République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Mohammed Seddik Benyahia-Jijel

Faculté Des Sciences Et Technologies

Département d'Electronique

Mémoire de fin d'études

Pour L'Obtention du Diplôme Master en Télécommunication

Option :

Systèmes Des Télécommunications

Thème :

SYSTEMES CHAOTIQUES POUR LA TRANSMISSION SECURISEE DE DONNEES

Réalisé par :

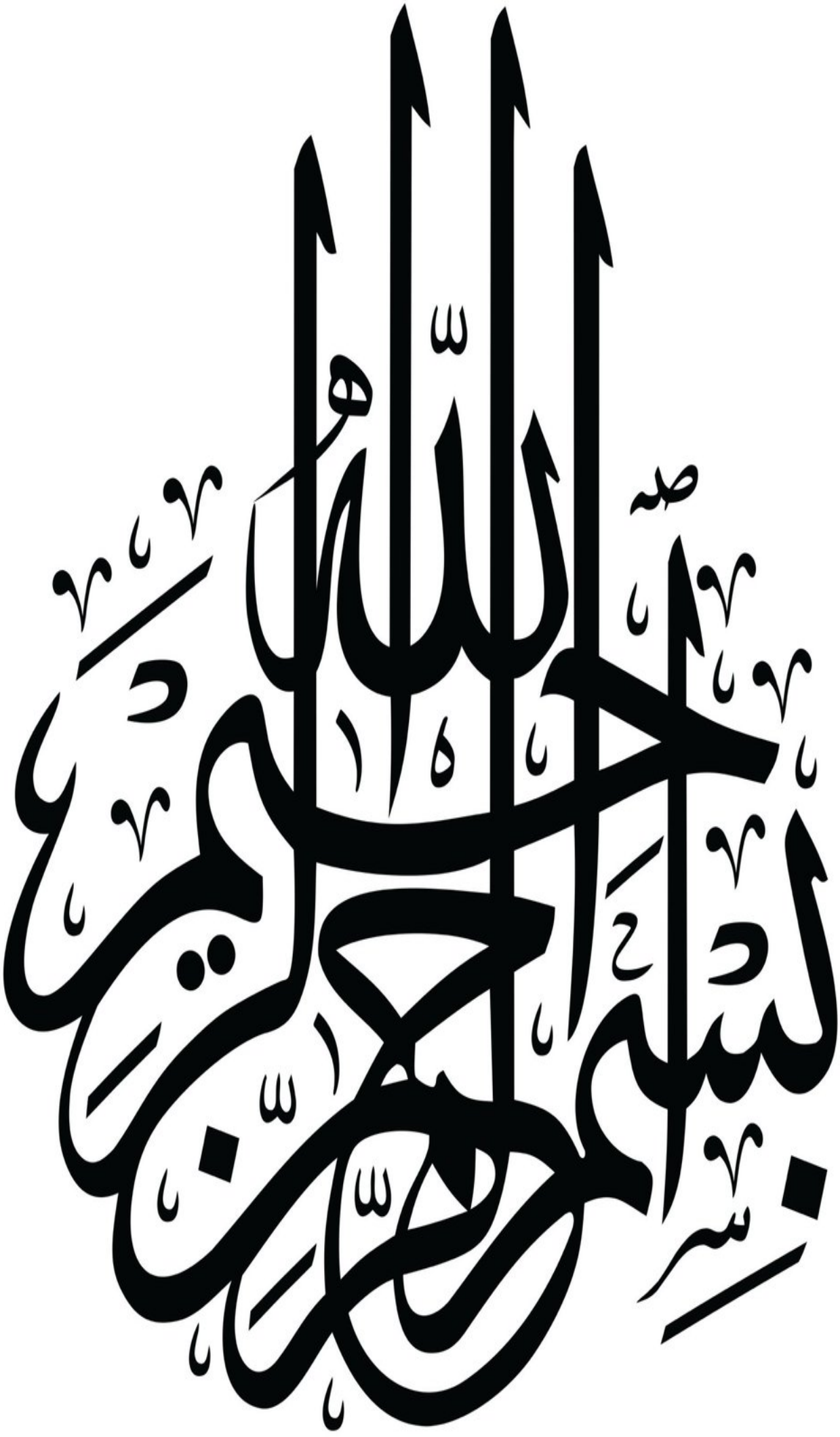
M^{elle}. HANK Amina

M^{elle}. YOUNSI Rofia

Proposé par :

Pr. KEMIH Karim

Promotion : 2019/2020


بسم الله الرحمن الرحيم

Remerciement

Nous remercions avant tout DIEU Allah tout puissant pour la volonté, le courage et la patience qu'il nous a donnée afin de réaliser ce modeste travail.

Nous exprimons notre plus grande reconnaissance et notre respect à notre encadreur Mr KEMIH Karim, pour avoir accepté de diriger ce travail, de nous avoir guidé et soutenu avec patience et indulgence, pour ces lectures enrichissantes de notre mémoire et pour les précieux conseils qu'il n'a cessé de nous prodiguer.

Nous tiendrons également à remercier tous les membres du jury, de l'honneur qu'ils nous ont fait en acceptant d'être membres du jury de ce modeste travail

Dédicaces

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

Je dédie ce modeste travail en signe de respect et de reconnaissance

A

Ma chère mère pour toute sa tendresse, son amour, son soutien, et ces sacrifices consentis et ses précieux conseils, pour toute son assistance et sa présence dans ma vie.

Mon cher père, À qui je dois ce que je suis, qui a consacré sa vie pour mon éducation.

Ma sœur ''Ryma'' et mon frère ''Fodil'', Pour toute leur compréhension et encouragements.

A mon binôme et mon amie ''Amina ''

Mes fidèles amies ''Chahla '' et ''Imene '' pour leur soutien.

Toutes mes chères amies de la promo Systèmes des Télécommunications, en particulier ''Yousra '' et ''Besma ''avec qui j'ai passé des moments mémorables.

Tous ceux que j'aime et ceux qui m'aiment

Rofia

Dédicace

En préambule à ce mémoire, on remercie Dieu tout puissant sans qui ce mémoire n'aurait jamais vu le jour.

Je dédie ce travail à ma famille,

Ma chère mère et mon cher père pour tous ses sacrifices son amour et tendresse, et surtout patience et soutien dont ils ont fait preuve pendant toute la durée de mes études.

Mes frères Mohammed et Ali, et ma sœur décédée Hajder qu'était la source de volonté pour moi, qu'Allah l'accueillir en son vaste paradis.

A mon binôme et mon amie ''Rofia''

Ainsi que mes amies ''Sara'' et ''Khadidja'' pour leur encouragement.

Toutes mes chères amies de la promo Systèmes des Télécommunications, en particulier ''Yousra '' et ''Besma '' Avec qui j'ai passé des moments merveilleux et mémorables.

Tous ceux qui m'encourager durant cette période merci infiniment.

Amina

Résumé :

Dans le cadre de notre projet de fin d'études, on s'intéresse à la sécurisation de l'information par le chaos dû aux caractéristiques de ces systèmes tels que la sensibilité aux conditions initiales et leurs trajectoires qui sont considérés comme un bruit pseudo aléatoire. Le circuit de cryptage proposé est basé sur l'inclusion du message dans la dynamique du système chaotique au niveau de l'émetteur. Pour établir la synchronisation entre l'émetteur et le récepteur et pour restituer le message transmis, l'observateur généralisé est utilisé. Les résultats de simulation montrent clairement l'efficacité de l'approche utilisée.

Mots clefs : système chaotique, cryptage, synchronisation de deux systèmes, observateur, chiffrement, sécurisation de l'information, hyper-chaotique.

ملخص :

في اطار مشروع تخرجنا، نحن مهتمون بتأمين المعلومات من خلال الفوضى نظرا لخصائص هذه الأنظمة مثل الحساسية للشروط الابتدائية ومساراتها التي تعتبر ضجيجا شبه عشوائي. تعتمد دائرة التشفير المقترحة على إدراج الرسالة في ديناميكيات النظام الفوضوي على مستوى المرسل. لتأسيس التزامن بين المرسل و المستقبل و استعادة الرسالة المرسلة، يتم استخدام المراقب المعمم. تظهر نتائج المحاكاة بوضوح فعالية النهج المستخدم.

الكلمات المفتاحية : نظام فوضوي ، تشفير ، تزامن ، مراقب ، تشفير ،تأمين المعلومات ، نظام فوضوي جدا.

Abstract:

As part of our end of studies project, we are interested in securing information by chaos due to the characteristics of these systems such as sensitivity to initial conditions and their trajectories which are considered as pseudo random noise. The proposed encryption circuit is based on the inclusion of the message in the dynamics of the chaotic system at the sender level. To establish synchronization between the sender and receiver and to reproduce the transmitted message, the generalized observer is used. The simulation results plainly show the effectiveness of the approach used.

Keywords: chaotic system, encryption, synchronization of two systems, observer, secure information, hyper-chaotic.

Sommaire

Chapitre 4 : Résultats de simulation

Liste des figures

Chapitre 1 : Etat de l'art du chaos

Chapitre 2 : Synchronisation des systèmes chaotiques

Chapitre 3 : Application de l'observateur pour la synchronisation du chaos

Chapitre 4 : Résultats de simulation

Liste des tableaux

Introduction Générale

Introduction Générale

Ces 20 dernières années ont été marquées par une révolution des systèmes de communications grâce au développement de la technologie de l'information avec l'avènement de l'Interne, les communications sans fil, et par satellite. Cette révolution a permis un échange facile des millions de kilo-octets d'informations. Reste qu'avec ces flux de données confidentielles sont transmises via des canaux de communication non sécurisés, et l'information peut à tout moment être interceptée par des individus indésirables.

En effet, la sécurisation de la chaîne de transmission est devenue une préoccupation majeure, les utilisateurs ont besoin d'authentifier et de protéger leurs données sensibles. De nos jours, tout système de communication performant nécessite un système de sécurisation afin de le protéger de tout intrus non autorisé. Pour cela, de nouvelles méthodes de cryptage sont développées. Le cryptage des informations garantit la sécurisation, la confidentialité, et la fiabilité des systèmes de transmissions de données, et ce en brouillant l'aspect du message envoyer de manière à le rendre imperceptible aux yeux des individus non autorisés à connaitre son contenue.

Les méthodes de cryptage reposé sur des algorithmes de calcule qui admette une certaine efficacité et rapidité pour chiffrer ou déchiffre l'information, devenue aujourd'hui avec le développement des techniques de cryptanalyse et la montée des calculateurs, faible en prenant un temps de calcule long. Ce qui a poussé les chercheurs à élaborer une alternative du cryptage prometteuse : la cryptographie chaotique [1].

La théorie du chaos a vu le jour à partir de 1960, par les travaux de nombreux chercheurs notamment ceux de Lorenz, où elle a connu un développement mathématique suivi d'un véritable essor scientifique. Les systèmes chaotiques sont des systèmes déterministes non linéaires avec des caractéristiques importantes tell l'aspect aléatoire, la sensibilité aux conditions initiales, la sensibilité aux variations des paramètres, et son comportement imprévisible dans le temps, ce qui rend les systèmes chaotiques très intéressants dans le cryptage des données.

Thomas Carol et Louis Pecorra ont découvert la synchronisation des signaux chaotiques en 1996 [2], qui consiste à synchroniser est rapprocher les trajectoires des deux systèmes jusqu'à ce qu'ils deviennent confondus. Plusieurs types et méthodes de synchronisation ont

été introduits pour effectuer l'échange de l'information de l'émetteur vers le récepteur afin de reconstruire le signal transmis.

Ce travail de fin d'études consiste à réaliser un système de transmission sécurisé par le chaos. Son principe de base consiste à transmettre un message utile dans le signal chaotique au niveau de l'émetteur, et de le récupère au niveau du récepteur on appliquant la synchronisation chaotique par observateur qui permet l'estimation de tous les états des systèmes.

Ce travail décompose en quatre chapitres :

Après une introduction générale, le premier chapitre est consacré aux généralités et aux notions de base sur les systèmes dynamiques, chaotiques et hyper chaotiques tout en pressentant les caractéristiques du chaos.

Le deuxième chapitre fait un tour d'horizon aux différents principes de la synchronisation des systèmes chaotiques en présentant les méthodes et les types de synchronisation, tel que : la synchronisation par couplage unidirectionnelle et bidirectionnelle, la synchronisation par décomposition du système, synchronisation par boucle fermée, synchronisation retardée, synchronisation identique, synchronisation par phase, synchronisation à l'aide d'un observateur, synchronisation impulsive. La méthode appliquée dans ce travail est la synchronisation à l'aide d'observateur. On parlera aussi de l'utilisation du chao pour la transmission sécurisée d'information et on termina se chapitre par quelque type de transmission basée sur la synchronisation de système chaotique.

Dans le troisième chapitre, on décrit le schéma de transmission chaotique proposé, mais avant, nous présenterons quelques définitions générales sur l'observateur et l'observabilité pour les systèmes linéaires et non linéaires, on donnera aussi le principe des inégalités matricielles linéaires LMI ainsi qu'un petit historique, est on finira par l'étude d'émetteur et du récepteur on développera les équations qui correspond on simulera ces équations avec MATLAB.

Dans le quatrième chapitre, on réalise le schéma de cryptage sous Simulink/Matlab avec présentation des différents résultats de simulations et discussions.

Enfin, on termine par une conclusion générale.

CHAPITRE 1

ETAT DE L'ART DU CHAOS

1.1. Introduction

L'un des plus merveilleux domaines des mathématiques modernes et de la physique qui a fourni une nouvelle façon de voir l'univers est la théorie du chaos, un outil important pour comprendre le comportement des processus dans le monde [3].

En 1963, le météorologue **Edward Lorenz**, du Massachusetts Institute of Technology (M.I.T), mette en évidence le caractère chaotique des conditions météorologiques et par conséquent des mouvements turbulents d'un fluide comme l'atmosphère [4].Ces prévisions se basent sur le déplacement des masses d'air, et par conséquent sur l'application des théories de Newton et des équations différentielles [5]. Alors qu'il cherchait à déterminer des conditions météorologiques futures à partir de données initiales sur son ordinateur, il constata qu'une modification minime des données initiales (de l'ordre d'un pour mille) entrainait des résultats radicalement différents. Pour améliorer cette découverte, il a programmé son ordinateur de façon à obtenir une simulation numérique. A l'époque, cela prenait beaucoup de temps. Un jour, pour ne pas recommencer les calculs depuis le début, il décida de reprendre son listing et de rentrer en tant que conditions initiales des valeurs prisent au cours de la simulation de la veille. L'ordinateur lui donnait une précision à cinq chiffres, cependant trois chiffres significatifs lui semblaient largement suffisants pour ce genre de mesures physiques. Il tronqua donc ces nombres et repris le calcul. Les résultats qui suivirent furent le déclic. D'abord la simulation semblait redonner les mêmes valeurs, mais au bout d'un moment rien ne concordait, tout se passait comme si le mouvement représenté par ces valeurs changeait complètement de trajectoire et ce à cause d'une approximation de l'ordre de 10^{-4}[6].

