République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Mouloud MAMMERI, Tizi-Ouzou

Faculté de Génie Electrique et d'Informatique
Département d'Automatique

MEMOIRE DE FIN D'ETUDES

En vue de l'obtention du diplôme

De MASTER ACADEMIQUE EN AUTOMATIQUE
OPTION: COMMANDE DES SYSTEMES

Thème

Synthèse d'observateurs à mode glissant à entrée inconnue: Application à la synchronisation des systèmes chaotiques de Chua

Proposé par:

M. Djennoune said

Co-dirigé par :

Mlle **Djeghali Nadia**

Présenté par:

M. Moulahoum mouloud

Soutenu le : 11/09/14

Promotion 2014

Ce travail a été préparé au laboratoire de conception et conduite des systèmes de production

Remerciement

Je remercie d'abord le Bon Dieu de m'avoir éclairé le droit chemin

Nos remerciements chaleureux à Notre promoteur Monsieur **DJENNOUNE. SAID** Professeur à L'UMMTO pour son soutien, son aide, ses conseils, ses réponses à nos diverses Questions, aussi De nous avoir proposé ce sujet attractif.

Nous remercions également Mlle **DJEGHALI Nadia** pour son aide dans la mise en œuvre de L'observateur à mode glissant étape par étape.

Nous tenons également à remercier le Président et les membres de jury qui nous ont fait L'honneur d'évaluer notre travail.

Notre gratitude et notre reconnaissance s'adressent à tous les enseignants qui ont contribué à Notre formation pendant notre cursus universitaire.

Dédicace

Avant tout je tiens à remercier le bon Dieu, et l'unique qui m'offre le courage et la volonté Nécessaire pour affronté les différentes difficultés dans la vie.

Je dédie ce travail :

A mes très chers parents

A mes frères et sœurs

A mon oncle Hamid et sa femme Dalila

A : La mémoire de mes très chers grands parents

A mes amis de la promotion Master II Automatique, (2013-2014)

A toute personne qui porte de l'estime pour moi

Tous ceux qui ont contribué à la réalisation de ce mémoire, de loin ou de près.

Sommaire

Sommaire

Liste des figures

Liste des figures

Introduction générale

Introduction générale

Dans les problèmes d'identification, d'analyse et de commande des systèmes dynamiques, il est nécessaire de disposer d'informations de mesure (observations) sur le système. Ces informations de mesures sont accessibles sur les signaux de sortie. Cependant, les sorties ne peuvent pas décrire de manière complète le comportement du système. Ce sont les variables d'état qui permettent de connaitre de manière le comportement dynamique du système. Le nombre de sortie reste souvent inférieur au nombre de variable d'état.

Afin de réaliser les techniques de commande par retour d'état ou bien d'implémenter les stratégies de surveillances et de diagnostic de défauts, il est impératif de disposer de la mesure des variables d'état. Recourir à la mesure de toutes les variables d'état est une solution fastidieuse sur les plans économique, de fiabilité et de sécurité, voire même irréalisable lorsque le capteur nécessaire à la mesure d'une variable d'état n'existe pas technologiquement.

Depuis déjà quelques décennies, il est reconnu que les observateurs d'état dont le rôle est de fournir des estimées des variables d'état à partir des informations des sorties et des entrées, offrent une solution très intéressante est qui est utilisée de manière systématique remplaçant aussi les capteurs dans les schémas classiques d'asservissements comme l'asservissement des machines électriques. Un observateur implémenté sur ordinateur devient un capteur logiciel permettant après exécution de quelques instructions de programme informatique de délivrer les estimées de toutes les variables d'état. L'observateur permet donc de reproduire le même comportement et de manière complète que celui du système. C'est donc une solution quasiment gratuite et évitant l'ajout de matériel encombrant sur le système.

De nombreux types d'observateurs sont proposés dans la littérature. Pour les systèmes linéaires, l'observateur de Luenberger est le plus utilisé **[8]**. Afin de minimiser le bruit de mesure sur les estimées, il est nécessaire de recourir au filtre de Kalman **[7]**. Pour les systèmes non linéaires, nous pouvons citer, sans être exhaustif, l'observateur à grand gain, l'observateur de Luenberger étendue, le filtre de Kalman étendu. Ces observateurs garantissent, en général, sous certaines hypothèses, une convergence asymptotique des variables estimées vers les variables réelles.

Les observateurs à modes glissants qui sont de par leur nature à comportement non linéaire peuvent offrir une convergence en temps finis. On peut les utiliser aussi bien pour les systèmes linéaires que pour les systèmes non linéaires. En plus de la convergence en temps finie qui est souhaitée dans la plupart des cas, ces observateurs possèdent aussi l'avantage de robustesse vis-à-vis des incertitudes de modélisation et vis-à-vis de certains signaux perturbateurs.

La transmission sécurisée de données à bas de système non linéaire chaotique a connue ces dernières années un grand succès. Un système non linéaire chaotique bien qu'il soit déterministe possède la propriété de générer des réponses stables avec un comportement aléatoire et désordonné **[4]**. De nombreux circuits électroniques (oscillateurs chaotiques) possèdent cette propriété comme le circuit de Colpitts, le circuit de Chua, le circuit de Qi, … . L'idée consiste à utiliser au niveau de l'émetteur un oscillateur électronique chaotique pour brouiller dans la dynamique chaotique le message à transmettre de manière sécurisée à travers le canal public. Au niveau de la réception on doit procéder à l'opération inverse. Pour cela, on doit disposer d'un récepteur qui reproduit le même comportement que celui d'un émetteur.

Dans un autre sens on doit assurer que le récepteur et l'émetteur soient synchronisés. L'une des solutions pour réaliser cette synchronisation est d'utiliser un observateur.

L'objectif de notre travail et de mettre en œuvre un observateur à modes glissants à entrée inconnue pour synchroniser deux systèmes non linéaires chaotiques de **Chua**. Cette étude est illustrée par un schéma de transmission sécurisée de données à base de systèmes chaotiques.

Nous organisons notre travail comme suit :

- Le premier chapitre aborde quelques notions fondamentales sur les systèmes chaotiques et sur les observateurs non linéaires.

- Dans le second chapitre, nous présentons dans la première partie les principes de synchronisation, puis dans la seconde partie, nous étudions la synchronisation des oscillateurs de **Chua** à base d'observateur à modes glissants étape par étape à entrée inconnue.

- Nous consacrons le troisième chapitre aux résultats de simulation illustrant l'étude théorique.

- Nous terminerons notre travail par une conclusion générale et quelques perspectives.

Chapitre 1

Systèmes chaotiques et observateurs non linéaires

1.1 Introduction

L'emploi du chaos dans divers domaines à été considérée dans ces dernières décennies comme une solution prometteuse pour augmenter les performances des systèmes de transmission actuels. Le chaos offre une solution possible pour les systèmes à probabilités réduites de détection et d'interception. En contradiction avec ces aspects positifs qui font du chaos une solution très attirante, il faut préciser qu'a priori la synchronisation entre deux systèmes dynamiques chaotiques, nécessite à la récupération de l'information transmise, nécessite une solution de synchronisation à estimation d'états, susceptibles d'offrir les meilleures performances possibles.

Les systèmes dynamiques chaotiques sont depuis longtemps connus dans le domaine des mathématiques, mais seulement au cours des dernières décennies que les applications concrètes se sont multipliées particulièrement dans le domaine de la transmission sécurisée de données à travers les canaux publics (faisceaux hertziens, internet et autres réseaux de communication).

Le chaos n'est pas aussi 'chaotique' que sa domination le laisse entendre ; son désordre n'est qu'apparent. Un système chaotique est imprévisible mais il est parfaitement décrit par des équations simples et déterministes. Un système est dit déterministe lorsqu'il est possible de prédire (de calculer) son évolution aux cours du temps : la connaissance exacte de l'état du système à un instant donné. L'instant initial, permet le calcul précis de l'état du système à n'importe quel autre moment. Le lien entre ces deux notions paradoxales déterminisme et imprévisibilité, se manifeste par la sensibilité aux conditions initiales : deux conditions initiales quasiment semblables peuvent conduire à des états très différents du système. Cette impossibilité pratique à calculer l'évolution de systèmes déterministe, due à la non connaissance de la solution exacte analytique (seule une solution numérique approximée est obtenue) est la principale caractéristique des systèmes chaotiques.

