الجمهورية الجزائرية الديمقراطية الشعبية

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR

ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE MOHAMED SEDDIK BENYAHIA JIJEL

Faculté des sciences et de la technologie

Département d'électronique

MEMOIRE DE FIN D'ETUDE

DOMAINE: Sciences et Technologies

FILIERE: Télécommunications

SPECIALITE: Systèmes de télécommunications

Thème

Application du chaos pour le cryptage des données

Présenté Par : Zine Zoubida **Encadré Par : Dr. Messadi Manel**

Bounar Feriel

Date de soutenance: 12/07/2022

Jury de Soutenance

Président : Dr. Bouridah Hachemi
Encadreur : Dr. Messadi Manel
Examinateur : Dr. Kemih Karim

Promotion : 2021 /2022


بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

REMERCIEMENT

Remerciement

EN premier lieu, nous tenons à remercier ALLAH pour nous avoir donné la force et le courage pour accomplir ce travail.

Nous tenons à remercier tout particulièrement notre promotrice, Dr.MESSADI MANEL ,pour nous avoir encadré et suivi également pour son aide, sa patience, sa disponibilité et surtout ses judicieux conseils.

Nos tenons à remercier chaleureusement les membres du jury de nous faire l'honneur d'accepter d'évaluer notre travail et de l'enrichir par leurs propoitions.

Nous sommes aussi reconnaissantes envers touts les Enseignants du département d'électronique, qui ont contribué à notre formation durant cinq années d'études.

Finalement, nous tenons à exprimer notre profonde gratitude à nos familles qui nous ont toujours soutenues et à tout ce qui participe de réaliser ce mémoire.

DEDICACES

DEDICACE

Merci « Allah» Dieu le tout puissant qui m'a donné le courage, la force et la patience pour réaliser ce travail.

Je dédie le fruit de mes années d'études à mes très chers parents, car sans leur soutient ce travail n'aurait jamais vu le jour.

À mes chers frères Abdelhak ,Ishak et Hichem à ma petite sœur Adoré lina que j'aime énormément

À toute ma famille

À mon binôme et ma meilleure amie « Feriel » pour son soutien et ses encouragements.

Zoubida 

DEDICACE

Aucune dédicace ne saurait exprimer mon respect, mon amour éternel et ma considération pour les sacrifices que vous avez consentis pour mon instruction et mon bien-être.Je vous remercient pour tout le soutien que vous me portez depuis mon enfance et j'espere que votre bénédiction m'accompagne toujours.Que ce modeste travail soit l'exaucement de vos vœux tant formulés,le fruit de vos innombrables sacrifices,bien que je ne vous en acquitterai jamais assez.Puisse ALLAH,le très Haut vous accorder santé ,bonheur et longue vie et faire en sorte que jamais je ne vous déçoive mon père « Zineddine » et la flamme de mon coeur maman « NABILA » .

À mon cher frère « TOUFIK » aucun mot ne pourrait exprimer l'attachement et la tendresse que j'éprouve pour vous,je prie le bon DIEU de te laisse pour nous.

À ma chère sœur « RANIA » présente dans tous mes beaux et mes pires moments par son soutien moral.Je te souhaite un avenir plein de joie , bonheur et sur tous de réussite notre chère docteur .

À celui que j'aime beaucoup et qui m'a soutenue tout au long de ce projet : mon fiancé « BADIS » et à mes chers beaux-parents que j'aime et à mes beaux-frères et à toutes ma belle-famille « BOUCHEMELA » .

À mes grands-parents,mes oncles,mes tantes merci pour leurs amours et leurs encouragements que dieu leur donne une longue et joyeuse vie et À toutes ma famille « BOUNAR ».

Sans oublier mon binome « ZOUBIDA » pour son soutien moral sa patience et sa comprehension.

feriel

Sommaire

Chapitre 3

Chapitre 4

Liste des figures

Chapitre 1

Chapitre 2

Chapitre 3

Chapitre 4

Liste des tableaux

Chapitre 1

RÉSUMÉ

Résumé :

ce présent travail abordé dans ce mémoire porte sur les systèmes chaotiques et leurs applications dans la sécurité de communication en temps continu. On a commencé par des généralités sur les définitions et les concepts des systèmes dynamiques et du chaos qui sont des systèmes déterministes non linéaires et très sensibles aux conditions initiales, Le cryptage d'un message par le chaos accomplir en superposant à l'information initiale un signal chaotique et on a parlé sur les techniques de cryptage actuelles .Pour fondé la synchronisation entre l'émetteur et le récepteur et pour restaurer le message transmis, l'observateur généralisé est utilisé. Les résultats de simulation montrent clairement l'efficacité de l'approche utilisée. Enfin on a mentionné un exemple sur un système hyper chaotique 3D.

Les mots clés: Systèmes dynamiques, chaos, synchronisation, système chaotique, observateur, la sécurité de communication, hyper-chaotique.

ملخص:

يركز هذا العمل الحالي الذي تم تناوله في هذه الرسالة على الأنظمة الفوضوية وتطبيقاتها في أمن الاتصالات في الوقت المستمر. بدأنا بعموميات حول تعريفات ومفاهيم الأنظمة الديناميكية والفوضى التي هي أنظمة حتمية غير خطية وحساسة جدًا للظروف الأولية ، ويتم تشفير الرسالة بالفوضى من خلال فرض إشارة فوضوية على المعلومات الأولية و تحدثنا عن تقنيات التشفير الحالية. لإنشاء التزامن بين المرسل والمستقبل ولاستعادة الرسالة المرسلة ، يتم استخدام المراقب المعمم. تظهر نتائج المحاكاة بوضوح فعالية النهج المستخدم أخيرًا ، ذكرنا مثالًا على نظام ثلاثي الأبعاد شديد الفوضى

الكلمات المفتاحية: الأنظمة الديناميكية ، الفوضى التزامن,نظام فوضوي ،.مراقب ، نظام فوضوي جدا ،امن الاتصالات.

Abstract:

This present work addressed in this dissertation focuses on chaotic systems and their applications in continuous-time communication security. We started with generalities on the definitions and concepts of dynamical systems and chaos which are nonlinear deterministic systems and very sensitive to initial conditions, The encryption of a message by chaos accomplish by superimposing on the initial information a chaotic signal and we talked about current encryption techniques. To establish the synchronization between the transmitter and the receiver and to restore the transmitted message, the generalized observer is used. . The simulation results clearly show the effectiveness of the approach used. Finally we mentioned an example on a 3D hyper chaotic system.

Keywords: Dynamical systems, chaos, synchronization, chaotic system, observer, communication security, hyper-chaotic.

INTRODUCTION GÉNÉRALE

Introduction générale

La recherche mathématique à propos du chaos remonte à 1890, époque à laquelle Henri Poincaré étudie la stabilité du système solaire. En 1970, David Ruelle et Floris Takins commencent à utiliser le concept du chaos pour décrire les phénomènes naturels. Depuis, le nombre de travaux relatifs aux chaos a littéralement explosé. Les scientifiques de toutes les disciplines prennent aujourd'hui conscience de la puissance des techniques développées durant cette période pour apprivoiser le chaos. Ils commencent à appliquer ces techniques à un nombre de plus en plus important de problèmes concernant la physique, la chimie, l'écologie et même l'économie. Mais, du désordre, la raison ne peut rien tirer. Lorsque les mathématiciens se sont intéressés au chaos, c'était pour tenter d'y trouver de l'ordre, et ils y sont parvenus ! Créer de l'ordre, voilà bien une des activités principales des mathématiques. [1]

La sécurisation de la chaîne de transmission devient de plus en plus nécessaire avec l'évolution des communications en termes de nombre d'utilisateurs et nature d'information à transmettre. Actuellement, tout système de communication performant nécessite un système de sécurisation afin de le protéger vis à vis des attaques possibles. Pour cela, de nouvelles méthodes de cryptage sont développées. Le cryptage des informations est maintenant utilisé pour interdire l'accès ou la modification des informations sensibles et garantir la confidentialité dans les communications. Certaines de ces nouvelles méthodes utilisent le chaos dans les systèmes de transmission. [2]

Introduite en 1990 par Picora et Carroll [3], la synchronisation est une technique qui, étant donné deux systèmes chaotiques, consiste à forcer la trajectoire d'un système à suivre celle de l'autre système. Plusieurs méthodes de synchronisation ont été proposées dans la littérature scientifique, elles se basent sur le principe du maître-esclave et permettent de réduire l'erreur entre les trajectoires de l'émetteur et du récepteur [3].

La cryptographie joue un rôle important dans la sécurité et la fiabilité des systèmes de la transmission de données, surtout avec le développement du commerce numérique. Les utilisateurs ont besoin d'authentifier et protéger des données sensibles dans leurs ordinateurs et de garantir la confidentialité des transactions sur des réseaux publics tels que l'internet. [4].

En 1997, H. Nijmeijer et I. Mareels [5] [6] ont montré que la synchronisation unidirectionnelle des systèmes chaotiques peut être considérée comme un problème de synthèse d'observateur. Différents types d'observateurs sont alors proposés par les systèmes chaotiques. Ces observateurs peuvent être destinés uniquement à reconstruire les états de l'émetteur ou servir à reconstruire les états de l'émetteur et récupérer l'information. Le fonctionnement correct de ces observateurs dépend de plusieurs conditions : la condition d'observabilité pour retrouver les états du système, la condition de recouvrement de l'observabilité pour retrouver les états du système et l'information noyée dans le système et la condition d'identifiable des paramètres qui représentent les clés de codage [7].

Dans ce travail de fin d'études, notre objectif consiste à réaliser un système de transmission sécurisé basé sur l'observateur généralisé. Le message à transmettre est injecté dans la dynamique du système chaotique au niveau de l'émetteur, et pour le récupère le message transmis au niveau du récepteur, on utilise un observateur.

Afin d'aborder ce travail, on a divisé ce mémoire en quatre chapitres :

Après une introduction générale, le premier chapitre est consacré à l'introduction et l'étude générale des systèmes chaotiques et on présente ses différentes propriétés et les caractéristiques principales de son comportement.

Dans le deuxième chapitre, nous présentons des généralités sur la cryptographie et les différentes méthodes de chiffrement et de cryptage existantes ainsi que le principe de synchronisation et ses différents types tel que la synchronisation par couplage, unidirectionnelle et bidirectionnelle, dans ce travail nous appliquons la synchronisation à l'aide d'observateur.

Le troisième chapitre traitera quelques concepts généraux sur l'observabilité et les observateurs des systèmes linéaires et non linéaires. Le problème est résolu à l'aide des outils LMI.

Dans le dernier chapitre, nous allons réaliser le schéma de cryptage sous Simulink/Matlab et nous exposons les différents résultats de simulations

Enfin, on termine notre mémoire par une conclusion générale.

CHAPITRE 1

1.1 Introduction

La théorie du chaos fait partie des sciences les plus récentes est devenue l'un des domaines les plus avancés dans la recherche contemporaine. Les origines de cette nouvelle théorie s'étendent aux mathématique et physique des débuts du 20ème siècle, mais elle a émergé dans les années 1960-1970 [3].

En 1963, le météorologue Edward Lorenz expérimentait une méthode lui permettant de prévoir les phénomènes météorologiques. C'est par hasard qu'il observa qu'une modification minime des données initiales pouvait changer de manière considérable ses résultats. Lorenz venait de découvrir le phénomène de sensibilité aux conditions initiales [8].

La théorie du chaos est définie comme une étude des systèmes dynamiques non-linéaires complexes ou les systèmes complexes qui sont exprimés par des récurrences et des algorithmes mathématiques et qui sont dynamiques non constants et non périodiques. Elle inclut l'étude qualitative et quantitative d'un comportement instable non périodique et aléatoire des systèmes dynamiques non linéaires déterministes. Le chaos peut être vu aussi comme un système avec des propriétés stochastiques. Dans toutes les définitions qui peuvent exister pour le chaos, un phénomène fondamental est indispensable : la sensibilité aux conditions initiales [3].

Le chaos a ainsi trouvé de nombreuses applications dans les domaines tant physiques que biologique, chimique ou économique. Ainsi, nous nous intéresserons principalement dans ce chapitre aux systèmes dynamiques chaotiques en nous attardant sur les espaces de phases, les attracteurs étranges et les scénarios de transition vers le chaos (appelés aussi bifurcations), lesquels nous permettront de mieux comprendre la nature du chaos [9].

1.2 Les systèmes dynamiques

Les systèmes dynamiques sont les modèles mathématiques permettant de décrire l'évolution au cours du temps des phénomènes, ces phénomènes pouvant provenir de la physique, la mécanique, l'économie, la biologie, la chimie, etc.

Un système dynamique est constitué d'un espace des phases, l'espace des états possibles du phénomène convenablement paramétré, muni d'une loi d'évolution qui décrit la variation temporelle de l'état du système [4]. On distingue deux types de systèmes dynamiques :

1.2.1 Système dynamique à temps continu

Un système dynamique présente deux aspects, son état et sa dynamique, c'est-à-dire son évolution en fonction du temps.

On appelle système dynamique tout système d'équations différentielles du premier ordre défini par :

$$\frac{dx}{dy} = \dot{x} = f(x, t, v) \quad (1.1)$$

Avec :

$x \in \cup \subseteq \mathbb{R}^n, v \in V \subseteq \mathbb{R}^p$

Le système (1.1) s'appelle un système dynamique, $\mathbb{R}^n$ est l'espace des phases, $\mathbb{R}^p$ est l'espace des paramètres et x est appelé vecteur d'état.

*$f = (f_1, f_2, \ldots \ldots . f_2)^T$ est un champ de vecteurs [10].

1.2.2 Système dynamique à temps discret

On appelle un système dynamique discret tout système d'équations algébriques récurrentes défini par :

$$X_{K+1} = \mathrm{F}\ (X_K\ ,) \quad (1.2)$$

Avec :

$$X_K \in V \subseteq \mathbb{R}^n$$

Et F est la fonction matricielle de récurrence, $X_K \in V \subseteq \mathbb{R}^n$ le vecteur d'état à l'instant t_k et $\mu \in V \subseteq \mathbb{R}^p$ le vecteur des paramètres et $k \in \mathbb{N}$.

* Quand (F) ne dépend pas explicitement du temps, mais seulement de x le système est dit "autonome", Dans le cas contraire, lorsque F dépend explicitement du temps, on a un système "non autonome".

Dans ce qui suit le système est autonome c'est-à-dire [10] :

$$\frac{dx}{dy} = \dot{x} = f(x) \quad (1.3)$$

1.3 Les systèmes dynamiques chaotique

Le phénomène du chaos est un phénomène complexe non linéaire, qui dépend de plusieurs paramètres et qui est caractérisé par une extrême sensibilité aux conditions initiales.

Les systèmes chaotiques sont des systèmes dont les trajectoires évoluent dans une région bornée présentant un caractère stable mais sans toutefois converger vers un point fixe ou un cycle limite. Ces trajectoires qui restent denses dans cette région sont très sensibles aux conditions initiales. Les solutions des équations différentielles non linéaires ne peuvent pas être calculées avec exactitude analytiquement car il n'existe pas de méthode de résolution analytique pour ces équations sauf pour certaines classes particulières. Elles sont alors déterminées numériquement et le comportement du système est analysé par simulation [11].

1.4 Propriétés des systèmes chaotiques

Bien qu'il n'y ait pas de définition mathématique du chaos universellement acceptée, une définition couramment utilisée stipule que pour qu'un système dynamique soit classifié en tant que chaotique, il doit comporter les propriétés suivantes [12] :

- ✓ La non-linéarité
- ✓ Sensibilité aux conditions initiales
- ✓ Le déterminisme
- ✓ Aspect aléatoire
- ✓ Notion d'attracteur
- ✓ Bifurcation
- ✓ Exposants de Lyapunov

1.4.1 La non-linéarité

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

Pour un système dynamique non linéaire, les propriétés de stabilité sont essentiellement plus compliquées que dans le cas linéaire. Quand des non-linéarités sont présentes, plusieurs caractéristiques peuvent apparaitre comme les cycles limites ou le phénomène du chaos. La non-linéarité est une condition nécessaire, mais non suffisante pour que le chaos apparaisse. Donc le comportement chaotique doit venir d'un système non linéaire, mais la non-linéarité n'implique pas nécessairement le chaos [13].