Cette anecdote [7], fut la base du chaos : une infime variation des conditions initiales d'un système bouleverse complètement son évolution. Lorenz venait de mettre en exergue la sensibilité aux conditions initiales .Il expliqua d'ailleurs très joliment cette notion à l'aide de l'image suivante : le battement d'ailes de quelques papillons peut provoquer des tempêtes aux antipodes [7].

Ainsi, le chaos est caractérisé par une nature complexe et un comportement imprévisible. En raison de cette complexité, les systèmes chaotiques sont extrêmement difficiles à contrôler et à prédire, ce qui les rend adaptés aux applications de sécurité, de cryptage, de communications sécurisées, de robotique et plus encore [8].

1.2. Les Systèmes dynamiques

D'une manière générale, le système dynamique est un phénomène physique quelconque qui progressant au fil du temps. Il est décrit par une équation différentielle de la forme :

$$\frac{dx}{dt} = \dot{x} \tag{1.1}$$

Le système peut être représenté à partir d'un ensemble de variables qui forment le vecteur d'état $X = \{x_i \epsilon \mathcal{R}\}, i = 1 \dots n$ où n présente la dimension du vecteur [10].

1.3. Modélisations des systèmes dynamiques non linéaires

Un système non linéaire ne peut pas être décrit par des équations différentielles linéaires à coefficients constants. Cette définition explique la complexité et la diversité des systèmes non linéaires et des méthodes qui s'y appliquent. Il n'y a pas une théorie générale pour ces systèmes, mais plusieurs méthodes adaptées à certaines classes de systèmes non linéaires [10].

L'évolution déterministe du système dynamique peut alors se modéliser de deux façons distinctes :

- Une évolution **continue** dans le temps, représentée par une équation différentielle ordinaire.

$$\begin{cases} \dot{x} = f(x(t)) \\ x(t_0) = x_0 \end{cases} \tag{1.2}$$

Où : $x \in \mathcal{R}^n$ est le vecteur d'état, f est une fonction $\mathcal{R}^n \rightarrow \mathcal{R}^n$ appelée champ de vecteur, et $x_0 \in \mathcal{R}^n$ représente le vecteur des états initiaux à l'instant initial t_0 [11].

- Une évolution **discrète** dans le temps, si un système prend ses valeurs uniquement à des instants régulièrement distribués. Sa représentation mathématique est donnée par le système d'équations suivant [11].

$$\begin{cases} x(k+1 = f(x(k)) \\ x(k_0) = x(0) \end{cases} \tag{1.3}$$

Avec : k est l'instant discret, k_0 est l'instant discret initial et $x(0)$ est le vecteur des états initiaux.

Le système dynamique progresse au cours du temps d'une manière causal et déterministe :

- Causale, où son avenir ne dépend que de phénomènes du passé ou du présent.
- Déterministe, c'est-à-dire qu'à partir d'une condition initiale donnée à l'instant présent va correspondre à chaque instant ultérieur un et un seul état futur possible [9].

1.4. Les Systèmes chaotiques

Henri Poincaré, à la fin du siècle dernier, réussit à mettre en évidence la possibilité de comportements irréguliers dans les systèmes déterministes et Edward Lorenz, qui fut le premier à comprendre et à déterminer un modèle mathématique du chaos.
Cependant une étude approfondies des dynamiques non-linéaires ont montre que le chaos apparaissait naturellement dans des systèmes naturels, ou en ingénierie. Il a d'abord été considère comme irrégulier et souvent attribue à des influences externes aléatoires [7].

Par définition on appelle donc un système dynamique chaotique, un système qui est impossible à prévoir son évolution au fil du temps, un système qui dépend de plusieurs paramètres et qui est caractérisé par une extrême sensibilité aux conditions initiales. Il n'est pas déterminé ou modélisé par des systèmes d'équations linéaires ni par les lois de la mécanique classique.

1.5. Propriétés des systèmes chaotiques

Il n'existe pas une définition exacte du chaos. En générale, le chaos est défini comme un comportement particulier d'un système dynamique [2]. Il existe un ensemble de propriétés qui résument les caractéristiques observées dans les systèmes chaotiques. Elles sont considérées comme des critères mathématiques qui définissent le chaos. Les plus connues sont :

1.5.1. La non-linéarité

Des études ont dévoilé que les phénomènes chaotiques étaient caractéristiques des systèmes non-linéaires la montre un système chaotique est un système dynamique non linéaire.

1.5.2. Le déterminisme

Le système chaotique c'est un système qui progresse au cours du temps d'une manière déterministe et non probabiliste. Il est généralement régi par des équations différentielles non linéaires qui sont connues, donc par des lois rigoureuses et parfaitement déterministes [12].

1.5.3. Sensibilité aux conditions initiales

Tout d'abord, les systèmes chaotiques sont extrêmement sensibles aux perturbations. Cette sensibilité a été observée pour la première fois par Edward Lorenz qu'il a illustré par l'effet papillon.

1.5.4. Aspect aléatoire

L'évoluent du système chaotique semble aléatoire.

1.5.5. Degré de liberté

La naissance du chaos nécessite de travaille sur trois degré de liberté. Tout système continu de moins de trois degré de liberté ne peut pas être chaotique [12].

1.6. Les systèmes hyper-chaotiques

Le système hyper chaotique est déterminé comme étant un comportement d'un système chaotique qui possède au moins deux exposants de Lyapunov positifs.

1.7. L'espace de phase

Le système dynamique est caractérisé par un certain nombre de variables d'état à un instant donné, Le comportement dynamique du système est ainsi relié à l'évolution de chacune de ces variables d'état. Cet espace est appelé « l'espace de phase », dont chaque point définit un état et le point associé à cet état défini une trajectoire appelé une orbite.

1.8. Notion d'attracteur

Dans l'étude des systèmes dynamiques, un attracteur est un ensemble ou un espace vers lequel un système évolue de façon irréversible en l'absence de perturbations[9].

L'étude du comportement asymptotique d'un système dynamique régi par un ensemble d'équations différentielles non linéaires révèle très souvent la notion d'attracteur, défini comme l'ensemble compact de l'espace des phases invariant par cet ensemble et

vers lequel convergent toutes les trajectoires du système. Il existe quatre cas de figures correspondants à des solutions différentes du flot, mettant en évidence des attracteurs différents [12] :

- Le point attracteur : correspondant à une solution stationnaire constante, donc de fréquence nulle.
- Le cycle limite attracteur : caractérisant un régime périodique, la solution possède une seule fréquence de base.
- Le tore supra Tr ($r \geq 2$) : cet attracteur correspond à un régime quasi-périodique ayant fréquences de base indépendantes (cas le plus simple r=2, dynamique bi-périodique).
- L'attracteur étrange : On peut définir l'attracteur étrange comme une carte des états imprévisibles et chaotiques ; il révèle un espace des phases vers lequel convergent des phénomènes chaotiques. On pourrait comparer cet espace des phases à une vallée dont toutes les eaux ruisselantes convergent vers un cours d'eau unique.

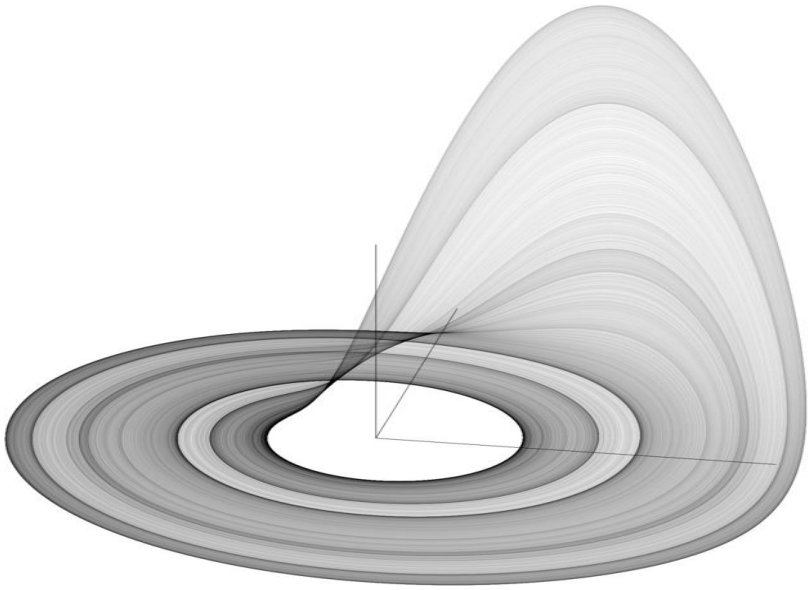


Figure 1.1 : attracteur étrange de Rosler.

1.9. 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 [11].

Donc deux trajectoires dans le plan de phase initialement séparées par un taux Z_1divergent après un temps $\Delta t = t_2 - t_1$ vers Z_2 tel que :

$$|Z_2| \approx e^{\lambda.\Delta t}|Z_1| \tag{1.4}$$

En passant à la limite on obtient l'exposant de Lyapunov qui représente le logarithme moyen de l'accroissement :

$$\lambda \approx lim_{\Delta t \to \infty} \frac{1}{\Delta t} ln \frac{|Z_2|}{|Z_1|} \tag{1.5}$$

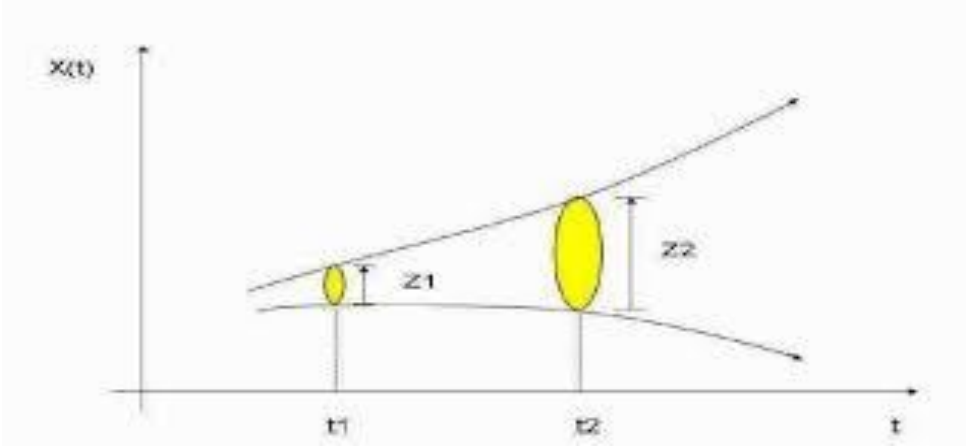


Figure 1.2 : Divergence de deux trajectoires dans le plan de phase.

Les exposants de Lyapunov considérées comme une détermination de la dynamique d'un système. Si les exposants sont tous négatifs ou tous égaux à zéro on dit que le système représente un attracteur non chaotique, l'attracteur étrange chaotique possède au moins trois (3) exposants dont un au moins est positif (voir le tableau 1.1).

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

Tableau1.1 : Classification des systèmes dynamiques selon leurs exposants de Lyapunov [11].

1.10. Bifurcation

La théorie de bifurcation est l'étude mathématique des changements qualitatifs ou topologiques de la structure d'un système dynamique. 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 [11].

Dans les systèmes dynamiques, un diagramme de bifurcation montre les comportements possibles d'un système, à long terme, en fonction des paramètres de bifurcation [11].

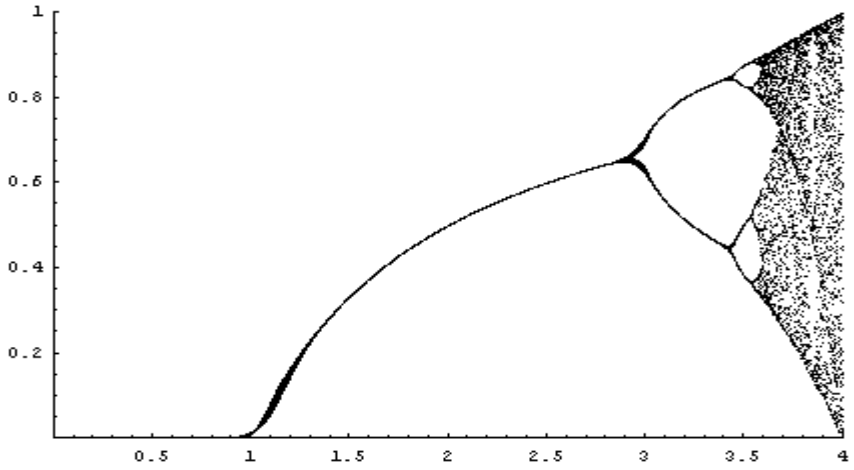


Figure1.3 : diagramme de bifurcation.

1.11. Les types du système dynamique chaotique

Après la découverte de l'attracteur de Lorenz en 1963, les chercheurs et les experts ont attiré par le domaine du chaos, donc plusieurs sortes de système chaotique et hyper-chaotique ont été présentés par la suite.

Les systèmes dynamiques chaotiques peuvent être classés selon un critère temporel en trois grandes catégories :

1.11.1. Les systèmes chaotiques continus

En 1963 Lorenz découvre que l'on peut obtenir un comportement chaotique avec seulement trois variables, soit un système non linéaire à trois degrés de liberté. Il montre donc qu'une dynamique très complexe peut apparaître dans un système formellement très simple, ç'est le système de Lorenz. On peut considérer : le système de Lorenz, le système de Rössler et l'oscillateur de Chua.

On obtient le système de Lorenz comme exemple des systèmes chaotiques continus qui définit par :

$$\begin{cases} \dot{x} = \sigma(y - x) \\ \dot{y} = x(\rho - z) - y \\ \dot{z} = xy - bz \end{cases} \tag{1.6}$$

Les figures suivantes représentent le comportement chaotique de système de Lorenz, La figure (1.4) représente la variation des états x, y et z d'une façon erratique.

