République **A**lgérienne **D**émocratique et **P**opulaire
Ministère de l'**E**nseignement **S**upérieur et de la **R**echerche **S**cientifique

UNIVERSITE **M**OULOUD **M**AMMERI DE **T**IZI-**O**UZOU

FACULTE DU **G**ENIE **E**LECTRIQUE 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
OULD SLIMANE Kahina
OUKIDJA Siham

Thème

Conception d'un crypto-système basé sur la synchronisation des systèmes chaotiques : application au cryptage d'image

Mémoire soutenu publiquement le 26 / 06 / 2024 devant le jury composé de :

Mme Sadia ALKAMA
MCA, UMMTO, Présidente

M Ahcene HAMOUDI
MAB, UMMTO, Encadrant

Mme Nadia DJEGHALI
Pr, UMMTO, Examinatrice

Mme Sarah KASSIM
MCB, UMMTO, Examinatrice

Remerciements

En premier lieu, nous tenons à remercier notre créateur, DIEU, pour nous avoir donné la force, la patience, la santé, la volonté et le courage nécessaires pour accomplir ce modeste travail.

Nos remerciements vont également, du fond du coeur, à nos parents pour nous avoir accompagnés, aidés, soutenus moralement et financièrement. Nous sommes également reconnaissante envers nos proches pour leur soutien indéfectible et leur compréhension durant cette période intense. Leur encouragement et leur présence ont été des sources d'inspiration qui ont rendu ce parcours plus enrichissant et mémorable.

Nous tenons à exprimer notre profonde gratitude envers notre promoteur, Monsieur Hamoudi Ahcene, pour son soutien, ses conseils et son dévouement tout au long de notre mémoire. Ses encouragements constants et son expertise ont été essentiels pour surmonter les défis rencontrés.

Nous exprimons nos vifs remerciements à tous nos professeurs qui nous ont enseignés pendant notre cursus d'étude.

Enfin, nous tenons à remercier chaleureusement les membres du jury de nous faire l'honneur d'accepter d'évaluer ce travail.

Dedicaces

je dédie ce modeste travail a :

À mes chers parents Boukhalfa et Tounssia,
qui m'ont soutenue et encouragée tout au long de ce parcours. Leur amour, leur soutien inconditionnel, leurs prières tout au long de mes études et leurs conseils avisés ont été ma source de force et d'inspiration. Ce mémoire leur est dédié en signe de gratitude et d'amour éternels.

À mes trois cher oncle Kamel, allal et Morad,
dont le soutien, les encouragements et la bienveillance ont toujours illuminé mon chemin. Leurs présence et leurs conseils précieux ont été des piliers dans ma vie. Ce travail leur est dédié en témoignage de ma profonde reconnaissance et de mon amour sincère.

À ma chère grand-mère Nouara,
À travers ta sagesse et ton amour infini, tu m'as enseigné tant de précieuses leçons qui ont façonné celle que je suis devenue aujourd'hui. Ce mémoire est dédié à toi, qui as toujours été ma source d'inspiration et de soutien inconditionnel. Merci pour ta tendresse et tes encouragements constants.

À mes chers soeurs et frère,
Chabane, Ouerdia, Thinhinane et Thanina, Votre soutien indéfectible et votre amour inconditionnel ont été les piliers qui ont guidé chacune de mes étapes. Ce mémoire est le fruit de nos discussions, de nos échanges et de notre complicité qui transcendent les défis et enrichissent les réussites. Merci d'avoir été mes anges gardiens, mes confidents et mes inspirations.

À mes meilleures amies lyna et lynda,

Qui ont toujours été mes complices, mes confidentes leurs amitié précieuse a été mon plus grand trésor. Ce travail est dédie en signe de gratitude pour leur présence inestimable dans ma vie.

À Mon meilleur,

Merci d'avoir accepté tout mes casse-têtes avec patience et compréhension. Ta présence a rendu ce chemin moins sinueux et beaucoup plus agréable. Je suis reconnaissante pour ton soutien constant et ta présence inestimable.

À mes chères tantes,

Votre amour, vos conseils et votre soutien ont été une source d'inspiration tout au long de ce parcours. Ce mémoire vous est dédié avec une profonde gratitude pour votre présence inestimable dans ma vie.

O.Kahina

je dédie mon travail,

a mon cher père pour mon soutient et a ma mère qui a était mon pilier de ma réussiteet a toute ma famille, Ainsi qu'a tout mes amis : Razene, Mounia, Amer, Kamel, Slimane, Idir, Mohamed, Souhil, Moumene.

O.Siham

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 $n \times m$
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
$\mathcal{O}$:	Matrice d'observabilité

Introduction Générale

Les systèmes chaotiques représentent un domaine fascinant des systèmes dynamiques non linéaires, captivant les chercheurs par leurs propriétés intrigantes et leur potentiel d'application dans divers domaines scientifiques et technologiques [6]. La complexité inhérente aux systèmes chaotiques réside dans leur capacité à générer des comportements apparemment aléatoires et imprévisibles à partir de règles déterministes. Cette caractéristique découle principalement de leur sensibilité extrême aux conditions initiales : de petites variations dans les conditions de départ peuvent conduire à des trajectoires évolutives totalement divergentes, un phénomène souvent désigné par l'expression célèbre de l'« effet papillon » [1].

Pour comprendre les systèmes chaotiques, il est crucial de s'immerger dans leurs fondements théoriques. La dynamique non linéaire, qui forme la base mathématique de ces systèmes, se distingue des systèmes linéaires par l'absence de proportionnalité directe entre les causes et les effets. Au lieu de cela, les interactions complexes entre les différentes variables conduisent à des comportements dynamiques qui défient l'intuition et qui peuvent souvent être modélisés par des équations différentielles ou des itérations récurrentes. C'est à travers ces représentations mathématiques que les systèmes chaotiques révèlent leur non-linéarité intrinsèque, leur propension à la bifurcation, et leur capacité à générer des motifs d'évolution complexes et non périodiques dans l'espace des phases [2][3].

Un aspect particulièrement remarquable des systèmes chaotiques est la présence d'attracteurs étranges. Contrairement aux attracteurs réguliers qui caractérisent les systèmes stables et périodiques, les attracteurs étranges décrivent des trajectoires dans l'espace des phases qui ne se répètent pas à intervalles fixes. L'attracteur de Lorenz, découvert par Edward Lorenz dans les années 1960, demeure l'exemple d'un tel phénomène, avec ses trajectoires en forme de papillon qui symbolisent la sensibilité aux conditions initiales et la complexité dynamique inhérente à ce type de système [1][4].

Outre leur caractère théorique profond, les systèmes chaotiques jouent un rôle crucial dans les applications pratiques modernes. La synchronisation des systèmes chaotiques, par exemple, explore la possibilité de coordonner les états de systèmes chaotiques distincts, souvent dans des contextes où la communication sécurisée et la transmission de l'information sont essentielles. Des méthodes variées telles que la synchronisation par rétroaction, la synchronisation impulsive et la synchronisation retardée permettent de contrôler et d'exploiter le chaos pour des applications telles que le cryptage des données et la sécurisation des communications numériques [7].

En particulier, le domaine émergent de la cryptographie d'image utilise les propriétés uniques des systèmes chaotiques pour générer des clés de chiffrement robustes et assurer la confidentialité des données visuelles dans un environnement numérique de plus en plus complexe et interconnecté. Des techniques telles que le cryptage par addition, le chaos shift keying (CSK), et le cryptage par inclusion exploitent la variabilité et la complexité des trajectoires chaotiques pour garantir une protection efficace contre les tentatives de compromission et de décodage non autorisé [5].

Notre étude se focalise sur une exploration approfondie des systèmes chaotiques, visant à comprendre leurs fondements théoriques, y compris leur représentation mathématique et leurs propriétés clés telles que la sensibilité aux conditions initiales. En parallèle, nous analysons les méthodes de synchronisation chaotique et leur application dans le domaine de la cryptographie d'image. L'objectif ultime est de contribuer à une meilleure compréhension des systèmes chaotiques et de leur utilisation novatrice pour renforcer la sécurité des données et les communications sécurisées.

Pour réaliser ce projet, nous avons organisé ce mémoire comme suit :

Chapitre 1 : Les fondations théoriques des systèmes dynamiques continus et discrets, mettant en évidence leur formalisation mathématique et leurs caractéristiques clés telles que la non-linéarité, le déterminisme et la sensibilité aux conditions initiales.

Chapitre 2 : Un examen détaillé des méthodes de synchronisation des systèmes chaotiques, cruciales pour comprendre la manière dont ces systèmes peuvent être régulés et utilisés. Cela inclut l'étude de différentes approches telles que la synchronisation par répartition et par inversion du système.

Chapitre 3 : Une application particulière des systèmes chaotiques dans le domaine de la cryptographie d'image. En exploitant les caractéristiques chaotiques pour le cryptage et la sécurisation des données visuelles, nous démontrons comment ces concepts peuvent être utilisés pour garantir la confidentialité et l'intégrité des informations numériques.

Chapitre 4 : Une application pratique en utilisant une carte Raspberry Pi pour expérimenter avec les systèmes chaotiques dans un environnement physique. Nous explorerons les composants fondamentaux de la carte Raspberry Pi 3 et démontrerons comment les concepts théoriques peuvent être mis en oeuvre et testés dans des projets réels.

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 observer lors d'étude consacrées a la stabilité du système solaire.Après cela 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 est généralement un comportement particulier et imprévisible d'un système dynamique déterminer non linéaire.La théorie du chaos peut être utile dans de nombreux domaines tels que le 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.

1.2 Les systèmes dynamiques

Un système dynamique est considéré comme chaotique lorsqu'il décrit des phénomènes évoluant au fil du temps. Globalement, le terme "système" désigne un ensemble de variables d'état.

1.3 Représentation mathématique

1.3.1 Les systèmes dynamiques continu

un système dynamique dans le cas continu est régi par un système d'équations différentielles

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

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

$$\{X_0 = (X(t0)) \tag{1.2}$$

X0= représente l'état initiale du système.

1.3.2 les systèmes dynamiques discret

un système dynamique dans le cas discret est représenté par des équations aux différences,appelées également «équation de récurrence».