1.2 Quelques définitions sur le chaos [1], [2], [3]

Selon la littérature que nous avons consultée, la notion du chaos répond aux définitions ci-dessous :

Définition 1

Le chaos est un phénomène qu'on peut liée au désordre ainsi d'impossibilité et imprévisibilité, cela signifie un système qui dépende de plusieurs paramètres comme la non linéarité et le déterminisme. Un système dynamique est dit chaotique si son comportement est irrégulier, désordonné tout en étant déterministe. En particulier, on dira d'un régime dynamique qu'il est chaotique s'il présente un phénomène fondamental d'instabilité transitoire appelé « sensibilité aux condition initiales ».

Définition 2

Un système dynamique est dit chaotique si son comportement est irrégulier, désordonné tout en étant déterministe. En particulier, on dira d'un régime dynamique qu'il est chaotique s'il présente un phénomène fondamental d'instabilité transitoire (le comportement chaotique est un comportement globalement stable et les solutions sont nécessairement bornées) appelé «sensibilité aux conditions initiales», autrement dit, si son spectre de puissance comporte une partie continue, une bande large, indépendamment de la présence éventuelle de quelques raies.

Définition 3

En pratique, on peut dire qu'un système chaotique a un comportement borné en régime permanent, qui ne correspond pas à un point d'équilibre, qu'il n'est ni périodique, ni quasi-périodique.

1.3 Caractéristiques essentielles du chaos

1.3.1 Déterminisme

Il existe une démarche pour comprendre ou prévoir un phénomène réel. Cette démarche consiste à construire un modèle mathématique qui établit une relation entre un ensemble de causes et un ensemble d'effets. Autrement dit, à partir de conditions initiales connues, le modèle permet de prévoir l'évolution d'un système au cours du temps.

On peut classer l'ensemble des modèles en deux catégories selon qu'ils sont probabilistes ou déterministes. Dans un modèle probabiliste, un ensemble de conditions initiales connues entraine des probabilités d'évolution du système. Celui-ci possède globalement plusieurs états finaux qui peuvent exister, chacun avec une certaine probabilité. Au contraire, dans le cas d'un modèle déterministe, des conditions initiales connues conduisent à une évolution parfaitement déterminée et les mêmes causes produisent toujours les mêmes effets. La notion de déterminisme est ainsi intrinsèquement liée à tous les systèmes dont l'évolution est définie par un ensemble d'équations différentielles.

Durant ces 30 dernières années, des chercheurs ont réussi à mettre certains phénomènes en équation et remarqué qu'il existe un côté déterministe dans ce qui paraît être à la première vue aléatoire. Il convient alors de distinguer les phénomènes aléatoires du chaos déterministe qui nous intéresse ici.

Une propriété importante liée aux systèmes déterministes est la prévisibilité. En effet, en connaissant le modèle et les conditions initiales à l'instant (t_0), l'état du système est prévisible à toute instant ($t > t_0$). Cependant, depuis la découverte des phénomènes chaotiques la prévisibilité n'est plus systématiquement liée au déterminisme.

1.3.2 Sensibilité aux conditions initiales

L'évolution d'un système dynamique chaotique est imprédictible en ce sens qu'elle est sensible aux conditions initiales, plus connue dans le langage courant sous l'appellation « effet papillon », popularisé par le météorologue **Edward Lorenz** dans la citation suivante prononcée lors d'un congrès international au Brésil, 1966, **[4].**

« *Le battement d'aile d'un papillon, aujourd'hui à Pékin, engendre dans l'air des remous qui peuvent se transformer en tempête le mois prochain à New York* ».
Edward Lorenz.

Ainsi, deux trajectoires de phases initialement voisines s'écartent toujours l'une de l'autre, et ceci quelle que soit leur proximité initiale. Il est en particulier clair que la moindre erreur ou simple imprécision sur la condition initiale interdit de décider à tout temps quelle sera la trajectoire effectivement suivie et, en conséquence, de faire une prédiction autre que statistique sur le devenir à long terme du système. Ainsi, bien que l'on traite de systèmes déterministes, il est impossible de prévoir à long terme leurs comportements.

1.3.3 Attracteur étrange

Un attracteur dans l'espace de phases est un objet géométrique vers lequel tendent un ensemble de trajectoires des points de cet espace, c'est-à-dire une situation ou un ensemble de situations vers lesquelles évolue un système dynamique, pour un ensemble des conditions initiales **[5].** On peut avoir plusieurs attracteurs dans un même espace de phase. Il existe deux types d'attracteurs : les attracteurs réguliers (le point fixe, le cycle limite, le tore) et les attracteurs étranges (chaotiques).

Le terme attracteur étrange a été utilisé pour la première fois par **David Ruelle** et **Floris Takens** en 1971 **[6],** afin de décrire l'attracteur obtenu par une série de bifurcations d'un système modélisant le courant d'un liquide. En effet, avant l'article de **Ruelle** et **Takens**, les attracteurs avaient déjà fait l'objet de publications mais ils sont restés ignorés. Cette appellation d'attracteur étrange fait appel à leur propriété peu commune, qui est leur dimension fractale.

En effet la structure géométrique des trajectoires générées par un système chaotique est extrêmement complexe à cause des étirements, repliements et contractions s'opérant dans une région bornée de l'espace d'état. Les caractéristiques de l'attracteur étrange sont alors :

- il est contenu dans un espace fini. Son volume est nul. Sa dimension est fractale et non entière.
- sa trajectoire est complexe.
- presque toutes les trajectoires sur l'attracteur ont la propriété de ne jamais passer deux fois par le même point. En d'autres termes, chaque trajectoire est apériodique.

- deux trajectoires proches à un instant « t » voient localement leur distance augmenter à une vitesse exponentielle. Ce phénomène traduit la sensibilité aux conditions initiales.
- toute condition initiale appartenant au bassin d'attraction, c'est-à-dire à la région de l'espace des phases dans laquelle tout phénomène dynamique sera « attiré » vers l'attracteur, produit une trajectoire qui tend à parcourir de façon spécifique et unique cet attracteur.

Un système chaotique est donc contraint d'évoluer de manière « imprévisible » dans une région bien définie de l'espace des phases. L'attracteur étrange le plus célèbre, qui a contribué au succès médiatique de la théorie du chaos, prend la forme *d'ailes de papillon* déployées. Ce fameux papillon est devenu en quelque sorte le symbole de la théorie du chaos un peu comme la pomme de Newton est devenue le symbole de la gravité.

Dans ce qui suit, nous allons présenter deux exemples d'attracteurs. Le premier est l'attracteur de Lorenz et le deuxième est celui de Rossler.

Modèle de Lorenz :

$$\begin{cases} \dot{x} = -\sigma x + \sigma y \\ \dot{y} = -xz + rx - y \\ \dot{z} = xy - bz \end{cases} \qquad \textbf{(1.1)}$$

Avec $\sigma = 8$; r = 26 ; b = 8/3.

Les Conditions Initiales sont : (0.01 ; 0.01 ; 0.01).