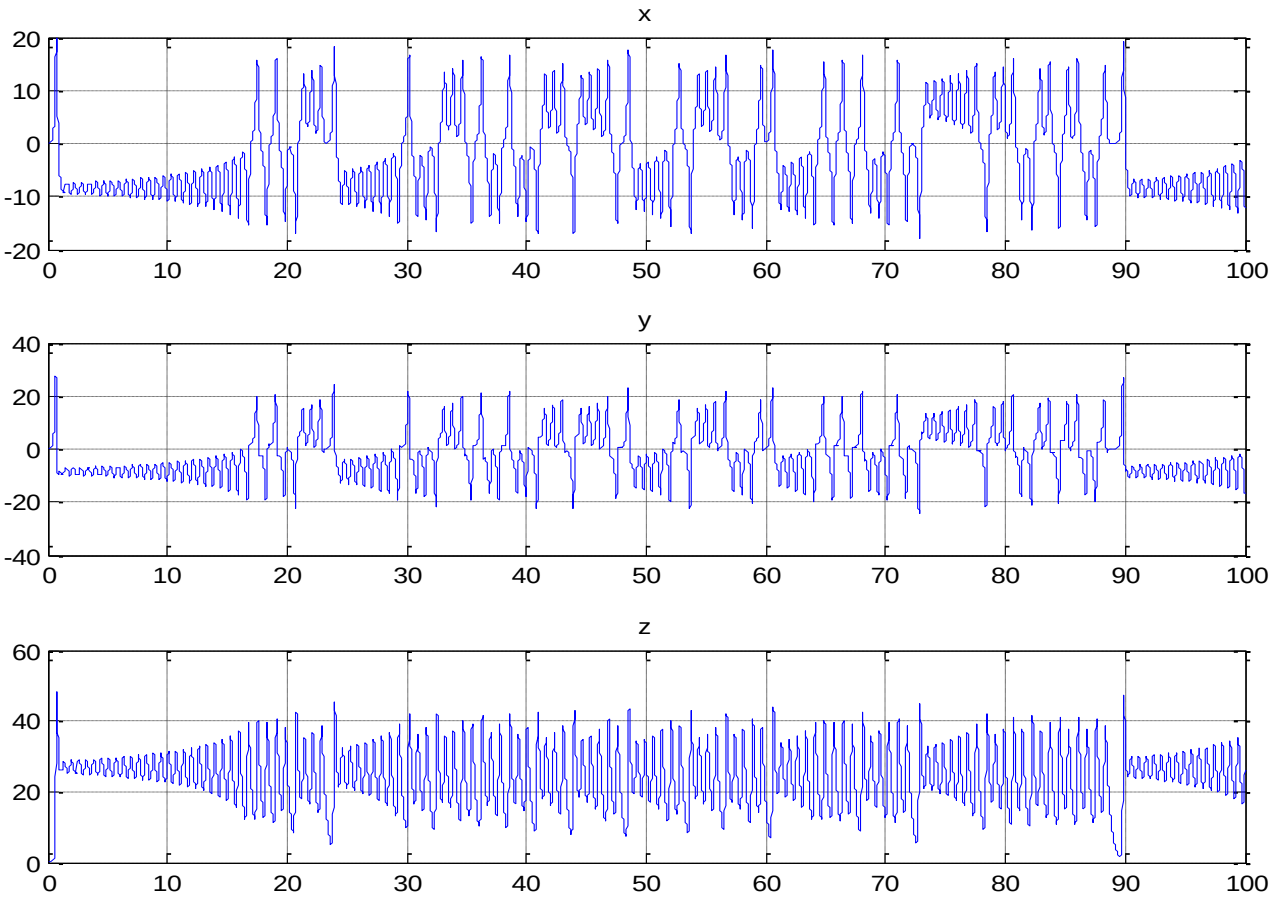


Figure1.4 : L'évolution des états x, y et z du système de Lorenz au cours du temps.

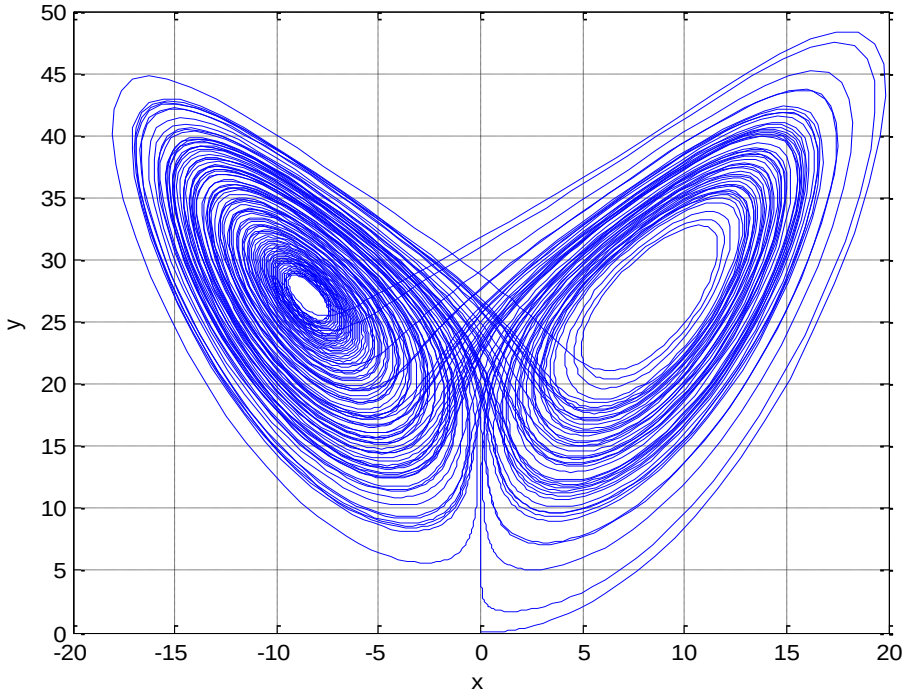


Figure1.5 : L'attracteur étrange de Lorenz.

L'attracteur étrange de Lorenz représente l'évolution des trois (3) états avec une condition initiale, la structure ressemble à deux (2) ailes de papillon.

Remarque : Si on prend une autre condition très voisine de point précédent, on observe que les deux évolutions vont séparer mais les trajectoires s'accumulent sur la même figure de papillon.

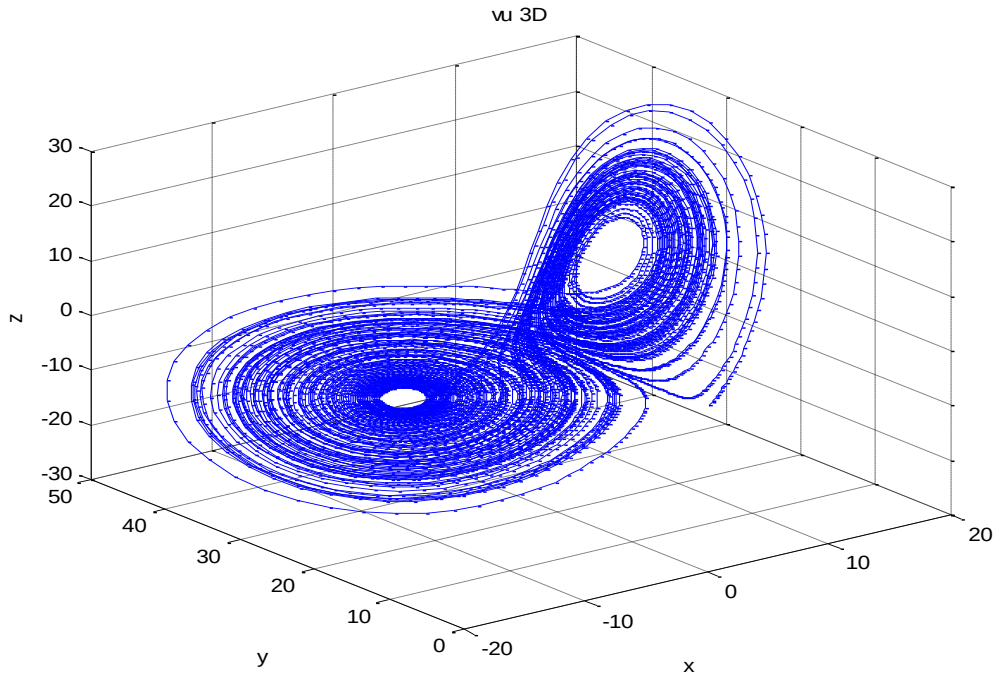


Figure1.6 : l'attracteur étrange de Lorenz en vue 3D.

1.11.2. Les systèmes chaotiques discrets

Le système chaotique discret veut dire que les variables n'évoluent pas d'une manière continue.

La fonction logistique est parmi les systèmes chaotiques discrets les plus connus, elle est une des systèmes de Chebychev, il existe d'autres systèmes comme la fonction Tent, la fonction Gaussienne discrète et le système de Henon.

On obtient le système de Henon comme exemple :

$$x_{(n+1)} = \left(y_{(n)} + 1\right) - \left(a * x_{(n)}\right) \qquad (1.7)$$

$$y_{(n+1)} = b * x_{(n)}$$

Puis on prend les valeurs suivantes pour la réalisation de système : a = 1.4, b = 0.3, avec l'initialisation par : x(1) = y(1) = 0.1.

Les figures qui convient représentent le comportement chaotique du système de Henon pour les paramètres précédents.

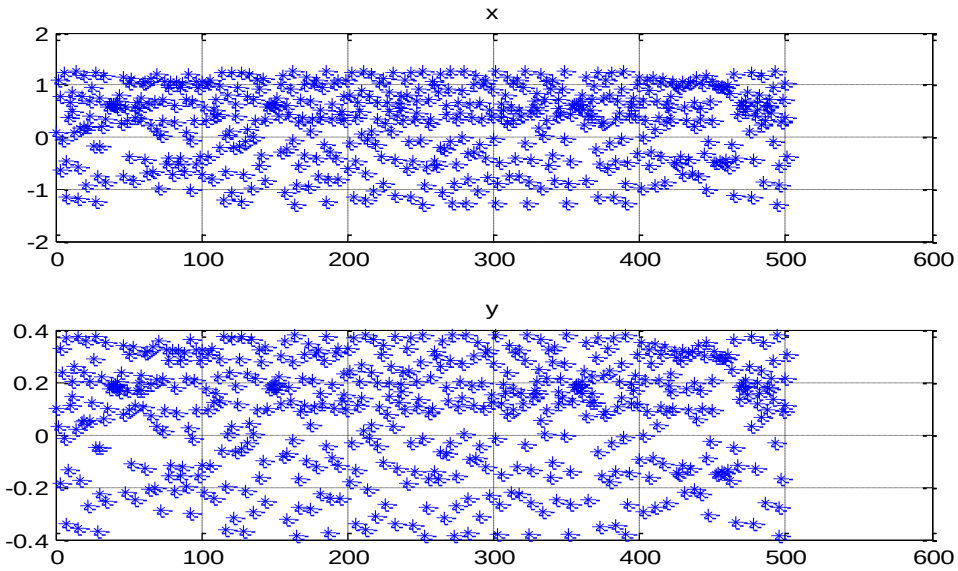


Figure1.7 : L'évolution des états x et y du système de Henon.

Toutes les valeurs qui convergent vers cette structure le font d'une manière différente. L'attracteur de Henon montre une infinité de fines structures à mesure qu'on effectue des grossissements successifs.

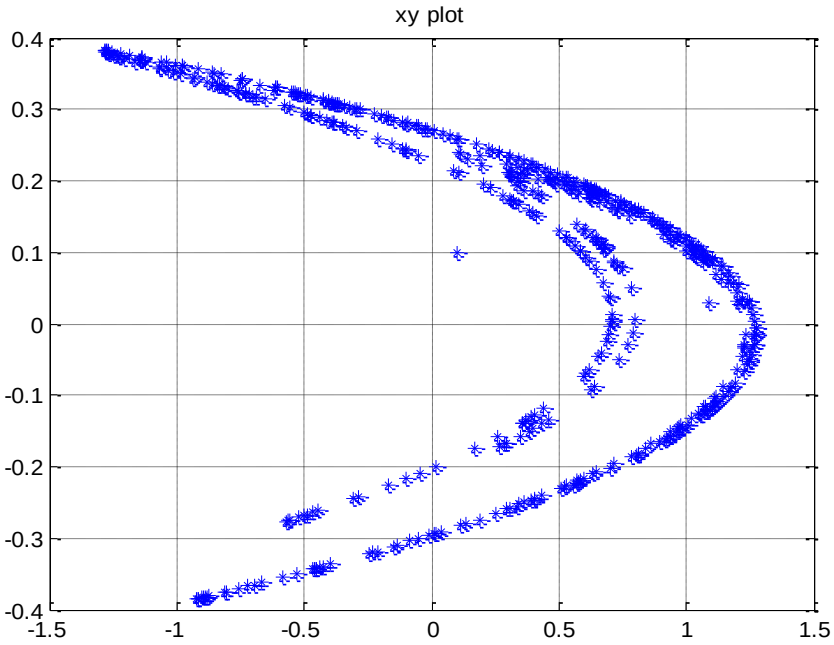


Figure1.8 : l'attracteur de système de Henon.

1.11.3. Les systèmes chaotiques à retard

L'année de 1977 était l'année de la découverte du premier système chaotique à retard à partir d'un modèle physiologique ç'est le système Mackey-Glass. En 1999 Chen et Uta ont découvert un nouvel attracteur chaotique, il s'agit du modèle de Chen.

Il est définit par le système d'équations à trois (3) dimensions suivant :

$$\begin{cases} \dot{x} = a(y - x) \\ \dot{y} = (c - a)x + cy - xz \\ \dot{z} = -bz + xy \end{cases} \quad (1.8)$$

Le comportement de ce système est chaotique pour les paramètres a, b et c avec les valeurs suivantes : a = 35, b = 8/3, c = 28, on va ajouter un terme de retard pour le système soit chaotique avec retard. Le modèle de Chen retardé est défini par :

$$\begin{cases} \dot{x} = a(y - x) + a_1 x(t - \tau_1) + a_2 x(t - \tau_2) \\ \dot{y} = cy - xz + a_3 y(t - \tau_1) \\ \dot{z} = -bz + xy + a_4 z(t - \tau_2) + d \end{cases} \quad (1.9)$$

Les valeurs des paramètres : a = 35, a_1= 1.4, a_2= 0.4, a_3 = a_4 = 0.5, b = 3, c = 20 et d = -300. Les retards: τ_1 = 1s, τ_2 = 2s. Les figures qui convient représentent le comportement chaotique du système de Chen retardé pour les paramètres précédents.