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

ou :

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

1.4 Propriétés des systèmes chaotiques

les systèmes dynamique chaotique sont des systèmes déterministe non linéaires qui montrent souvent un comportement non divergent,apériodique et éventuellement borné.
Les signaux qui évoluent dans ces système sont on génitale a large bande ce qui fait apparaitre leur trajectoire comme du bruit pseudo aléatoire.En raison de ces propriétés et a cause de la fragilité des cryptosystème classique,les signaux chaotique fournissent potentiellement une classe importante des signaux qui peuvent être utilisé pour masqué les information dans une transmition sécurisé.
Parmi les caractéristique principale permettant d'évoquer un comportement chaotique,on peut retenir les propriétés suivantes :

1.4.1 Non linéarité

un système linéaire admet toujours des solution,les effets sont prévisible et proportionnels aux causes qui les ont engendrés.On peut le décomposer en sous ensemble ou le composer avec d'autre systèmes sans qu'il perde ses propriétés mais un système non linéaire,n'est en général pas soluble plus on tente de le décomposer plus la complexité interne se révèle.Pour cela tout

système linéaire ne peut pas être chaotique car un système chaotique est un système dynamique non linéaire.

1.4.2 Déterminisme et imprévisibilité

Dans le cas des systèmes déterministe,théoriquement la connaissance de l'état initial,de l'entrée et du modèle permet de prédire l'état futur du système,cependant il est difficile de calculer la solution analytique théorique de certaine système non linéaire qui est le cas pour les systèmes chaotique déterministe,car ils sont caractérisés par une sensibilité aux conditions initiales dont une simple erreur de mesure ou un simple arrondi conduit a des solutions différentes ce qui les rendent imprévisibles,en conséquence la prévisibilité n'est plus liée au déterminisme.

1.4.3 Sensibilité aux condition initiales

La sensibilité aux conditions initiales est l'une des caractéristique fondamentales des systèmes chaotiques explicitée par lorenz dans sa célébré citation :"l'effet papillon" une légère variation des conditions initiales sur un système chaotique entraine deux trajectoires qui sont initialement voisines puis qui divergent exponentiellement par la suite les deux trajectoires sont incomparables,ce qui rend les systèmes chaotique prédictibilité a long terme .
il est donc clair que la moindre erreur ou imprécision sur la condition initiale ne permet pas de décider a tout temps qu'elle sera la trajectoire effectivement suivie .Pour illustrer cette propriété on prend comme exemple le système de lorenz décrit par le système d'équations suivant
de lorenz :

$$\dot{X} = a(y - x) \tag{1.4}$$

$$\dot{y} = bx - y - xz \tag{1.5}$$

$$\dot{z} = xy - cz \tag{1.6}$$

avec :

(x,y,z) :le vecteur d'état.

(a,b,c) :sont les vecteur des paramètres pour les quelles le système présente un comportement chaotique .

pour deux condition initiales très proches :(x01,y01,z01)=(0.1,0.1,0.1).

(x02,y02,z02)=(0.1001,0.1001,0.1001).

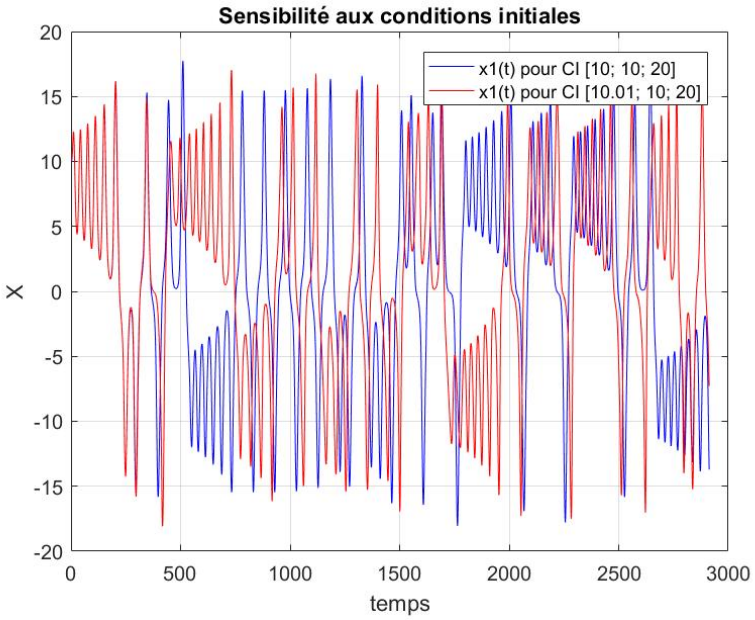


FIGURE 1.1: sensibilite aux conditions initiales de lorenz

1.4.4 Aspect aléatoire

Bien que les systèmes chaotique soient déterministes,tout les état d'un système chaotique présentent des aspects aléatoires,comme on peut l'observer dans la figure.

1.4.5 Attracteur étrange

Lorsque edward lorenz entreprit graphiquement la solution de son système (lorenz)au moyen de son ordinateur en traçant deux courbes divergent,mais a sa grande surprise,les deux courbes étaient plus au moins identique,elles ressemblaient a deux ailes de papillon.

Le physicien david ruelle qui s'est penché sur la question a qualifié cette figure«d'attracteur étrange»en remarquant que les trajectoires ne se coupent jamais et bien qu'elles semblent évoluer au hasard,elle forment des figures indiscutablement reconnaissables .

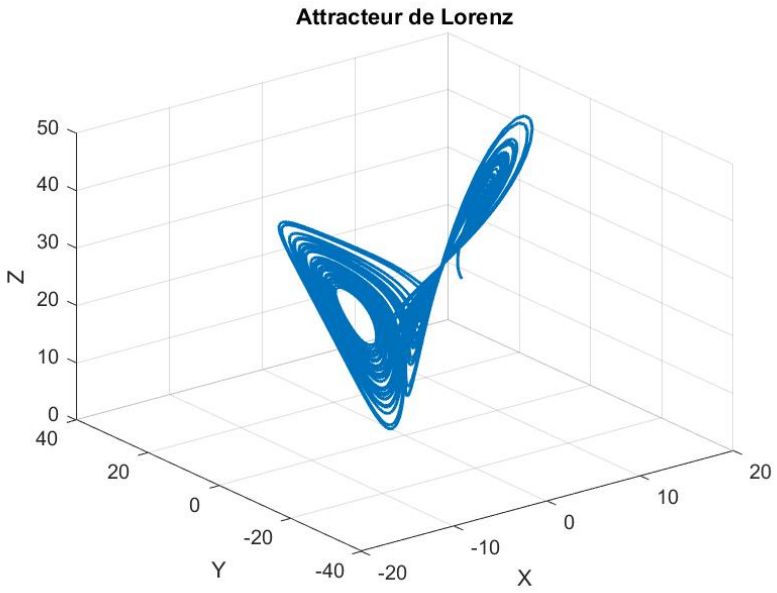


FIGURE 1.2: attracteur de lorenz

Par conséquent,lorsque le régime d'un système est chaotique l'attracteur correspondant est un attracteur étrange qui a des propriétés topologique différentes de celles d'un attracteur simple .

1.5 Exposants Lyapunov

Le mathématicien Alexander Lyapounov a étudié le phénomène de la sensibilité aux conditions initiales des systèmes chaotiques et a développé un degré permettant de mesurer la vitesse à laquelle ces petites variations peuvent s'amplifier,cette quantité est appelée « Exposant de Lyapounov ». Autrement dit, l'exposant de Lyapounov est le taux de divergence entre l'évolution des trajectoires issues de conditions initiales proches au sein de l'attracteur étrange.
soit $f : \mathbb{R} \to \mathbb{R}$ une fonction de C^1. Pour chaque point x_0 on définit un exposant de Lyapunov $\lambda(x_0)$ comme suit :

$$\lambda(x_0) = \lim_{n\to\infty} \sup \frac{1}{n} \log(|f(n)'(x_0)|) = \lim_{n\to\infty} \sup \frac{1}{n} \sum_{i=0}^{n-1} \log(|f(x_j)|) \tag{1.7}$$

avec $x_j = f_j(x_0)$

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

TABLE 1.1: Exposants Lyapunov

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

$$|Z_2| \approx e^{\lambda \Delta t} \tag{1.8}$$

ou λ est l'exposant de Lyapunov.
aux conditions initiales, mais aussi de pouvoir séparer le comportement chaotique du comportement prévisible.

Si λ est strictement positif, alors la sensibilité aux conditions initiales est très grande, et le système est considéré comme chaotique.
En revanche, si λ est négatif ou égal à zéro, nous sommes en présence d'un phénomène stable ou périodique.
Si $\lambda > 0$, le système est chaotique et nous obtenons deux évolutions très différentes (divergentes). Sinon, nous aurons deux courbes qui se confondent.

En conclusion, la valeur de l'exposant de Lyapunov permet de déterminer la nature du système ainsi que le type de son attracteur.

1.5.1 Bifurcation

La théorie des bifurcations est l'étude mathématique des changements qualitatifs ou topologiques de la structure d'un système dynamique. Une bifurcation se produit lorsqu'un changement se produit dans les paramètres dont dépend le système. Plus précisément, il s'agit de la disparition ou du changement de stabilité, ou de l'apparition de nouvelles solutions. Il existe deux types de bifurcations : locales et globales. Chacune de ces bifurcations est caractérisée 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 période. L'évolution vers le chaos dans les systèmes dynamiques peut être observée

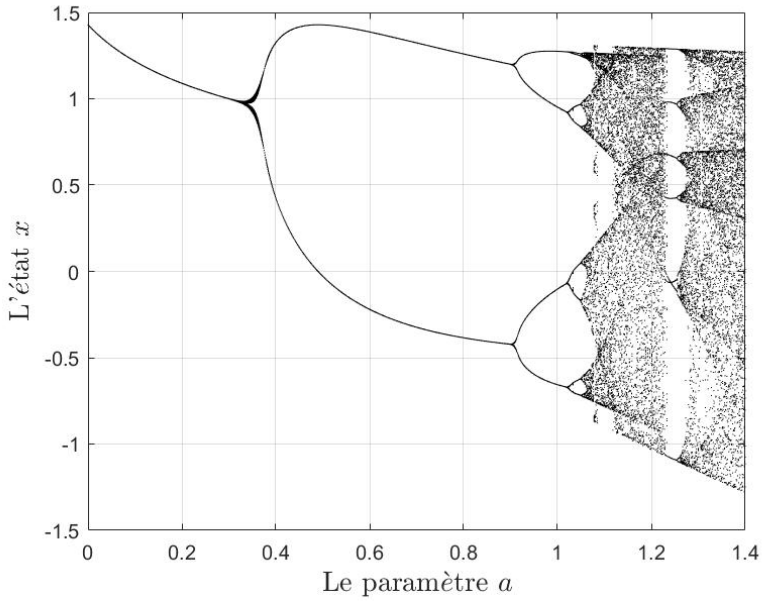


FIGURE 1.3: bifurcation

en ajustant la valeur d'un paramètre, que ce soit par des études théoriques ou expérimentales. Trois scénarios théoriques principaux décrivent ces transitions vers le chaos.

