2014.

[13]- A.Benkhelifa et A.Ghoul« Synchronisation des Systèmes Chaotiques Fractionnaires »Mémoire de Master,Université de larbi Tébessi – Tébessa ,2016.-

[14] AMIMER,« Modélisation et Commande des Systèmes Non Linéaires Fractionnaires par des Réseaux de Neurones Fractionnaires »,Mémoire de Magister,Université Mouloud Mammeri Tizi Ouzou,2015.

[15] A.Zemouche,« Sur l'observation de l'état des systèmes dynamiques non linéaires »,Thèse Doctorat,Université Louis Pasteur Strasbourg I,2007.

[16] G. ZHENG,« Formes Normales d'Observabilité Paramétrées par les Sorties : Appli-

cations au Cryptage par Synchronisation de Systμemes Chaotiques »Thèse Doctorat,Ecole Doctorale Sciences et Ingenierie de L'université de Cergy-Pontoise,2006.

[17] Yann Gaudeau ; « Contributions en compression d'images médicales 3D et images naturelles 2D » ; Thèse de doctorat ; Université Henri Poincaré de Nancy 1 ; France ; 2006.

[18]N. HAMRENE, D. IDIR, L. HAMOUDI ; « Codage d'images en sous bande par fractales : appliqué aux images médicales » ; Thèse d'ingénieur d'état en électronique ; UMMTO ; 2005.

[19]Kahina Lemikchi, Fatiha Ousmaal, Aldjia Rahali. Segmentation Markovienne des images multispectrales MSG. Mémoire d'ingénieur, département d'Electronique, faculté de Génie Electrique et Informatique, université Mouloud Mammeri de Tizi.

[20] Upton, E., & Halfacree, G. (2016). *Raspberry Pi User Guide*. John Wiley & Sons.

[21] LaForest, G. (2013). SD Card Projects Using the PIC Microcontroller. Elektor.

[22]Graves, M. (2012). *Digital Interface Handbook*. Elsevier.

[23] I. Belmouhoub, M. Demai and J.P. Barbot, « Observability quadtatic normal Form for discrete-Time système », IEEE Transactions on Automatic control, vol 50, July 2005.

[24] M.Djemai, J-P Barbot and I. Belmouhoub, « Discrete-Time Normal From for Left Invertibilily problem », Eur, J.Control, Vol.15, p194-2014, 2009.