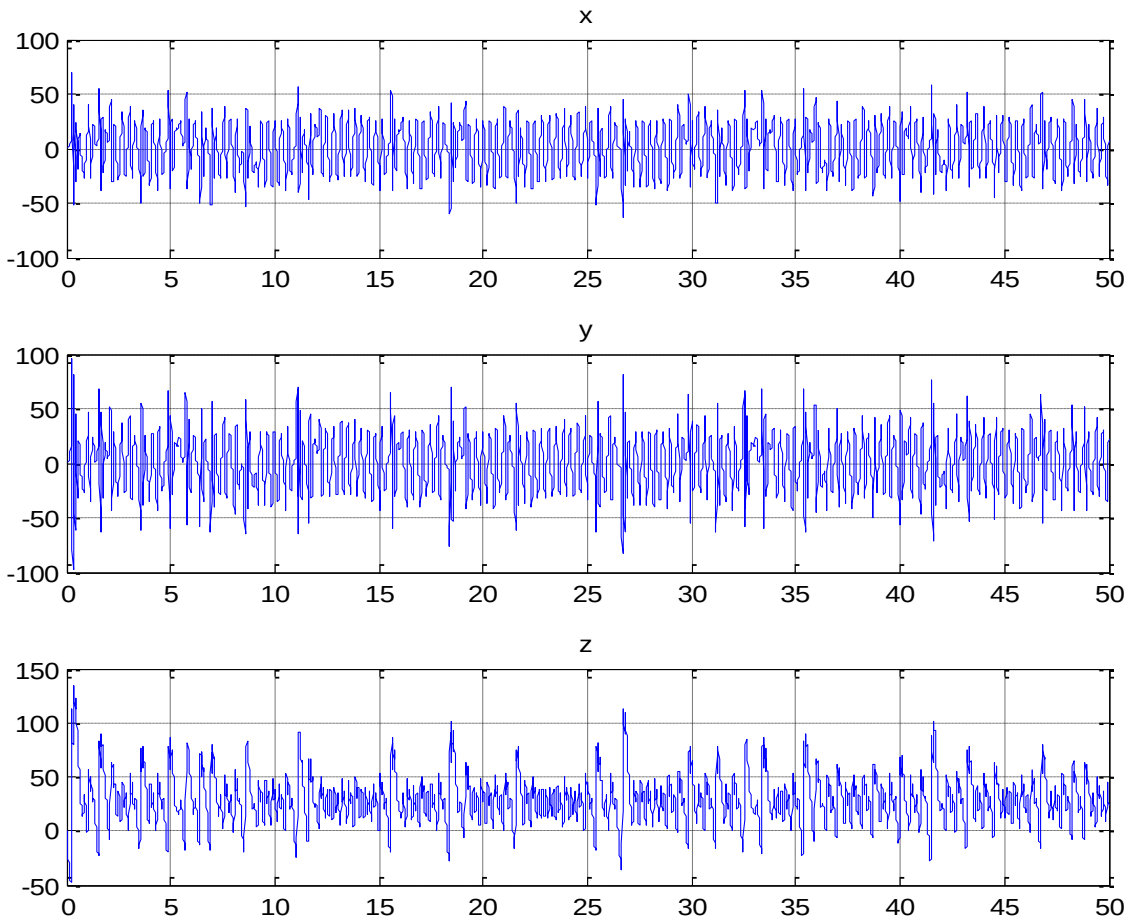


Figure1.9 : L'évolution des états x, y et z en fonction du temps du système de Chen retardé.

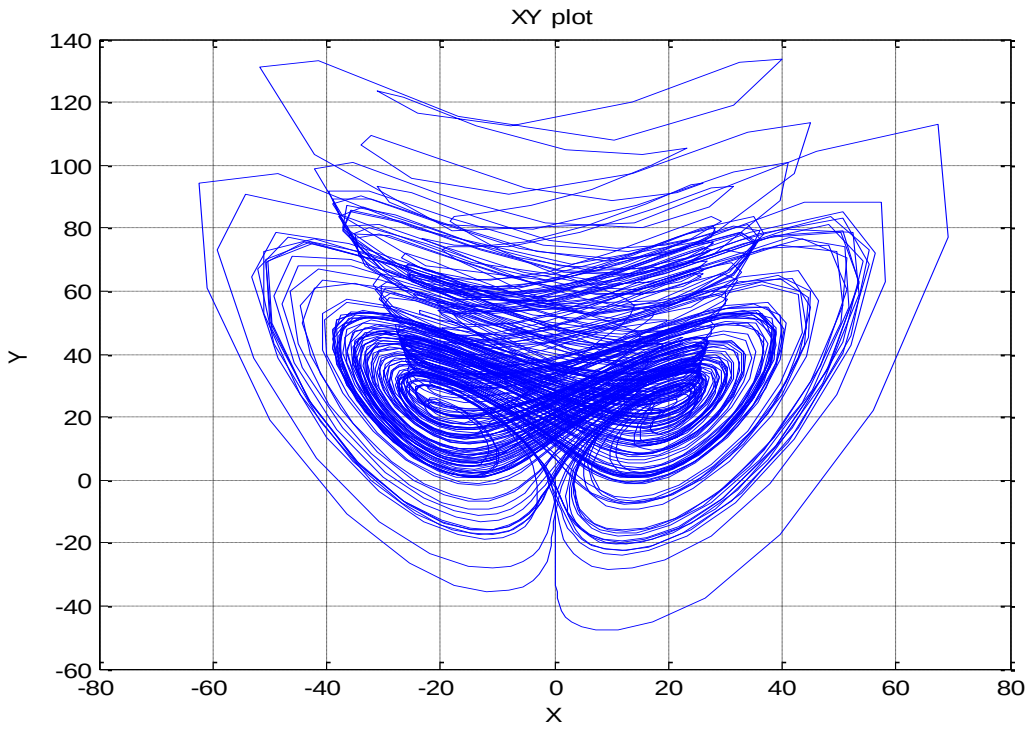


Figure1.10 : L'attracteur du système de Chen retardé.

1.12. Conclusion

Ce chapitre avait comme objectif de présenter les notions fondamentales des systèmes dynamiques chaotiques ainsi que des simples définitions. Il faut retenir que la nature d'un système chaotique est complexe, irrégulière et d'apparence aléatoire, son comportement lié aux conditions initiales.

Les propriétés du chaos présentent un grand intérêt dans le domaine de la sécurité des informations, cet intérêt consiste à ajouter l'information à transmettre à un signal chaotique, cette information sera déchiffrée au niveau de récepteur avec une synchronisation.

Dans le prochain chapitre, nous allons présenter les différentes approches de synchronisation des systèmes chaotiques ainsi que l'utilisation du chaos pour la sécurisation d'information.

CHAPITRE 2

SYNCHRONISATIONS DES SYSTEMES CHAOTIQUES

2.1 Introduction

L'utilisation du chaos dans les systèmes de télécommunication a été rendue possible depuis la maitrise de la synchronisation des systèmes chaotiques. Un signal chaotique se présente sous forme d'un bruit blanc dans les deux domaines temporel et fréquentiel. Ce qui différencie un signal chaotique d'un bruit aléatoire est la notion de déterminisme. En effet, le bruit ne peut être décrit que comme un processus aléatoire alors qu'un système chaotique est représentable par des équations différentielles. Ainsi il est possible de synchroniser deux systèmes chaotiques [21].

La synchronisation est une exigence de nombreux types de systèmes de communication, elle vient du mot grec ''συν'' (**syn)** qui veux dire 'Avec ' et "χρνος " **(chronos)** qui signifie le 'temps', c'est une action d'accorder au même temps plusieurs mouvement, opération, phénomène, évènement.

2.2 Principe de synchronisation des systèmes chaotiques

La synchronisation des signaux chaotique a été découverte par Thomas carol et louis Peccora en 1996.

La synchronisation c'est un phénomène qui se produit lorsque deux système dynamique identique qui c'évoluant en fonction du temps. Elle consiste à synchroniser est rapprocher les trajectoires des deux systèmes jusqu'à ce qu'ils deviennent confondues. La synchronisation obéis a la plus populaire des configurations de synchronisation ou cette dernier consiste à obliger un système dynamique dit **esclave** à se synchroniser (suivant la même trajectoire) avec un deuxième système dynamique dit **maître**.

2.3 Type de synchronisation des systèmes chaotiques

Suite à cette découverte de Pecora et Caroll plusieurs types de synchronisation ont été introduits, ils sont en général basés sur le même principe de l'utilisation des circuits identiques. Supposons deux systèmes chaotiques identiques oscillant de façon totalement indépendante. Si, par un moyen quelconque, on leur permet d'échanger de l'énergie, qui est l'action que l'on nomme «couplage», les deux systèmes finiront par céder la place à un comportement commun, c'est la synchronisation [13].

On trouve deux types de synchronisation classés selon la direction de l'énergie échangée entre les deux systèmes chaotiques : La synchronisation par couplage unidirectionnelle et synchronisation par couplage bidirectionnelle.

Dans ce qui suit nous allons définir et donner le principe des deux types de synchronisation.

2.3.1 Synchronisation par couplage 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 [16].

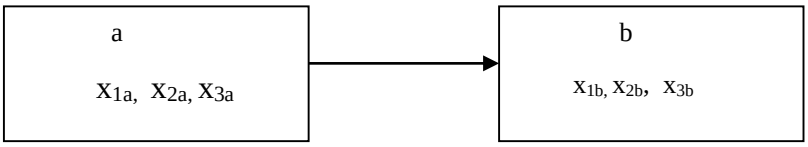


Figure 2.1 : Schéma de couplage découplage unidirectionnel.

2.3.2 Synchronisation par couplage bidirectionnelle

Pour la synchronisation bidirectionnelle, le couplage entre les deux systèmes identiques a et b, se fait par un élément qui permet échange de l'énergie dans les deux sens, cette élément peut être par exemple une résistance [12].

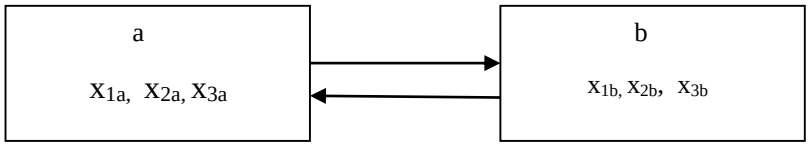


Figure 2.2 : Schéma de couplage bidirectionnel.

2.4 Méthodes de synchronisation

Plusieurs méthodes de synchronisation ont été proposées dans la littérature. Dans ce qui suit nous citons quelque approche en expliquant leurs principes.

2.4.1 Synchronisation Par Décomposition Du Système

Apelle aussi par répartition du système, consiste à divisée le signal chaotique d'origine qui possède plusieurs exposants Lyapunov positifs, en deux sous-système maître et esclave. Pecora et Carrol on proposée un système chaotique donnée par l'équation $\dot{x}$ et sa sortie y :

$$\begin{cases} \dot{x} = f(x) \\ y = h(x) \end{cases} \tag{2.1}$$

Le système maître est décomposé en deux sous-systèmes dont les états sont x_1 et x_2 respectivement :

$$\dot{x}_1 = f_1(x_1, x_2) \tag{2.2}$$

Et

$$\dot{x}_2 = f_1(x_2, y) \tag{2.3}$$

Avec

$X=\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$

Les exposants de Lyaponuv conditionnelle du système (2.3) doivent être négative [13].

2.4.2 Synchronisation identique

Ou synchronisation complète, c'est la plus ancienne et simple de synchronisation des systèmes chaotiques couplés, et donne une solution simple et performante. Son principe consiste à ce que le système esclave reproduit l'état du système maître [14].

Considérant deux systèmes dynamiques :

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

Et

$$\dot{x}_s(t) = f(x_s(t)) \tag{2.5}$$

Où $x_m(t), x_s(t) \in \mathcal{R}^n$ sont des vecteurs d'état de dimension n.

Alors (2.4) et (2.5) sont identiquement synchronisés si, quelles que soient leurs conditions initiales :

$$lim_{\,t\to\infty} |x_s(t) - x_m(t)| = 0 \tag{2.6}$$

2.4.3 Synchronisation par boucle fermée

L'idée de la synchronisation par boucle fermée c'est de corrigée le comportement du système récepteur en fonction d'une erreur qu'on injecte à ce dernier, cette erreur est due entre le signal transmis par le premier système et le signal régénéré par l'autre.

La figure suivante indique un schéma simplifié de la synchronisation par boucle fermée.

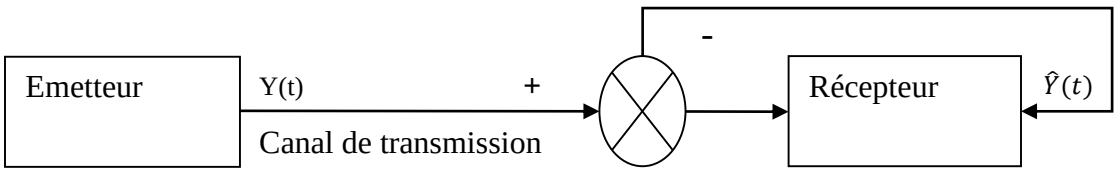


Figure 2.3 : Synchronisation par boucle fermée.

2.4.4 Synchronisation de Phases

Les phases des deux systèmes, maître et esclave sont φ_1 et φ_2 respectivement. La synchronisation de phase entre ces deux systèmes chaotiques est exprimée par la relation :

$$|m\,\varphi_1 - n\varphi_2| < \varepsilon \tag{2.7}$$

Avec m et n, deux nombres entiers et ε un nombre positive constant très petite.

Cette notion classique de synchronisation a été étendue aux systèmes chaotiques. Les amplitudes de ces systèmes restent non corrélées [17].

2.4.5 Synchronisation retardée

Dans la synchronisation retardée l'état du système esclave tend vers l'état décalé dans le temps du système maître c'est-à-dire [15]

$$\lim_{t\to\infty} \|\hat{x}_1(t) - x(t-\tau)\| = 0 \tag{2.8}$$

Ou $x(t)$est l'état du système émetteur, $\hat{x}(t)$l'état du système récepteur, et τ est un retard positif [15].

2.4.6 Synchronisation projective

Dans cette méthode, l'état du système récepteur se synchronise avec un multiple de l'état du système émetteur, Donc il existe a et τ tell que :

$$\lim_{t\to 0} \|\hat{x}_1(t) - ax(t-\tau)\| = 0 \tag{2.9}$$

Où a est le facteur d'échelle, $x(t)$est l'état du système émetteur, $\hat{x}(t)$ l'état du système récepteur, τ est un retard positif [16].

Ce type de synchronisation est utilisé pour des systèmes partiellement linéaires et permet de synchroniser à un facteur prés les états qui ne peuvent être synchronisée [16].

2.4.7 Synchronisation impulsive

Dans un schème de transmission usuel, un des états du système dynamique est transmis afin de réaliser la synchronisation par le récepteur. Dans le but de réduire la redondance du signal transmis la synchronisation impulsive a été proposée.

Le control impulsive d'un système signifie qu'à des moments choisis, les étés du système changent soudainement.

Considérons le système maître suivant :

$$\dot{x}(t) = f(x(t)) \tag{2.10}$$

On définit un signal impulsif qui consiste en une suite d'instants discrets auxquelles un signal $y(t) = Cx(t)$ est envoyé par le système maître au système esclave, dont les variables d'état subissent un saut et un changement d'état. La figure représente le schéma synoptique de la synchronisation impulsive.

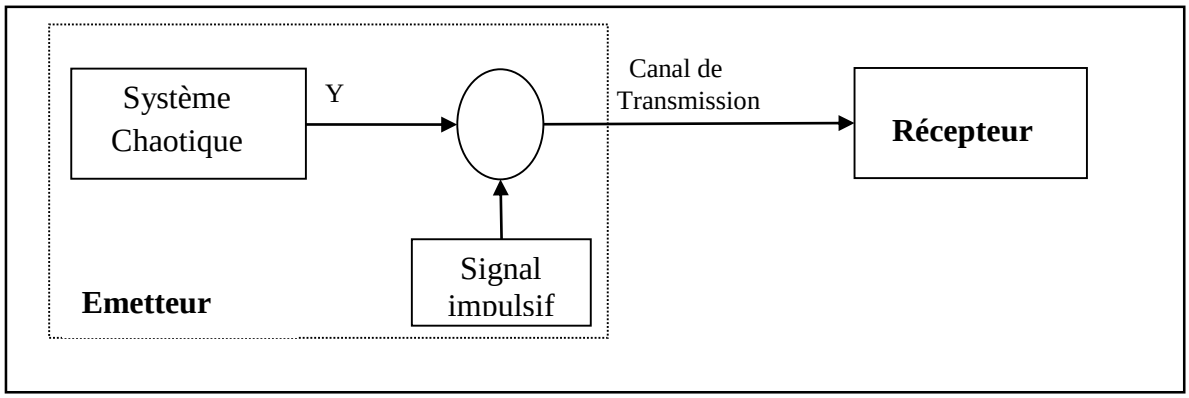


Figure 2.4 : Synchronisation impulsive.