1.5.2 Quelques autres exemples d'attracteurs étranges

1.5.3 Cas continu

1.5.4 a. l'attracteur de Lorenz

C'est une simplification extrême des équations régissant le mouvement de l'atmosphère. Lorenz les a étudiées pour démontrer la sensibilité aux conditions initiales, qu'il a observée sur un système simple. Il s'interrogeait sur ce qui allait se passer, et bien que le point de départ soit proche, la deuxième trajectoire s'éloignait de plus en plus de la première. À la surprise de Lorenz, elle finissait également par décrire deux boucles. Elle semblait évoluer de manière aléatoire, changeant de direction de manière imprévisible, comme un papillon battant des ailes. Pourtant, quel que soit le point de départ, le système semblait irrésistiblement attiré par ces deux boucles, les ailes du papillon, autour desquelles il tournait sans jamais couper sa trajectoire. Lorenz a étudié ce phénomène pour mettre en évidence, sur un système simple, la sensibilité aux conditions initiales qu'il avait observée.

1.5.5 b. Système chaotique de Rössler

Le système de Rössler, proposé par l'Allemand Otto Rössler, est lié à l'étude de l'écoulement des fluides et découle des équations de Navier-Stokes. Les équations de ce système ont été découvertes à la suite de recherches en cinétique chimique. Voici les équations de ce système :

$$\begin{cases} \dot{x} = -(y+z) \\ \dot{y} = x + ay \\ \dot{z} = b + z(x-c) \end{cases} \tag{1.9}$$

ou :

- x, y, z est le vecteur d'état.
- a, b, c sont les paramétrés du système de Rossler .

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

1.5.6 Cas discret

1.5.7 Système de Henon

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

$$\begin{cases} x(k+1) = 1 - ax(k)^2 + y(k) \\ y(k+1) = bx(k) \end{cases} \tag{1.10}$$

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

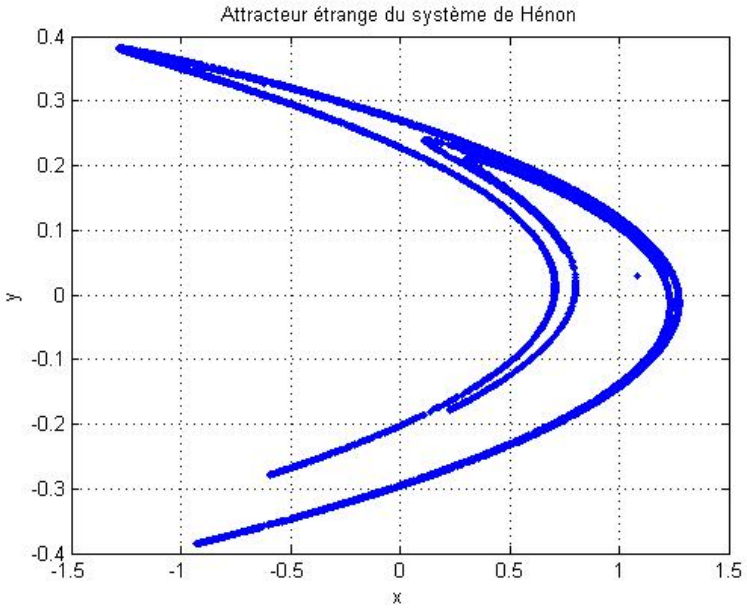


FIGURE 1.4: Hattracteur

1.6 Conclusion

Un système est considéré comme chaotique s'il est basé sur des lois déterministes bien connues, mais son évolution échappe encore à toutes les prédictions à long terme. La racine de ce phé-

nomène réside dans la dépendance aux conditions initiales. Le comportement chaotique d'un système est principalement dû à sa sensibilité aux conditions initiales, et se caractérise par un spectre de puissance continu, une fonction d'auto-correction tendant vers zéro à l'infini, et au moins un exposant de Lyapunov positif. Dans ce chapitre, nous avons observé toutes ces caractéristiques à l'aide de divers exemples sur Matlab, tels que le système de Hénon, qui illustre les caractéristiques des systèmes chaotiques et des systèmes dynamiques non linéaires. Les systèmes chaotiques présentent un comportement infiniment complexe et sont irrésistiblement attirés par une structure géométriquement infiniment complexe : l'attracteur étrange. Dans le prochain chapitre, nous aborderons la synchronisation du chaos.

Chapitre 2

Synchronisation des systèmes chaotiques

2.1 Introduction

L'application du chaos à la transmission numérique a gagné en intérêt depuis les travaux de Pecora et Carroll sur la synchronisation chaotique.Ils ont montré que deux systèmes chaotiques identiques en configuration maître-esclave peuvent se synchroniser parfaitement malgré leur sensibilité aux conditions initiales,grâce à la nature déterministe du chaos. Ces recherches sont motivées par les enjeux de sécurité de l'information,où le code chaotique, utilisé comme clé de chiffrement, minimise les risques de détection et d'interruption de signal.La transmission chaotique d'informations, réalisée par le principe de commutation (Chaos Shift Keying),permet de coder les bits à l'émetteur et de les détecter à la réception en comparant les erreurs de synchronisation. Bien que le bruit de canal limite la synchronisation parfaite,des méthodes généralisées permettent de coupler et synchroniser des systèmes chaotiques différents.Récemment, des approches ont exploré les systèmes discrets et hybrides,proposant des méthodes pour évaluer la qualité et la sensibilité de la synchronisation [12][13].

2.2 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[14].

2.3 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 [15].

2.3.1 Synchronisation par répartition du système

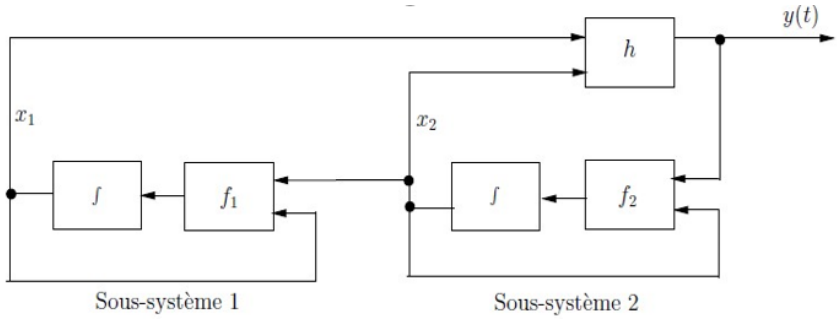


FIGURE 2.1: Principe de Pecora et Carroll.

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 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[15] :

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

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 $y(t)$ [15].

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 [12].

Supposons les deux systèmes suivants :
Émetteur :

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

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.

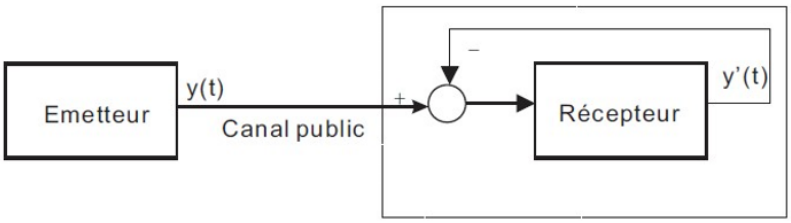


FIGURE 2.2: La synchronisation par la boucle fermée.

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[13].

Son schéma est illustré par cette figure :

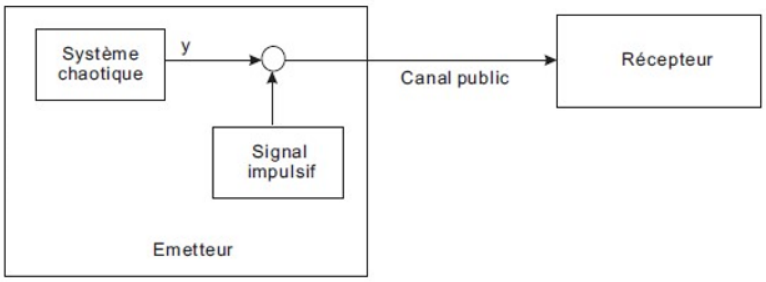


FIGURE 2.3: Synchronisation impulsive.

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 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 [16].

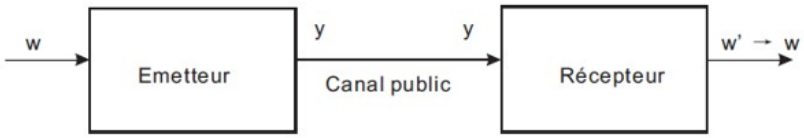


FIGURE 2.4: Synchronisation par l'inversion du système.

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 un difféomorphisme Ψ tel que :

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

indépendamment des conditions initiales.

Remarque 2.1 *Il est à noter que le difféomorphisme Ψ doit être inversible et indépendant des conditions initiales $x_m(0)$ et $x_s(0)$. La synchronisation complète est un cas particulier de la synchronisation généralisée, où la fonction Ψ est égale à l'unité.*

2.3.6 Synchronisation retardée

L'état du système esclave converge vers l'état décalé dans le temps du système maître :

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

où τ est un retard positif[16].

2.3.7 Synchronisation projective

L'état du système récepteur se synchronise avec un multiple de l'état du système émetteur.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 [16] :

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

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.