1.4.2 Sensibilité aux conditions initiales

La sensibilité aux conditions initiales est l'une des caractéristiques fondamentales des systèmes chaotiques explicitée par Lorenz dans sa célèbre 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 chaotiques imprédictibles à long terme [14].

1.4.3 Le déterminisme

Un système chaotique est un système déterministe qui réagit toujours de la même façon à un événement, c'est-à-dire que, quoi qu'il se soit passé auparavant, à partir du moment où le système arrive dans un état donné, son évolution sera toujours identique. Le système chaotique a des règles fondamentales déterministes et non probabilistes [15].

1.4.4 Aspect aléatoire

Les systèmes chaotiques se comportent, en effet d'une manière qui peut sembler aléatoire. Cet aspect aléatoire du chaos vient du fait que l'on est incapable de donner une description mathématique du mouvement, mais ce comportement est en fait décrit par des équations non linéaires parfaitement déterministes, comme par exemple les équations de Newton régissant l'évolution d'au moins trois corps en interaction [12].

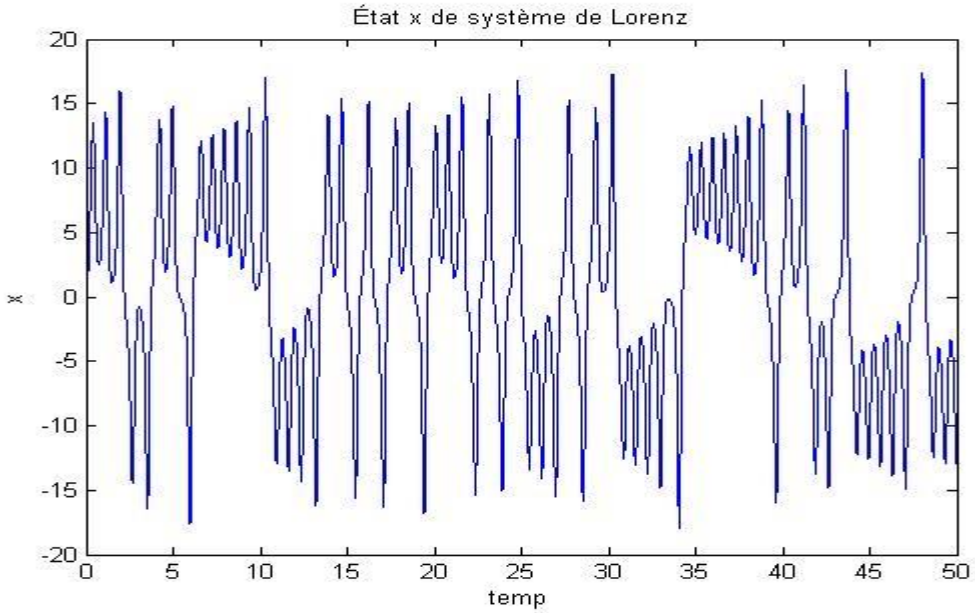

Figure 1.1 : État x de système de Lorenz.

1.4.5 Notion D'attracteur

Tous les points de l'espace de phase sont caractérisés par des trajectoires. Ces dernières sont attirées vers un objet géométrique qui se nomme attracteur, qui est un ensemble où un espace vers lequel un système évolue de façon irréversible. Constituants de base de la théorie de chaos au moins cinq types d'attracteurs sont définit : Ponctuel, Périodique, Ponctuel périodique, Spatial, Étrange [16].

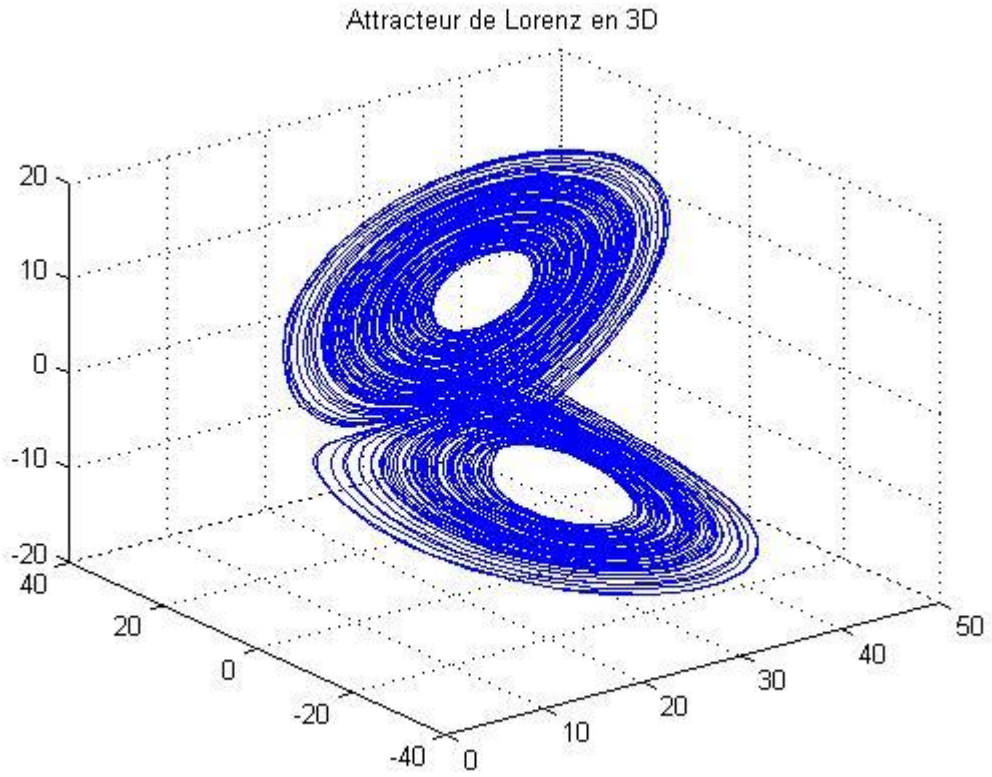

Figure 1.2 : Attracteur de Lorenz.

1.4.6 Bifurcation

La théorie de bifurcation est l'étude mathématique des changements qualitatifs ou topologiques de la structure d'un système dynamique [17].

Une bifurcation survient lorsqu'une variation quantitative d'un paramètre du système engendre un changement qualitatif des propriétés d'un système telles que la stabilité, le nombre de points d'équilibre ou la nature des régimes permanents. Les valeurs des paramètres au moment du changement sont appelées valeurs de bifurcation [18].

La figure ci-dessous illustre le diagramme de la carte logistique.

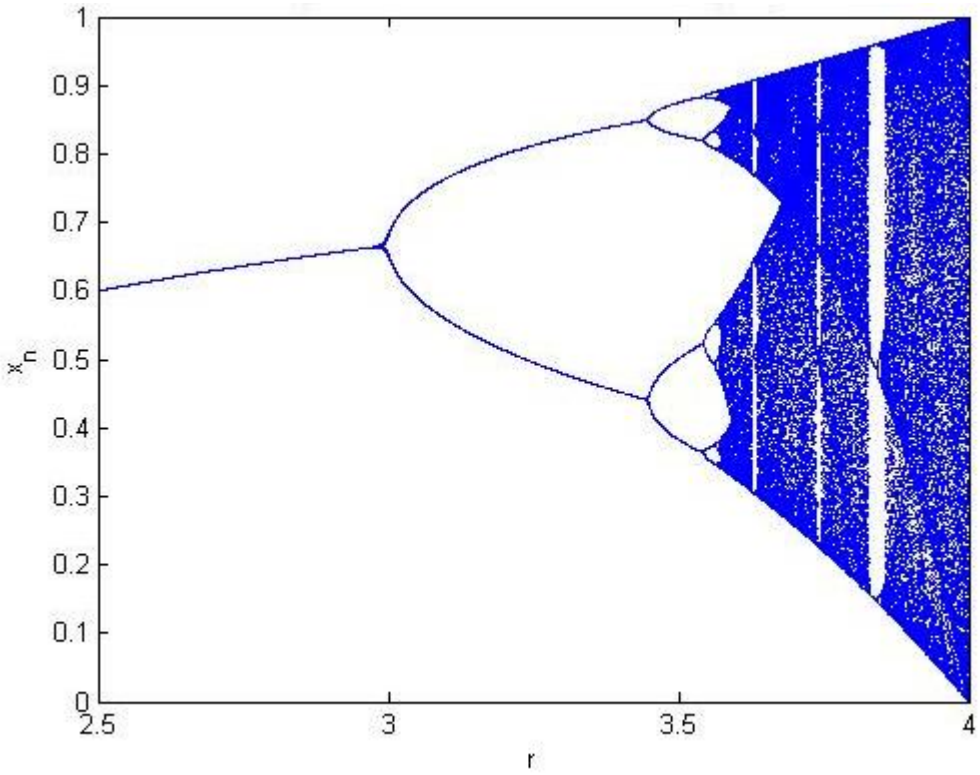

Figure 1.3 : Diagramme de bifurcation de la carte logistique.

1.4.7 Les exposants de Lyapunov

L'évolution chaotique est difficile à appréhender car la divergence des trajectoires sur l'attracteur est rapide. Pour cette raison on essaye si c'est possible de mesurer sinon d'estimer la vitesse de divergence ou de convergence. Cette vitesse est donnée par l'exposant de Lyapunov qui caractérise le taux de séparation de deux trajectoires très proches.

Donc deux trajectoires dans le plan de phase initialement séparées par un taux Z_1 divergent après un temps $\Delta t = t_1 - t_2$ vers Z_2 tel que :

$$|Z_2| \approx \exp(\lambda . \Delta t)|Z_1 \qquad (1.4)$$

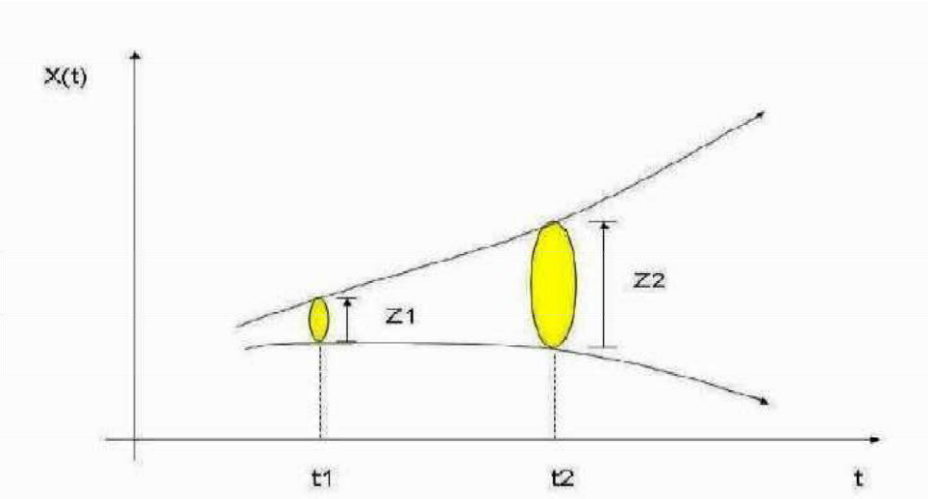

Figure 1.4 : Divergence de deux trajectoires dans le plan de phase.

Considérons un système dynamique dont l'espace des phases est de dimension n et prenons à t=0 une hyper sphère infiniment centré en X appartenant à l'attracteur ($X \epsilon \mathbb{R}^n$) avec un rayon ε_0.

Au temps t cette hyper sphère se transforme en hyper-ellipsoïde de demi-axes

$$\varepsilon_0(t) \approx \exp(\lambda_i\, t) \tag{1.5}$$

i= 1, 2, ……n $\frac{\varepsilon_i}{\varepsilon_0}$

Les exposant de Lyapunov sont tels que

$$\lambda_i = \lim_{t\to\infty} \lim_{\varepsilon_0\to 0} \frac{1}{t} \log(\frac{\varepsilon_i}{\varepsilon_0}) \tag{1.6}$$

Ils caractérisent de façon assez précise la dynamique du système.

Pour un attracteur non chaotique, les exposants de Lyapunov sont tous inférieurs ou égaux à zéro et leur somme est négative. Un attracteur étrange possèdera toujours au moins trois exposants de Lyapunov, dont un au moins doit être positif (voir Tableau 1.1) [9].

Tableau 1.1 : Exposants de Lyapunov et Dimensions.

Etat	**Attracteur**	**Dimension**	**Exposants de Lyapunov**
Point d'équilibre	Point	0	$\lambda_i \leq \cdots \leq \lambda_1 \leq 0$
Périodique	Cercle	1	$\lambda_i = 0$ $\lambda_i \leq \cdots \leq \lambda_1 \leq 0$
Période d'ordre 2	Tore	2	$\lambda_1 = \lambda_2 = 0$ $\lambda_n \leq \cdots \leq \lambda_3 \leq 0$
Période d'ordre K	K-Tore	K	$\lambda_1 = \cdots = \lambda_k = 0$ $\lambda_n \leq \cdots \leq \lambda_{1k+1} \leq 0$
Chaotique		Non entier	$\lambda_1 > 0$ $\sum_{k=0}^{n} \lambda_1 < 0$
Hyper chaotique		Non entier	$\lambda_1 > 0\ \lambda_2 > 0$ $\sum_{i=1}^{n} \lambda_i < 0$

1.5 Les types du système chaotique

1.5.1 Système chaotique à temps continu [19]

Le pendule de Moon est un système physique.

Il est constitué d'un pendule (avec une boule métallique à son extrémité) accroché à une potence légèrement flexible. De plus, le pendule est placé entre deux aimants situés à égale distance de la boule lorsque celle-ci et la potence sont au repos.

La potence est ensuite excitée à l'aide d'un mouvement oscillatoire harmonique d'amplitude constante.

Stimulé, le pendule se met en mouvement et les forces magnétiques dûes aux aimants. Le mouvement est alors chaotique.

L'équation de ce système est dite équation de Duffing :

$$\ddot{X} + m\dot{X} - \frac{1}{2}(1 - X^2) \tag{1.7}$$

X est la position du pendule.

m est la masse de la boule métallique, *a* est l'amplitude de l'excitation et *w* est la pulsation de cette excitation.

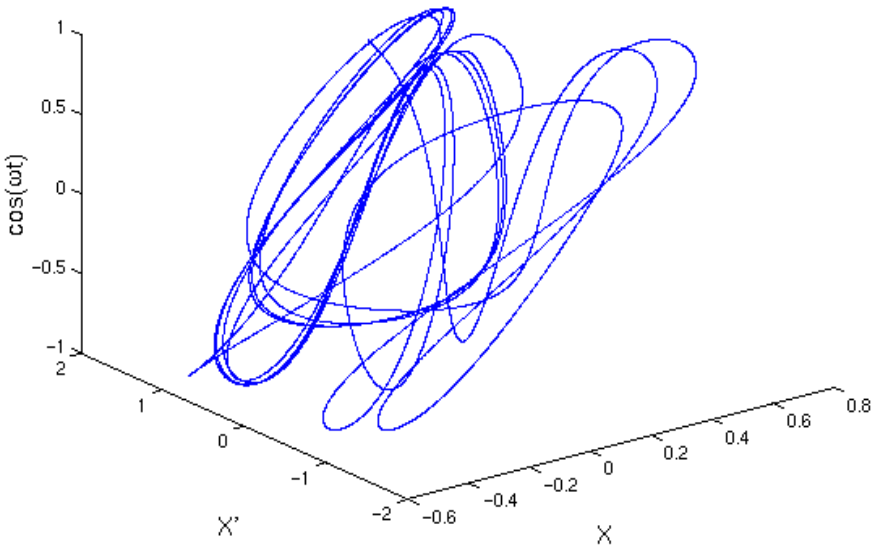

Figure 1.5 : Porterait de phase du système chaotique de Duffing

Pour *m = 0.15*, *a = 0.15* (en fait, entre *0.1* et *0.2* environ) et *w = 0.81* (en fait, entre *0.8* et *0.82*)

1.5.2 Systèmes chaotiques à temps discrets

1.5.2.1 Système de Hénon

En 1976 le mathématicien Michel Hénon proposa le système de Hénon.