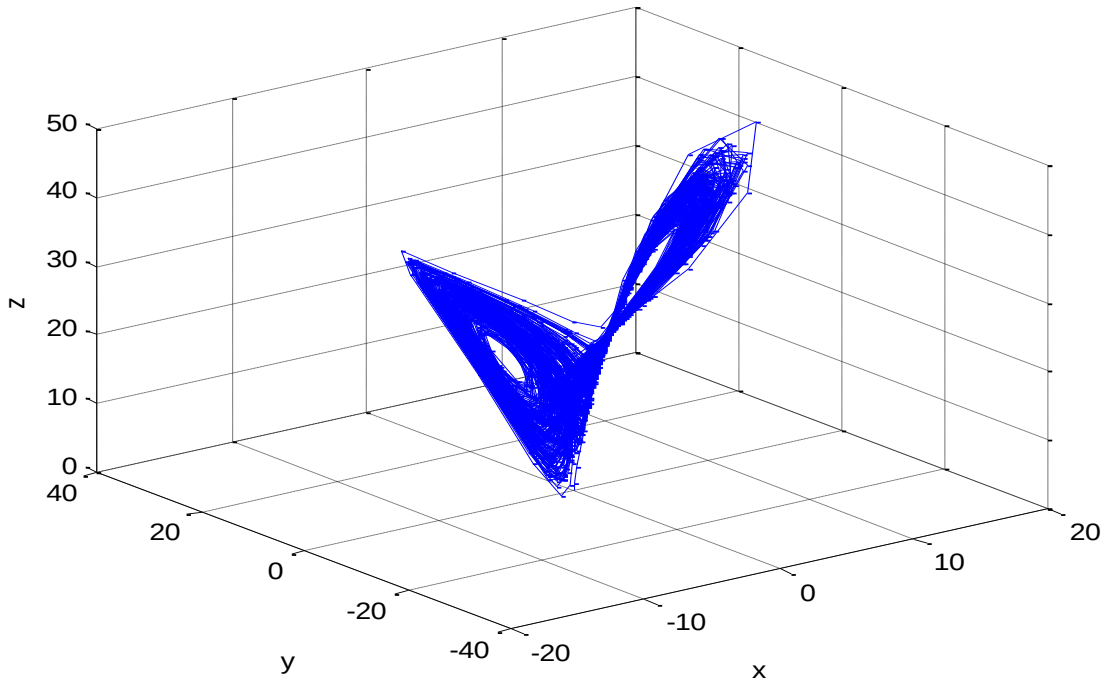


Fig. 1.1 Attracteur de Lorenz

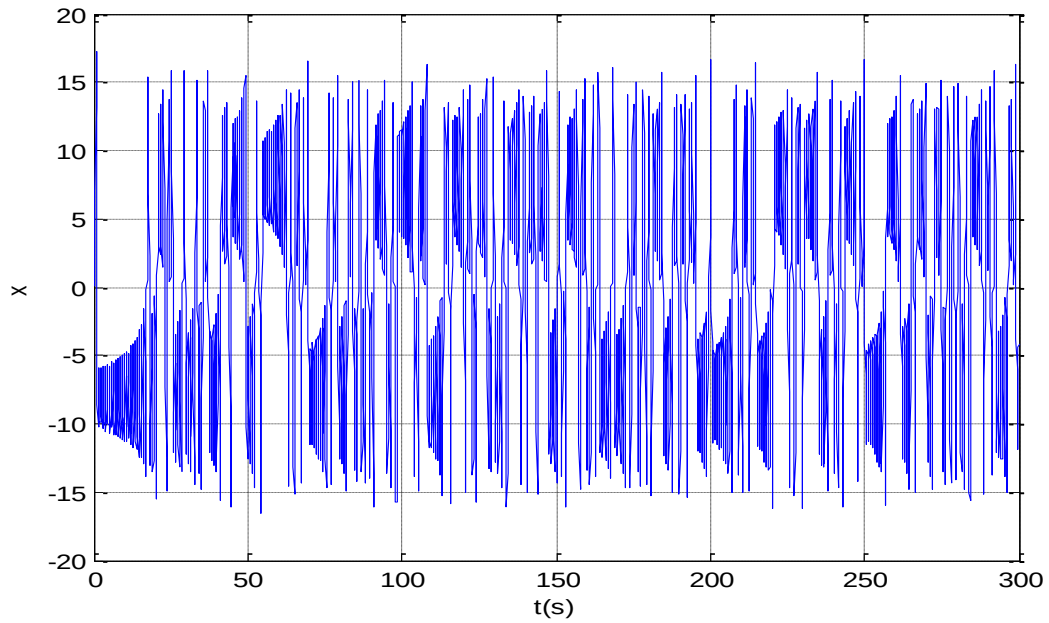


Fig. 1.2 Réponse temporelle de l'état (x)

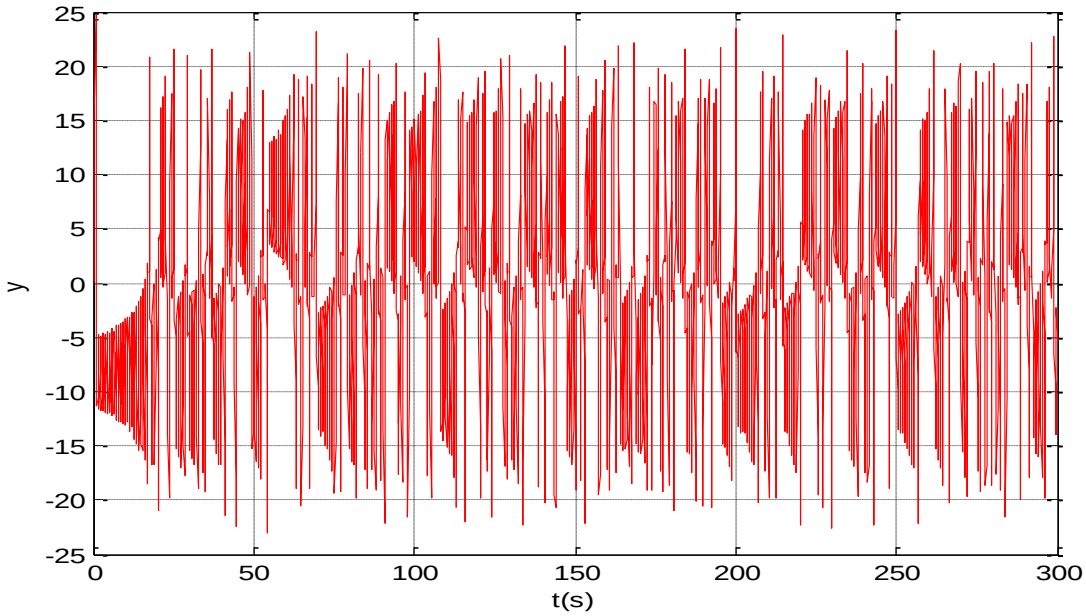


Fig. 1.3 Réponse temporelle de l'état (y)

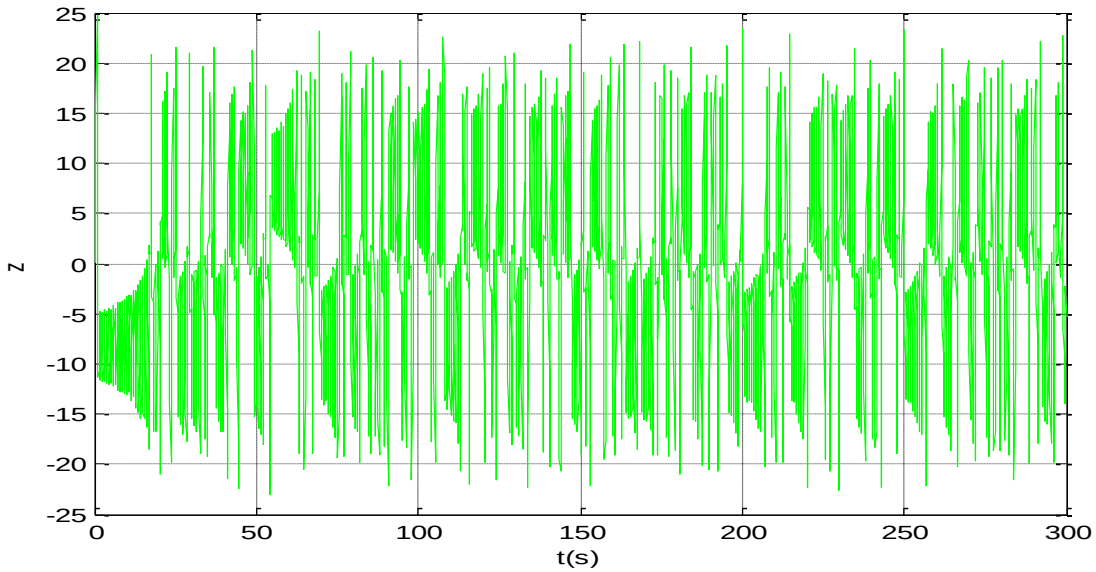


Fig. 1.4 Réponse temporelle de l'état (z)