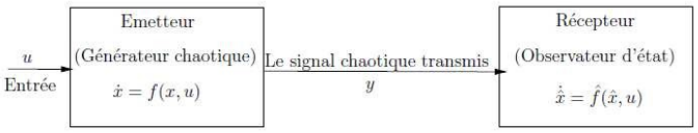


FIGURE 2.5: Principe de la synchronisation à base d'observateur.

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 :

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

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[25].

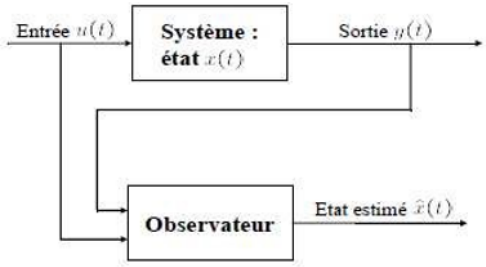


FIGURE 2.6: Principe d'un observateur.

2.4 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 [17].

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.

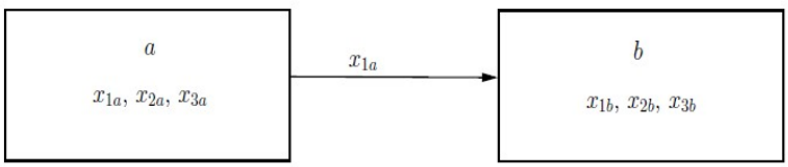


FIGURE 2.7: Schémas de couplage unidirectionnel.

2.4.2 Synchronisation bidirectionnelle

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

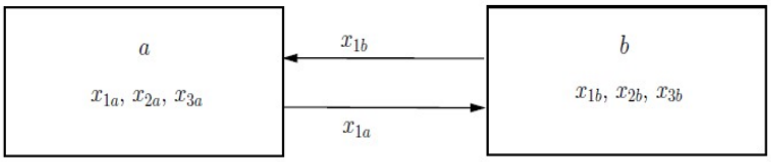


FIGURE 2.8: Schémas de couplage bidirectionnel.

Synchronisation à base d'observateurs : Précédemment,nous avons exploré la notion de synchronisation chaotique basée sur la commande, reposant sur la distinction entre un système maître et un système esclave. À présent, nous allons nous pencher sur une autre approche : celle de la synchronisation basée sur les observateurs, où le maître est un système chaotique et l'esclave est un observateur[25].

Observabilité : Avant d'entamer une procédure de conception d'observateur pour un système dynamique,il est essentiel de s'assurer que l'état de ce dernier peut être estimé à partir des informations sur l'entrée et la sortie. Considérons le système suivant[25] :

$$\begin{cases} \dot{x} = Ax + Bu \\ y = Cx + Du \end{cases} \tag{2.8}$$

où A, B, C et D sont respectivement des matrices constantes de dimensions $n \times n$, $n \times p$, $q \times n$ et $q \times p$.

L'équation d'état (2.8) est dite observable si, pour tout état initial $x(0)$ inconnu, il existe un temps fini $t_1 > 0$ tel que la connaissance de l'entrée u et de la sortie y sur l'intervalle $[0, t_1]$ suffise à déterminer de manière unique l'état initial $x(0)$. Sinon, l'équation est dite non observable.

Observabilité des systèmes linéaires : Pour un système linéaire parfaitement connu, en supposant que l'entrée $u(t)$ est connue et que la matrice B n'intervient pas dans les critères d'observabilité, on peut ramener l'étude de l'observabilité à l'étude de la paire (A, C).

La matrice d'observabilité est définie par :

$$O(A,C) = \begin{bmatrix} C \\ CA \\ CA^2 \\ \vdots \\ CA^{n-1} \end{bmatrix} \tag{2.9}$$

On dit qu'un système linéaire est observable si le rang de $O(A,C)$ est égal à n, où n est la dimension du système.

Observateurs linéaires : Pour la grande majorité des systèmes, la dimension du vecteur d'état est supérieure à celle du vecteur de sortie ($l < n$). Cette considération signifie que, pour tout instant t, le vecteur $x(t)$ ne peut pas être complètement mesuré ou déduit des sorties. Toutefois, sous certaines conditions, il est possible de reconstruire l'état avec l'aide d'un observateur. Une conception astucieuse de cet observateur devrait faciliter une estimation précise et rapide des composantes du vecteur d'état $x(t)$.

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

$$SYS : \begin{cases} \dot{x}(t) = Ax(t) + Bu(t), \\ y(t) = Cx(t), \end{cases} \tag{2.10}$$

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

$$\text{OBS} : \begin{cases} \dot{\hat{x}}(t) = A\hat{x}(t) + Bu(t) + L(y(t) - C\hat{x}(t)) \\ \hat{y}(t) = C\hat{x}(t) + Du(t) \end{cases} \tag{2.11}$$

Avec $x(t) \in \mathbb{R}^n$, $u(t) \in \mathbb{R}^m$ et $y(t) \in \mathbb{R}^l$ représentant respectivement l'état, l'entrée et la sortie du système, et $\hat{x}(t) \in \mathbb{R}^n$ le vecteur d'état de l'observateur, tel qu'il tende asymptotiquement vers $x(t)$, et $\hat{y}(t)$ représentant la sortie du système observateur.

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

$$\lim_{t\to\infty} e(t) = x(t) - \hat{x}(t) = 0 \tag{2.12}$$

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

$$\begin{cases} \dot{\hat{x}}(t) = A\hat{x}(t) + Bu(t) + L(y(t) - \hat{y}(t)) \\ \hat{y}(t) = C\hat{x}(t) \end{cases} \tag{2.13}$$

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

$$e_x(t) = x(t) - \hat{x}(t) \tag{2.14}$$

Observateurs non linéaire : On considère le système non linéaire :

$$\begin{cases} \dot{x} = f(x,u) \\ y = h(x,u) \end{cases} \tag{2.15}$$

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

Indistinguabilité : soient $y_u^0(t), \quad t \geq 0$ et $y_u^1(t), \quad t \geq 0$ deux signaux de sortie générés par l'application de signal d'entrée $u(t), \quad t \geq 0$ au système (2.15) avec les conditions initiales x^0 et x^1 sont indistinguables si :

$y_u^0(t) = y_u^1(t)$, $\forall t \geq 0$, pour tout entrée u. Dans le cas contraire, on dit que x^0 et x^1 sont distinguable.

Observabilité :

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

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

$$L_f h(x) = \sum_{i=1}^{n} f_i(x) \frac{\partial h}{\partial x_i}(x) \tag{2.16}$$

Par définition, on écrit :

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

avec :

$$f(x) = \begin{pmatrix} f_1(x) \\ f_2(x) \\ \vdots \\ f_n(x) \end{pmatrix} \tag{2.17}$$

Le système (2.15) doit satisfaire la condition du rang d'observabilité,c'est-à-dire :

$$\text{rang}(O) = n \quad \text{où} \quad O = \begin{pmatrix} dh \\ dL_f h \\ \vdots \\ dL_f^{n-1} h \end{pmatrix} \tag{2.18}$$

avec n : la dimension du système.

Exemples d'observateurs non linéaires :

Dans le domaine des observateurs non linéaires, on peut citer l'observateur étendu de Luenberger, le filtre de Kalman étendu, ainsi que les observateurs à modes glissants...etc.

2.5 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 [24].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 :

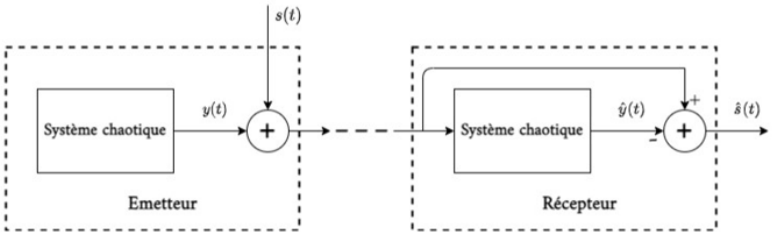


FIGURE 2.9: Cryptage par addition(masquage additif)

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 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.

2.5.2 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 [23]. 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.

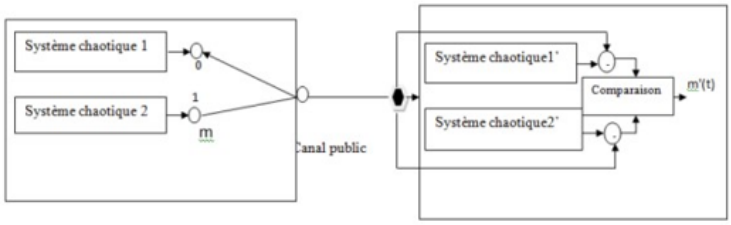


FIGURE 2.10: Cryptage par commutation.

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.

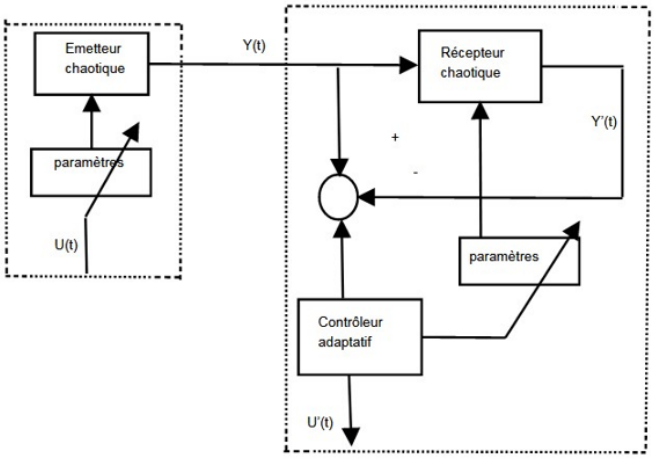


FIGURE 2.11: Cryptage par commutation.

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.

2.5.3 Cryptage par inclusion

Cette technique de cryptage, illustrée ci-dessous, consiste à intégrer le message dans la dynamique de l'émetteur[24]. a 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. Cette méthode présente de nombreux avantages et reste largement utilisée en pratique.

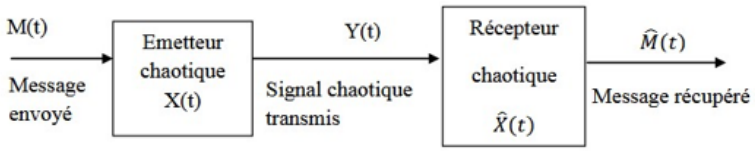


FIGURE 2.12: Cryptage par inclusion.