L'attracteur de Hénon est un système dynamique à temps discret. C'est l'un des systèmes dynamiques ayant un comportement chaotique les plus étudiés.

L'attracteur de Hénon prend tout point du plan (x, y) et lui associe le nouveau point [20] :

$$\begin{cases} x(n+1) = 1 - a * x(n)^2 + y(n) \\ y(n+1) = x(n) \end{cases} \quad (1.8)$$

Il dépend de deux paramètres, *a* et *b*, qui ont pour valeurs *canoniques* : *a* = 1.4 et *b* = 0.3. Pour ces valeurs, l'attracteur de Hénon est chaotique

La figure (1.4) présente l'attracteur de système de Hénon

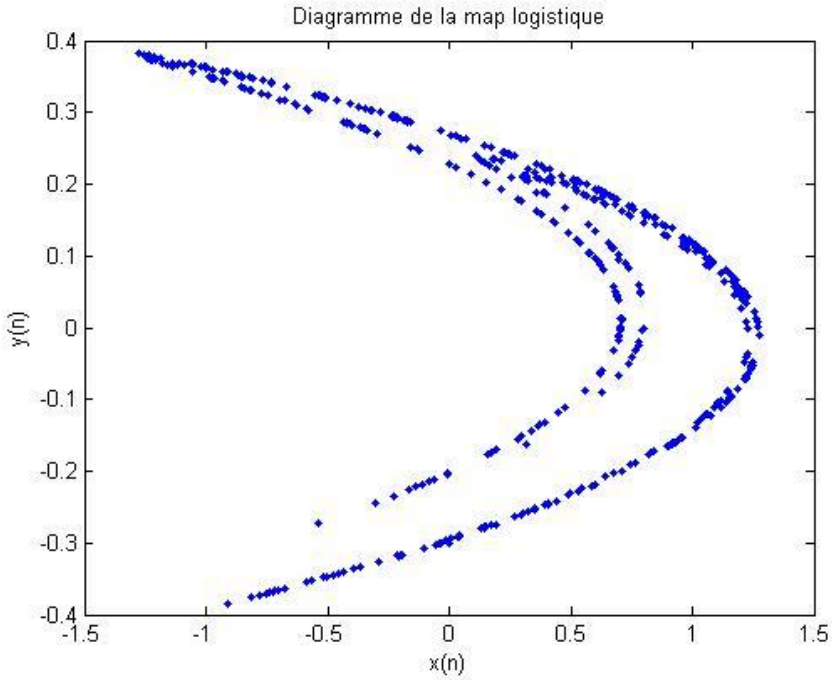

Figure 1.6 : L'attracteur de système de Hénon.

1.6 Conclusion

L'objectif de ce chapitre est de présenté les notions principales des systèmes chaotiques. Nous avons commencé par présenter quelques définitions concernant les systèmes dynamiques en général et les systèmes chaotiques en particulier ainsi que leurs propriétés, telle que la sensibilité aux conditions initiales, les exposants de Lyapunov etc.... Nous avons ensuite cité des types des systèmes chaotiques, à savoir les systèmes à temps continu et à temps discret à travers quelques exemples.

Le prochain chapitre sera consacré à la synchronisation des systèmes chaotiques ainsi que leurs applications pour le cryptage d'information.

CHAPITRE 2

2.1 Introduction et histoire

La cryptographie a eu une histoire intéressante, ses racines remontent vers 2000 avant J.C en Égypte lorsque les hiéroglyphes furent utilisés pour décorer les tombes an de raconter l'histoire de la vie du défunt. Une méthode de cryptographie de l'alphabet Hébreu requis pour être retournée an que chaque lettre dans l'alphabet d'origine est associée à une lettre différente dans l'alphabet inversé. Cette méthode de cryptage a été appelée méthode d'**Atbash**.

Vers 400 avant J.C, les Spartiates utilisaient un système de cryptage des informations en écrivant un message sur une bande de papyrus, ou une lanière de cuir, puis l'enroulaient autour d'une scytale, cette dernière est considérée comme l'ancêtre des systèmes de transmissions secrète. Jules César a développé une autre méthode simple de déplacer les lettres de l'alphabet, analogue au système Atbash, cela consiste en un chiffrement par un simple décalage. Au XXe siècle, une nouvelle machine à chiffrer est apparue, les messages créés par cette machine ont été difficile à briser. Ce travail a fait place à la machine de chiffrement la plus célèbre de l'histoire à ce jour : **La machine allemande Enigma**.

Avec les ordinateurs, la cryptographie se développe de manière importante et de nombreuses méthodes de cryptage sont apparues. Jusqu'à maintenant, Il existe de nombreuses méthodes de crypter, notamment : DES, AES, RSA, DSS ... etc.

Le chaos joue un rôle essentiel dans de nombreux algorithmes de cryptage, dans ce chapitre, nous expliquerons le concept de cryptage et de cryptage qui dépend du chaos [21].

2.2 Définitions

La cryptographie est l'étude des techniques mathématiques liées à la sécurité de l'information [22].

Le terme cryptographie provient des deux mots grecs anciens « Kruptos » qui signifie « cacher » et « graphein » qui signifie « écrire ». Ce qui signifie littéralement, « cacher l'écriture ». Le Petit Larousse donne la définition suivante : « Ensemble des techniques de chiffrement qui assurent l'inviolabilité de textes et, en informatique, de données. » On présente quelques définitions et concepts basiques en cryptographie :

Cryptographie : est la science de l'écriture secrète, qui nous permet de stocker et de transmettre les données sous une forme qui est disponible uniquement pour les individus auxquels elles sont destinées.

Crypto-système : est l'ensemble des deux méthodes de chiffrement et de déchiffrement, il est le matériel ou logiciel de mise en œuvre de la cryptographie, qui transforme un texte clair en un texte chiffré et de retour au clair.

Algorithme : ensemble de règles mathématiques utilisées dans le cryptage (chiffrement) et le décryptage (déchiffrement).

Cryptage : processus de masquer un message an de cacher son contenu.

Décryptage : est l'opération qui permet de retrouver le message clair correspondant à un message chiffré sans posséder la clé de déchiffrement.

Chiffrement : est l'opération qui consiste à transformer, au moyen d'une information appelée clé, un message afin d'en cacher le sens à tous ceux qui ne sont pas autorisés à le connaître.

Déchiffrement : est l'opération inverse du chiffrement. Il a pour but de récupérer l'information masquée, connaissant la clé secrète.

Cryptanalyse : Ensemble des techniques mises en œuvre pour tenter de déchiffrer un message codé dont on ne connaît pas la clé vaut dire c'est une science consistant à obtenir le texte clair à partir du texte crypté (chiffré) sans avoir la clé, ou briser le ciphertext [23].

Cryptologie : l'étude de la cryptographie et la cryptanalyse est la science du secret. Elle réunit la cryptographie « écriture secrète » et la cryptanalyse (étude des attaques contre les mécanismes de cryptographie) [24].

Ciphertext : le texte crypté (chiffré) ou illisible. Décryptage : processus de convertir le ciphertext en plaintext.

Plaintext : le texte clair (texte, audio, image, vidéo,...etc).

Clé secrète : séquence de caractères et d'instructions qui régit l'acte de cryptage et décryptage au regroupement.

Clé symétrique : clé utilisée pour le cryptage et le décryptage.

Clé asymétrique : paire de clés (publique, privée) la clé publique est utilisée pour le cryptage, et la clé privée est utilisée pour le décryptage.

Espace de clés : ensemble des valeurs possibles que les clés peuvent prendre [25].

Clef : Dans un système de chiffrement, elle correspond à un nombre, un mot, une phrase, etc. qui permet, grâce à l'algorithme de chiffrement, de chiffrer ou de déchiffrer un message [26].

Le cryptage proprement dit, ou comment mélanger et séparer les données du signal chaotique, est l'étape finale pour construire le système de communication chaotique. Un signal chaotique porteur d'informations représente une généralisation de systèmes conventionnels de modulation. Ainsi, un message source à faible amplitude est masqué par un signal chaotique plus large [1].

Etymologiquement la cryptographie veut dire écriture secrète mais sa définition générale qu'on peut donner est : l'art de rendre les messages échangés entre deux entités communicantes à

travers un canal non sécurisé, incompréhensibles sauf par leur destination légitime qui possède la clé de déchiffrage de ces messages.

En parallèle de la cryptographie, s'est développée la cryptanalyse ; c'est en quelque sorte l'opposée de la cryptographie. En effet, si déchiffrer consiste à retrouver le clair au moyen d'une clé, cryptanalyser c'est tenter de briser le message crypté ou tester la robustesse d'un crypto-système. Ces deux domaines sont regroupés sous la dénomination de la cryptologie qui désigne la science des messages secrets [27].

2.3 Méthodes de chiffrement

Les méthodes de chiffrement sont classées en deux types, le chiffrement classique qui traite des systèmes reposant sur les lettres et caractères d'une langue quelconque. Ses principaux outils utilisés remplacent des caractères par d'autres et les transposent dans des ordres différents, avec de différents degrés de difficulté, en revanche le chiffrement moderne utilise des méthodes plus complexes, appelées : « algorithmes » en raison de l'apparition des ordinateurs et il opère directement sur des bits [11].

2.3.1 Cryptographie classique

Cette partie traite quelques crypto-systèmes célèbres, avant l'ère des ordinateurs qui ont été les bases pour l'évolution de plusieurs algorithmes de cryptographie utilisés actuellement. Les crypto-systèmes classiques sont regroupés en chiffrement monoalphabétique et polyalphabétique [28] [29].

- **Chiffrement par substitution**

Le chiffrement par substitution consiste à substituer chaque caractère du message clair par un autre caractère, et pour que le récepteur puisse le déchiffrer, il lui faudra appliquer la substitution en inverser, la complexité des systèmes à substitutions dépend de trois facteurs :

- la composition spécifique de l'alphabet utilisé pour chiffrer ou pour communiquer.
- le nombre d'alphabets utilisés dans le cryptogramme.
- la manière spécifique dont ils sont utilisés. Et on distingue quatre types de chiffrement par substitution :

– Substitutions mono-alphabétiques : consistent à remplacer chaque lettre du message clair par une autre lettre ou caractère.

– Substitutions poly-alphabétiques : opèrent en remplaçant chaque lettre du message clair par plusieurs caractères ou plusieurs lettres à la fois.

– Substitutions polygrammiques : contrairement aux autres types de substitutions, celles-ci consistent à chiffrer les lettres par groupes et non séparément.

– Substitutions tomographiques : opèrent d'abord par substitutions poly-alphabétiques en remplaçant chaque lettre par plusieurs lettres où symboles puis ensuite elles sont chiffrées séparément par substitution ou transposition [11].

2.3.2 Chiffrement moderne

De nos jours pratiquement, la cryptographie est englobée par deux grands algorithmes de chiffrement. On distingue les algorithmes à clef secrète et les algorithmes à clef publique. La sécurité de ces systèmes est calculatoire [28]. Ainsi leur puissance réside dans l'incapacité des calculateurs à les casser dans un temps humainement raisonnable.

2.3.2.1 La cryptographie à clé secrète (symétrique)

Le cryptage symétrique est une forme de crypto-système, également appelé cryptage conventionnel ou chiffrement à clé secrète. Il est caractérisé par l'utilisation d'une même clé pour le chiffrement et pour le déchiffrement, qui est choisie préalablement par l'émetteur et le récepteur et qui doit être gardée secrète, car la sécurité de ces algorithmes repose sur cette clé [11].

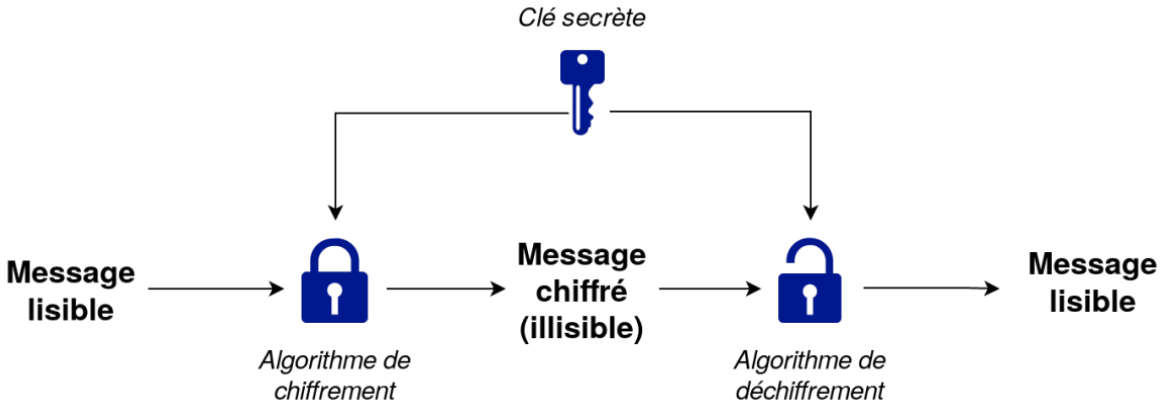

Figure 2.1 : schéma du chiffrement symétrique.

2.3.2.2 Système de chiffrement à clé publique ou asymétrique

Dans ces crypto-systèmes, chaque acteur de la communication sécurisée possède 2 clés distinctes (une privée, une publique) avec l'impossibilité de déduire la clé privée à partir de la clé publique qui est distribuée librement. Ce principe est illustré sur la figure 2.2 [23] .

Les principaux algorithmes asymétriques à clé publique les plus utilisés sont :

1. RSA.
2. DSA.
3. Diffie-Hellman [11].

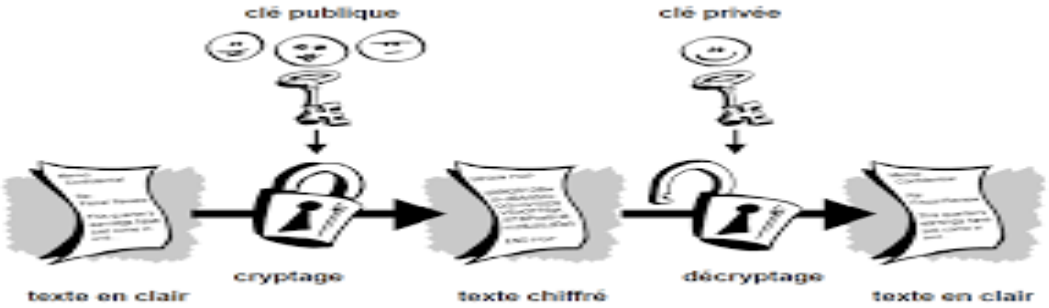

Figure 2.2 : Schéma du chiffrement asymétrique.

2.4 Synchronisation des systèmes chaotiques

2.4.1 Définition

La synchronisation de deux systèmes dynamiques signifie que chaque système évolue en suivant le comportement de l'autre. Ce concept repose sur le fait qu'un système chaotique est déterministe et possède un ou plusieurs exposants de Lyapunov positifs et qu'il est instable. Supposons deux systèmes chaotiques identiques oscillant de façon totalement indépendante, Si par un moyen quelconque, on leur permet d'échanger de l'énergie, action que l'on nomme "Couplage'', les deux systèmes finiront par céder la place à un comportement commun, ils finiront par se synchroniser [30].

La synchronisation de deux systèmes S_1 et S_2 peut être définie comme suit :

$$\begin{cases} S_1 : \dot{x} = f_1(x,u) \\ S_2 : \hat{x} = f_2(x,u) \end{cases} \qquad (2.1)$$

Avec $\dot{x}(t), \hat{x}(t) \in \mathbb{R}^n$, f_1 et f_2 des fonctions non linéaires définies de $\mathbb{R}^n \to \mathbb{R}$.

Les deux systèmes sont synchronisés si :

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

Avec :

$\dot{x}(t)$: L'état du système maître (S_1).

$\hat{x}(t)$: L'état du système esclave (S_2) [31].