2.4.8 Synchronisation à l'aide d'observateur

La synchronisation peut s'effectuer également en employant un observateur. L'observateur est un système dynamique qui permet d'estimer les états inconnus d'un système qui ne peut être mesuré directement (inaccessible à la mesure pour des raisons technologiques ou économique). Un système dynamique est dit observable si on peut récupérer toutes ses grandeurs (de façon statique ou dynamique) par une combinaison de mesures de ses sorties et de leurs dérivées [15].

La synthèse d'observateur des systèmes linéaires a fait l'objet de beaucoup de travaux [13], en effet les premiers travaux sur les observateurs, publier vers les années soixante par Kalman et Luenberger, le premier s'intéressant au système linéaire variant dans le temps, et le second pour les systèmes linéaires invariant dans le temps.

Dans la synchronisation à l'aide d'observateur, le système maître est un système chaotique quelconque et le système esclave est un observateur d'état correspondant. La Figure (2.5) illustre ce principe de synchronisation.

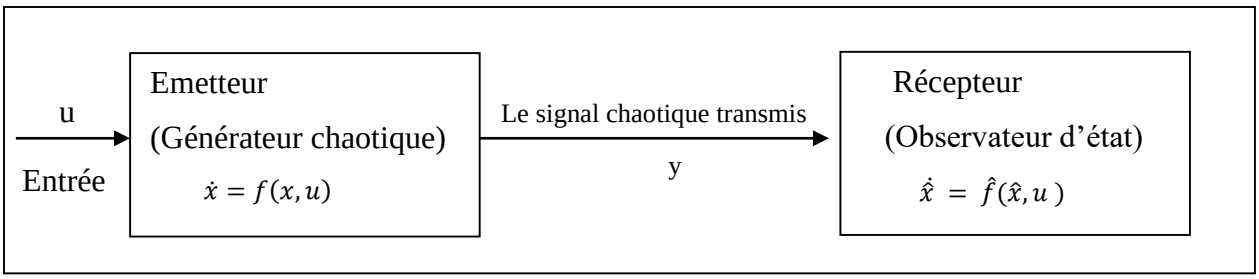


Figure 2.5 : Principe de synchronisation à l'aide d'observateur.

Ainsi l'émetteur et le récepteur se synchronisent si les systèmes $\dot{\hat{x}} = \hat{f}(\hat{x}, u)$ (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 :

$$\lim_{t \to \infty} \|x(t) - \hat{x}(t)\| = 0 \qquad (2.11)$$

Des différents types d'observateur (en temps continue et en temps discret) dans différent buts ont été proposés :

- L'observateur de Kalman étendu.
- Les observateurs à grand gain.
- Les observateurs à modes glissants est basé sur la théorie des systèmes à structures variable.
- L'observateur adaptatif, pour l'évaluation des états et les paramètres du système dynamique.
- L'observateur dead-beat pour les systèmes en temps discret.

2.5. L'utilisation du chaos pour la transmission sécurisée d'information

L'idée d'utilisation du chaos pour sécuriser les informations est venue à base de ses caractéristiques et de son comportement. Comme on a vu que le chaos déterministe génère des comportements dynamiques d'apparence aléatoires, donc il était possible d'utiliser ce phénomène comme porteur d'information en télécommunication.

Le principe de chiffrement par chaos consiste à transmettre un message à travers un signal chaotique d'un émetteur vers un récepteur connaissant les conditions initiales pour extraire le message original.

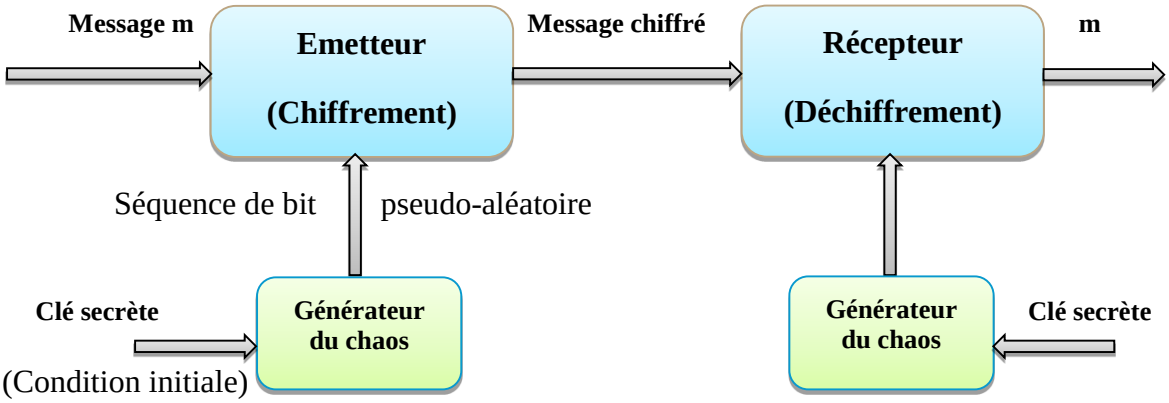


Figure2.6 : Principe de transmission sécurisé à base du chaos.

On prend un exemple de chiffrement par chaos qui est le masquage, cette méthode consiste à cacher un signal d'information dans un signal chaotique ayant un spectre plus répandu et qui a une allure pseudo-aléatoire. On va cacher le message C dans un signal chaotique dont la formule serra $y = x + C$, Le message C serra difficile à déchiffré lors de son trajet sur le canal public. A la réception on verra que le récepteur connaisse les conditions initiales et il va déchiffrer facilement le message original.

2.6. Transmission basée sur la synchronisation de système chaotique

Il existe plusieurs techniques qui peuvent servir comme moyen de masquage de l'information dans le chaos, nous décrivons ici quelques-uns :

2.6.1. Chiffrement par addition

Ç'est la première méthode utilisée pour la synchronisation du chaos. Dans cette méthode appelée, masquage chaotique, l'émetteur est un système chaotique autonome dont le signal de sortie y(t) est ajouté au signal du message m(t). La somme de deux signaux est transmise au récepteur à travers le canal de transmission, qui est un canal public. Le récepteur est constitué d'un système chaotique identique à l'émetteur et un simple soustracteur. Ainsi, après la synchronisation des deux systèmes chaotique (émetteur et récepteur), le message est extrait à l'aide d'une opération de soustraction [9].

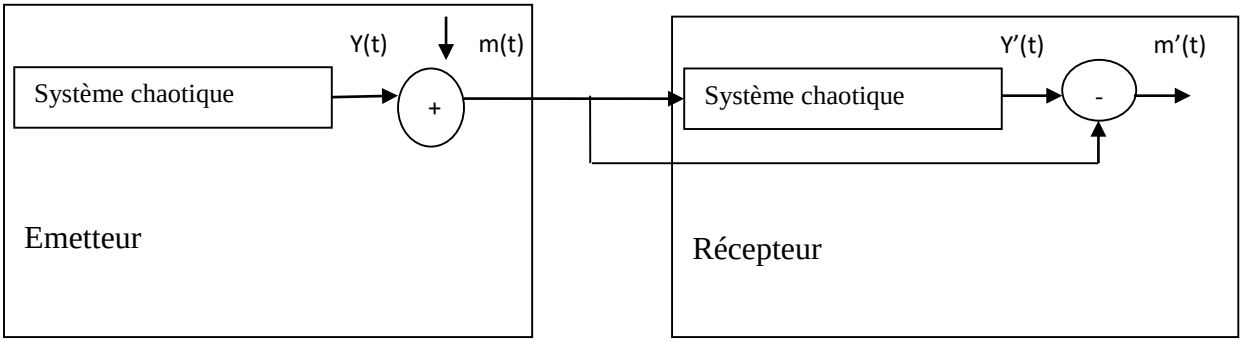


Figure2.7 : Principe du chiffrement chaotique par addition.

Le principal avantage de cette méthode réside dans la simplicité du cryptage. On peut souligner que cette technique peut être appliquée à des messages continus ou discrets.
L'inconvénient de cette méthode est qu'afin de garantir la synchronisation le message doit être au moins de 20 à 30 dB inférieur à la sortie de l'émetteur [11].

2.6.2. Chiffrement par commutation

Cette méthode est utilisée pour transmettre les messages binaires, et réservée aux messages prenant un nombre fini de valeurs. L'émetteur est composé de deux ou plusieurs systèmes chaotiques et pour chaque niveau de message m(t), l'un des systèmes envoi sa sortie sur la ligne de transmission. Ainsi, le signal transmis commute entre deux attracteurs étrange. Le récepteur est constitué de deux systèmes chaotiques identiques (ou totalement différents) à ceux de l'émetteur et un bloc de comparaison permet de relever la valeur du message m'(t).

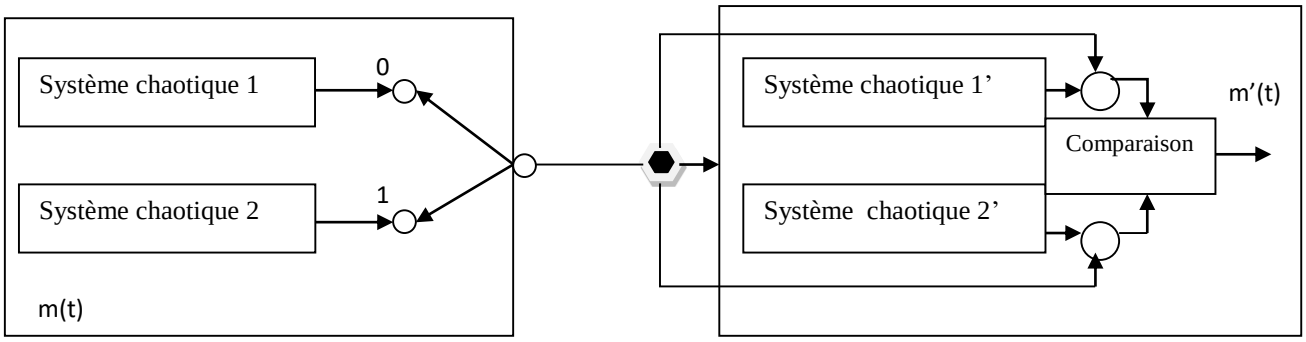


Figure 2.8 : Principe de chiffrement par commutation.

2.6.3. Chiffrement par modulation

Cette technique est basée sur la modulation d'un ou plusieurs paramètres de l'émetteur chaotique utilisant le message contenant l'information.

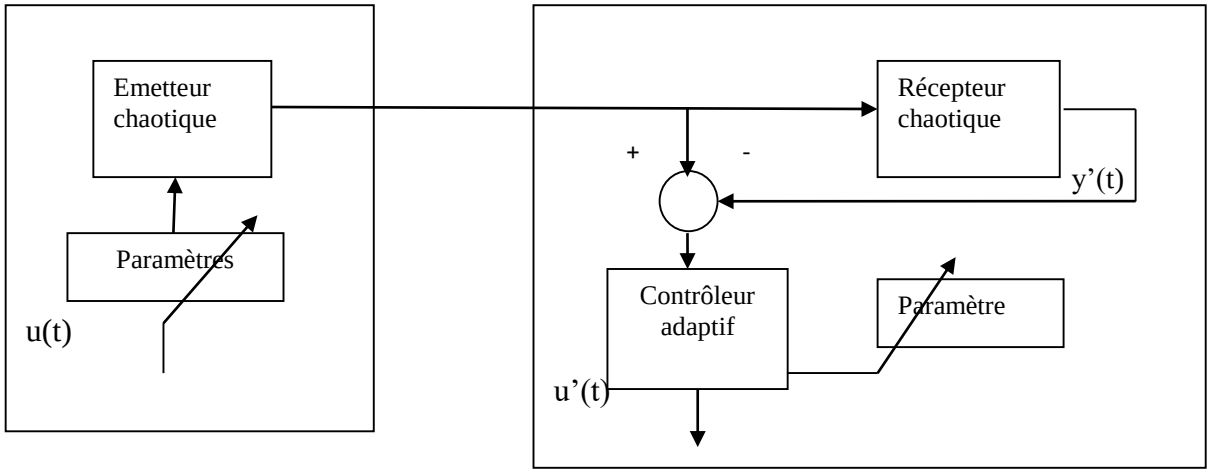


Figure 2.9 : Principe de chiffrement par modulation.

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. 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 [11].

2.7. Conclusion

Ce chapitre a comme objectif de faire le lien entre les systèmes dynamiques chaotiques et le domaine des télécommunications et la sécurité des informations.

Dans ce chapitre, nous avons expliqué le concept de synchronisation des systèmes chaotiques ainsi que les différents modes de synchronisation. Cette démarche nous sera très utile pour notre système de transmission. Nous avons expliqué aussi l'idée d'utilisation du chaos pour sécuriser les informations et les techniques qui peuvent servir comme moyen de masquage de l'information dans le chaos.

Le prochain chapitre sera une réalisation de la sécurisation d'un signal avec une synchronisation entre l'émetteur et le récepteur utilisant un observateur.

CHAPITRE 3

APPLICATION DE L'OBSERVATEUR POUR LA SYNCHRONISATION DU CHAOS

3.1. Introduction

Une bonne maitrise d'un procédé exige la connaissance complète de ces différentes variables d'état. Sur le plan pratique il est souvent difficile d'accéder à toutes les variables qui constituent le vecteur d'état à cause d'une part, au fait que ces variable d'état non pas toujours une signification physique donc leur mesure directe est impossible à réaliser, et d'autre part, quand la variable d'état existe physiquement, sa mesure ne peut être calculé pour des raisons économiques, technologiques et même de fiabilité. Alors, pour remédia à ce problème, on utilise un système dynamique appelé observateur. La théorie d'observation d'état déterministe a été initié vers les années soixante par Luenberger et Kalman, ce qui a conduit ces dernier à l'élaboration d'un modèle qui a pour but de fournir en temps réel l'estimation d'état du système abordé en fonction de ses entrées et ses sorties et de son modèle. L'utilisation des observateurs est liée avec la notion d'observabilité des systèmes.

3.2. Observateurs

L'objectif d'un observateur est de fournir une estimation asymptotiquement ou exponentiellement la valeur courante de l'état en fonction des entrées et des sorties passées du système en temps réel.

D'une manière générale, on appelle observateur ou l'estimateur d'état d'un système dynamique (S) [17]:

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

Un système dynamique auxiliaire (O) dont les entrées sont constituées des vecteurs d'entrée et de sortie du système à observer et dont le vecteur de sortie $\hat{x}(t)$ est l'état estimé :

$$(O)\quad \begin{cases} \dot{z}(t) = \hat{f}(z(t), u(t), y(t)) \\ \hat{x}(t) = \hat{h}(z(t), u(t), y(t)) \end{cases} \tag{3.2}$$

L'erreur entre le vecteur d'état x(t) et $\hat{x}(t)$ tend asymptotiquement vers zéro.