2.6 Conclusion

La synchronisation des systèmes chaotiques ouvre de nouvelles perspectives pour la transmission numérique sécurisée. Les recherches de Pecora et Carroll ont démontré que, malgré l'imprévisibilité inhérente au chaos, il est possible de synchroniser précisément des systèmes identiques. Cette découverte offre des solutions robustes et sécurisées, cruciales dans le domaine de la sécurité de l'information. L'utilisation du chaos pour le cryptage présente des avantages significatifs, tels qu'une détection faible des symboles d'information et une résilience accrue face aux perturbations du signal. Les techniques de synchronisation chaotique étudiées proposent diverses approches, allant de la synchronisation par répartition du système à l'intégration du message dans la dynamique de l'émetteur.

Dans le prochain chapitre, nous examinerons la conception d'un cryptosystème pour le cryptage d'images.

Chapitre 3

Application au cryptage d'image

3.1 Introduction

L'essor de la numérisation a engendre un impératif croissant de sécuriser les données visuelles contre toute intrusion non autorisée, en particulier les images contenant des informations sensibles. Ce chapitre se concentre sur le cryptage des images, en explorant en détail les méthodes pour sécuriser ces données visuelles, tant du point de vue théorique que pratique. Nous commencerons par définir ce qu'est une image et expliquer son importance dans notre société numérique. Ensuite, nous aborderons les techniques de cryptage utilisées pour protéger les images, en mettant en lumière les étapes clés du processus et leurs résultats. Cette exploration révélera l'importance cruciale de la cryptographie des images dans un monde oe les données visuelles jouent un rôle central. En sécurisant les images, nous assurons la confidentialité et la sécurité des données dans divers domaines. Ainsi, ce chapitre vise e offrir une vue exhaustive de l'application du cryptage sur les images, illustrant son importance croissante dans notre société hautement connectée et soulignant les défis et opportunités dans ce domaine en constante évolution. Il se termine par un exemple de déchiffrement d'image.

3.2 Définition de l'image

Une image est une représentation visuelle voir mentale de quelque chose (objet, être vivant et/ou concept). Elle peut être naturelle ou artificielle [17].

3.3 Définition de l'image numérique

Une image numérique est une image dont la surface est divisée en éléments de taille fixe appelé pixels, dont chacun est caractérisé par une échelle de gris ou un niveau de couleur pris a un emplacement correspondant dans l'image réelle, ou de l'intérieur de la scène ou la description des calculs sont représentés [17].

3.4 Caractéristiques de l'image numérique

L'image est un ensemble structure d'informations caractérisé par les paramètres suivants [18][19] :

3.4.1 Pixel

Un pixel est le plus petit élément d'une image numérique, quand on examine l'image. il se présente comme un carre de couleur uniforme [19].

3.4.2 Dimension

La dimension elle correspond a la taille de l'image. Cette dernière se présente sous la forme d'une matrice dont les éléments sont des valeurs numériques représentant des intensités lumineuses (pixels) [19].

3.4.3 Contour

Les contours se définissent comme la démarcation entre deux pixels ou les niveaux de gris présentent une variation notable.En termes plus simples,ils marquent la transition entre les différents objets présents dans l'image[19].

3.4.4 Résolution

La résolution d'une image numérique désigne la qualité des détails reproduits par un écran ou une imprimante lors de la création d'une image. Pour les écrans d'ordinateur, la résolution est mesurée en nombre de pixels par unité de longueur, généralement en pouces ou en centimètres [18].

3.4.5 Luminance

C'est le degré de luminosité des points de l'image. Elle est définie aussi comme étant le quotient de l'intensité lumineuse d'une surface par l'aire apparente de cette surface lumineuses[18].

3.4.6 Contraste

Le contraste c'est l'opposition apparente entre deux zones d'une image, plus précisément entre les zones sombres et claires de cette image. Le contraste est défini en fonction de la luminosité de deux zones de l'image[19].

3.4.7 Voisinage

Le voisinage dans une image désigne les pixels qui entourent un pixel donne dans un espace bidimensionnel.Ces pixels voisins peuvent être situes au différentes distances et directions par rapport au pixel central,selon la définition spécifique du voisinage utilisée dans le contexte de traitement d'images[19].

3.5 Types d'images numériques

Il existe trois types d'images : binaire, en niveau de gris et couleur qu'on citera ci-dessous [19] :

3.5.1 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 représente le noir absolu tandis que le 1 représente le blanc [19].

3.5.2 Image en niveaux de gris

Le niveau de gris est la valeur d'intensité lumineuse d'un point avec un nombre limite de couches intermédiaires,les pixels peuvent prendre des valeurs allant du noir au blanc.Ainsi, pour représenter une image en niveaux de gris,nous pouvons attribuer a chaque pixel de l'image une valeur qui correspond a la quantité de lumière envoyée [19].

3.5.3 image couleur

Ces images couleurs sont en général codées par les trois couleurs fondamentales 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 code comme une image en niveau de gris avec des valeurs allant de 0 a 225 [19].

3.6 Application de cryptage sur une image

L'application du cryptage sur une image consiste à utiliser des techniques de cryptographie pour rendre une image illisible sans la clé de déchiffrement appropriée. Ce processus peut impliquer différentes méthodes, telles que le chiffrement de l'image entière ou de parties spécifiques de l'image. L'objectif principal est de sécuriser l'image contre l'accès non autorise, en garantissant que seules les personnes disposant de la clé appropriée peuvent la visualiser ou la modifier.

3.6.1 Chargement et Pre-traitement de l'image

- Lecture de l'image "Lena.jpg"
- Charger et convertir l'image en niveaux de gris puis vectoriser l'image
- Obtenir les dimensions nombres de lignes row et nombres de colonnes col et calculer la taille totale des pixels : $s \leftarrow row \times col$

3.6.2 Génération de la séquence de Lozi

- Initialiser les paramètres et conditions initiales : $a_1 = 1.7$, $b_1 = 0.5$, $z_1(1) = 0.1$, $z_2(1) = -0.1$
-
$$\begin{aligned} z_1(i+1) &= 1 - a_1 \left|(z_1(i))\right| + b_1 z_2(i) \\ z_2(i+1) &= z_1(i) \end{aligned} \tag{3.1}$$
- Créer la variable k et générée la clé de cryptage key

$$k(i+1) = 0.628z1(i) + \left|(z_2(i))\right|$$

$k = abs(round(k * 255))$

$ktemp = de2bi(k)$

$ktemp = circshift(ktemp, 1)$

$ktemp = bi2de(ktemp,' left - msb')'$

$key = bitxor(k, ktemp)$

3.6.3 Chiffrement de l'image et transmission avec la carte de Hénon modifié

- Chiffrer l'image : en utilisant bitxor entre key et l'image vectoriser.
- Initialiser les paramètres de la carte de Hénon modifié : $a = 1.6$, $b = 0.1$, $x_1(1) = -0.3$, $x_2(1) = 0.2$, $x_3(1) = 0.4$

$$\begin{aligned} m1(i) &= me(i) * abs(x_1(i)) \\ x_1(i+1) &= a - (x_2(i).^2) - b * x_3(i) \\ x_2(i+1) &= x_1(i) \\ x_3(i+1) &= x_2(i) + m1(i) \\ y(i) &= x_2(i) \end{aligned} \tag{3.2}$$

- transmission de la sortie y du système de Hénon modifie vers le récepteur.

3.6.4 Synchronisation à base d'observateur retardé étape par étape du système de Hénon modifié

$$\begin{aligned} \hat{x}_2(i) &= y(i) \\ \hat{x}_1(i-1) &= y(i) \\ \hat{x}_3(i-2) &= (1/b) * (a - (y(i-2).^2) - \hat{x}_1(i-1)) \\ \hat{m}(i-3) &= \hat{x}_3(i-2) - y(i-3) \\ \hat{m}(i-3) &= \hat{m}(i-3)/abs(\hat{x}_1(i-3)) \end{aligned} \tag{3.3}$$

3.6.5 Synchronisation à base d'observateur retardé étape par étape du système de Lozi et génération de la clé de décryptage

- Observateur pour le Lozi :

$$\hat{z}_2(i-1) = (1/b1) * (\hat{z}_1(i) - 1 + a1 * abs(\hat{z}_1(i-1))) \tag{3.4}$$

- Créer la variable $k1$ et générée la clé de cryptage $key1$

$$k1(i+1) = 0.628\hat{z}_1(i) + |(\hat{z}_2(i))|$$

$k1 = abs(round(k1 * 255))$

$ktemp1 = de2bi(k1)$

$ktemp1 = circshift(ktemp1, 1)$

$ktemp1 = bi2de(ktemp1,' left - msb')'$

$key1 = bitxor(k1, ktemp1)$

– Déchiffrement de l'image : en utilisant bitxor entre $key1$ et le message $\hat{m}$. Puis reconstruction de l'image sous forme de matrice.

3.6.6 Analyse de la sensibilité de la clé

L'analyse de la sensibilité a la clé permet de dévoiler des informations sur la clé secrète d'un schéma de transmission sécurisée. Dans ce type d'analyse, deux clés légèrement différentes sont utilisées pour chiffrer la même image. Les images chiffrées obtenues doivent être totalement indépendantes l'une de l'autre, indiquant une faible corrélation. De plus, une image chiffrée ne doit pas pouvoir être correctement déchiffrée si la clé secrète est légèrement modifiée lors du déchiffrement. Pour vérifier cette sensibilité,on utilise le taux de changement du nombre de pixels (NPCR - Number of Pixels Change Rate) et la moyenne unifiée du changement d'intensité (UACI - Unified Averaged Changed Intensity). Ces critères sont définis comme suit :

$$\text{NPCR} = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} D(i,j) \times 100 \tag{3.5}$$

$$\text{UACI} = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} \frac{|C_1(i,j) - C_2(i,j)|}{255} \times 100 \tag{3.6}$$

Ou M et N representent respectivement la largeur et la hauteur de l'image. Les valeurs $C_1(i,j)$ et $C_2(i,j)$ sont les pixels a la position (i,j) des deux images chiffrees utilisant des cles de chiffrement legerement differentes. Parfois, C_1 et C_2 sont utilises pour designer l'image originale et l'image chiffree. $D(i,j)$ est une matrice de la meme taille que C_1 et C_2 definie comme suit :

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

Calcul du pourcentage de pixels différents entre l'image originale et l'image chiffrée pour l'algorithme proposer le NPCR est de 99.6078‰.