2.4.2 Principe de la synchronisation chaotique

Lorsque un message $m(t)$ est injecté à l'entrée d'un émetteur chaotique, celui-ci génère un signal $y(t)$ qui est transmis au récepteur par l'intermédiaire d'un canal. Le récepteur doit donc se charger de récupérer l'information en effectuant l'opération inverse de l'émetteur, il est donc nécessaire de synchroniser les deux systèmes afin de reconstruire l'information exacte. En conséquence, la synchronisation consiste principalement à raccorder l'émetteur et le récepteur d'une manière à restituer l'information telle quelle. La figure 2.3 illustre le principe de la communication chaotique.

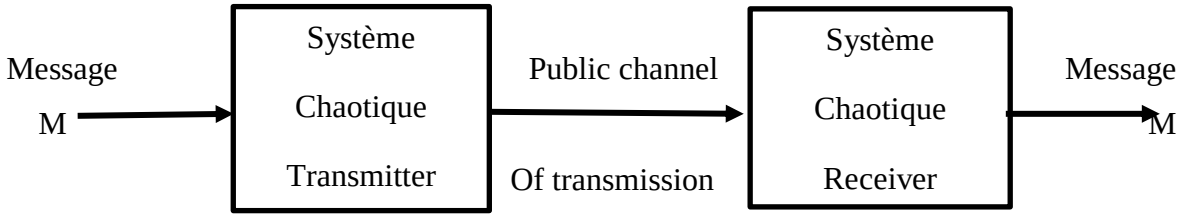

Figure 2.3 : Principe de la communication chaotique.

Si on suppose que l'on dispose de deux systèmes chaotiques identiques, le problème qui se pose est la sensibilité aux conditions initiales qui se traduit par une instabilité au sens de Lyapunov, et qui conduit à des signaux totalement différents. Cela signifie qu'il est impossible de reproduire ces conditions initiales dans un système réel. En 1990, Pecora et Caroll [32] ont montré que deux systèmes chaotiques identiques avec des conditions initiales différentes peuvent éventuellement se synchroniser s'ils sont couplés de façon à placer l'émetteur en maître du récepteur afin qu'il force la synchronisation du récepteur en esclave, comme le montre la figure 2.4.

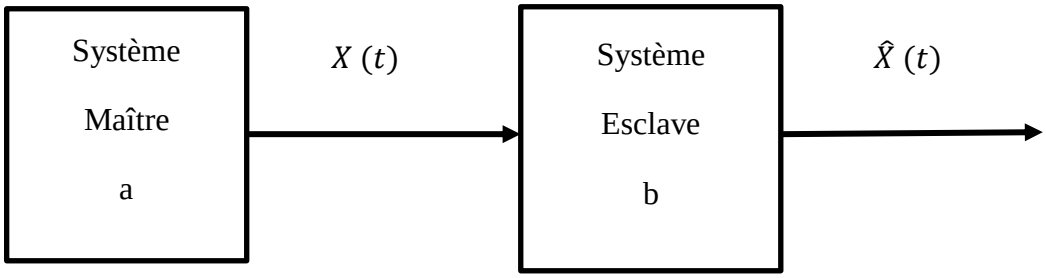

Figure 2.4 : Système maître-esclave pour réaliser la synchronisation.

2.5 Méthodes de synchronisation

Il y a plusieurs méthodes de synchronisations, dans ce que suit, nous allons présenter les méthodes les plus performantes et principales.

2.5.1 Synchronisations identiques

Pour illustrer la méthode de synchronisation par couplage entre deux systèmes chaotiques on a choisi de présenter la synchronisation identique proposée par Pecora et Carroll. Celle-ci a l'avantage de représenter une solution simple et performante de synchronisation dont l'objectif est que l'esclave reproduise le plus fidèlement possible l'état du maître, après un régime transitoire [32] [33].

2.5.2 Synchronisation par couplage

On dit que deux oscillateurs sont couplés, si l'existence d'une petite perturbation dans l'un des oscillateurs entraîne une perturbation dans l'autre. Physiquement, cet effet se traduit par un transfert d'énergie entre les deux oscillateurs. Ce type d'accouplement s'appelle en général accouplement mutuel [34].

Il est possible de coupler les systèmes chaotiques dans un sens (couplage unidirectionnelle) ou dans deux sens (couplage bidirectionnelle). Dans le cas d'un couplage unidirectionnel, l'énergie est transférée d'un système à un autre à l'aide d'un élément de couplage fonctionnant dans un seul sens comme le cas d'un suiveur. Par contre dans le couplage bidirectionnel l'élément de couplage permet l'échange de l'énergie dans les deux sens, ceci par une résistance [35].

2.5.2.1 Synchronisation unidirectionnelle

Dans le cas d'une synchronisation unidirectionnelle, le couplage entre deux systèmes identiques a et b est réalisé à l'aide d'un élément fonctionnant dans un seul sens, par exemple l'utilisation d'un circuit électrique suiveur [14].

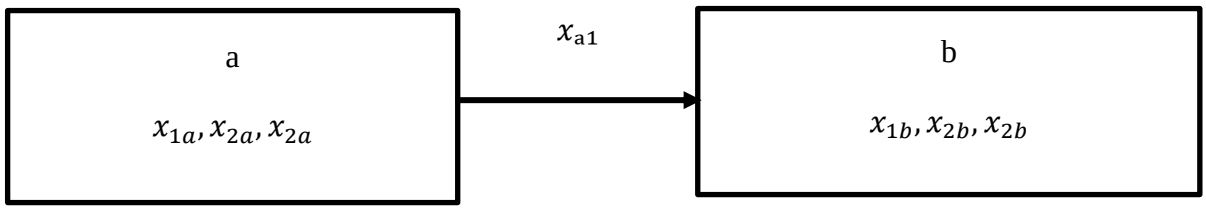

Figure 2.5 : Couplage unidirectionnel.

2.5.2.2 Synchronisation bidirectionnelle

Dans le cas d'une synchronisation bidirectionnelle, le couplage entre deux systèmes identiques a et b est réalisé à l'aide d'un élément permettant l'échange d'énergie dans les deux sens, par exemple l'utilisation d'une simple résistance [14].

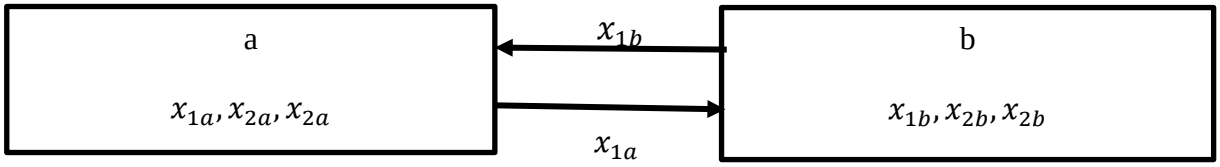

Figure 2.6 : Couplage bidirectionnel.

2.5.3 Synchronisation par boucle fermée

La synchronisation des systèmes chaotiques par les méthodes en boucle ouverte implique une sensibilité aux variations paramétriques. Pour y remédier, de nouvelles techniques basées sur un bouclage par contre-réaction ont été proposées. L'idée est d'appliquer une correction au système en fonction de l'erreur entre le signal transmis par le premier système et le signal régénère par L'autre. Cette erreur est ainsi injectée en contre-réaction d'ou l'appellation de l'approche. Cette technique permet également la synchronisation entre des paires différentes de systèmes chaotiques [18].

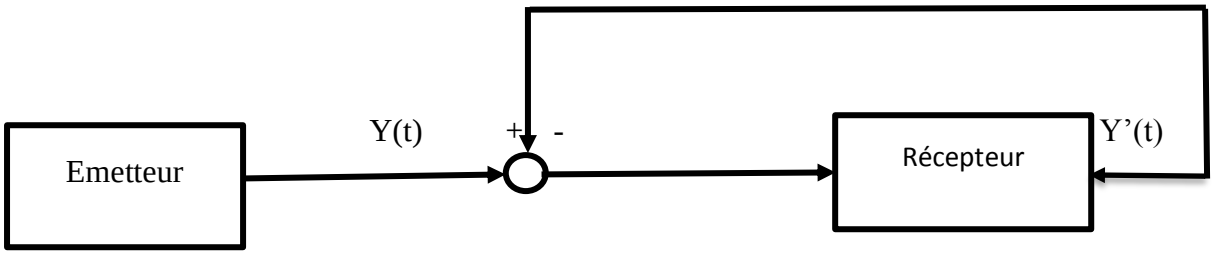

Figure 2.7 : Synchronisation par boucle fermée.

2.5.4 Synchronisation par l'inversion du système

Jusqu'à présent, toutes les approches mentionnées sont dans le but de synchroniser Seulement les états du système, et ne concernent pas la synchronisation (ou plus exactement l'estimation) des entrées inconnues du système. Cependant, la possibilité d'estimer les entrées inconnues est évidemment essentielle à la transmission chaotique de donnés puisque l'entrée inconnue est généralement un message confidentiel [36].

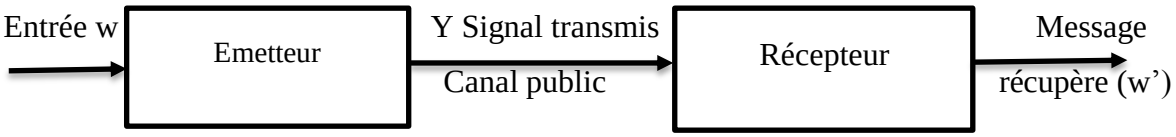

Figure 2.8 : Synchronisation par l'inversion du système.

2.5.5 Synchronisation retardée

Dans cette synchronisation l'état du système tend vers l'état décalé dans le temps du système maître c'est-à-dire :

$$\lim_{t\to 0}\|x'(t) - x(t-\tau)\| = 0$$

Où $x(t)$ ⟶ L'état du système émetteur.

$x'(t)$ ⟶ L'état du système récepteur et τ est un retard positif.

2.5.6 Synchronisation à base d'observateurs

Grâce aux résultats de synchronisation à base d'observateurs, obtenus pour le cas de systèmes entiers, et aux nombreux travaux et théories élaborées dans le cas de systèmes dynamiques d'ordre fractionnaire, plusieurs observateurs ont été proposés pour l'estimation des états de systèmes chaotiques d'ordre fractionnaire. Les observateurs d'ordre fractionnaire jouent un rôle important dans les systèmes de communications sécurisées. Nous citerons ci-dessous quelques exemples d'observateurs proposés pour la synchronisation des systèmes chaotiques d'ordre fractionnaire [37].

Il existe plusieurs peuvent être utilisés pour la synchronisation, on peut citer :

- Observateur à mode glissants
- Observateur à grand gain
- Observateur adaptatif
- Observateur numérique,…… etc.

2.5.6.1 Observateurs à modes glissants

Ce type d'observateurs est basé sur la théorie des systèmes à structures variables. Le choix de cet observateur est justifié par le fait que la commande à mode glissant est très efficace pour faire face aux incertitudes du système et aux perturbations externes. Ce type d'observateurs a été utilisé dans de nombreux schémas de synchronisation des systèmes chaotiques fractionnaire continus [38] [39] et discrets [40].

2.5.6.2 Observateurs à grand gain

Cet observateur est très populaire et a été intensément utilisé pour l'estimation des systèmes non linéaires d'ordre entier. Il présente plusieurs avantages comme la convergence globale ou semi globale indépendante des conditions initiales pour un grand nombre de systèmes non linéaires. De plus, il offre une robustesse remarquable vis à vis des incertitudes et perturbations externes. Il a été généralisé pour la première fois aux cas de systèmes d'ordre fractionnaire par Bettayeb et al dans [41]. Les auteurs de la contribution ont appliqué une chaine d'observateurs à grand gain d'ordre fractionnaire mis en cascade pour la synchronisation de systèmes chaotiques d'Arneodo d'ordre fractionnaire.

2.6 Technique de cryptage par le chaos

Le cryptage proprement dit, ou comment mélanger et séparer les données et le signal chaotique, est l'étape finale pour construire le système de communication chaotique. Un signal chaotique porteur d'information représente une généralisation des systèmes conventionnels de modulation. Ainsi, un message source à faible amplitude est masque par un signal chaotique plus large.

Cependant, contrairement aux porteuses sinusoïdales conventionnelles, et à cause de l'absence de notions précises d'amplitude, de phase et de fréquence ; le signal chaotique est mélange avec le message source de différentes façons [42].

Il existe plusieurs techniques de cryptages, nous décrivons ici quelques-uns :

2.6.1 Cryptage par addition (additive chaos masking scheme)

La première et la plus simple des méthodes de cryptage, illustrée dans la figure 2.9, développe en 1993 [30]. Elle consiste en deux systèmes chaotiques identiques, l'émetteur et le récepteur. Le signal chaotique $c(t)$ est l'une des variables d'état du système dans l'émetteur. Le message d'information (le signal utile qui doit être crypte) $c(t)$, qui est typiquement très faible devant $c(t)$, est ajoute au signal $c(t)$ et donne le signal transmis $s(t)$. Comme $c(t)$ est très complexe et $m(t)$ est beaucoup plus petit que $c(t)$, alors il est difficile de séparer $m(t)$ du signal $s(t)$ sans connaitre $c(t)$. Le même système est utilisé à la fois à l'émetteur et au récepteur, avec la différence que le récepteur est contrôlé par le signal émis pour obtenir la synchronisation. Au niveau du récepteur, après synchronisation grâce au signal reçu, on récupère le message original par une simple soustraction.

Par conséquent, un intrus ne soupçonnera pas qu'un message est transmis, même s'il intercepte le signal $y(t)$ (porteuse chaotique plus le message), donc il ne cherchera pas à appliquer des techniques de décryptage [42].

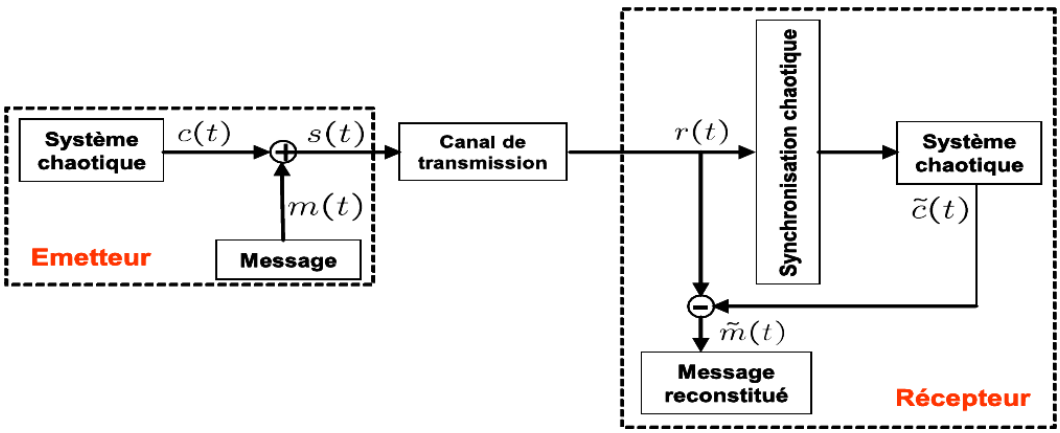

Figure 2.9 : Cryptage par addition.

2.6.2 Cryptage par commutation (Chaotic Shift Keying, CSK)

Appelé aussi cryptage par décalage, est une technique réservée aux messages numériques. Dans le schéma de communication, illustré dans la figure 2.10, le message d'information est utilisé pour commuter le signal transmis entre deux attracteurs chaotiques statistiquement similaires, qui sont utilisés respectivement pour coder le bit 0 et le bit 1 du message d'information numérique.

Ces deux attracteurs sont générés par deux systèmes chaotiques de même structure et de paramètres différents. A ka réception, le signal reçu est utilisé pour produire un système chaotique identique à ceux de l'émetteur. Le message d'information est restitué par application d'un filtre passe-bas et ensuite un seuillage de l'erreur de synchronisation $e(t)$ [30].