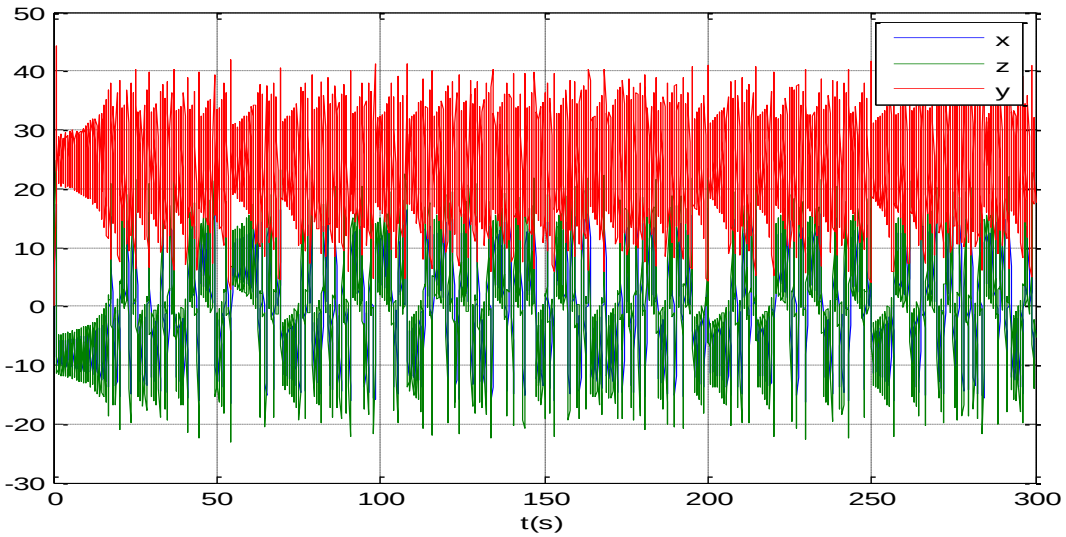


Fig. 1.5 Réponse temporelle de différents états (x y z)

Modèle de Rössler :

$$\Rightarrow \begin{cases} \dot{x} = -y - z \\ \dot{y} = x + ay \\ \dot{z} = b + z(x - c) \end{cases} \quad \textbf{(1.2)}$$

Avec a = 0.1 ; b = 0.1 ; c = 14.

Les Conditions Initiales sont : (0.01 ; 0.01 ; 0.01).

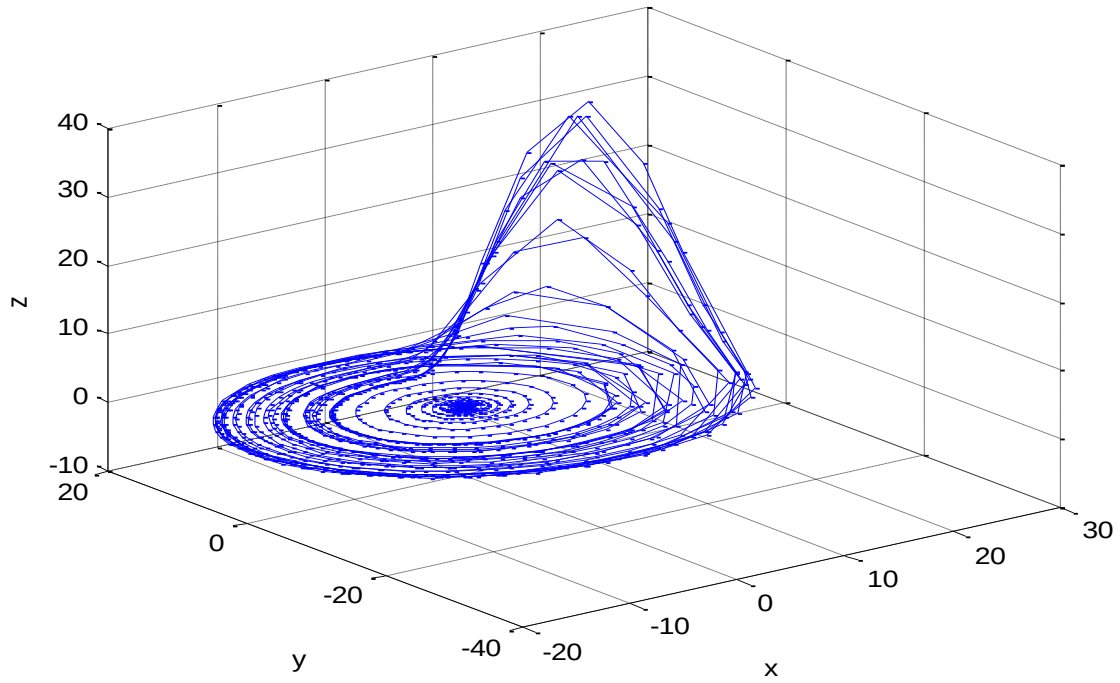


Fig. 1.6 Portrait de phase de Rössler

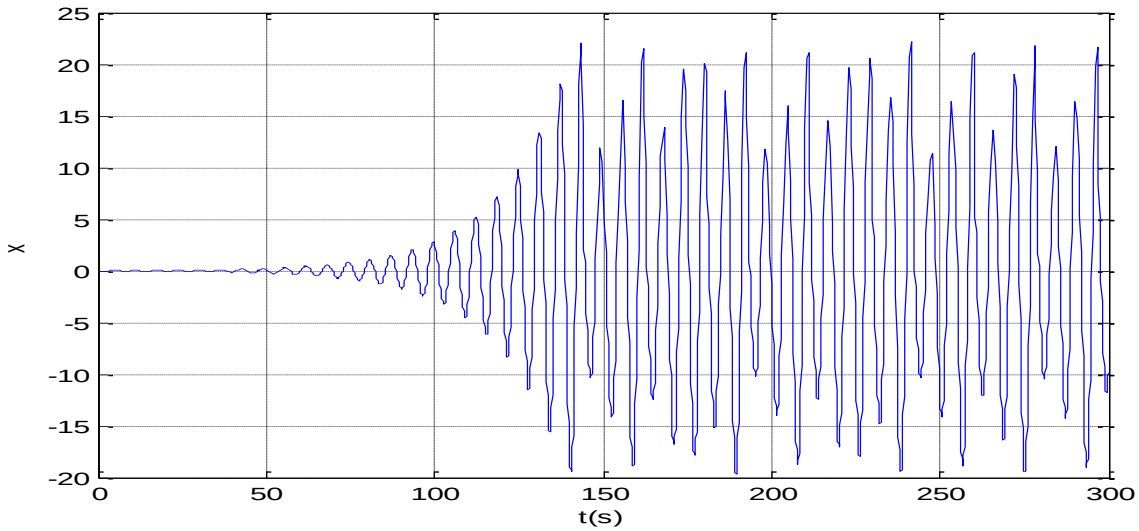


Fig. 1.7 Réponse temporelle de l'état (x)

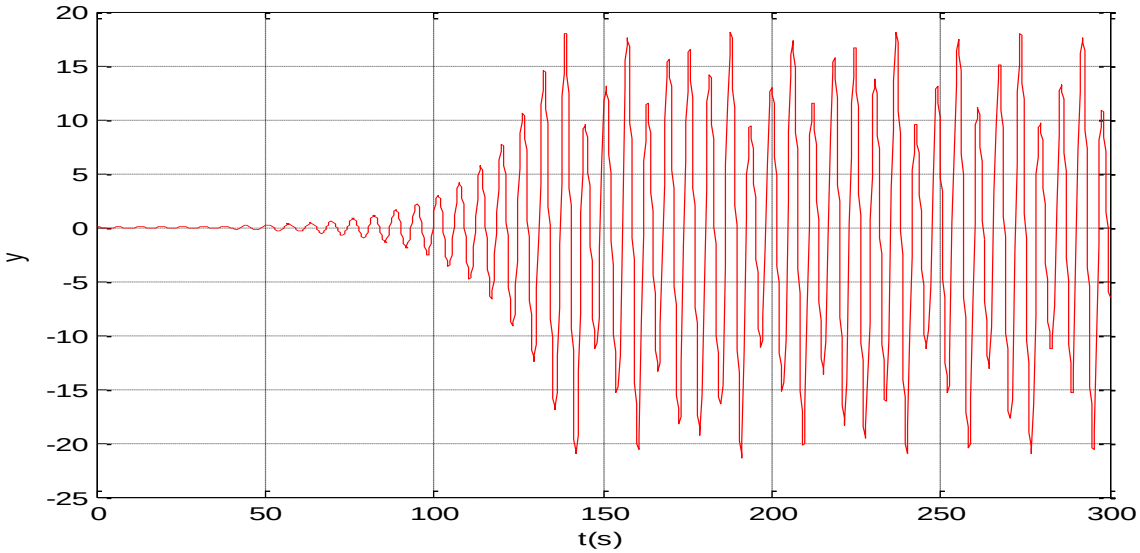


Fig. 1.8 Réponse temporelle de l'état (y)