Nous avons remplace le paramètre k par k_1' pour créer une autre clé lors de l'opération de décryptage, avec $k_1' = 0.628 + 10^{-8}$. Le NPCR (Number of Pixel Change Rate) obtenu est alors de 98,78%.

Ensuite,pour l'observateur du système de Hénon modifié, nous avons modifie a en $a + 10^{-7}$ et b en $b + 10^{-7}$, ce qui a donne un NPCR de 99,36%.

Pour l'observateur du système de Lozi, en modifiant a_1 en $a_1 + 10^{-7}$ et b_1 en $b_1 + 10^{-7}$, le NPCR obtenu est de 99,05%. Enfin, le UACI (Unified Average Changing Intensity) du cryptage est de 33,66%.

3.6.7 Entropie d'information

$$H(C) = -\sum_{i=0}^{n} p(c_i) \log_2 \frac{1}{p(c_i)} \tag{3.7}$$

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

Calcul de l'entropie pour l'image originale, chiffrée et déchiffrée.

Image	Originale	Crypter	Décrypter
Entropie	7.4461	7.9991	7.4461

3.6.8 Affichage des histogrammes

Affichage des histogrammes des niveaux de gris de l'image originale, de l'image chiffrée et de l'image déchiffrée pour comparer leurs distributions.

$$\chi^2 = \sum_{i=0}^{Q-1} \frac{(o_i - e_i)^2}{e_i} \tag{3.8}$$

Dans l'equation (3.3), Q est le nombre de niveaux, o_i est la frequence d'occurrence observée de

chaque niveau de couleur (0 – 255) sur l'histogramme de l'image chiffree,et e_i est la frequence d'occurrence attendue de la repartition uniforme, donnee par $e_i = \frac{M \times N \times P}{Q}$,ou M et N presentent la taille de l'image.Pour un bon schema de transmission securisee, la valeur experimentale du χ^2 doit etre inferieure au χ^2 theorique, soit 293 pour $\alpha = 0.05$ (α presente le niveau de signification) et $Q = 256$.

3.6.9 Calcul de la corrélation des pixels

Calcul de la corrélation entre les pixels de l'image originale et de l'image chiffrée dans différentes directions (horizontale, verticale, diagonale). Affichage des résultats sous forme de graphiques pour visualiser la corrélation.

$$r_{xy} = \frac{\text{cov}(x, y)}{\sqrt{D(x)D(y)}} \tag{3.9}$$

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

$$\text{cov}(x, y) = \frac{1}{N} \sum_{i=1}^{N} E(x_i - E(x))(y_i - E(y)) \tag{3.10}$$

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

$$E(x) = \frac{1}{N} \sum_{i=1}^{N} x_i \tag{3.11}$$

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

$$D(x) = \frac{1}{N} \sum_{i=1}^{N} (x_i - E(x))^2 \tag{3.12}$$

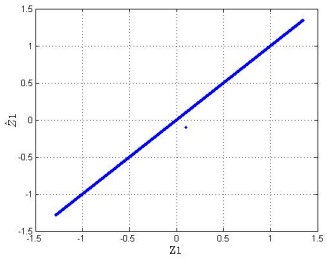
Avec N est le nombre de pixels utilises. La figure 3.10 montre la corrélation des images originales dans les directions horizontale, verticale et diagonale, toutes proches d'une droite. Le tableau illustre ces résultats. En revanche, les images cryptées présentent des coefficients de corrélation

	Image originale	Image crypte
Horizontale	0.9722	-0.005
Verticale	0.9858	-0.0014
Diagonale	0.9593	-0.0027

TABLE 3.1: Les résultats des coefficients de corrélation.

très faibles, ce qui démontre l'efficacité du cryptage proposé.

La figure et les résultats des coefficients obtenus dans le tableau confirment cette observation.



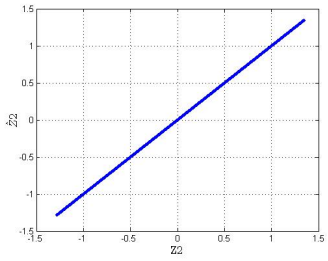
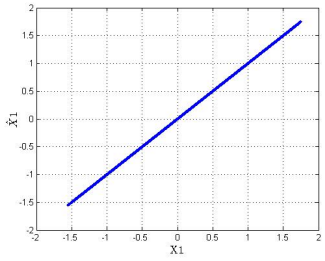
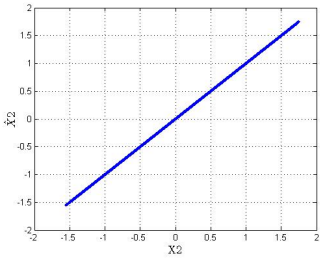


FIGURE 3.1: z_1 versus $\hat{z}_1$. FIGURE 3.2: z_2 versus $\hat{z}_2$.

D'après la figure(3.1) et(3.2) on remarque que les états du système de Lozi et de l'observateur sont synchronisées.





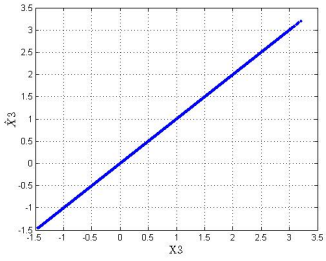


FIGURE 3.3: x_1 versus $\hat{x}_1$. FIGURE 3.4: x_2 versus $\hat{x}_2$. FIGURE 3.5: x_3 versus $\hat{x}_3$.

D'après la figure (3.3),(3.4)et(3.5) on remarque que les états du système de Hénon modifié et les états de l'observateur sont synchronisées.

cette figure(3.6) represente l'image original (celle qu'on va crypter).

Cette figure (3.7) illustre la réussite de cryptage,en effet on a aucune information relative a l'image original sur l'image crypter.

FIGURE 3.6: L'image original.

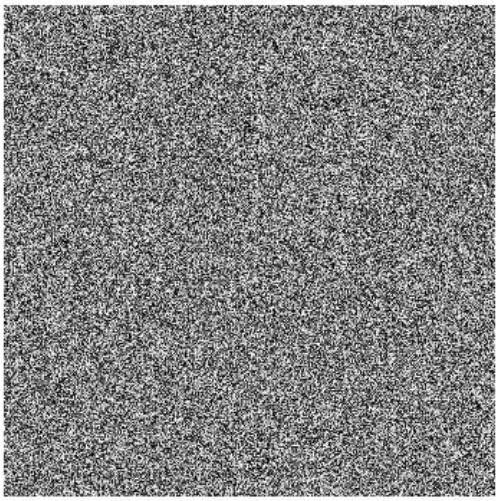


FIGURE 3.7: L'image crypter.

FIGURE 3.8: L'image décrypter.

Cette figure illustre l'image qu'on a réussi a décrypter.

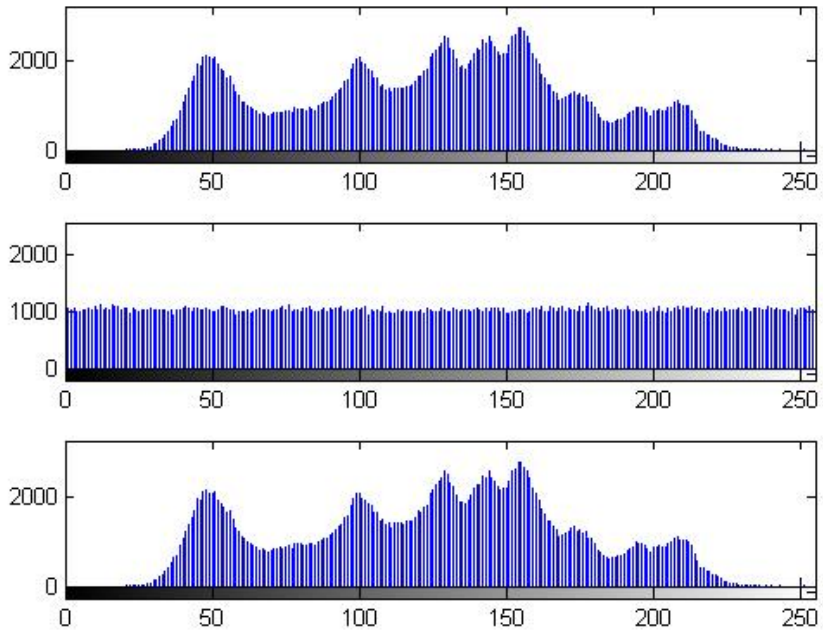


FIGURE 3.9: L'histogramme de l'image original, crypter et décrypter.

L'histogramme est une représentation visuelle des zones de lumière d'une image. La figure 3.9 présente les histogrammes de l'image originale, cryptée et décryptée.

– La première figure montre l'histogramme de l'image originale.

– La deuxième figure montre la distribution uniforme des pixels de l'image cryptée.

– La troisième figure montre l'histogramme de l'image décryptée, qui est similaire à celui de l'image originale. Cela indique que le cryptage a été réussi, car les histogrammes de l'image originale et de l'image décryptée se ressemblent, tandis que l'image cryptée présente une distribution uniforme.

Par exemple, dans l'image cryptée, le nombre de pixels revient régulièrement, alors que dans les deux autres images, certains pixels n'existent pas.