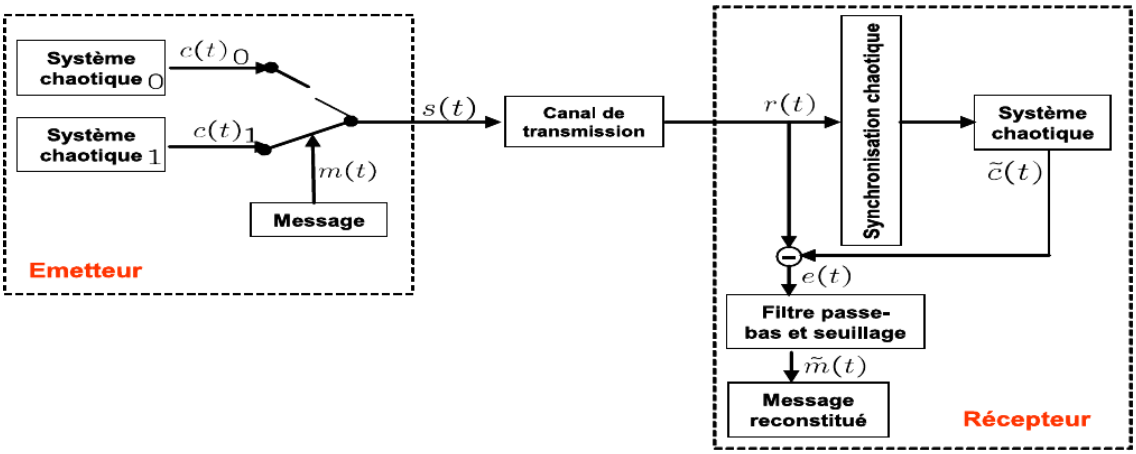

Figure 2.10 : Cryptage CSK.

2.6.3 Cryptage Par Modulation

Cette technique utilise le message contenant l'information pour moduler un paramètre de l'émetteur chaotique. Un contrôleur adaptatif est chargé de maintenir la synchronisation au niveau du récepteur, tout en suivant les changements du paramètre modulé. Le schéma correspondant est présenté à la figure 2.13. Au niveau de l'émetteur, le fait de moduler un (ou plusieurs) paramètre(s) impose à la trajectoire de changer continûment d'attracteur, et de ce fait, le signal transmis est plus Complexe qu'un signal chaotique normal. Cependant, la façon d'injecter le message et donc la fonction de modulation des paramètres ne doivent pas supprimer le caractère chaotique du signal envoyé au récepteur. Il est important de souligner que cette technique exploite pleinement les qualités des systèmes chaotiques.

Elle n'a pas d'équivalent parmi les systèmes de communication classique. Cependant, le cryptage par modulation s'est avéré sensibles à certaines attaques [9].

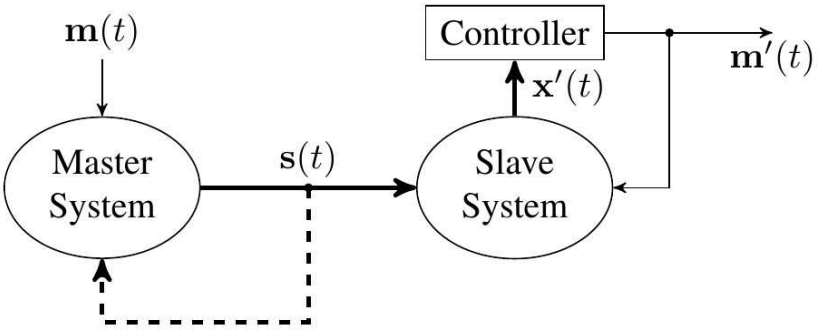

Figure 2.11 : Cryptage par modulation.

Il existe deux types de cryptage par modulation :

- Modulation de paramètre, où le signal $m(t)$ module la valeur d'un ou plusieurs paramètres de contrôle.

-Modulation directe, où le signal $m(t)$ est injecté dans une ou plusieurs variables du système maître sans changer aucune valeur des paramètres de contrôle.

Comparé au cryptage par addition, la modulation du chaos peut récupérer de manière très fidèle le message transmis si certaines conditions sont satisfaites. Comme étant le cryptage CSK est utilisé seulement pour les signauxnumériques, la modulation a une meilleure performance que le CSK. Le cryptage par modulation peut transmettre, si bien conçu, plusieurs messages. Il fautmoduler *n* paramètres de contrôle du système maître avec *n* signaux de message.Un sérieux des avantages du cryptage par modulation est que le contrôleur dépend de la structure des systèmes maîtres et esclave, ce qui signifie qu'il faut concevoir différent contrôleurs pour différents systèmes maîtres, et aussi, il se peut qu'il n'existe pas de contrôleurs certains systèmes à cause de défauts dans les systèmes maître/esclave [43].

2.6.4 Cryptage par inclusion

Cette technique de cryptage consiste à injecter le message dans la dynamique de l'émetteur chaotique comme étant une entrée, sans toutefois réaliser une modulation de paramètres, la récupération du message devient alors un problème d'entrée inconnue dans le cas de la théorie du contrôle où les observateurs sont utilisés, dont le système doit satisfaire la condition d'observabilité ainsi que la propriété d'inversion à gauche par conséquent la restauration de l'information se fait principalement par deux techniques, reposant soit sur les

observateurs à entrées inconnues, soit sur l'inversion du système émetteur. Ainsi elle présente beaucoup d'avantages et reste très utilisée en pratique [14].

Figure 2.12 : Cryptage par inclusion.

2.6.5 Cryptage Mixte

Afin de faire face aux problèmes de sécurité des méthodes précédentes, une nouvelle technique combinant les principes de la cryptographie standard et la synchronisation chaotique a été proposée. Le message $u(t)$ contenant l'information est crypté grâce à une clé, $c(t)$, générée par l'émetteur chaotique.

Le message crypté est alors injecté dans la dynamique du système chaotique, pour la rendre plus complexe. Ensuite, un signal $y(t)$ fonction des variables d'étatde l'émetteur est transmis au récepteur, qui établit une synchronisation avec l'émetteur. La clé est alors reconstruite par le récepteur, qui peut finalement décoder le message. Le principe général de cette méthode est illustré par la figure 2.13 [18].

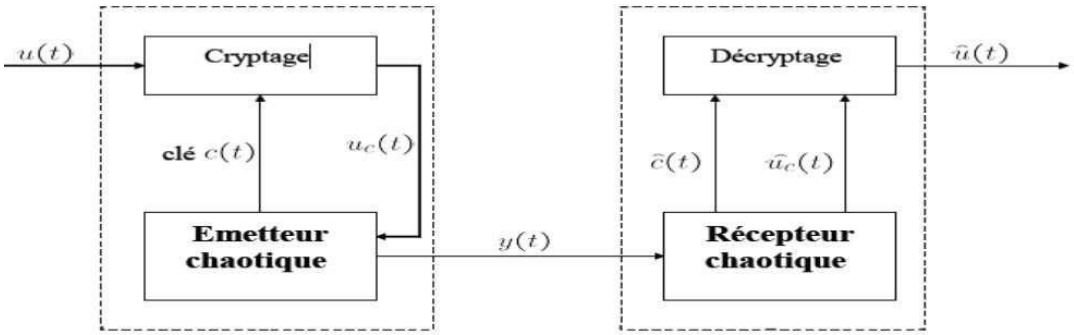

Figure 2.13 : Cryptage mixte.

2.7 Conclusion

Dans ce chapitre, nous avons vu le principe de synchronisation des systèmes chaotiques ainsi que les différentes méthodes utilisées pour la synchronisation. L'objectif est d'exposer d'une part, l'état de l'art sur les techniques de cryptage actuelles

CHAPITRE 3

3.1 Introduction

Une bonne maitrise d'un procédé passe en général par une bonne information sur ce procédé. La disponibilité de toutes les variables d'état est rarement possible dans la pratique. En effet, pour des raisons techniques et/ou économiques, il est difficile, voire impossible, de mesurer la totalité des variables d'état du système, d'où la nécessité d'estimer ces dernières à partir d'un jeu de données entrées/sorties en utilisant des capteurs logiciels appelés observateurs. De façon générale, le besoin d'information sur l'état est motivé par le fait qu'elle est une étape importance, voire indispensable pour la synthèse de lois de commande, pour l'identification, la détection et diagnostic de défauts ou la supervision des systèmes industriels.

Au cours des dernières décennies, une part importance des activités de recherche en automatique s'est focalisée sur le problème d'estimation d'état des systèmes dynamiques.

La conception d'observateurs pour les systèmes linéaires bénéficie d'une abondante littérature où beaucoup de travaux ont été dédiés, initiés par les travaux de Kalman [44] sur les systèmes stochastiques et Luenberger [45].

A travers ce chapitre, nous proposons de revoir quelques concepts et notions utilisés dans la suite de ce mémoire sur l'estimation d'état par l'observateur de Luenberger ainsi qu'une vue d'ensemble sur les observateurs des systèmes non linéaires [46].

3.2 Définition de l'observateur

Un observateur est un moyen de mesure 'informatique' qui permet de retrouver tous les états d'un système industriel en disposant du minimum d'information sur ces états. Ce minimum est obtenu à l'aide d'un capteur. Un observateur permet donc d'optimiser le nombre de capteurs dans une application industrielle, d'où son intérêt économique dans l'industrie. Durant ces dernières décennies beaucoup de travaux en automatique ont été menés sur la conception d'observateurs. Une manière brute d'observer les états d'un système consiste à dérivée numériquement l'information mesurée grâce aux capteurs. L'expérience a montré que cette méthode à l'inconvénient de donner des résultats erronés à cause de l'amplification du bruit due aux imperfections de mesures [47].

3.3 Principe d'observation

Soit un système dynamique décrit par les équations d'état et de sortie suivantes :

$$\begin{cases} \dot{x}(t) = f(x(t), u(t)) \\ y(t) = h(x(t), u(t) \end{cases} \tag{3.1}$$

Avec $x \epsilon \mathbb{R}^n$ représente l'état du système $u(t) \epsilon \mathbb{R}^m$ est l'entrée et $y(t) \epsilon \mathbb{R}^p$ est la sortie, f et h sont des fonctions non linéaire.

Un observateur est un système dynamique qui reconstruit l'état de système à partir des entrées et des sorties du système réel. Les entrées d'un observateur sont donc les entrées $u(t)$et les sorties $y(t)$ du système originale et la sortie d'un observateur est l'état estimé $\hat{x}(t)$.

$$\begin{cases} \dot{z}(t) = g(z(t), x(t), u(t)) \\ \hat{x}(t) = \zeta(z(t), u(t), y(t)) \end{cases} \tag{3.2}$$

Tel que l'erreur d'estimation d'état $e(t) = x(t) - \hat{x}(t)$ tende asymptotiquement vers zéro :

$$||e(t)|| = ||x(t) - \hat{x}(t)|| \to 0 \; quand \; t \to 0$$

L'objectif d'un observateur est de déterminer les fonctions $g(z(t), x(t), u(t))$ Et $\zeta(z(t), u(t), y(t))$ pour assurer la convergence de l'erreur d'estimation vers zéro.

Avant d'entamer la procédure de conception d'un observateur pour un système dynamique, il est important et nécessaire de vérifier que l'état (t) peut être estimé à partir des entrées et sorties du système. En d'autres termes, s'assurer que le système est observable [48].

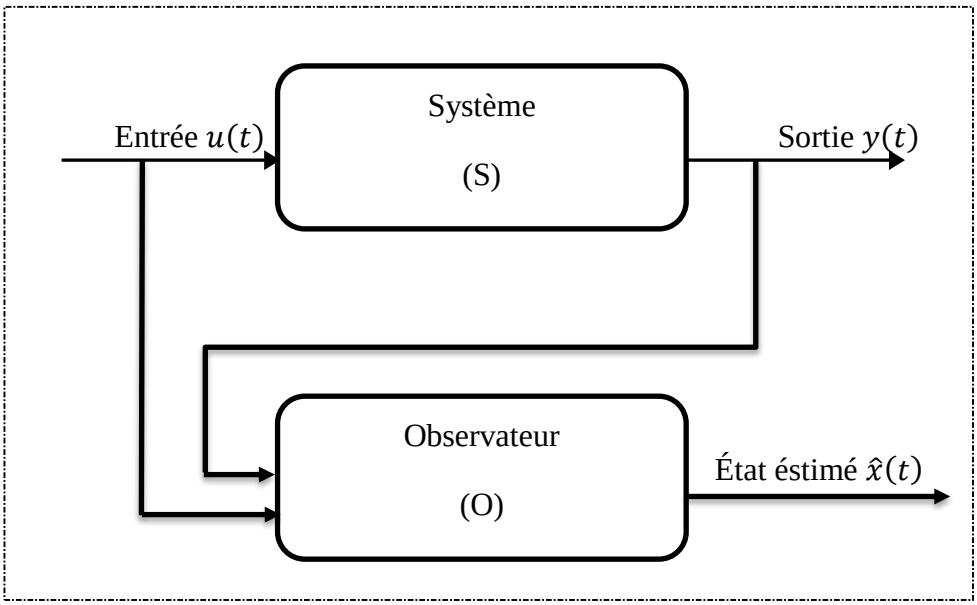

Figure 3.1 : Observateur.

3.4 Observabilité

Dans la littérature, il est démontré qu'un observateur existe si et seulement si la réalisation d'état du système en question est observable. En effet, l'observabilité d'un système exprime la possibilité de reconstruire l'état à partir de la seule connaissance des signaux d'entrées et de sorties [49].

3.4.1 Observabilité des systèmes linéaires

Avant de passer au cas non linéaire, une description générale des observateurs linéaires est présentée dans cette partie pour mieux illustrer le principe d'un observateur. Considérons le système linéaire suivant [50] :

$$\begin{cases} \dot{x}(t) = A(x(t) + Bu(t) \\ y(t) = Cx(t) \end{cases} \tag{3.3}$$

Où : $x \in \mathbb{R}^n$ représente l'état du système, $u(t) \in \mathbb{R}^m$ est l'entrée, $y(t) \in \mathbb{R}^p$ est la sortie et les matrices A, B et C sont des matrices constantes de dimensions appropriées.

La propriété d'observabilité du système linéaire peut être formalisée de la façon suivante :

Définition 3.1 : Observabilité [50]

Le système (3.3) est observable si, étant donné l'instant t_0, il existe un instant t_1 fini tel que la connaissance de $y(t_0, t_1)$ et $u(t_0, t_1)$ permette de déterminer de manière unique l'état $x(t_0) = x_0$ quelque soit l'état du système.

Définition 3.2 : Condition du rang [50]

L'observabilité du système (3.3) est garantie si le rang de la matrice d'observabilité est égal à n.

On dit alors que le système est observable.

$$rang(O) = rang \begin{pmatrix} C \\ CA \\ \vdots \\ CA^{n-1} \end{pmatrix} = n \tag{3.4}$$

Une fois l'observabilité du système linéaire (3.4) est garantie par l'application de condition du *rang*, il est possible de lui construire un observateur.

3.4.2 Observabilité des systèmes non linéaires

Les processus physiques sont très souvent représentés par des modèles non linéaires décrits sous la forme suivante [51] :

$$\begin{cases} \dot{x}(t) = f(x(t), u(t)) \\ y(t) = h(x(t)) \end{cases} \quad (3.5)$$

L'observabilité du système non linéaire (3.5) est caractérisée par le fait qu'à partir de la sortie mesurée, il faut être capable de discerner les différents états initiaux. L'observabilité est donc définie à partir de la notion d'indiscernabilité dont voici la définition

Définition 3.3 : Indiscernabilité [51]

Deux états initiaux $x(t_0) = x_1$ et $x(t_0) = x_2$ du systéme non linéaire (3.5) sont dit indistinguables sur l'intervalle de temps $[t_0, t_1]$ si, pour toute entrée $u(t)$, leurs sorties réspectives $y_1(t)$ et $y_2(t)$ sont identiques sur cet intervalle.

Définition 3.4 : Observabilité [52]

Le système non linéaire (3.5) est dit observable s'il ne contient pas de paire $x(t_0) = x_1$et $x(t_0) = x_2$ indiscernable.

Définition 3.5 : Condition de rang d'observabilité [53]

On définit :

$$L_f h(x) = \sum_{i=1}^{n} f_i(x) \, \frac{\partial y}{\partial x_i} \, (x) \quad (3.6)$$

Où

$L_{f0}^k h$ est la iéme-dérivée de Lie de h dans la direction de f_0 et $L_{f0}^0(h) = h$.