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

Le schéma de principe d'un tel observateur est donné par la figure 3.1.

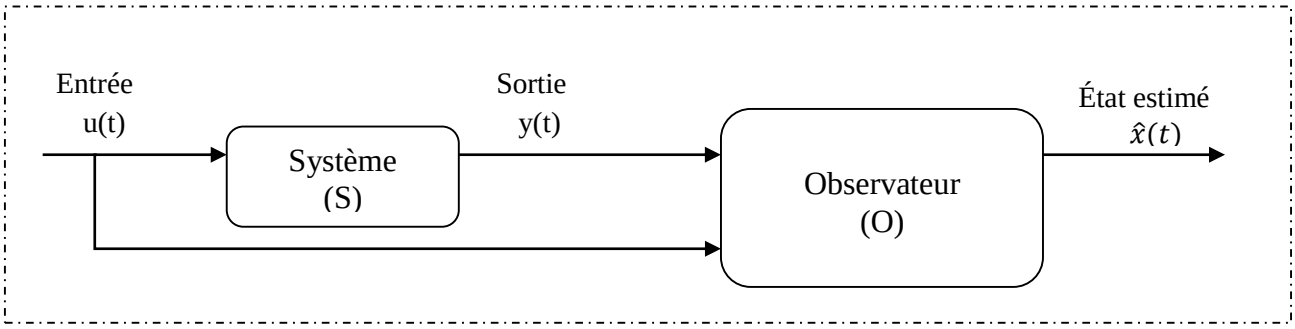


Figure 3.1 : Observateur.

3.3. Observabilité

L'observabilité d'un système est la propriété qui permet de dire si l'état peut être déterminé uniquement à partir de la connaissance des signaux d'entrée et de sortie.

3.3.1. Observabilité des systèmes linéaires [22][11][23]

La notion d'observabilité a été introduite par Kalman pour les systèmes linéaires :

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

Avec $x(t) \in \mathcal{R}^n$ le vecteur d'état, $u(t) \in \mathcal{R}^m$ le vecteur d'entrée et $y(t) \in \mathcal{R}^p$ le vecteur de sortie. Les matrices *A*, *B* et *C* ont des dimensions appropriées.

On appelle observabilité d'un système, la possibilité d'évaluer le vecteur d'état *x* à partir de mesures effectuées sur le système. On dit que le système (3.1) est observable à l'instant t_1 si à partir de la connaissance du vecteur de sortie *y* et du vecteur d'entrée *u*, il est possible en un temps fini $t_2 > t_1$ de déterminer l'état $x(t_1)$. Le critère d'observabilité de *Kalman* est donné par la matrice d'observabilité suivante :

$$Obs = \begin{bmatrix} C \\ CA \\ \vdots \\ CA^{n-1} \end{bmatrix} \tag{3.4}$$

La dimension du sous-espace d'état observable est égale au rang de la matrice d'observabilité.

Autrement dit, le système (3.1) est observable si *rang(O) = n*.

Une solution simple et optimale au problème de l'estimation de l'état des systèmes linéaires a été proposée par Luenberger [31] reposant essentiellement sur des techniques de placement de pôles.

Luenberger proposa l'observateur suivant pour le système (3.1) :

$$\dot{\hat{x}}(t) = A\hat{x}(t) + Bu(t) + K(y(t) - C\hat{x}(t)) \tag{3.5}$$

La dynamique de l'erreur d'estimation $\mathrm{x(t)} - \hat{\mathrm{x}}\mathrm{(t)}$ a pour expression :

$$\dot{e}(t) = (A - KC)e(t) \tag{3.6}$$

En utilisant une technique de placement de pôles, il suffit alors de choisir le gain K de l'observateur de telle sorte que les valeurs propres de la matrice $(A - KC)$ soient dans le demi-plan complexe gauche.

3.3.2. Observabilité des systèmes non linéaires [22][11][23]

Soit le système non linéaire :

$$\begin{cases} \dot{x}(t) = f\big(x(t), u(t)\big) \\ y = h(x(t), u(t)) \end{cases} \tag{3.7}$$

Avec $t \geq 0$.

$x \in \mathcal{R}^n$ est le vecteur d'état, $u \in \mathcal{R}^m$ est le vecteur d'entrée, $y \in \mathcal{R}^p$ est le vecteur de sortieet, les conditions initiales sont données par $x_0 = x(0)$.

Définition 3.1.Condition de rang d'Observabilité.

On définit :

$$L_f h(x) = \sum_{i=1}^{n} f_i(x) \frac{\partial h}{\partial x_i}(x) \tag{3.8}$$

Donc on peut écrire :

$$L_f^0 h = h \text{et} L_f^k h = L_f\big(L_f^{k-1} h\big), \forall\, k \geq 1 \tag{3.9}$$

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

$$rang \begin{bmatrix} dh \\ dL_f h \\ \vdots \\ dL_f^{n-1} h \end{bmatrix} = n \tag{3.10}$$

Ou bien avec une définition algébrique équivalente :

$$rang \begin{bmatrix} dy \\ d\dot{y} \\ \vdots \\ dy^{(n-1)} \end{bmatrix} = n \tag{3.11}$$

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

Définition 3.2.Observateur du système non linéaire **[22][11][23]**.

On considère le système dynamique :

$$\begin{cases} \dot{z}(t) = \hat{f}\big(z(t), u(t), y(t)\big) \\ \hat{x}(t) = \hat{h}(z(t), u(t), y(t)) \end{cases} \tag{3.12}$$

où $z \in \mathfrak{R}^q$, $q \leq n$ avec les conditions initia les $z_0 = z(0)$. Les entrées de ce système sont *u* et *y*, et la sortie est l'état estimé$\hat{x} \in \mathfrak{R}^n$.

Si les hypothèses suivantes sont vérifiées :

(i) $\hat{x}(t_0) = x(t_0) => \hat{x}(t) = x(t),\ \forall t > t_0$,

(ii) l'erreur d'estimation $e(t) = x(t) - \hat{x}(t)$ tend asymptotiquement (respectivement exponentiellement) vers zéro, alors le système (3.12) est un observateur (respectivement un observateur exponentiel) du système (3.7), d'ordre plein si $q = n$, d'ordre réduit si $q < n$.

Le problème de la synthèse d'un observateur consiste donc à trouver des fonctions $\hat{f}$ et $\hat{h}$ qui assurent la convergence de l'état estimé $\hat{x}$ vers l'état réel x du système, et ce, indépendamment de$x_0, z_0, u(t)$. Pour étudier la convergence de l'observateur d'un système, des outils concernant la stabilité des systèmes dynamiques sont utilisés, et notamment la théorie élaborée par *Lyapunov.*

Définition 3.3.Observability Matching Condition et la propriété d'inversion à gauche.

On a le système non-linéaire suivant :

$$\begin{cases} \dot{x} = f(x) + p(x)w \\ y = h(x) \end{cases} \tag{3.13}$$

Où : *w* représente une entrée inconnue, qui peut être une perturbation, un défaut, ou bien, comme dans notre cas un message.

Le vecteur de sortie du système (3.13) sera transmis vers le récepteur, qui doit générer un vecteur de sortie qui converge asymptotiquement vers le vecteur d'entrée de l'émetteur. Cela constitue le problème d'inversion à gauche. Il est possible de concevoir un observateur pour le système (3.13), appelé *'observateur à modes glissants'*, en considérant quelques hypothèses :

h₁) Les états et les perturbations inconnues.

h₂) $\mathrm{rang}\left(\mathrm{dh}, \mathrm{dL_f h}, \dots, \mathrm{dL_f^{n-1} h}\right)^{\mathrm{T}} = \mathrm{n},$

h₃) $\left((\mathrm{dh})^{\mathrm{T}}, (\mathrm{dL_f h})^{\mathrm{T}}, \dots, \left(\mathrm{dL_f^{n-1} h}\right)^{\mathrm{T}}\right)^{\mathrm{T}} \mathrm{p(x)} = (0 \dots 0\ \theta)^{\mathrm{T}}$

Où : θ est une fonction non nulle.

L'hypothèse *h3* est la condition '*observability matching condition*' qui garantit la propriété de l'inversion à gauche (possibilité de reconstruire toutes les états de l'émetteur ainsi que le message à partir de y).

3.4. Les inégalités matricielles linéaires LMI

À l'automatique, on trouve un grand nombre de problème concernant l'optimisation, l'analyse et la synthèse des systèmes dynamiques ainsi que les spécifications de robustesse ou de performance, il a fallu une solution ou (un outil) qui satisfait ces contraintes. Ces problèmes sont généralement difficiles voire impossibles à résoudre de façon analytique (algorithme). Pourquoi ? Parce que ce dernier admet un minimal local à partir d'un point initial, et si par ailleurs elle admet plusieurs solutions minimales le résultat va dépendre du point initial. Cependant ces problèmes peuvent être résolus numériquement en utilisant la programmation convexe par l'approche LMI.

L'intérêt principal des LMIs est la possibilité de calculer le minimum global indépendamment du point initial.

L'histoire des LMIs a plus de 100 ans, et elles se retrouvent dans plusieurs travaux depuis. Ainsi, en 1890 lyapunov a conditionné la stabilité d'un système par LMI. Plus tard, Kalman, Yakubovich et Popov ont généralisé le résultat de stabilité proposé par Lyapunov.

3.5. Etude émetteur

Nous développons un système chaotique constituant l'émetteur.

Notre étude se porte sur un nouveau système continu qui a quatre dimensions, il est régi par le système d'équation suivant :

$$\begin{cases} \dot{x} = a(y - x) \\ \dot{y} = xz + w \\ \dot{z} = b - xy \\ \dot{w} = yz - cw \end{cases} \tag{3.14}$$

Définition des paramètres : x, y, z et w sont les variables d'état. On prend :

- les paramètres du système : a = 6, b = 11, et c = 5.
- Les valeurs initiales : x(0) = 10, y(0) = 10, z(0) = 0, w(0) = 0.

Pour ces valeurs le système présente un comportement chaotique.

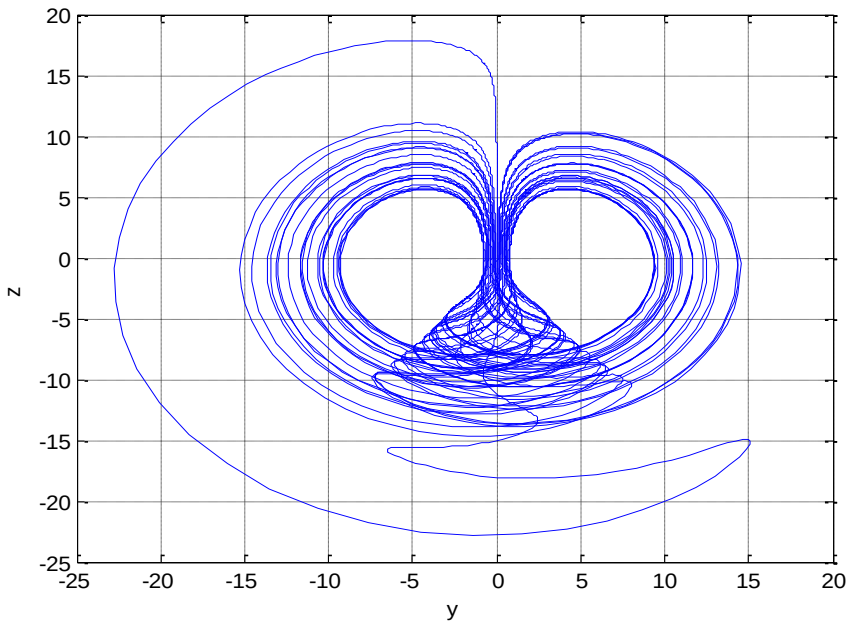


Figure 3.2 : attracteur étrange du système.

Le signal d'information:

$$s = 2 \sin 0.1\pi t$$

On va ajouter ce message au système principal afin de le chiffrer, le nouveau système est désormais comme suit :

$$\begin{cases} \dot{x} = a(y - x) + a_1 s \\ \dot{y} = xz + w + a_2 s \\ \dot{z} = b - xy + a_3 s \\ \dot{w} = yz - cw + a_4 s \end{cases} \quad (3.15)$$

Avec : $a_1 = 1$,$a_2 = 1$,$a_3 = 1$, $a_4 = 0$.

3.6. Etude récepteur

L'observation est proposée pour but d'estimer les états inconnus d'un système qui ne sont pas mesurables directement. Un système est dit observable si on permet de déterminer l'état initial à l'aide de l'observation de ses entrées et sorties pendant un intervalle de temps fini.

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

$$\begin{cases} \dot{x} = Ax + Bs + f(x, s, y) \\ y = Cx + Ds \end{cases} \quad (3.16)$$

Avec $x \in R^n, y \in R^p \; et \; s \in R^m$ représentent respectivement le vecteur d'état, la sortie et le message informatif. A, B, C et D sont des matrices réelles 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 :

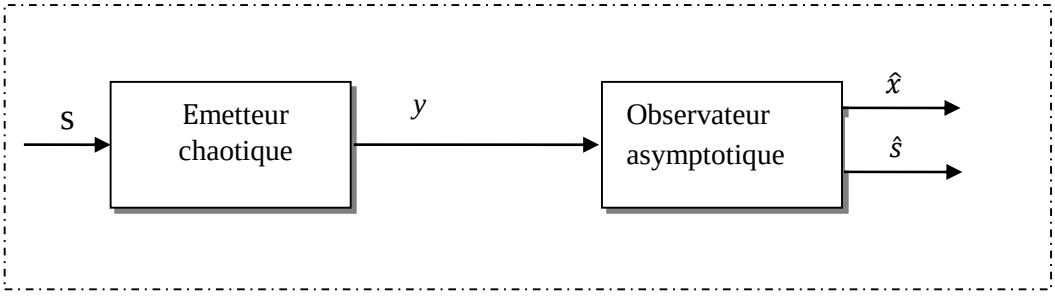


Figure 3. 3 : Principe de la transmission chaotique sécurisée à base d'observateur.