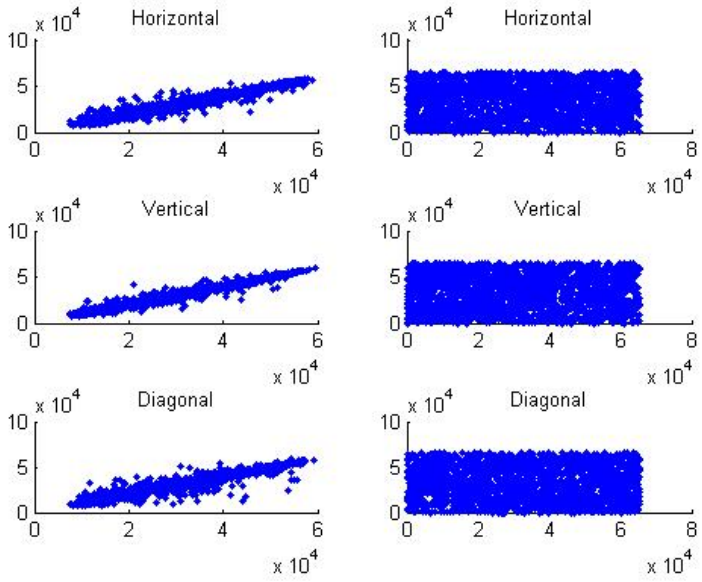


FIGURE 3.10: La corrélation de l'image entre les pixels.

3.7 Conclusion

Cette application de cryptage d'images illustre comment les avancées en cryptographie peuvent protéger les données visuelles. Elle répond e la demande croissante en matière de sécurité et de confidentialité, en soulignant l'importance de la sécurisation des images dans le cadre de la sécurité globale de l'information. En utilisant des mesures d'évaluation de la qualité du chiffrement, elle garantit l'efficacité du système de sécurité. En conclusion, cette application offre une solution puissante pour sécuriser les données visuelles dans un monde numérique en constante évolution, soulignant l'importance de la recherche continue en cryptographie pour relever les défis de sécu-

rité. Dans le prochain chapitre, nous développerons une application sur Raspberry Pi.

Chapitre 4

Application au cryptage d'image avec Raspberry

4.1 Introduction

Ce chapitre présente l'application du crypto-systèmes basés sur des systèmes chaotiques pour le chiffrement d'image à l'aide de la carte Raspberry Pi 3. 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 [20].

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 [20][22].

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 [23].

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 [21].

4.3.1 Introduction des bibliothèques

Pour installer la bibliothèque opencv :

- Commencez par effectuer une recherche sur google en tapant sur (pypi.org) et la fenêtre d'accueil de python s'affichera.
- Ensuite lancez la recherche (opencv).
- Choisir la plus récente.
- Choisissez la clé suivante (pip installe opencv-contrib-python).

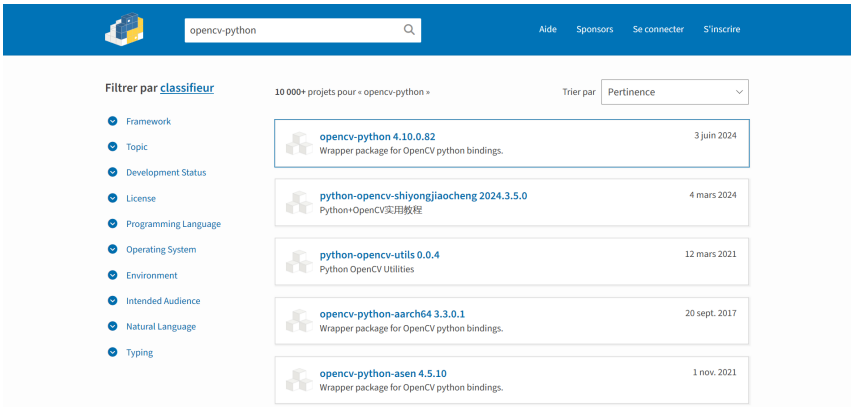


FIGURE 4.1: Choix d'une version

– Lancez "IDLE vous cliquez sur "AppData", puis "programme",puis "python" et "python.12" .
– Ouvrez la commande-cmd.pngs et changez le répertoire en tapant "cd",laissez de l'espace puis collé le chemins d'accès en appuyant sur "entrée".Enfin collé la clé et appuyez sur entré pour lancé l'installation.

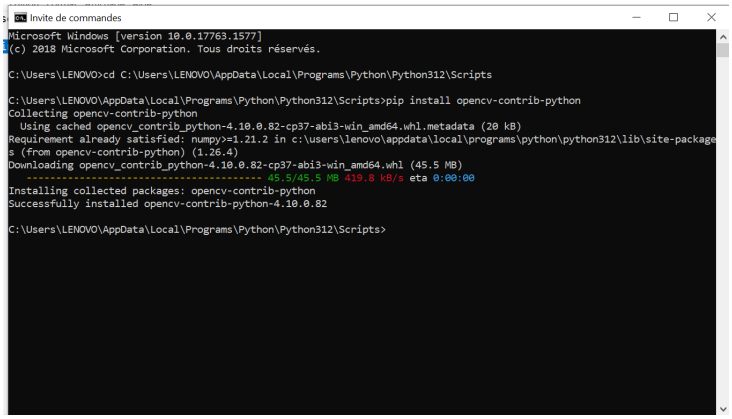


FIGURE 4.2: Installation de opencv

4.3.2 Fonctionnement d'une carte Raspberry

Insertion de la carte mémoire dans l'ordinateur portable, création d'un fichier "SHH",l'enregistrement de ce fichier dans la carte mémoire, puis l'éjecter .

Insertion de la carte mémoire dans la carte Raspberry, puis cliquez sur la barre de recherche "putty" pour ce connecté a la carte.

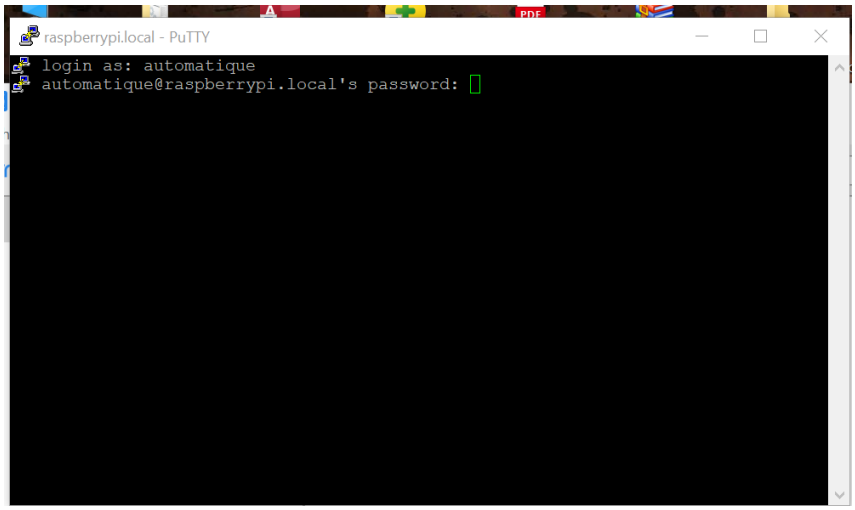


FIGURE 4.3: Connexion à la carte

Ouvrez la fenêtre "realVNC viewer",il s'affiche sur l'écran "putty configuration" et dans HOST Name écrivez "raspberrypi.local" et sélectionnez le "SHH" dans "conection type" puis cliqué sur "open".

Par un double clique sur "raspberrypi.local", la fenêtre s'affiche "authentification" pour intro-

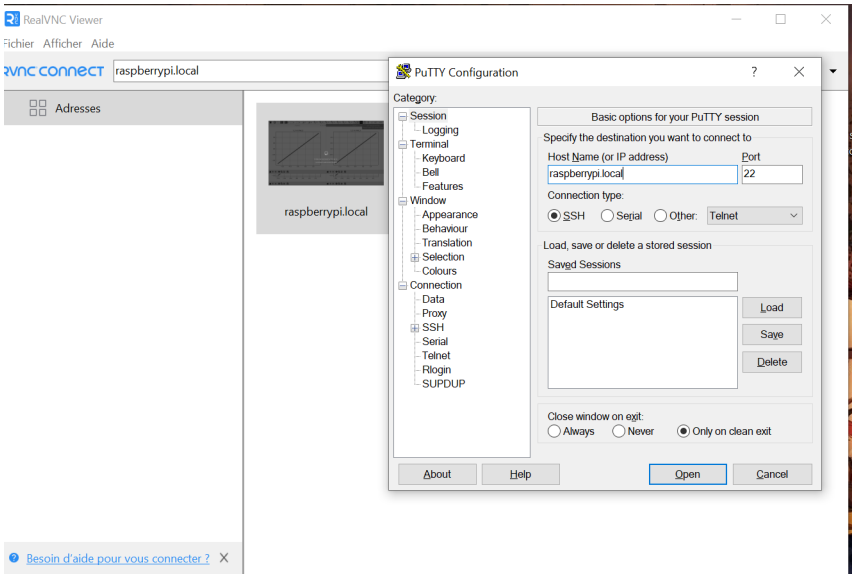


FIGURE 4.4: Connexion au serveur

duire "nom d'utilisateur" et "le mot de passe ".

L'interface de carte Raspberry s'affiche.

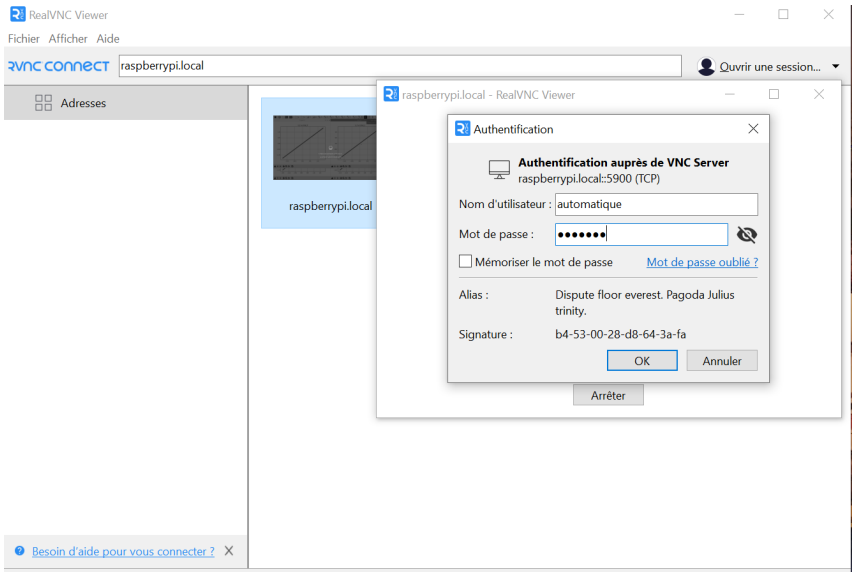


FIGURE 4.5: Connexion à Raspberry

•un clique droit sur le logo "Raspberry", il affichera plusieurs proposition, cliqué sur "IDLE" puis fichier, puis sélectionné le fichier dans vous avez enregistré le programme,ensuite cliqué sur "run" .