On peut écrire :

$$L_f^0 h = h \text{ et } L_f^k h = L_f\left(L_f^{k-1} h\right), \forall\, k \geq 1 \quad (3.7)$$

Le système (3.5) vérifie la condition de rang d'observabilité si :

$$rang \begin{bmatrix} dh \\ dL_f h \\ \vdots \\ dL_f^{n-1} h \end{bmatrix} = n \quad (3.8)$$

Où bien avec une définition algébrique équivalente :

$$rang \begin{bmatrix} dy \\ d\dot{y} \\ \vdots \\ dy^{(n-1)} \end{bmatrix} = n \quad (3.9)$$

Cela implique que l'état x peut être déduit de la connaissance de la sortie et d'un nombre fini de ses dérivées.

3.5 Observateur des systèmes linéaires [54]

Une solution simple et optimale au problème de l'estimation de l'état des systèmes linéaires a été proposée par Luenberger dans le cadre déterministe, et par Kalman dans le cadre stochastique. Dans les deux cas, on considère le modèle dynamique du système linéaire défini par :

$$\begin{cases} \dot{x}(t) = Ax(t) + Bu(t) + Lw(t) \\ y(t) = Cx(t) + v(t) \end{cases} \quad (3.10)$$

Où $x(t) \in \mathbb{R}^n$, $u(t) \in \mathbb{R}^m$, $y(t) \in \mathbb{R}^r$, $v(t) \in \mathbb{R}^p$ sont deux bruit blancs gaussiens d'espérance nulle, de covariance respectives Q et R. Ces bruits sont supposés non corrélés. Les matrices du système sont de dimensions appropriées, et les conditions initiales sont définies par $x(0) = x_0$.

3.5.1 Observateur de Luenberger [49]

La théorie de l'observation repose essentiellement sur des techniques de placement de pôles.

Soit $\hat{x}(t)$ l'estimé de $x(t)$, et $\hat{y}(t)$ l'estimé de $x(t)$.

L'observateur proposé par Luenberger pour le système (3.3) est décrit par les equations suivantes :

$$\begin{cases} \dot{\hat{x}}(t) = A\hat{x}(t) + Bu(t) + K\big(y(t) - \hat{y}(t)\big); \hat{x}(t_0) = \hat{x}_0 \\ \hat{y}(t) = C\hat{x}(t) \end{cases} \quad (3.11)$$

Où $K \in \mathbb{R}^{n \times p}$ est les gain de l'observateur (3.11). Le schéma bloc de l'observateur est illustré par la figure (3.1). L'erreur d'estimation est donnée par :

$$e(t) = x(t) - \hat{x}(t) \quad (3.12)$$

La dynamique de cette erreur est régie par l'équation suivante :

$$\begin{cases} \dot{e}(t) = (A - KC) \\ e(t_0) = e_0 = x_0 - \hat{x}_0 \end{cases} \quad (3.13)$$

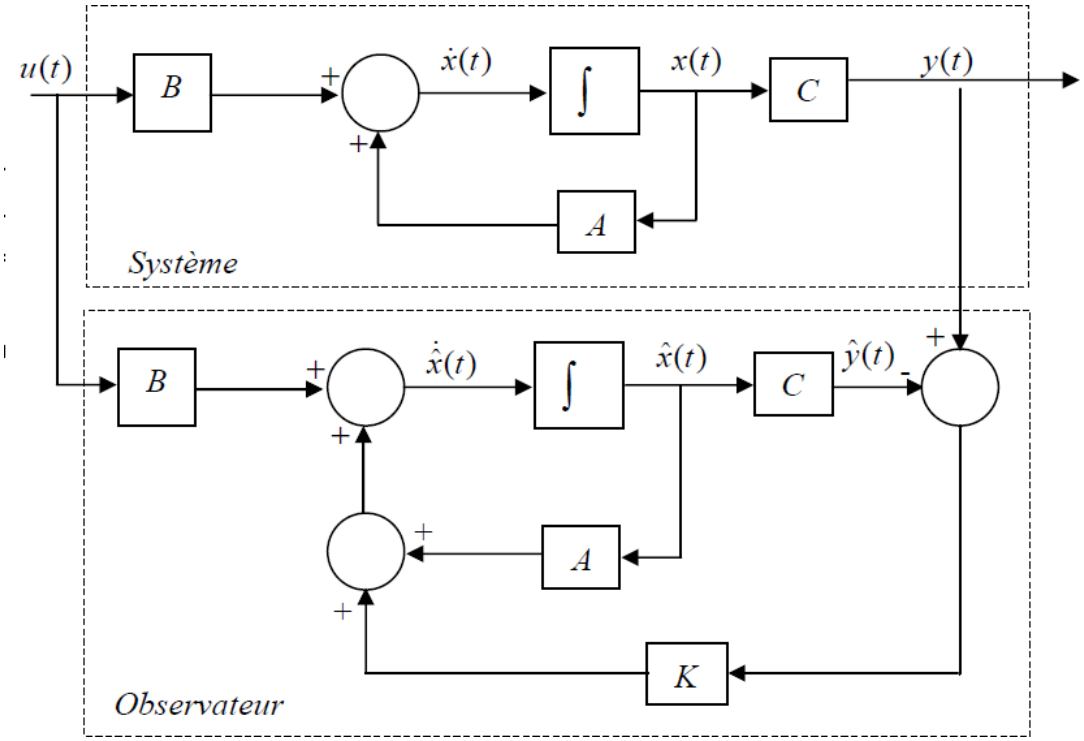

Figure 3.2 : Schéma fonctionnel de l'observateur de Luenberger.

Si le gain est choisi de telle manière que la matrice $(A - KC)$ soit de Hurwitz, c'est-à-direayant des valeurs propres à parties strictement négatives, alors l'erreur d'estimation converge asymptotiquement vers zéro. Comme l'observateur remplace le capteur, on doit donc assurer une convergence de l'erreur d'estimation vers zéro très rapide au moins dix fois plus rapide que la dynamique du système. Si le couple (A, C) est observable, alors il est possible de déterminer legain K pour avoir une dynamique de convergence choisie au préalable. Le problème de construction de l'observateur revient donc à résoudre un problème de placement de pôles. On choisit une dynamique désirée (choix des valeurs propres désirées de $(A - KC)$, puis en utilisant le principede placement de pôle, on détermine le gain K .

3.5.2 Filtre de Kalman [55]

L'observateur de Kalman exige la résolution d'une équation de Riccati. Kalman utilise les propriétés statistiques des bruits w et v et propose la structure d'observateur suivante :

$$\dot{\hat{x}}(t) = A\hat{x}(t) + Bu(t) + K\big(y(t) - C\hat{x}(t)\big) \tag{3.14}$$

En minimisant la matrice de covariance de l'erreur d'estimation $P = E[e(t)e(t)^T]$, on obtient l'expression du gain de l'observateur :

$$K = PC^T R^{-1} \tag{3.15}$$

Ou P est solution de l'équation de Riccati :

$$\dot{p}(t) = AP + PA^T - PC^T R^{-1} CP + LQL^T \tag{3.16}$$

Sous certaines conditions, on peut montrer que la matrice P tend vers une limite et que le filtre est stable, ce qui permet éventuellement de conserver pour K sa valeur en régime permanent.

3.6 Observateur des systèmes non linéaires [15]

La majorité des observateurs des systèmes non linéaires proposés dans la littérature ont la structure suivante :

$$\dot{\hat{x}}(t) = f(\hat{x}, u) + n(y, \hat{x}) \qquad (3.17)$$

C'est-à-dire une copie du modèle plus un terme correcteur $n(y, \hat{x})$ qui assure la convergence de l'état estimé $\hat{x}$ vers l'état réel x dans un temps bien défini. En général le gain d'observation et la stabilité de l'observateur synthétisé pour les systèmes non linéaires dépendent de l'entrée. L'un des premiers observateurs utilisés pour l'estimation des états des systèmes non linéaire est le filtre de Kalman étendu**.**

3.6.1 Filtre de Kalman étendu [4]

Le filtre de Kalman étendu est l'une des techniques d'estimation des systèmes dynamiques non linéaires. Le principe consiste à utiliser les équations du filtre de Kalman classique au modèle non linéaire, qui est linéarisé par la formule de Taylor au premier ordre.

Comme pour les systèmes linéaires, le filtre de Kalman étendu permet de prendre en compte l'influence du bruit de sortie sur la qualité de l'estimateur en synthétisant au gain optimal de Kalman étendu souffre d'une insuffisance théorique. La convergence des erreurs d'estimation vers zéro n'est pas démontée .

3.6.2 Observateur de Luenberger étendu [56]

L'observateur de Luenberger étendu intervient, soit au niveau du système original avec un gain constant, ou soit par un changement de coordonnées avec un gain dépendant de l'état à estimer. Dans le premier cas, un modèle linéaire est nécessaire, et le gain de l'observateur est calculé par le placement de pôles. Ce type d'observateur ne peut être utilisé que lorsqu'on est sûr que l'état restera au voisinage de l'état d'équilibre. Pour cette raison, l'utilisation de cet observateur peut être comprise par les instabilités qui peuvent se révéler si l'on s'éloigne du point de fonctionnement. Dans le deuxième cas, les méthodes de changement de beaucoup d'approches utilisant les changements de coordonnées nécessitent l'intégration d'un ensemble d'équations aux dérivées partielles non linéaires, ce qui est souvent très délicat à réaliser. De ce fait, l'utilisation de solutions approchées est envisageable .

3.7 Observateur généralisé

Considérons l'émetteur décrit par la représentation d'état suivante :

$$\begin{cases} \dot{x} = Ax + B + f(x, s, y) \\ y = Cx + Ds \end{cases} \tag{3.19}$$

Où : $x \in \mathbb{R}^n$ représente le vecteur d'état du, $s \in \mathbb{R}^m$ est le message informatif, $y \in \mathbb{R}^p$ est le vecteur de sortie. Les matrices. A, B et C sont des matrices constantes de dimensions appropriées.

$f(x, s, y)$ est un vecteur non linéaire présentant la partie non linéaire du système.

L'objectif consiste à construire un observateur asymptotique pour estimer l'état x et le message s à partir de la sortie mesurée y, comme le montre la figure suivante :

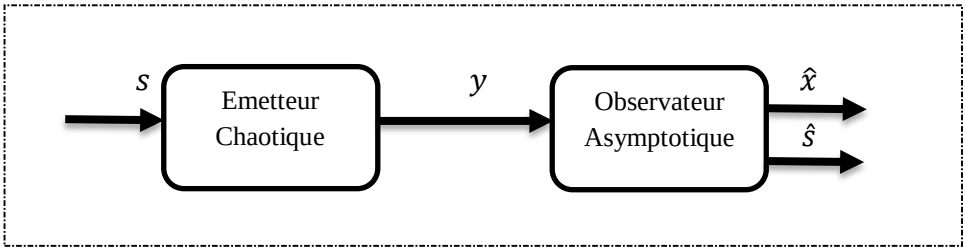

Figure 3.3 : Principe de la transmission chaotique sécurisée à base d'observateur.

En introduisant les notions [57] : $E = [I_n\ 0], M = [A\ B], H = [C\ D], et\ \xi = \binom{x}{s}$, le système (3.19) peut s'écrire :

$$\begin{cases} E\dot{\xi} = M\xi + f(\xi, y) \\ y = H\xi \end{cases} \tag{3.20}$$

Ainsi, on note [57] :

$$[P\ Q] = \left(\binom{E}{H}^T \binom{E}{H}\right)^{-1} \binom{E}{H}^T \tag{3.21}$$

Où P et Q sont des matrices réelles de dimension $(n+m).n$ et $(n+m).p$, respectivement. Ceci permet de déduire :

$$PE + QH = I_{n+m} \tag{3.22}$$

L'observateur d'état qui a proposé en [57], est de la forme suivante :

$$\begin{cases} \dot{z} = Nz + Ly + g(z, y) \\ \hat{\xi} = z + Qy \end{cases} \tag{3.23}$$

Avec $\hat{\xi}$ dénote le vecteur d'état estimé de ξ, et les matrices N, L et g doivent être déterminées tel que $\hat{\xi}$ converge asymptotiquement vers ξ.

Considérons le vecteur d'erreur :

$$e = \hat{\xi} - \xi \tag{3.24}$$

En substituant (3.23) et (3.20) dans (3.24), on obtient :

$$e = z + (QH - I_{n+m})\xi \tag{3.25}$$

En utilisant (3.22),(3.25) devient :

$$e = z - PE\xi \tag{3.26}$$

Donc la dynamique de l'erreur est :

$$\dot{e} = \dot{z} - PE\dot{\xi} \tag{3.27}$$

D'après (3.19) et (3.23) et en utilisant (3.27) on obtient :

$$\dot{e} = Ne + (N + FH - PM)\xi + g(z, y) - Pf(\xi, y) \tag{3.28}$$

Avec

$$F = L - NQ \tag{3.29}$$

En supposant que :

$$N = PM - FH \tag{3.30}$$

Et :

$$g(z, y) = Pf\left(\hat{\xi}, y\right) = Pf(z + Qy, y) \tag{3.31}$$

La dynamique de l'erreur devient alors :

$$\dot{e} = Ne + Pf\left(\hat{\xi}, y\right) - Pf(\xi, y) \tag{3.32}$$

Avant de donner le théorème qu'on va l'appliquer dans notre travail, on rappelle d'abord dans le lemme suivant les conditions nécessaires et suffisantes pour l'existence d'une matrice de stabilité N de la partie linéaire de (3.32).

Lemme 1 : N est une matrice de stabilité si seulement si le système (A, B, C, D) est minimum de phase c'est-à-dire :

$$rang\begin{pmatrix} \mu I_n - A & B \\ C & D \end{pmatrix} = n + rang\binom{B}{D} = n + m, \qquad \forall \mu \in \mathbb{C} \ avec \ r\acute{e}el(\mu) \geq 0$$

Démonstration :

$N = PM - FH$ est une matrice de stabilité si et seulement si la paire (H, PM) est détectable ceci est équivalent à :

$$Rang\begin{pmatrix}\mu I_{n+m} - PM \\ H\end{pmatrix} = n+m, \qquad \forall \mu \in \mathbb{C}\ avec\ réel(\mu) \geq 0$$

D'autre part, en utilisant (3.21), nous avons :

$$P = \Psi\begin{pmatrix}I_n \\ 0\end{pmatrix}, \text{où } \Psi = \begin{pmatrix}I_n + C^TC & C^TD \\ D^TC & D^TD\end{pmatrix}^{-1}$$

Donc nous avons :

$$Rang\begin{pmatrix}\mu I_{n+m} - PM \\ H\end{pmatrix} = Rang\begin{pmatrix}\mu\Psi^{-1} - \begin{pmatrix}A & B \\ 0 & 0\end{pmatrix} \\ C \qquad D\end{pmatrix}$$

$$= Rang\begin{pmatrix}\mu(I_n + C^TC) - A & \mu C^TD - B \\ \mu D^TC & \mu D^TD \\ C & D\end{pmatrix}$$

$$= Rang\begin{pmatrix}I_n & 0 & -\mu C^T \\ 0 & I_m & \mu D^T \\ 0 & 0 & I_P\end{pmatrix}.\begin{pmatrix}\mu(I_n + C^TC) - A & \mu C^TD - B \\ \mu D^TC & \mu D^TD \\ C & D\end{pmatrix}$$

$$= Rang\begin{pmatrix}\mu I_n - A & B \\ C & D\end{pmatrix} = n+m \qquad \forall \mu \in \mathbb{C}\ avec\ réel(\mu) \geq 0$$

Théorème 1 : Faisons les hypothèses suivantes :

1. $f(x,s,y)$ est supposée être Lipchitzienne par rapport à x et s, c.à.d :

$$\|f(x,s,y) - f(z,r,y)\| < \lambda \left\|\begin{pmatrix}x-z \\ s-r\end{pmatrix}\right\|, pour\ tout\ y$$

Où λ est une constante réelle positive.

2. La matrice D est supposée être à rang plein. Pour les systèmes à une seule sortie, cette condition peut se traduit par $D \neq 0$.