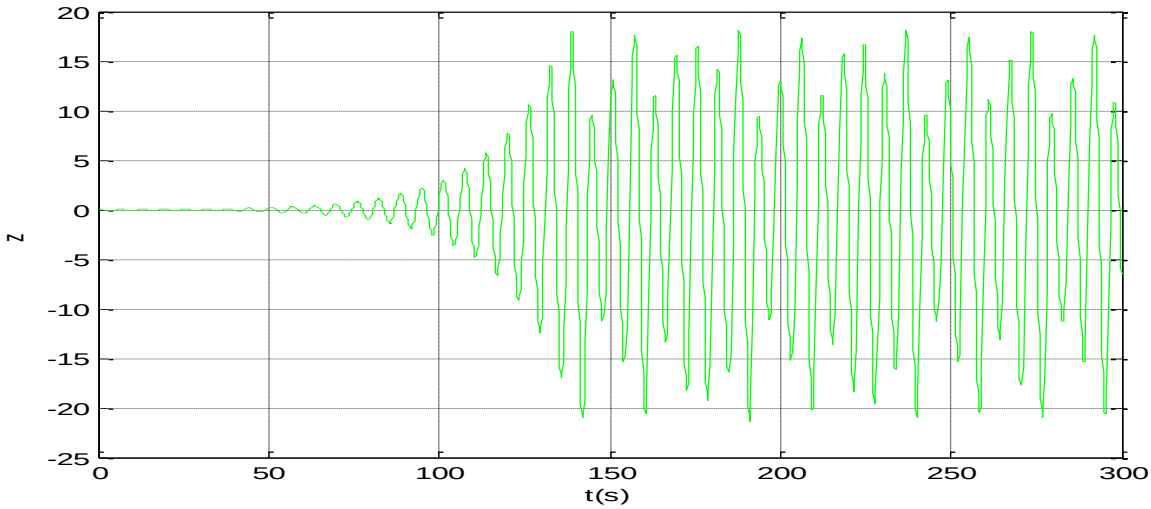


Fig. 1.9 Réponse temporelle de l'état (z)

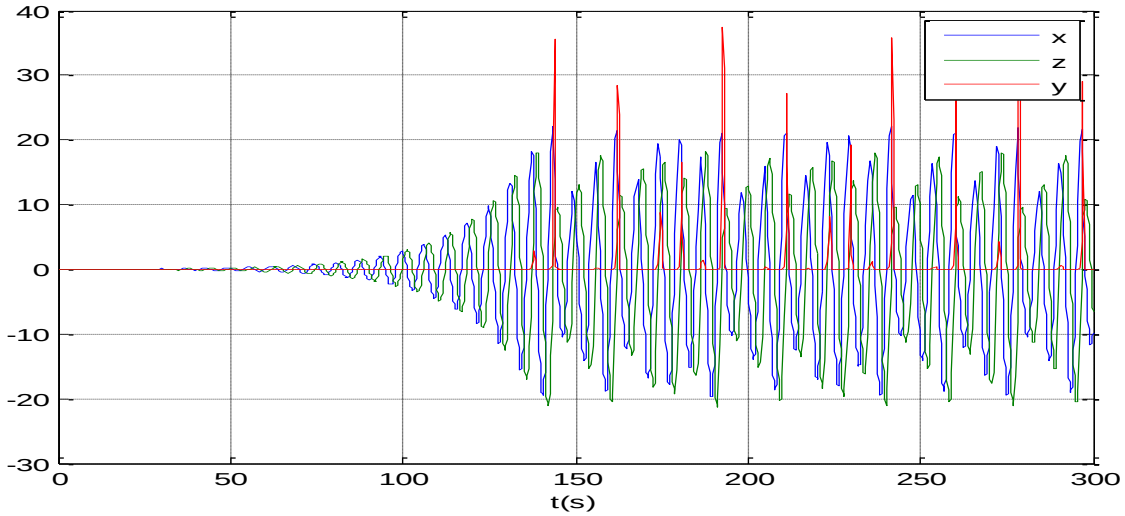


Fig. 1.10 Réponse temporelle des différents états (x y z)

1.4 La notion de bifurcation

Il existe plusieurs comportements d'un système dynamique non-linéaire, en citant (point fixe, oscillation périodiques et quasi-périodiques, chaos). Ces systèmes passent d'un comportement à un autre en fonction du changement de certains paramètres important du système.les transitions entre régime dynamique est appelé paramètre de bifurcation. L'ensemble de l'évolution dynamique d'un système peut se présenter sous la forme d'un diagramme de bifurcation.

On distingue trois scénarios théoriques vers le chaos, et la présence de ce dernier (le chaos) est due à une modification d'un paramètre théorique ou expérimentale.

1.4.1 ***Le doublement de période*** **:** ce scénario a été découvert en même temps par **Mitchell Feigenbaum** et par les chercheurs français **Pierre Coullet** et **Charles Tresser**. L'augmentation d'un paramètre provoque, pour un système périodique, l'apparition d'un doublement de sa période. La période est ensuite multipliée par 4, 8, 16. . . D'un doublement au suivant, l'augmentation du paramètre est de plus en plus faible, et, à partir d'une certaine valeur, le chaos apparaît : lorsque la période devienne infinie, les mouvements deviennent chaotiques. L'augmentation du paramètre conduit ensuite à la réapparition de régimes périodiques intercalés dans des zones chaotiques. Ce scénario peut être observé dans un grand nombre d'expériences comme un robinet qui fuit, l'étude d'oscillateurs forcés, ou encore l'apparition de la turbulence dans les fluides.

1.4.2 ***L'intermittence*** **:** ce scénario a été décrit par **Yves Pomeau**. L'intermittence se caractérise plutôt par un mouvement périodique stable entrecoupé par des bouffées chaotiques. Ces perturbations apparaissent de manière irrégulière. L'augmentation d'un

paramètre produit l'augmentation de la fréquence des perturbations, puis le chaos domine le comportement du système. Ce scénario a été observé dans des expériences sur la convection des fluides et dans des réactions chimiques.

1.4.3 **Le quasi périodicité :** le troisième scénario fait intervenir, pour un système périodique, l'apparition d'une deuxième période dont le rapport avec la première n'est pas rationnel. Ce régime est appelée « quasi périodique ». Il peut, de lui-même ou avec l'apparition d'une troisième fréquence gigantesque, donner un régime chaotique. Ce scénario intervient quand on considère deux oscillateurs fortement couplés. Les variations du champ magnétique terrestre, le déroulement des séismes pourrait être expliqué par un modèle de ce genre. On le retrouve aussi dans le cas d'un pendule qui serait stimulé verticalement.Une bifurcation correspond à une sorte de changement d'état du système plus exactement à un changement de stabilité du régime dynamique lorsqu'un des paramètres du système varie. Nous pouvons constater trois états différents du système un régime stable, puis périodique à n états et enfin un régime chaotique. Cette sorte de représentation permet d'avoir une vue globale d'un ensemble de comportements dynamiques différents. Il s'agit alors plus de méthode de représentation que d'outil d'analyse. Pour mieux comprendre l'aspect de bifurcation nous présentons ces deux exemples :

Exemple 1

Soit le système :

$$\dot{x} = \dot{\mu} - 2x \qquad \textbf{(1.3)}$$

Avec $x \in \mathbb{R}$ l'état et $\mu \in \mathbb{R}$ le paramètre. Les points d'équilibre sont les solutions de $\dot{x} = 0$: $x_e = \pm\sqrt{\mu}$.