En introduisant les notations [19]: $E = [I_n \; 0], M = [A \; B], H = [C \; D], et \; \xi = \binom{x}{s}$, le système (3.16) peut s'écrire :

$$\begin{cases} E\dot{\xi} = M\xi + f(\xi, y) \\ y = H\xi \end{cases} \quad (3.17)$$

Ainsi, on note [20]:

$$[P\ Q] = \left(\binom{E}{H}^T \binom{E}{H}\right)^{-1} \binom{E}{H}^T \tag{3.18}$$

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

$$PE + QH = I_{n+m} \tag{3.19}$$

Utilisons l'observateur d'état, proposé en [19], de la forme :

$$\begin{cases} \dot{z} = Nz + Ly + g(z, y) \\ \hat{\xi} = z + Qy \end{cases} \tag{3.20}$$

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

Considérons le vecteur d'erreur :

$$e = \hat{\xi} - \xi \tag{3.21}$$

En substituant (3.20) et (3.17) dans (3.21), on obtient :

$$e = z + (QH - I_{n+m})\xi \tag{3.22}$$

En utilisant (3.19), (3.22) devient :

$$e = z - PE\xi \tag{3.23}$$

Donc la dynamique de l'erreur est :

$$\dot{e} = z - PE\dot{\xi} \tag{3.24}$$

D'après (3.16) et (3.20) et en utilisant (3.24), on obtient :

$$\dot{e} = Ne + (N + FH - PM)\xi + g(z, y) - Pf(\xi, y) \tag{3.25}$$

Avec : $$F = L - NQ \tag{3.26}$$

En supposant que :

$$N = PM - FH \tag{3.27}$$

Et :

$$g(z,y) = Pf\left(\hat{\xi},y\right) = Pf(z+Qy,y) \tag{3.28}$$

La dynamique de l'erreur devient alors :

$$\dot{e} = Ne + Pf\left(\hat{\xi},y\right) - Pf(\xi,y) \tag{3.29}$$

Avant de donner le théorème qu'on va l'appliquer dans notre travail, on rappelle d'abord le lemme donnant les conditions nécessaires et suffisantes pour l'existence d'une matrice de stabilité *N* de la partie linéaire de (3.29).

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

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

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 (3.18), nous avons :

$$P = \psi\begin{pmatrix} I_n \\ 0 \end{pmatrix}\,, \quad o\grave{u}\ \ \psi = \begin{pmatrix} I_n + C^T C & C^T D \\ D^T C & D^T D \end{pmatrix}^{-1}$$

Nous avons donc :

$$Rang\begin{pmatrix} \mu I_{n+m} - PM \\ H \end{pmatrix} = Rang\left(\mu\psi^{-1} - \begin{pmatrix} A & B \\ 0 & 0 \end{pmatrix} \atop \begin{pmatrix} C & D \end{pmatrix}\right)$$

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

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

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

Théorème 1: *Faisons les hypothèses suivantes :*

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

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

Où λ *est une constante réelle positive.*

2) *La matrice Dest supposée être à rang plein. Pour les systèmes à une seule sortie, cette condition peut se traduit par* $D \neq 0$ [19].

Sous les hypothèses ***1)*** *and* ***2)****, si on suppose que :*

3) *(A, B, C, D) est minimum de phase,*

4) $W - \sigma I_{n+m}$ *est une matrice définit positive, avec* $\sigma = \|RP\| + \|P^T R\|$ *; R et W sont des matrices définit positive reliées par l'équation de Lyapunov :*$RN + N^T R = -W$.

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

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

Démonstration :

Considérant la fonction de Lyapunov :$V = e^T Re$*, et sa dérivé :*

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

Sous la supposition 3) du théorème1 et d'après la relation (3.27), il existe une matrice du gain inconnue F tel que les valeurs propres de N possèdent 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 :

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

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

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

Ou :

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

Alors, si la matrice $(W - \lambda\sigma I_{n+m})$ est définie positive, le vecteur d'erreur de l'observateur (3.20) tend asymptotiquement vers 0.

Remarque :

Le calcul de la matrice du gain F peut être réalisé par des outils LMI (voir Annexe B) dans le but de vérifier l'hypothèse **4)** du théorème. Un algorithme très utile, pour déterminer F, est donné en [20].

Avant de formuler 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* [19] :**

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

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

Lemme 3*[19]*: *Soient x et y deux vecteurs de dimension n, et ρ un nombre réel positif, alors l'inégalité suivante est toujours vrais :* $2x^T y \leq \rho x^T x + \rho^{-1} y^T y$.

Nous considérons la fonction de *Lyapunov* suivante : $V(e) = e^T Re$, sa dérivée est donc :

$$\dot{V}(e) = \dot{e}^T R\dot{e} \qquad (3.30)$$

En remplaçant (3.29) dans (3.30) on obtient :

$$\dot{V}(e) = [e^T N^T + g(z,y) - f(\xi,y)P^T]R[Ne + g(z,y) - Pf(\xi,y)]$$

$$= e^T(RN^T + N^T R)e + 2e^T R\big(g(z,y) - Pf(\xi,y)\big)$$

$$\leq e^T\left(RN + N^T R - \frac{1}{\delta}RPP^T + \delta\gamma^2 I\right)e \qquad (3.31)$$

$\dot{V}(e) < 0$ si :

$$RN + N^T R - \frac{1}{\delta}RPP^T + \delta\gamma^2 I < 0 \qquad (3.32)$$

Cela est équivalent à :

$$\begin{bmatrix} RN + N^T R + \delta\gamma^2 I_4 & RP \\ P^T R & -\delta I_3 \end{bmatrix} < 0 \qquad (3.33)$$

Sous la supposition (3.27), (3.33) devient :

$$\begin{bmatrix} RPM - RFH - H^T FR + M^T P^T R + \delta\gamma^2 I_4 & RP \\ P^T R & -\delta I_3 \end{bmatrix} < 0 \qquad (3.34)$$

En posant : $y = RF$, nous devons résoudre les *LMIs* suivantes :

$$LMI\ (1): \begin{bmatrix} RPM + M^T P^T R - yH - H^T y^T + \delta\gamma^2 I_4 & RP \\ P^T R & -\delta I_3 \end{bmatrix} < 0 \qquad (3.35)$$

$$LMI\ (2): \quad R < 0. \qquad (3.36)$$

En utilisant la matrice *R*, obtenue grâce à ces *LMIs*, les gains *N* et *L* de l'observateur (3.20) peuvent être obtenus par les expressions (3.27) et (3.26) respectivement.

3.7. Conclusion

Dans ce chapitre, nous avons développé une approche pour la synchronisation et le chiffrement d'informations à base d'observateur. Nous avons rappelé quelques notions relatives aux observateurs et observabilité des systèmes linéaires et non linéaires.

Dans le chapitre suivant, nous donnerons les résultats de simulation obtenus et nous discuterons ces résultats.

CHAPITRE 4

RESULTATS DE SIMULATION

4.1 Introduction

Dans ce chapitre, on va étaler les différents résultats de simulation sous Matlab 2017. Le système chaotique choisit pour le cryptage est le nouveau système chaotique à quatre dimensions qui est construit sur la base du système chaotique Sprott B [18], La méthode d'intégration Runge-Kutta de quatrième ordre est utilisée pour résoudre les systèmes de l'équation différentielle avec un pas du temps 0,001.

4.2 Emetteur

On considère le système dynamique hyper chaotique 4D suivant [18]:

$$\begin{cases} \dot{x}_1 = a * (x_2 - x_1) \\ \dot{x}_2 = x_1 * x_3 + x_4 \\ \dot{x}_3 = b - x_1 * x_2 \\ \dot{x}_4 = x_2 * x_3 - c * x_4 \end{cases} \quad (4.1)$$

Avec : a = 6, b = 11, c = 5 et $x = [x_1\ x_2\ x_3\ x_4]^T$.

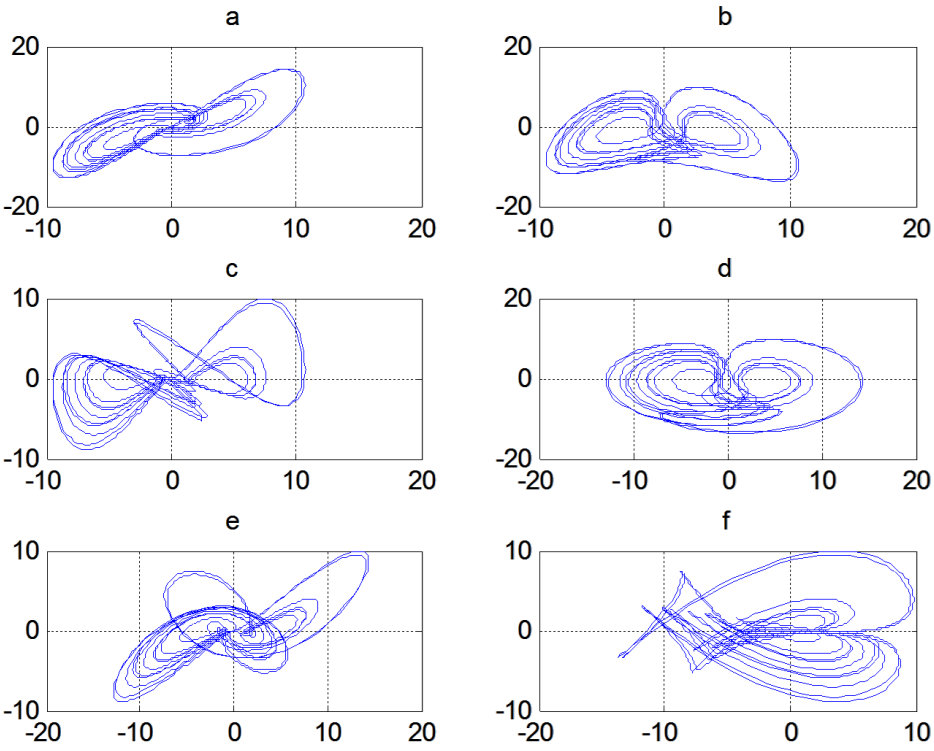


Figure 4.1 : Attracteur étrange du système dans :(a) plan x1 x2, (b) plan x1 x3, (c) plan x1 x4, (d) plan x2 x3, (e) plan x2 x4 et plan (f) x3 x4.

La matrice d'observabilité est donnée par :

$$obs = \begin{bmatrix} dh \\ dL_f h \\ dL_f^2 h \\ dL_f^3 h \end{bmatrix} \tag{4.2}$$

En utilisant *Matlab*, nous avons obtenu $rang(obs) = 4$ donc le système est observable.

Afin de réaliser la transmission d'un message, on injecte un signal sinusoïdal d'amplitude (2) et de pulsation (0.3rad/s) linéairement dans le système et y (t) est la sortie mesurable :

$$\begin{cases} \dot{x}_1 = (a * (x_2 - x_1)) + a_1 * s \\ \dot{x}_2 = x_1 * x_3 + x_4 + a_2 * s \\ \dot{x}_3 = b - x_1 * x_2 + a_3 * s \\ \dot{x}_4 = x_2 * x_3 - c * x_4 + a_4 * s \\ y = C * x(t) + s(t) \end{cases} \tag{4.3}$$

Avec : $a_1 = 1$, $a_2 = 1$, $a_3 = 1$, $a_4 = 0$.

Le système (4.3) peut être mis sous la forme (3.16) tel que :

$$A=\begin{bmatrix} -a & a & 0 & 0 & a_1 \\ 0 & 0 & 0 & 1 & a_2 \\ 0 & 0 & 0 & 0 & a_3 \\ 0 & 0 & 0 & -c & a_4 \end{bmatrix},\ B=\begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \end{bmatrix},\ C = [1,1,1,1,1],\ D = 1,\quad x(t) = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ s \end{bmatrix}$$

$$\text{Et}\quad f(x) = \begin{pmatrix} 0 \\ x_1 x_3 \\ -x_1 x_2 \\ x_2 x_3 \end{pmatrix}.$$

Et sous la forme (3.17), avec :

$$E = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix},\qquad M=\begin{bmatrix} -0.000000000000000 \\ -0.000000000000000 \\ 0.000000000000000 \\ -0.000000000000000 \\ 1.000000000000000 \end{bmatrix}, H = [1\ 1\ 1\ 1\ 1]$$

Les matrices *P* et *Q* qui vérifient la relation (3.19) sont données par :

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

4.3 Récepteur

On utilise l'observateur d'état proposé dans le chapitre précédent sous l'équation (3.20), pour estimer le message transmit. Et les gains N et L vont calculer selon les équations (3.27) et (3.26) respectivement en utilisant la matrice *R*, obtenue. On obtient les résultats suivants :

$$R = \begin{bmatrix} 0.9999 & 0.0001 & 0.0000 & 0.0000 \\ -0.0000 & 0.9999 & 0.0000 & 0.0000 \\ -0.0000 & -0.0000 & 1.0000 & 0.0000 \\ -0.0001 & -0.0000 & 0.0000 & 1.0000 \\ -0.9999 & -1.0000 & -1.0002 & -1.0001 \end{bmatrix}$$

$$F = \begin{bmatrix} 0.300066915042599 \\ 0.500066921800062 \\ 0.300054492213100 \\ -0.899937216920311 \\ 0.300062777441383 \end{bmatrix},$$

$$N = \begin{bmatrix} -6.30006 & 5.69993 & -0.30006 & -0.30006 & 0.69993 \\ -0.50006 & -0.50006 & -0.50006 & 0.49993 & 0.49993 \\ -0.30005 & -0.30005 & -0.30005 & -0.30005 & 0.69994 \\ 0.89993 & 0.89993 & 0.89993 & -4.10006 & 0.89993 \\ 5.69993 & -6.30006 & -0.30006 & 3.69993 & -3.30006 \end{bmatrix}$$

Et $$L = \begin{bmatrix} 1.000000000000000 \\ 1.000000000000000 \\ 1.000000000000000 \\ -0.000000000000000 \\ -3.000000000000000 \end{bmatrix}$$

4.4 Résultats de la simulation

Utilisant les commandes Matlab on obtient les figures qui convient :

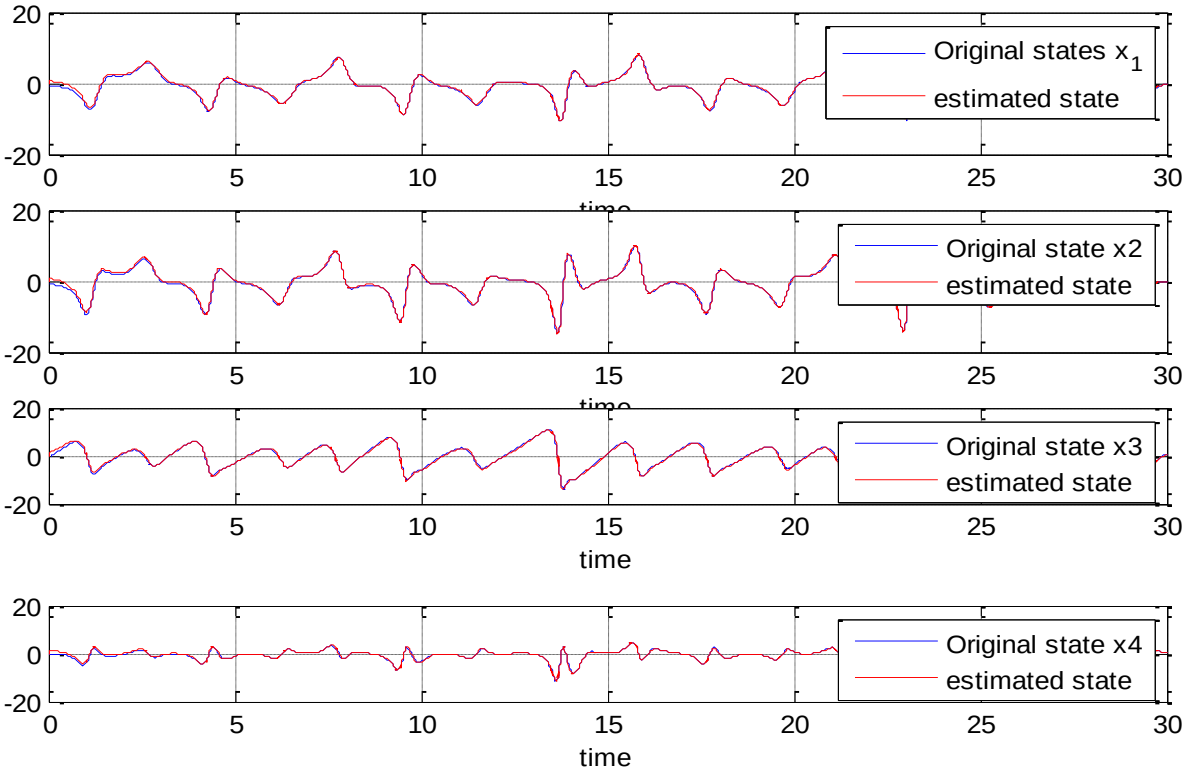


Figure 4.2 : La comparaison entre les états du système transmis et ceux de l'observateur.