4.3.3 Application de l'algorithme de cryptage d'image sous Raspberry Pi 3

Algorithme de cryptage proposer :

1. Initialisation :

- Importer numpy, cv2, matplotlib.pyplot, scipy.stats.

- Lire 'Lena.jpg' et convertir en niveaux de gris : img gray.

- Obtenir row, col et s.

2. Système de Lozi :

- Initialiser $a1, b1$.

- Initialiser $z1[0] = 0.1, z2[0] = -0.1$.

- Pour i de 1 à $s-1$:

$$z1[i] = 1 - a1 * abs(z1[i-1]) + b1 * z2[i-1]$$

$$z2[i] = z1[i-1]$$

$$w[i] = z1[i]$$

$$k[i] = 0.628 * z1[i-1] + abs(z2[i-1])$$

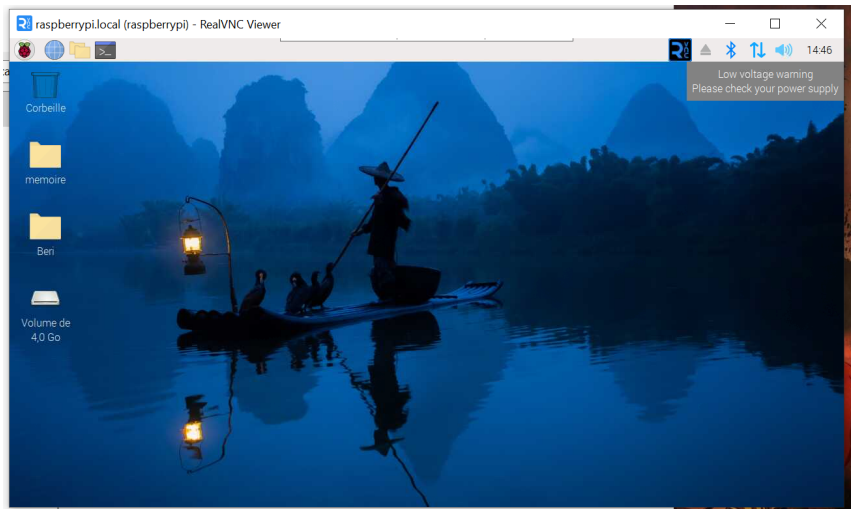


FIGURE 4.6: l'interface de Raspberry

3. Tri et permutation :

- Trier w pour obtenir sorted.

- timg = e[sorted].

4. Génération de la clé pour le cryptage :

$k = abs(np.round(k * 255))$

$ktemp = np.roll(np.unpackbits(k[:, np.newaxis]), 1, axis = 1)$

$ktemp = np.packbits(ktemp).flatten()$

$key = np.bitwise_xor(k, ktemp)$

$timg = np.bitwise_xor(key, timg)$

5. Système Hénon map modifié :

- Initialiser a, b.

- Initialiser $x1[0] = -0.3, x2[0] = 0.2, x3[0] = 0.4$.

- Pour i de 1 à $s - 1$:

$$m1 = me[i-1] * abs(x1[i-1])$$

$$x1[i] = a - (x2[i-1] * *2) - b * x3[i-1]$$

$$x2[i] = x1[i-1]$$

$$x3[i] = x2[i-1] + m1$$

$$y[i] = x2[i]$$

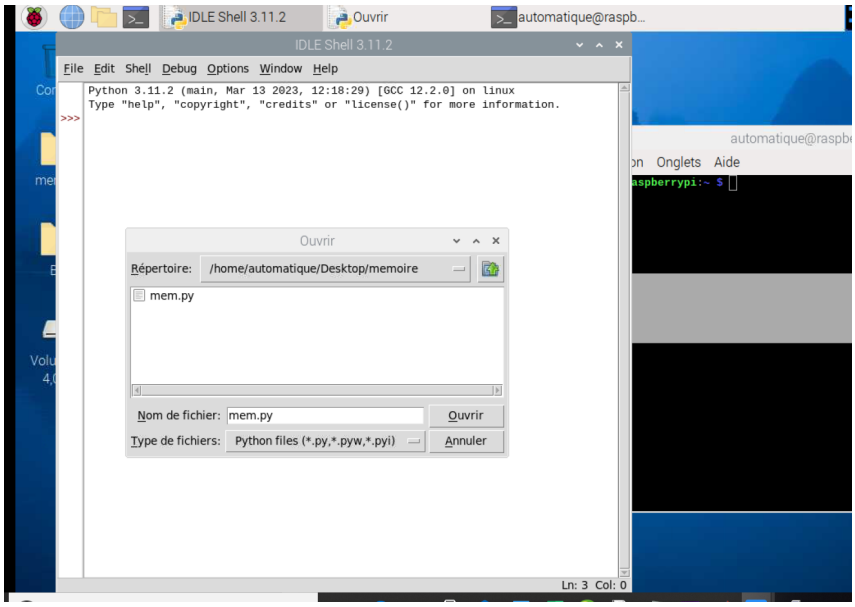


FIGURE 4.7: L'ouverture de L'IDLE sur Raspberry

6. Conversion et reformatage de l'image :

- himg = (timg * 255).

- Reformater himg en (row, col).

7. Observateur 1 :

- Initialiser $xhat2 = y$.

- Pour i de 1 à $s - 1$:

$$xhat1[i-1] = y[i]$$

- Pour i de 2 à $s - 1$:

$$xhat3[i-2] = (1/b) * (a - (y[i-2] * *2) - xhat1[i-1])$$

- Pour i de 3 à $s - 1$:

$$mhat[i-3] = (xhat3[i-2] - x2[i-3])/abs(xhat1[i-3])$$

$mhat1 = (mhat * 255)$

$m3 = append(mhat1, [0, 0, 0])$

$timg = m3.flatten()$

$timg = np.bitwisexor(key, timg)$

8. Observateur 2 :

- Initialiser $zhat1 = w$. - Pour i de 1 à $s - 1$:

$$zhat2[i-1] = (1/b1) * (zhat1[i] - 1 + a1 * abs(zhat1[i-1]))$$

9. Permutation inverse et reformatage de l'image :

- sorted inv = argsort(sorted).

- timg = timg[sorted inv].

- Reformater timg en (row, col).

10. Affichage des résultats :

- Afficher les figures et graphiques pour visualiser les résultats.

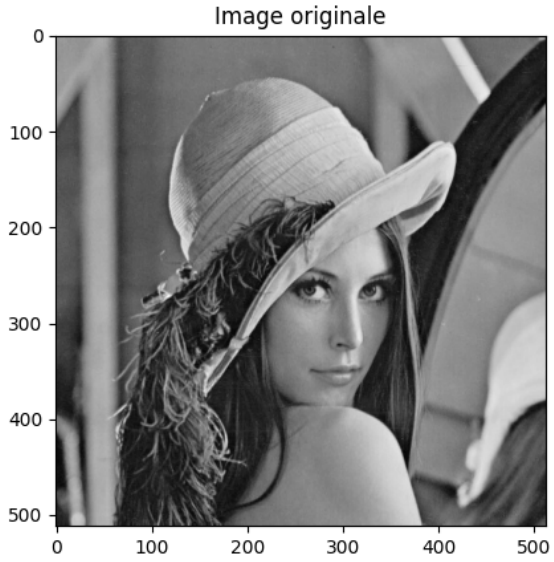


FIGURE 4.8: L'image original

4.3.4 conclusion

Dans l'application du cryptage d'images utilisant le Raspberry Pi, nous avons démontré comment un micro-ordinateur doté de capacités de traitement avancées et d'une grande 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

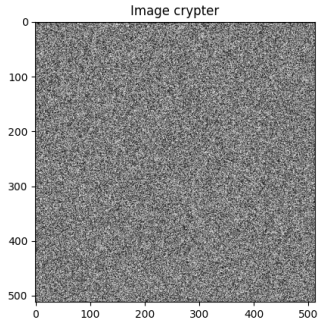
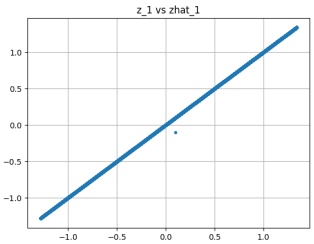


FIGURE 4.9: L'image crypter

FIGURE 4.10: L'image décrypté



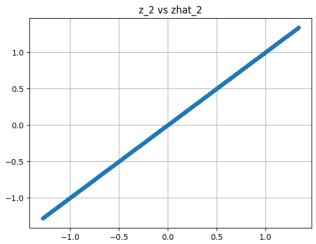


FIGURE 4.11: z1 vs zhat1 FIGURE 4.12: z2 vs zhat2

seulement la fiabilité technique du Raspberry Pi, mais également son rôle crucial dans l'innovation et l'accessibilité des technologies de cryptage, enrichies par nos recherches approfondies.

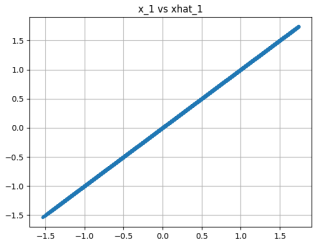


FIGURE 4.13: x1 vs xhat1

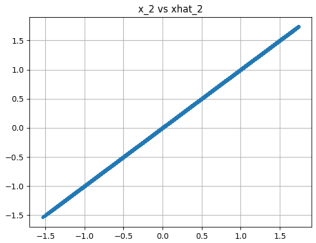


FIGURE 4.14: x2 vs xhat2

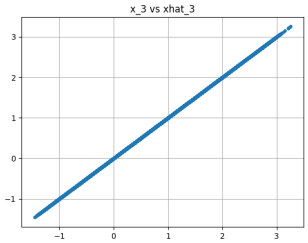


FIGURE 4.15: x3 vs xhat3

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 modifié.

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.

Bibliographie

[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.
[25] The Quantum Universe: (And Why Anything That Can Happen, Does

[26] "Cryptography and Network Security: Principles and Practice" par William Stallings