Ces solutions n'existent que pour $\mu \geq 0$. Un changement qualitatif dans la dynamique apparaît lorsque $\mu = 0$. Pour $\mu \geq 0$. Le point d'équilibre $x_e = -\sqrt{\mu}$ est instable, alors que

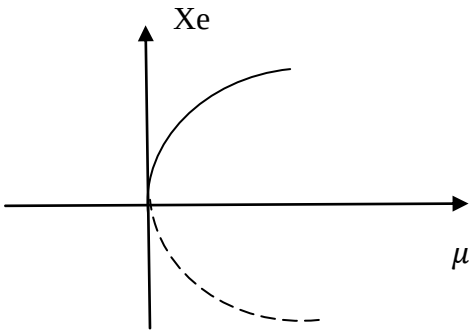


Fig. 1.11 Diagramme de bifurcation

Le point d'équilibre $x_e = \sqrt{\mu}$ est stable. Les deux états (stable et instable) se coïncident alors en $(\mu = 0)$. Cette bifurcation est montrée dans la figure (1.11).

Exemple 2

Dans la figure (1.12), nous présentons le diagramme de bifurcation de l'équation logistique [20]. Nous pouvons constater qu'il y a deux états différents dans ce système: un régime stable et un régime chaotique.

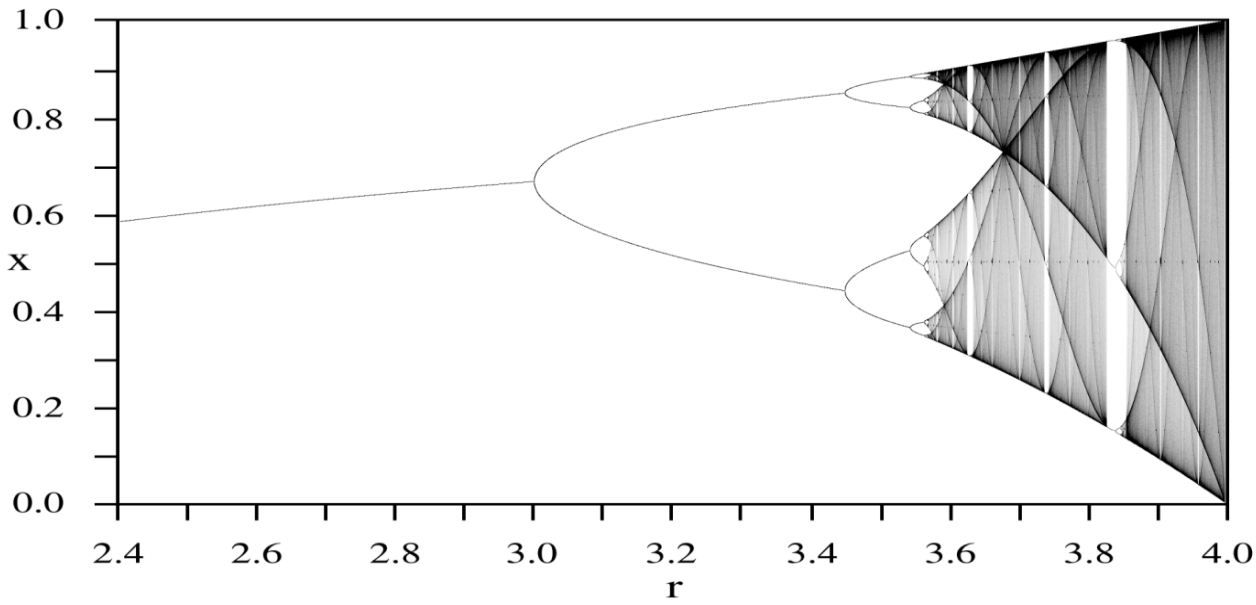


Fig. 1.12 Diagramme de bifurcation en fonction du paramètre (r)

1.5 Observateurs non linéaires

1.5.1 Introduction

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'ou 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 à montré que cette méthode à l'inconvénient de donner des résultats erronés à cause de l'amplification du bruit due aux imperfections de mesures.

Pour remédier à ce problème, **Kalman-Bucy [7]** a introduit en 1961 une solution pour les systèmes linéaire stochastiques. Leur résultat est connu actuellement par le filtre de Kalman. Ce filtre donne aussi de bons résultats pour les systèmes déterministes. En 1964-1971, **Luenberger** a fondé la théorie d'un observateur qui porte son nom « Observateur de Luenberger » **[8].** Son idée est d'ajouter au modèle mis sous la forme canonique compagnon **(Brunowsky)** une correction à l'aide de la mesure fournie par les capteurs.

Pour les systèmes non linéaires, les ingénieurs utilisent le filtre de Kalman étendu qui malheureusement ne présente pas de bonnes propriétés de convergence. Pour cette raison la conception d'observateurs pour les systèmes non linéaire est un problème pour les travaux de recherche, restent très intensifs.

En 1983, **Krener-Isidori [9]** ont fourni des conditions nécessaires et suffisantes pour une linéarisation de l'erreur de l'observation des modèles non linéaires afin de leur appliquer l'observateur de Lunberger. Cependant, leurs résultats ne s'appliquent qu'à une classe réduite de systèmes non linéaires.

A la même époque **Fliess et Kupka [10]** fournisse des conditions suffisantes et nécessaires pour une linéarisation exacte des systèmes non linéaires en mettant en évidence le concept de l'immersion.

Un autre résultat dû à **Krener** et **Rsepondek [11]** viennent pour élargir la classe des systèmes dynamiques étudiés par **Krener** – **Isodiri** en se mettant un diffeomorphisme sur la sortie.

1.5.2 Observateur de Luenberger étendu [12]

L'observateur de Luenberger étendu intervient, soit au niveau du système original avec un gain constant, soit par le biais d'un changement de coordonnée 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 placement de pôles. Ce type d'observateur ne peut être utilisé que l'orsque on est sur que l'état restera au voisinage de l'état d'équilibre. Pour cette raison l'utilisation de cet observateur peut être compromise par des instabilités qui peuvent se révéler si l'on s'éloigne du point de fonctionnement. Dans le deuxième cas, les méthodes de changement de coordonnées ne concernent qu'une classe restreinte de système non linéaire. Ce qui est souvent très délicat à réaliser. De ce fait, l'utilisation de solution approchée est envisageable.

1.5.3 Filtre de Kalman étendu [13]

Le filtre de Kalman étendue est l'une des techniques d'estimation les plus populaires, et largement étudiée dans le domaine d'estimation d'état des systèmes dynamiques non linéaires. Ce filtre étendu consiste à utiliser les équations de filtre de Kalman standard au modèle non linéaire linéarité par la formule de Taylor au premier ordre.

Ce filtre étendu à été appliqué avec succès sur différents type de procédé non linéaire. Malheureusement, les preuves de stabilité et de convergence établie dans le cas de systèmes linéaires, ne peuvent être étendues de manière générale au cas de systèmes non linéaires.

1.5.4 Observateur à grand gain [14]

La conception de cet observateur est conditionnée par deux hypothèses comme suit :

- *La non linéarité doit être lipchitzienne.*
- *Les fonctions* g_i *avec* $i = 1,...,n$ *doit être continument différentiable par rapport à* x.
- *Les fonctions* g_i *avec* $i = 1,...,n$ *et leurs dérivée sont bornées pour tout* $x \in R^n$ *et* $u \in R^m$.