Sous les hypothèses 1 et 2, si on suppose que :

3. (A,B,C,D) est minimum de phase.
4. $W - \lambda\sigma I_{n+m}$ est une matrice définit positive, avec $\sigma = \|RP\| + \|P^TR\|$, R et W sont des matrices définit positive reliées par l'équation de Lyapunov :

$RN + N^T = -W$.

Alors le vecteur d'erreur e converge asymptotiquement vers 0 :

$$\lim_{t\to\infty}(\xi - \hat{\xi}) = \lim_{t\to\infty}\left(\begin{pmatrix}x \\ s\end{pmatrix} - \begin{pmatrix}\hat{x} \\ s\end{pmatrix}\right) = 0.$$

Démonstration :

On Considère la fonction de Lyapunov suivante : $V = e^TRe$, sa dérivée est :

$$\dot{V} = e^T(N^TR + RN)e + e^TR\big(g(z,y) - Pf(\xi,y)\big) + (g(z,y) - Pf(\xi,y))^TRe$$

Sous la supposition 3 du théorème 1 et d'après la relation (3.30), il existe une matrice du gain inconnu F tel que les valeurs propres de N possédent une partie réelle négative. Par conséquent, pour une matrice définie positive W, existe l'unique matrice définie positive R tel que :$N^T R + RN = -W$.

D'où

$$\dot{V} = -e^T We + e^T RP\left((f(\hat{\xi}, y) - f(\xi, y)\right) + (f(\hat{\xi}, y) - f(\xi, y))^T P^T Re$$

D'autre part, $\dot{V}$ vérifie l'inégalité :

$$\dot{V} \leq -e^T We + \lambda(\|RP\| + \|P^T R\|)\|e\|^2$$

Où :

$$\dot{V} \leq -e^T(W - \lambda\sigma I_{n+m})e, \qquad avec\ \sigma = \|RP\| + \|P^T P\|.$$

Alors, si la matrice $(W - \lambda\sigma I_{n+m})$ est définie positive, le vecteur d'erreur de l'observateur (3.23) tend asymptotiquement vers 0.

Remarque :

Le calcul de la matrice du gain F peut être réalisé par des outils LMI dans le but de vérifier l'hypothèse 4 du théorème. Un algorithme très utile, pour déterminer, est donné en [57].

Avant de résoudre notre problème grâce à des LMIs, on rappelle les lemmes suivants qui vont être utilisés lors des étapes de calcul.

Lemme 2 : complément de Schur [58] :

Soit une matrice symétrique $\begin{bmatrix} S_{11} & S_{12} \\ S_{12}^T & S_{22} \end{bmatrix} < 0$, avec $S_{ij}(i,j = 1,2)$ ont des dimensions appropriées, les inégalités suivantes sont équivalents :

1. $S < 0$.
2. $S_{11} < 0, S_{22} - S_{12}^T S_{11}^{-1} S_{12} < 0$.
3. $S_{22} < 0, S_{12} S_{22}^{-1} S_{12}^T < 0$.

Lemme 3 [59] : Soient x et y deux vecteurs de dimension n, et p un nombre réel positif, alors l'inégalité suivante est toujours vrais : $2x^T y \leq px^T x + p^{-1} y^T y$.

On Considère la fonction de Lyapunov suivante : $V = e^T Re$, sa dérivée est :

$$\dot{V} = \dot{e}^T R\dot{e} \tag{3.33}$$

En remplaçant (3.32) dans (3.33) on obtient :

$$\dot{V} = e^T(RN^T + N^T R)e + 2e^T RP(f(\hat{\xi}, y) - f(\xi, y)] \tag{3.34}$$

D'après lemme 3, l'équation (3.34) devient :

$$\dot{V} \leq e^T(RN^T + N^TR)e + \frac{1}{\delta}e^TRPP^TRe + \delta(f(\hat{\xi},y) - f(\xi,y))^T(f(\hat{\xi},y) - f(\xi,y))$$

$$\leq \left(RN^T + N^TR + \frac{1}{\delta}RPP^TR\right)e + \delta y^2 e^T e$$

$$= e^T\left(RN^T + N^TR + \tfrac{1}{\delta}RPP^TR + \delta y^2 I\right)e \quad (3.35)$$

Si : $$RN^T + N^TR + \tfrac{1}{\delta}RPP^TR + \delta y^2 I < 0 \quad (3.36)$$

donc : $\dot{V} < 0$

D'après **lemme 2** :

$$RN + N^TR - \tfrac{1}{\delta}RPP^TR + \delta y^2 I < 0 \quad (3.37)$$

Cela est équivalent à :

$$\begin{bmatrix} RN + N^TR + \delta y^2 I & RP \\ P^TR & -\delta I \end{bmatrix} < 0 \quad (3.38)$$

Sous la supposition (3.30),(3.38) devient :

$$\begin{bmatrix} RPM + RFH - H^TFR + M^TP^TR + \delta y^2 I & RP \\ P^TR & -\delta I \end{bmatrix} < 0 \quad (3.39)$$

On fait un changement de variable et en posant : $y = RF$, pour résoudre les LMIs suivantes :

$$LMI(1): \begin{bmatrix} RPM + RFH - H^TFR + M^TP^TR + \delta y^2 I & RP \\ P^TR & -\delta I \end{bmatrix} < 0 \quad (3.40)$$

$$LMI(2): R < 0 \quad (3.41)$$

L'inégalité (3.39) qui nous résoudrons à l'aide de ces LMIs donne la matrice, Les gains

N et L de l'observateur (3.23) peuvent être obtenus par les expressions (3.29) et (3.30) respectivement.

3.8 Conclusion

Dans ce chapitre, on a donné quelques concepts généraux sur l'observabilité et les observateurs des systèmes linéaires et non linéaires ainsi que quelque notion élémentaire sur la résolution des conditions LMI issues de l'observateur.

CHAPITRE 4

4.1 Introduction

Dans ce chapitre nous présentons les différents résultats de simulations obtenues sous Matlab. On a choisi un système chaotique de trois dimensions [60] et nous avons utilisé la méthode d'intégration de Runge-Kutta de troisième ordre pour résoudre les systèmes d'équation différentiels.

4.2 Emetteur

Nous considérons le système dynamique suivant hyper chaotique 3D suivant :

$$\begin{cases} \dot{x}_1 = x_2 + x_3 \\ \dot{x}_2 = -x_1 + 0.5 * x_2 \\ \dot{x}_3 = x_1 * x_1 - x_3 \end{cases} \quad (4.1)$$

Avec $a = 2, b = 6, c = 1, d = 1.$

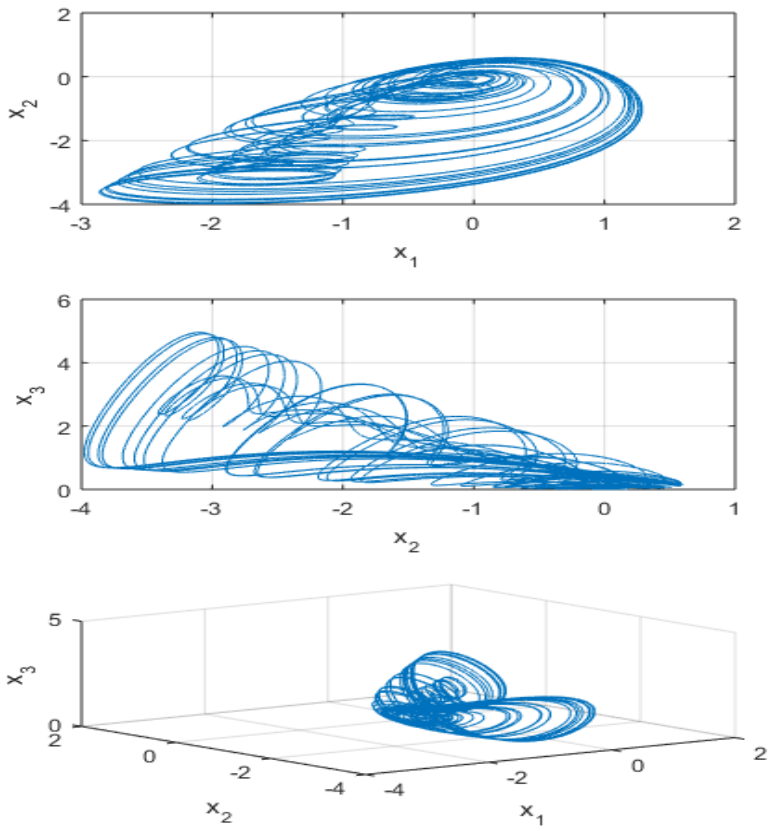

Figure 4.1 : Attracteur étrange du système

Le système (4.1) peut être écrit sous la forme (3.19) tel que :

$$A = \begin{bmatrix} 0 & 1 & 1 \\ -1 & 0.5 & 0 \\ 0 & 0 & -1 \end{bmatrix}, B = \begin{bmatrix} 25 \\ 25 \\ 1 \end{bmatrix}, C = [1,0,0], D = 1, \qquad x(t) = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ s \end{bmatrix}$$

Et $f(x) = \begin{pmatrix} 0 \\ 0 \\ \dot{x}_1^2 \end{pmatrix}$.

Sous la forme (3.22), avec

$$E = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}, M = \begin{bmatrix} 0 & 1.0000 & 1.000 & 25.0000 \\ -1.0000 & 0.5000 & 0 & 25.0000 \\ 0 & 0 & -1.0000 & 1.000 \end{bmatrix}, \quad H = [1 \quad 0 \quad 0 \quad 1]$$

Les matrices P et Q qui vérifient la relation (3.22) sont données par :

$$P = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ -1 & 0 & 0 \end{bmatrix} \qquad \text{et} \qquad Q = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

4.3. Récepteur

Pour estimer le message transmit nous allons utiliser l'observateur d'état proposé sous l'équation (3.23) :

$$\begin{cases} \dot{z} = Nz + Ly + g(z, y) \\ \hat{\xi} = z + Qy \end{cases} \qquad (4.2)$$

L'objectif est de calculé les gains N et L de l'observateur (3.23) selon les équations (3.29),(3.30) respectivement. D'après lemme 2, en utilisant la matrice R obtenue à l'aide des LMIs (3.40). On obtient les résultats suivants :

$$R = \begin{bmatrix} 3.4571 & -2.2247 & 1.6238 & -0.1673 \\ -2.2247 & 2.6714 & -1.4136 & 0.2275 \\ 1.6238 & -1.4136 & 3.1674 & 0.4327 \\ -0.1673 & 0.2275 & 0.4327 & 3.5245 \end{bmatrix}, F = \begin{bmatrix} 4.1375 \\ 3.6589 \\ 0.1443 \\ 0.3683 \end{bmatrix}$$

$$N = \begin{bmatrix} -4.1375 & 1.0000 & 1.0000 & 20.8625 \\ -4.6589 & 0.5000 & 0 & 21.3411 \\ -0.1443 & 0 & -1.0000 & 0.8557 \\ -0.3683 & -1.0000 & -1.0000 & -25.3683 \end{bmatrix}, L = \begin{bmatrix} 25 \\ 25 \\ 1 \\ -25 \end{bmatrix}$$

4.4 Résultats de simulation

En simulant le système sous Simulink de Matlab on obtient les figures suivantes :

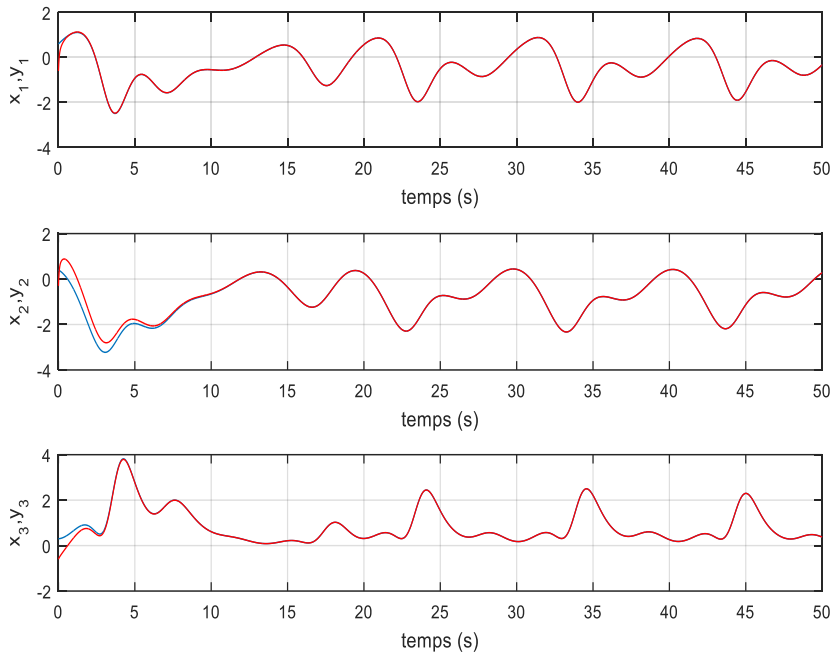

Figure 4.2 : Synchronisation des états émetteur/récepteur

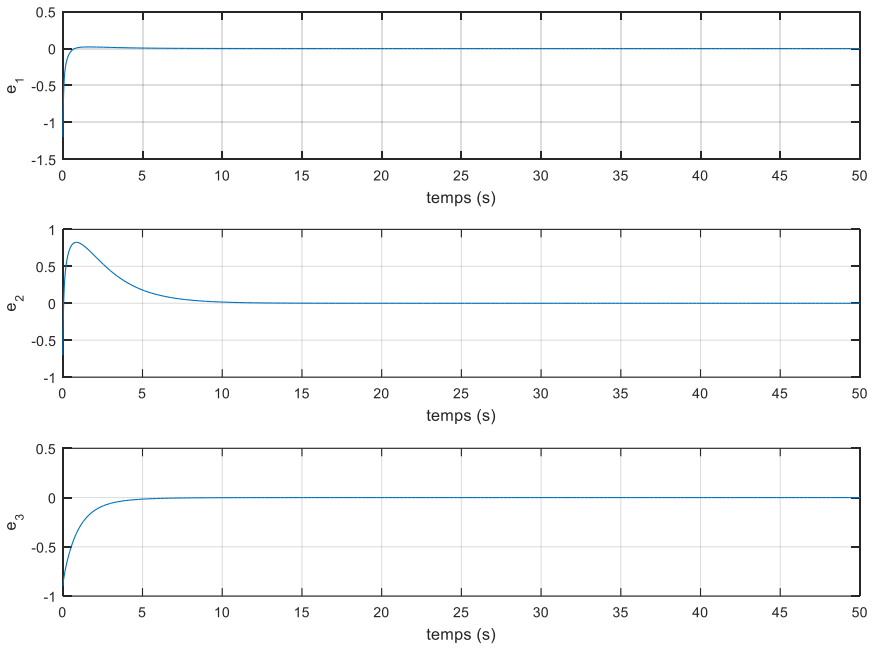

Figure 4.3 : L'erreur entre les états d'émetteur /récepteur

D'après la figure 4.2 et la figure 4.3, on remarque que les graphs sont presque les mêmes avec un petit décalage au début de l'estimation, ce dernier exprime l'erreur de synchronisation. Les états ont été bien estimés au niveau du récepteur.

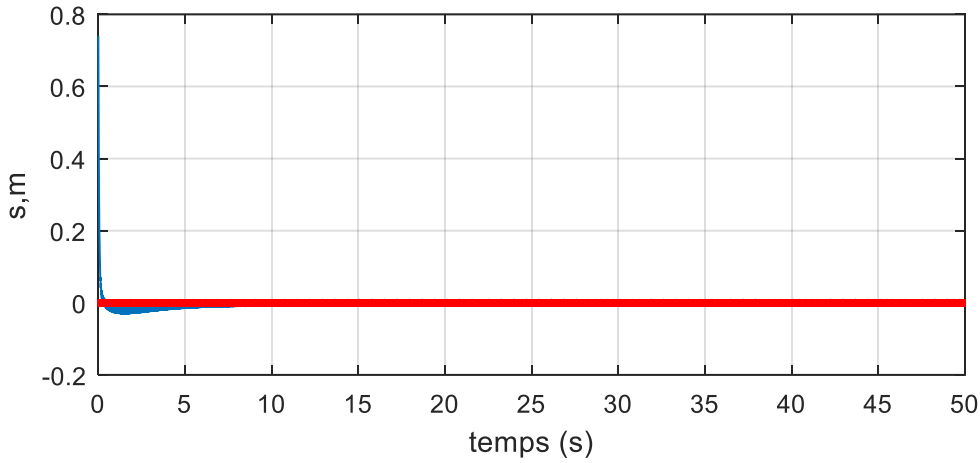

Figure 4.4 : Comparaison entre le signal transmit et celui reçu.