Pour mieux illustrer les résultats on fait un zoom de la figure ci-dessus (on minimise l'intervalle de temps).

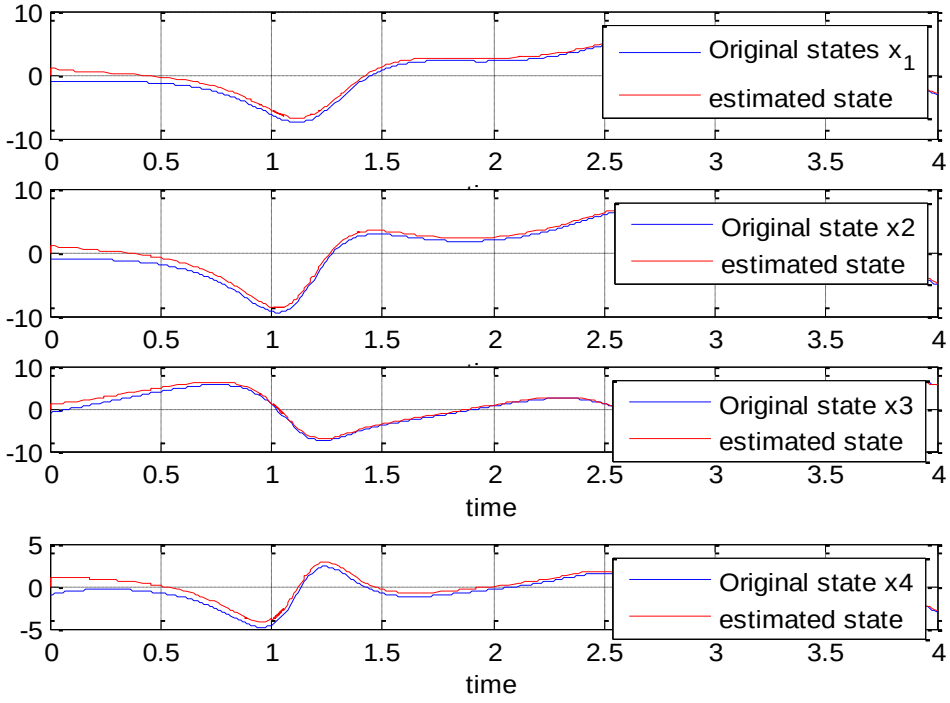


Figure 4.3 : Zoom de la figure 4.2.

On remarque que les graphs sont presque identiques avec un petit décalage au début de l'estimation, ce décalage représente l'erreur de synchronisation. Les états ont été bien estimés au niveau du récepteur.

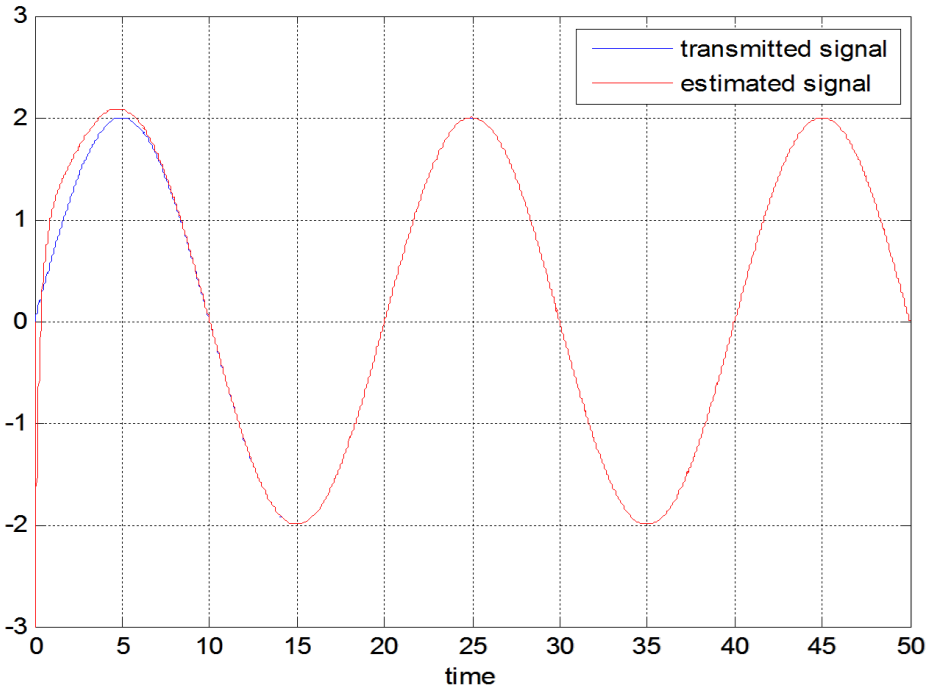


Figure 4.4 : Comparaison entre le signal transmis et le reconstruit.

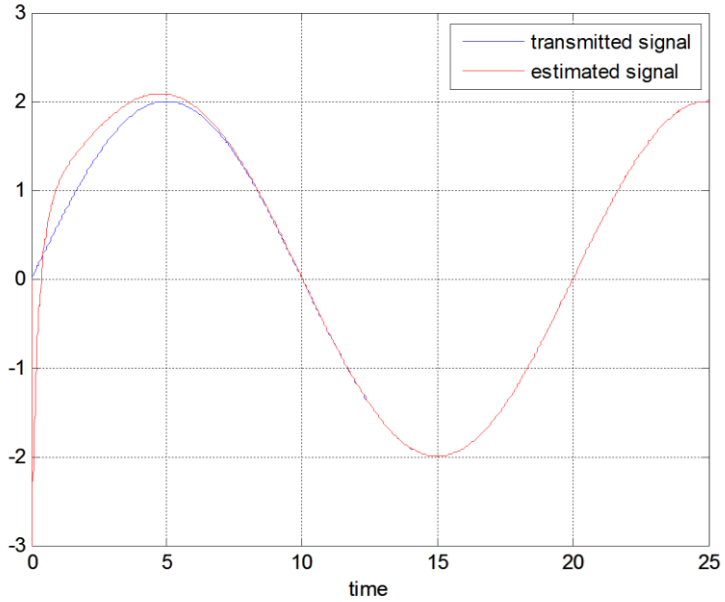


Figure 4.5: zoom de la figure 4.3.

On remarque que les graphs sont presque identiques avec un petit décalage au début de l'estimation, ce décalage représente l'erreur de synchronisation qui converge rapidement vers le zéro. On conclut que notre signal a été bien récupéré au niveau de récepteur.

On constate alors que l'observateur d'état non linéaire généralisé permette la synchronisation des états de l'émetteur et du récepteur, ainsi que la reconstruction du message informatif.

4.5 Conclusion

Dans ce chapitre, nous avons conçu un observateur d'état non linéaire généralisé pour l'estimation du message transmis injecté dans le système chaotique. Les résultats de simulation obtenus montrent l'efficacité des observateurs non linéaires pour la synchronisation des systèmes chaotiques et la reconstruction du message transmit.

Conclusion Générale

Conclusion Générale

Ce travail consiste à réaliser la synchronisation d'un système hyper-chaotique à base d'observateur pour la transmission sécurisée de l'information.

Le premier chapitre a abordé un état de l'art du système chaotique, dans lequel nous avons défini les notions de base des systèmes dynamiques et chaotique, ainsi que leurs conceptions et types. D'après les caractéristiques du chaos, il était possible de l'utiliser comme porteur d'information en télécommunication mais avec le processus de synchronisation.

Dans le deuxième chapitre on a présenté ce processus, leurs types, leurs méthodes et les techniques de transmission par synchronisation.

La synchronisation d'un système chaotique de l'émetteur vers un récepteur est basé sur un observateur pour estimer asymptotiquement ou exponentiellement la valeur courante des états en fonction des entrées et des sorties passées du système en temps réel. Donc le troisième chapitre était une explication de l'application de l'observateur pour la synchronisation du chaos, on a vu la notion d'observabilité et l'utilisation de la programmation convexe par l'approche LMI. Afin de présenter notre système d'équation pour appliquer notre synchronisation utilisant deux blocs émetteur et récepteur.

Dans le dernier chapitre on a exposé les résultats de simulation, La réalisation se fait par code MATLAB. Les résultats de simulation illustrent les performances du système de transmission proposé, les états du système et le signal message envoyés de l'émetteur ont été bien récupérés au niveau du récepteur.
On peut constater l'efficacité des observateurs non linéaires pour la synchronisation des systèmes chaotiques ainsi que pour le cryptage des données.

Comme suite a ce travail, propose l'implémentions de cette approche sur une carte arduino, pour une application réelle.

Bibliographie

Bibliographie

[1] A. Benzerrouki et Z. Guemidi, “Application des systèmes chaotiques à la cryptographie”, Mémoire de master, Université Dr. Tahar Moulay Saida, Algérie, 2018.

[2] S. Chouat, “Synchronisation identique des systèmes chaotiques”, Université Mohamed Khider, Biskra, Juin 2019.

[3] https://theconversation.com/explainer-what-is-chaos-theory-10620.

[4] J.L. Chabert et A. D. Dalmendico. *Chaos et déterminisme : les idées nouvelles de Poincaré*, Paris Edirions du seuil, 1992

[5] https://owl-ge.ch/travaux-d-eleves/2007-2008/article/la-decouverte-du-chaos.

[6] N. Witkowski et P. Bergé, Le chaos. Magazine Scientifique Européen Archimède, Jan 1998.

[7] C. Morel, “Analyse et contrôle de dynamiques chaotiques, application à des circuits électroniques non-linéaires”, Université D’angers, Déc 2005.

[8] L. Moysis, C. Volos, H. Takhi, K. Kemih, S. Goudos, H.E. Nistazakis, "Analysis, Synchronization and Microcontroller Implementation of a Generalized Hyperjerk System, with Application to Secure Communications Usinga Descriptor Observer",2019.

[9] B. Chouaib, “Etude d’un système chaotique pour la sécurisation Des Communications Optiques”, Mémoire de master télécommunications, Université de Abou BekrBelkaid, Juin, 2014.

[10] E. NECHADI, Cours Systèmes Non Linéaires, Universite Ferhat Abbas de Setif 1.

[11] O. Megherbi, “Etude et réalisation d’un système sécurisé à base de systèmes chaotique”, Thèse de magister, Université Mouloud Mammeri Tizi-Ouzou, 2013.

[12] H. Kenouni, “Synchronisation des systémes hyper-chaotiques à retard sous l’effet des perturbation : application au chiffrement d’information”, Mémoire de master, Université de Jijel, 2016.

[13] H. Hamiche, “Inversion à gauche des systèmes dynamiques hybrides chaotiques. Application à la transmission sécurisée de données”, Thèse de doctorat, Université Mouloud Memmri, Tizi-Ouzou, Algerie,2011 .

[14] W. Mahboub, “Synchronisation non identique entre deux systèmes chaotiques au moyen d’un système auxiliaire”, Mémoire de fin d’études, Université Mohamed Khider, Biskra, Algérie, Juin 2019.

[15] S. Kassim, “Contribution à la transmission numérique sécurisée de données à base de générateurs de séquence chaotique d’ordre non entier”, Thèse de doctorat, Université Mouloud Memmri, Tizi-Ouzou, Algérie, 2018.
[16] M. Ait hammi Abdelfateh, “Etude et réalisation d'un système chaotique basé sur le circuit de Chua”, Mémoire de fin d’études, Université Mouloud Memmri, Tizi-Ouzou, Algérie, 2013.
[17] M. Halimi, “Etude et réalisation d’une transmission sécurisée à base de circuit chaotique de Chua”, Mémoire de fin d’études, Université de Jijel, Algérie, Juin 2010.
[18] H. Lilian, Z. Zhang, J. Xiang and S. Wang, “A new 4D chaotic system with two-wing, four-wing, and coexisting attractors and its circuit simulation”, Wiley, vol. 2019, pp. 13, Oct 2019.
[19] BOUTAYEB, Mohamed, DAROUACH, Mohamed, et RAFARALAHY, H. Generalized state-space observers for chaotic synchronization and secure communication. IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, 2002, vol. 49, no 3, p. 345-349.
[20] L. Moysis, C. Volos, V .T Pham, S. Goudos, I. Stouboulos, M.K Gupta,“Synchronization of a Chaotic System with Line Equilibrium using a Descriptor Observer for Secure Communication’’, Conference Paper, May 2019.
[21] A.Berkane,’’Transmission sécurisée à base de la synchronisation impulsive de deux systémes chaotiques discréts’’, Mémoire de Master Professionnel, Université Mouloud Memmri, Tizi-Ouzou, 2016.
[22] R. Berraho, ‘’Observabilité des systèmes non linéaires’’, Mémoire de fin d’études, Université de Aboubakr Belkaid, Tlemcen, 2016.
[23] H. Wang, Z. Han, W. Zhang,’’ Chaotic synchronization and secure communication based On descriptor observer’’, Springer Science+Business Media B.V. 2008, Sep 2008.
[24] N. Rebhi, M.A Ben Farah, A. Kachouri, M. Samet, ‘’Mounir SAMET Analyse De Sécurité d’une Nouvelle Méthode De Cryptage Chaotique’’, 4th International Conference: Sciences of Electronic, Technologies of Information and Telecommunications, Tunisia, March, 2007.
[25] S. Vaidyanathan, S. Sampath, A. T. Azar,’’ Global chaos synchronisation of identical chaotic systems via novel sliding mode control method and its application to Zhu system’’, Int. J. Modelling, Identification and Control, Vol. 23, No. 1, 2015.
[26] M. JUNGERS, Y. CHITOUR,’’ Commande Des Processus Représentation D’état’’, Master IST1 & IFIPS EI2, Université Paris-Sud XI, 2005.

[27] H. Bouraoui, K. Kemih,'' Observer-Based Synchronization of a New Hybrid Chaotic System and Its Application to Secure Communications'', Proceedings of the 2nd International Congress APMAS2012, Vol. 123, No. 2 ,2013.