L'observateur est sur la forme suivante :

$$\dot{\hat{x}}(t) = A\hat{x} + g(\hat{x},u) - S_\theta^{-1} C^T (C\hat{x} - y) \qquad \textbf{(1.4)}$$

Où x *et* $\hat{x}$ *représentent le vecteur d'état du système est son estimé, respectivement.*
y *est le vecteur de sortie. Et les matrices* A *et* C *sont les matrices d'évolution et la matrice d'observation du système mises sous la forme suivante :*

$$A = \begin{bmatrix} 0 & 1 & \cdots & 0 \\ 0 & 0 & \ddots & 0 \\ \vdots & 0 & \cdots & 1 \\ 0 & 0 & \cdots & 0 \end{bmatrix}$$

$$C = \begin{bmatrix} 1 & 0 & \cdots & 0 \end{bmatrix}$$

1.5.5 Observateurs basés sur l'observabilité différentielle [15]

Le difféomorphisme précité $z = \varphi(x)$ définit un changement de coordonnées global, sous les trois hypothèses suivantes :

H1 : $z = \phi(x)$ est lipchitzienne et inversible, c'est-à-dire :

$$\left\|\phi(x_1) - \phi(x_2)\right\| \le \gamma_\phi \left\|x_1 - x_2\right\|$$

H2 : l'inverse $x = \phi^{-1}(z)$ et lipchitzienne et inversible, à savoir :

$$\left\|\phi^{-1}(z_1) - \phi^{-1}(z_2)\right\| \le \gamma_{\phi^{-1}} \left\|z_1 - z_2\right\|$$

$\gamma_\phi et \gamma_{\phi^{-1}}$: sont les constantes de Lipchitz.

H3 : la fonction $\tilde{H}$ est Lipchitzienne, sa constante de Lipchitz est $\gamma_{\tilde{H}}$, c'est-à-dire :

$$\left\|\tilde{H}(z_1, u) - \tilde{H}(z_2, u)\right\| \le \gamma_{\tilde{H}}(|u|)\left\|z_1 - z_2\right\|$$

Ainsi, leurs matrices jacobéennes sont données par :

$$Q(x) = \frac{\partial \phi(x)}{\partial x}$$

$$Q^{-1}(x) = \left.\frac{\partial \phi^{-1}(z)}{\partial z}\right|_{z=\phi(x)}$$

L'observateur proposé est donné sous la forme :

$$\dot{\hat{x}}(t) = f(\hat{x}(t)) + g(\hat{x}(t))u(t) + Q^{-1}(\hat{x}(t))K(y(t) - h(\hat{x}(t))), \qquad \textbf{(1.5)}$$

Tous les observateurs précités reposent dans leurs principes sur une dynamique d'erreur d'estimation linéaire, ce que n'est pas toujours possible. Outre, ils présentent tous une sensibilité non négligeable vis-à-vis des bruits de mesure et des variations paramétriques.

1.5.6 Observateur à mode glissants [16]

Un observateur à mode glissants est un observateur dont le terme correcteur est une fonction il s'agit de contraindre, à l'aide des fonctions discontinues, les dynamiques du système à converger sur une « surface de glissement ».

$$\begin{cases} \dot{x} = f(x) + g(x)u \\ y = h(x) \end{cases} \qquad \textbf{(1.6)}$$

L'observateur à mode glissant pour ce système s'écrit comme suit :

$$\begin{cases} \dot{\hat{x}} = f(\hat{x}) + g(\hat{x})u + \lambda sign(y - \hat{y}) \\ \hat{y} = h(\hat{x}) \end{cases} \quad \textbf{(1.7)}$$

Ou (λ) est une matrice de gain de dimension (np) . Dans ce cas on impose l'évolution des dynamiques du système sur la variété sur laquelle l'erreur d'estimation de la sortie $(e_y = y - \hat{y})$ est nulle. Ainsi cette erreur converge vers zéro au bout d'un temps fini, et la dynamique du système de (n) à $(n-p)$.

L'étude de stabilité et de la convergence pour de tels observateurs, est basée sur l'utilisation des fonctions de Lyapunov.

Définition 1

Une surface $s = 0$ est attractive pour un domaine de convergence donné si toute trajectoire évoluant dans le domaine d'attraction est dirigée vers cette surface.

Définition 2

Une surface ($s = 0$) est invariante si toute trajectoire débutant dans cette surface ou atteignant cette surface, ne peut en sortir et évolue donc sur cette surface. La surface ($s = 0$) divise l'espace d'état en deux régions. La première région (ε^+) correspond à ($s > 0$) et la seconde notée (ε^-) correspond à ($s < 0$). Si l'état du système est de côté (ε^+) de l'espace d'état (ou du côté ε^-), il rejoindra forcément la surface $(s = 0)$. S'il dépasse de l'autre côté (ε^-) ou du côté (ε^+), il se ramènera vers $(s = 0)$ (figure 3.7). Cette surface ($s = 0$) est donc appelée surface glissante et le mouvement sur cette surface est un mode glissant dont l'équation détermine la dynamique désirée du système.

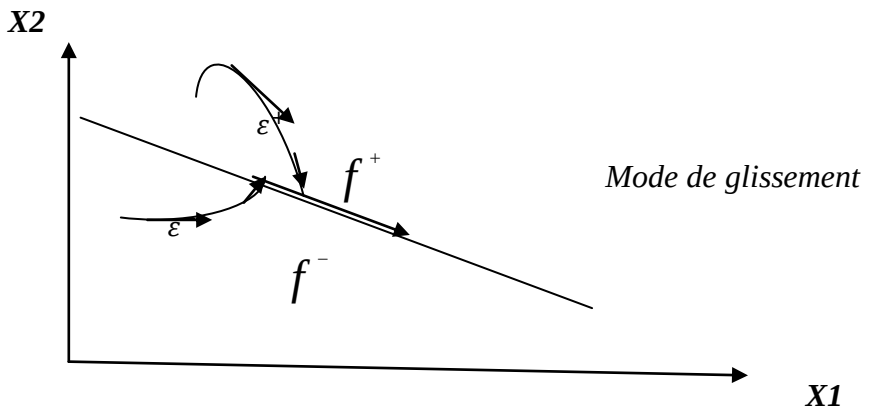


Fig. 1.13 Mode de glissement idéal pour système planaire

Une surface de discontinuité $(s = 0)$ *, suivant que l'état du système est sur* (ε^+) *ou sur* (ε^-) *il atteint la surface respectivement avec les vitesses (* f^+*) ou (* f^- *).*
Avec :(ε^+*) et (*ε^-*) sont respectivement (* $s > 0$*) et* $(s < 0)$*, (* f^+ *) et* (f^-) *sont les vecteurs de vitesse* où *:*

$$f = \begin{cases} f^+ \ si \ s > 0 \\ f^- \ si \ s < 0 \end{cases} \quad \textbf{(1.8)}$$

L'étude de l'existence du mode de glissement, comme l'étude de la stabilité d'un point d'équilibre, est basée sur la deuxième méthode de Lyapunov. La condition d'existence du mode de glissement est l'attractivité de la surface de commutation $(s = 0)$. Géométriquement, les vecteurs vitesses (f^+) et (f^-) vont être dirigés vers la surface de commutation. Cependant, dans certains cas, le glissement n'a pas lieu sur n'importe quel point de la surface de commutation car l'attractivité de cette dernière n'est assurée que dans un domaine restreint D_g, que l'on appelle domaine de glissement. Alors pour que la surface $(s = 0)$ soit attractive sur tout le domaine de fonctionnement, il faut que cette condition soit satisfaite :

$$\boldsymbol{s\dot{s} < 0 \quad \forall \ s \neq 0} \quad \textbf{(1.9)}$$

Cette condition est appelée « condition d'attractivité »

Nous étudions la stabilité asymptotique de la surface de glissement (s) en posant une fonction de Lyapunov ($\boldsymbol{V}$) de la façon suivante **[16]** :

$$V = \frac{1}{2}s^2 \quad \textbf{(1.10)}$$

Alors la condition de stabilité est déduite :

$$\frac{dV}{dt} < 0 \Rightarrow s\frac{ds}{dt} < 0; \ \forall \ s \neq 0 \quad \textbf{(1.11)}$$

1.5.7 Observateur à mode glissants étape par étape à entrées inconnues [16]

La présence d'entrée inconnue dans un système est due soit à une perturbation, soit à un défaut ou bien comme dans le cas qui nous intéresse une information cachée qu'on doit reconstruire. Selon l'objectif fixé, le rôle d'un observateur à entrée inconnue est de reconstruire les variables d'état en éliminant l'influence des entrées inconnues sur la qualité de l'estimation ou bien l'observateur doit non seulement reconstruire les variables d'état mais aussi les entrées inconnues. Ce dernier type d'observateur est utilisé pour estimer les défauts afin de résoudre le problème de commande tolérante aux fautes ou de reconstruire le message cachée dans les dispositifs de transmission sécurisée de données. Dans le cas des systèmes linéaires, l'observateur à entrée inconnue le plus utilisé est celui développée par **Walcotts** et **Zak [17]** ainsi que les nombreuses variantes qui ont suivi. Dans cette section, nous allons présenter l'observateur à entrée inconnue pour les systèmes non linéaires utilisant la technique

des modes glissants étape par étape [Barbot, …]. Deux conditions fondamentales doivent être satisfaites pour garantir la construction et la convergence de ce type d'observateur. Il s'agit de l'observabilité et l'inversion à gauche (« observability matching condition »). Nous donnons ci dessous les définitions simplifiées de ces propriétés.