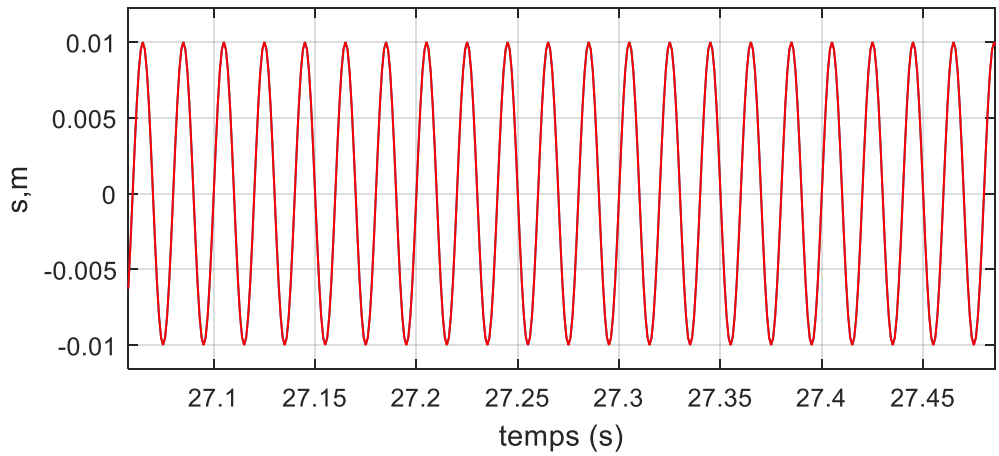

Figure 4.5 : Zoom de la figure 4.4.

Les graphs sont presque identiques, avec un petit décalage au début de l'estimation, ce décalage exprime l'erreur de synchronisation qui convergent rapidement vers zéro. On conclut que le message envoyé a été bien récupéré au niveau de récepteur.

On constate que l'utilisation d'observateur permet la synchronisation des états de l'émetteur et de récepteur ainsi que la reconstruction du message informatif.

4.5. Conclusion

A travers ce chapitre, nous avons présenté les résultats de simulation de notre système de transmission, il est composé d'un émetteur et d'un récepteur, la partie récepteur est constitué d'un observateur d'état qui permet l'estimation du message transmis injecté dans le système chaotique. Les résultats de simulation ont montré l'efficacité des observateurs non linéaires pour la synchronisation des systèmes chaotiques.

CONCLUSION GÉNÉRALE

Conclusion générale

Ce travail a comme objectif la transmission sécurisée de l'information à l'aide d'observateur basé sur la synchronisation des systèmes hyper-chaotique.

Dans le premier chapitre nous avons introduit la théorie du chaos et on a défini les systèmes dynamiques qu'ils soient en temps continu ou en temps discret ainsi que les systèmes chaotiques en donnant leurs propriétés les plus connues telle que le déterminisme, l'aspect aléatoire …. etc.

Dans le deuxième chapitre nous avons exposé quelques techniques de cryptage ainsi que la synchronisation et leurs déférentes méthodes. La synchronisation d'un système chaotique est basée sur un observateur qui permet l'estimation de tous les états des systèmes.

Dans le troisième chapitre nous avons vu l'application des observateurs pour la synchronisation des systèmes chaotiques et on a défini quelques types d'observateurs linéaires et non linéaires tels que l'observateur de Luenberger, le filtre de Kalman et le filtre de Kalman étendu, nous avons exposé les notions de base sur l'observabilité et l'utilisation de la technique LMI pour résoudre le problème proposé.

Dans le quatrième chapitre on a présenté les résultats de simulations réalisées sous Matlab. Les résultats de simulation illustrent les performances de la méthode proposée. Les états du système et le signal informatif envoyés de l'émetteur ont été bien récupérés à l'aide d'observateur au niveau du récepteur.

Comme suite à ce travail, on propose l'implémentation de cette approche dans une carte FPGA pour des applications réelle.

BIBLIOGRAPHIE

[1] K. Atman, F. Khettaoui, "*Synchronisation impulsive de deux systèmes chaotiques de Colpitts,* " Mémoire de fin d'études, Université Mouloud Mammeri, Tizi-Ouzou, 2011.

[2] A. Berkane, "*Transmission sécurisée à base de la synchronisation impulsive de deux systèmes chaotiques discrets*," Mémoire de Master Professionnel, Université Mouloud Mammeri, Tizi-Ouzou, Septembre 2016.

[3] S.Ssastry « Nonlinear Système », Edition Spriger, New York, 1999.

[4] F. Doudjedid, K. Berrouche, "*Transmission sécurisée de données à base de systèmes chaotiques*," Mémoire de Fin d'étude de Master Académique, Université Mouloud Mammeri, Septembre 2014.

[5] H. Nijmeijer. «On Synchronization of Chaotic Systems.» *IEEE 36 th Conférence on Decision and Control CDC'97*, 1997.

[6] H. Nijmeijer, M. Y. Ivan. Mareels. «An observerLooks at Synchronization.» *IEEE transaction on circuits and Systems : Fundamantal Theory and Applications*, vol.44 1997:882-890.

[7] H. Hamiche, M. Ghanes, J.P. Barbot, S.Djennoune. "Secure digital communication based on hybrid dynamical systems." *IEEE, IET International Symposium on Communication Systems, Networksand Digital Signal Processing*, 2010: 244-249.

[8] J. ODEN « Le chaos dans les systèmes dynamiques » 5 juillet 2007

[9] C. Benhabib, "*ETUDE D'UN SYSTEME CHAOTIQUE POUR LA SECURISATION DES COMMUNICATION OPTIQUES,* " Master Télécommunications, Université AbouBekr Belkaid, Tlemcen, 2014.

[10] W. Laouira, "*Contrôle des systèmes dynamiques chaotiques,* " Thèse de doctorat, Université Constantine 1, Novembre 2018.

[11] D. Arbane, K. Arab, "*Conception de crypto-systèmes à base de systèmes chaotiques d'ordre fractionnaire : Application au cryptage de la parole*," Mémoire de Fin d'étude de Master Académique, Université Mouloud Mammeri, Juillet 2018.

[12] E. Goncalvès « introduction au système dynamiques et Chaos ». Cours de l'institut National Polytechnique de Grenoble, 2004.

[13] A. Senouci, "*Elaboration de nouvelles approches de transmission sécurisée et cryptage par chaos* , " Thèse de doctorat, Université De Jijel, 2014.

[14] H. Hamiche, "*Inversion à Gauche des Systèmes Dynamiques Hybrides Chaotiques. Application à la Transmission Sécurisée de Données*," Thèse de doctorat, Université Mouloud Mammeri, Tizi-Ouzou, 2011.

[15] A. Bouhous, "*Sécurisation de l'information via un canal optique*, " Thèse de doctorat, Université De Jijel, Novembre 2018.

[16] S. Allouache, N. Hamma, "*Conception et réalisation d'un système de transmission sécurisé de données à base de systèmes chaotiques sur cartes Arduino*," Mémoire De Fin D'Etude De Master Académique, Université Mouloud Mammeri, Tizi-Ouzou, Juillet 2015.

[17] H. Zhang. Chaos Synchronization and Its Application to Secure Communication. Thèse de Doctorat, Université de Waterloo, Ontario, Canada, 2010.

[18] O. Mgherbi, "*Etude et réalisation d'un système sécurisé à base de systèmes chaotiques*," Mémoire De Magister, Université Mouloud Mammeri, Tizi-Ouzou, Octobre 2013.

[19] F. Launay « Cours Commande Robuste Multi-variables Application au Chaos ». Cours De Laboratoire D'Automatique Et D'Informatique Industrielle. Université De Poitiers, 2 Mars 2011.

[20] https://fr-academic.com/dic.nsf/frwiki/152734

[21] Fekhr El Islam Khelil, "*Les systèmes chaotiques pour le chiffrement*," Mémoire de fin d'études, Université Larbi Ben M'hidi, Oum El Bouaghi, Juillet 2021.

[22] Floriane Anstett. " *Les systèmes dynamiques chaotiques pour le chiffrement : synthèse et cryptanalyse*, " Thèse, Université Henri Poincaré- Nancy 1, Juillet 2006.

[23] A. Kihal, "*SYSTEMES CHAOTIQUES POUR LA TRANSMISSION SECURISEE DE DONNEES*, " Mémoire De Magister En Electronique, Université Mohamed Khider, Biskra, Novembre 2013.

[24]https://www.cnil.fr/fr/comprendre-les-grands-principes-de-la-cryptologie-et-du-chiffrement.

[25] I. Talbi, "*Système dynamique non linéaire et phénomène de chaos*, "Mémoire de Magistère en Mathématiques, Université Mentouri de Constantine, Juin 2010.

[26] Didier Müller. Lexique de cryptologie, site : https ://www.apprendreen-ligne.net/crypto/lexique.html. date : 14/06/2021, May 2005

[27] C. Giraud, "*Attaques de crypto systèmes embarqués et contre-mesures associées*, "Thèse de Doctorat en Informatique , Université de Versailles Saint-Quentin , France , 2007 .

[28] J.M.M. Rodrigues. *Transfert sécurisé d'images par combinaison de techniques de compression, cryptage et marquage*. Thèse de doctorat en informatique, université Montpellier II, France ,2006.

[29] J.P. Tual " *Cryptographie* " *Techniques de l'Ingénieur,* H2 248, 1996.

[30] A. Zemouche,"*Sur l'observation de l'état des systèmes dynamiques non linéaires*," Thèse de doctorat, Université Louis Pasteur-Strasbourg 1, France ,2007

[31] N. Mezar, S. Sebti, "*Etude d'un système de transmission de données robuste à base de la synchronisation impulsive chaotique*, " Mémoire de Fin d'étude de Master Académique, Université Mouloud Mammeri, Septembre 2017.

[32] L.M. Pecora, T.L .Carroll, Synchronization in chaotic systems, Edition Elsevier ,Phys. Rev. Lett.64, pp.821- 824 ,1990.

[33] MB. Luca. "*Application du chaos et des estimateurs d'états pour la transmission sécurisée de l'information*," Thèse de doctorat, Université de Bretagne Occidentale. Année 2006.

[34] S. Bouchelaghem, I. Zentout, "*Nouveau schéma de communication sécurisée à base du chaos*," Mémoire de Master, Université Abd Elhafid Bousouf, Mila, 2020.

[35] M.Hernault-Zanganeh, "*Faisibilité d'un système d'émission-réception analogique pour les communications sécurisées par le chaos*, " Thèse de Doctorat, Université Paris 6, Année 2007.

[36] E.Cherrier "*Estimation de l'état et des entées inconnues pour une classe de systèmes non linéaires*, " Thèse doctorat, Institue Polytechnique Lorraine, Année 2006.

[37] O. Mgherbi, "*Synchronisation des systèmes chaotiques discrets d'ordre fractionnaire pour la sûreté de communication à base d'observateurs impulsifs*," Thèse De Doctorat, Université Mouloud Mammeri, Tizi-Ouzou, juin 2018.

[38] K. Rabah, S. Ladaci, M. Lashab. A novel fractional sliding mode control configuration for synchronizing disturbed fractional-order chaotic systems. Pramana - J.Phys., 89 :46, 2017.

[39] U.M. Al-Saggaf, M. Bettayeb, S. Djennoune. Super-Twisting Algorithm-Based Sliding-Mode Observer for Synchronization of Nonlinear Incommensurate Fractional-Order Chaotic Systems Subject to Unknown Inputs. Arabian Journal for Science and Engineering, 42(7), pp. 3065-3075, 2017.

[40] L. Huang, L. Wang, D. Shi. Discrete Fractional Order Chaotic Systems Synchronization Based on the Variable Structure Control with a New Discrete Reaching-law.IEEE/CAA Journal of Automatica Sinica, 2016.

[41] M. Bettayeb, U. M. Al-Saggaf, S. Djennoune. High gain observer design for fractional-order non-linear systems with delayed measurements : application to synchronisation of fractional-order chaotic systems. IET Control Theory and Applications, 11(17), pp. 3171-3178, 2017

[42] M. Ait Hammi, Abdelfateh, "*ÉTUDE ET RÉALISATION D'UN SYSTEME CHAOTIQUE BASÉ SUR LE CIRCUIT DE CHUA*, " Mémoire de Fin d'Etude de Master Professionnel, Université Mouloud Mammeri, Tizi-Ouzou, 2014.

[43] Shujun Li , Gonzalo Alvarez, Zhong Li and Wolfgang A. Halang, Analog Chaos-based Secure Communications and Cryptanalysis: A Brief Survey, 3rd International IEEE Scientific Conference on Physics and Control (PhysCon 2007), (2007).

[44] R. E. KALMAN. A new approach to linear filtering and prediction problems. Journal of Basic Engineering, 82 : 35-45,1960.

[45] D.G. Luenberger. An introduction to observers. IEEE Transactions on Automatic Control, 16 :596–602, 1971.

[46] L. Yidjouimat, K. Tiguercha, "*Observateur pour les systèmes chaotiques représentés par une représentation Takagi Sugeno*," Mémoire De Fin D'Étude, Université Mouloud Mammeri, Tizi-Ouzou.

[47] M. Moulahoum Mouloud, "*Synthèse d'observateurs à mode glissant à entrée inconnue : Application à la synchronisation des systèmes chaotiques de Chua*," Mémoire De Fin D'Étude, Université Mouloud Mammeri, Tizi-Ouzou, 2014.

[48] H. Dif, M. Brahimi "*Synthèse d'observateurs ey de contrôleurs pour les systèmes non linèaires représentés par des modèles Takagi-Sugeno*," Mémoire De Fin D'Étude Master Académique, Université Mouloud Mammeri, Tizi-Ouzou, septembre 2016.

[49] H. Nechaf, "*Observation et Synthèse d'Observateurs pour les Systèmes à Retard*," Mémoire De Magister, Université Mouloud Mammeri, Tizi-Ouzou, Novembre 2015.

[50] H. Bouchareb, "*Observateur non linéaire mode glissant*," Mémoire de Magistère. Université de Sétif, 2013.

[51] A.J.Fossad and D.Normand-Cryot .Nonlinear Systems.Masson.Paris, 1993.

[52] Frédéric Rotella, "Observation", Ecole Nationale d'Ingénieurs de Tarbes.

[53] Marwa Mohamed Moustafa EZZAT, "*Commande non linéaire sans capteur de la machine synchrone à aimants permanents*," Thèse de Doctorat ? Université de Nantes, 2011.

[54] Nait Slimani Boukhalfa, "Synthèse d'o*bservateurs non linéaires : Application au diagnostic de défauts*," Mémoire De Magistère, Université Mouloud Mammeri, Tizi-Ouzou.

[55] R.E. Kalman, "A new approach to linear filtering", Transactions of the ASME Journal of Basic Engineering. Vol 82. pp 35-45. 1960.

[56] J.Birk and M.Zeit. Extended Luenberger for nonlinear multivariable systems. International Jornal of Control, Vol. 47, N. 6, P. 1823, 1988.

[57] M. Boutayeb, M. Darouach, H. Rafaralahy. "Generalized State-Space Observers for Chaotic Synchronization and Secure Communication", IEEE Trans. Circuits Syst. I, tome 49, no3, pages 345-349, 2002.

[58] Y. Cao, Y. Sun, C. Cheng, "Delay-dependent robust stabilization of uncertain systems with multiple state delays", IEEE Trans. Autom. Control 43, 1608-1612 (1998).

[59] J. Vegas, "Reduced stability of parameter-dependent matrices", Linear Algebra Appl.268. pp 289-321, 1998.

[60] PHAM, Viet-Thanh, VAIDYANATHAN, Sundarapandian, VOLOS, Christos, et al. (ed.). "Nonlinear dynamical systems with self-excited and hidden attractors". Springer, 2018.