Considérons le système non linéaire affine par rapport à l'entrée décrit par les équations ci-dessous :

$$\dot{x}(t) = f\big(x(t)\big) + g(x(t))\,u(t) \quad \textbf{(1.12)}$$

$$y(t) = h\big(x(t)\big) \quad \textbf{(1.13)}$$

L'entrée u(t) est supposée inconnue.

Observabilité : Le système (1.12) est dit observable s'il vérifie le critère de rang ci-dessous

$$\text{rang}\{dh \quad dL_f h \quad dL_f^2 h \cdots \quad \cdots \quad dL_f^{n-1} h\} = n \quad \textbf{(1.14)}$$

Où $L_f^k h$ désigne la dérivée de Lie de la fonction h(x) le long du champ de vecteur f(x) définie par :

$$\begin{cases} L_f^0 h = h(x) \\ L_f\, h = \frac{\partial h(x)}{\partial x} f(x) \\ L_f^k h = L_f\left(L_f^{k-1} h\right) \end{cases} \quad \textbf{(1.15)}$$

***Inversion à gauche* :** Le système (1.12) vérifie la propriété d'inversion à gauche si la condition suivante est satisfaite :

$$\left\{(dh)^T \quad (dL_f h)^T \quad \cdots \quad \cdots \quad \left(dL_f^{n-1} h\right)^T\right\}^T g(x) = \langle 0 \quad 0 \quad \cdots \quad \theta(x)\rangle^T \quad \textbf{(1.16)}$$

Où θ(x) est une fonction non nulle pour tout (x) appartenant à un domaine considéré.

La condition d'inversion à gauche permet de reconstruire l'entrée inconnue u(t). Afin de mètre en œuvre l'observateur à mode glissant étape par étape, il est nécessaire de transformer le système (1.12), (1.13) en une forme dite triangulaire suivante :

$$\begin{cases} \dot{x}_1 = x_2 + \bar{g}_1(x_1) \\ \dot{x}_2 = x_3 + \bar{g}_2(x_1, x_2) \\ \vdots \\ \dot{x}_{n-1} = x_n + \bar{g}_{n-1}(x_1, \dots, x_{n-1}) \\ \dot{x}_n = \bar{f}_n + \bar{g}_n(x)u \\ y = x_1 \end{cases} \quad \textbf{(1.17)}$$

Observateur à mode glissant pour le système triangulaire

La structure de l'observateur proposé pour le système triangulaire est :

$$\begin{cases} \dot{\hat{x}}_1 = \hat{x}_2 + \bar{g}_1(x_1) + \lambda_1 sign_1(x_1 - \hat{x}_1) \\ \dot{\hat{x}}_2 = \hat{x}_3 + \bar{g}_2(x_1, \tilde{x}_2) + \lambda_2 sign_2(\tilde{x}_2 - \hat{x}_2) \\ \vdots \\ \dot{\hat{x}}_{n-1} = \hat{x}_n + \bar{g}_{n-1}(x_1, \tilde{x}_2 \dots, \tilde{x}_{n-1}) + \lambda_{n-1} sign_{n-1}(\tilde{x}_{n-1} - \hat{x}_{n-1}) \\ \dot{\hat{x}}_n = \bar{f}_n + \bar{g}_n(x_1, \tilde{x}_2, \dots, \tilde{x}_n)\hat{u} + \lambda_n sign_n(\tilde{x}_n - \hat{x}_n) \end{cases} \quad \textbf{(1.18)}$$

Où les variables $\tilde{x}_i$ sont données par :

$$\begin{cases} \tilde{x}_2 = \hat{x}_2 + \lambda_1 sign_1(x_1 - \hat{x}_1) \\ \tilde{x}_3 = \hat{x}_3 + \lambda_2\, sign_1\ (\tilde{x}_2 - \hat{x}_2) \\ \vdots \\ \tilde{x}_n = \hat{x}_n + \lambda_n\, sign_n(\tilde{x}_{n-1} - \hat{x}_{n-1}) \end{cases} \quad \textbf{(1.19)}$$

Et dans lequel $sign_i = E_i sign$ avec $E_i = 1\ \ si\ E_1 = \cdots = E_{i-1} = 1$ et $(x_1 - \hat{x}_1) = 0$, sinon $(E_i) = 0$. Dans la structure de l'observateur, la fonction $sign_i$ permet la convergence de $(\tilde{x}_i - \hat{x}_i)$ vers zéro si toutes les $(\tilde{x}_j - \hat{x}_j)$; $j < i$ sont convergés vers zéro. Le message estimé est donné par :

$$\hat{u} = sign_{n+1}(\tilde{x}_n - \hat{x}_n) \quad \textbf{(1.20)}$$

Remarque. Nous pouvons choisir les gains λ_i de l'observateur à modes glissants tels que l'état $(\hat{x})$ de l'observateur converge vers (x) en temps fini, et si l'entrée inconnue (u) est continue ou au moins continue par morceaux, alors son estimation $(\widehat{u})$ converge vers (u) en temps fini. Dans ce travail nous avons utilisé la forme originale du système de Chua normalisé afin de construire un observateur à mode glissant.

1.6 Conclusion

Dans ce chapitre, nous avons donné les notions fondamentales sur les systèmes non linéaires chaotiques et les observateurs non linéaires. Nous sommes limités à quelques techniques de synthèse d'observateurs sans être exhaustifs. Ces notions seront exploitées dans les chapitres suivants.

Chapitre2

Généralités sur la transmission sécurisée de données

2.1 Introduction

De part les siècles, de nombreuses techniques furent élaborées pour protéger les échanges d'informations. Les premières se basaient uniquement sur des méthodes issues de la cryptographie et développées par les militaires afin de protéger des informations secrètes. Ces méthodes utilisent une clé privée connue uniquement des deux participants. La transmission de cette clé qui s'effectuait, il y a encore quelques années, par un échange physique entre personnes de confiance, constitue une étape primordiale dans le protocole de communication. La perte de cette clé à des conséquences catastrophiques pour la confidentialité de la communication. Grâce aux avancées récentes des cryptographes, qui mirent au point des méthodes de chiffrement à clé publique, l'échange de cette clé privée entre deux participants est réalisé à l'aide d'un premier protocole de communication cryptographique utilisant un chiffrement asymétrique. Ainsi, aujourd'hui, les communications sécurisées s'effectuent entre deux individus distants de plusieurs milliers de kilomètres, rapidement et à moindre coût, grâce aux avancées technologiques des moyens de communication et aux progrès des techniques de chiffrement. Nous proposons dans ce chapitre d'exposer les principes généraux de la transmission sécurisée. L'intérêt se portera essentiellement sur la transmission sécurisée à base de systèmes chaotiques et sur le problème de la synchronisation. Nous présentons les techniques de cryptage utilisées habituellement et les méthodes de la synchronisation.

2.2 Principes de la transmission de données [1], [18]

Un système de communication est constitué globalement de trois éléments principaux (figure 2.1): un émetteur, un canal de transmission et un récepteur utilisé pour transmettre une information sur une certaine distance.
L'émetteur : il met en forme une information selon un codage donné, pour la préparer à la transmission.
Le récepteur : il permet de récupérer l'information transmise et de la décoder selon le même code que celui utilisé à l'émetteur.
Le canal de transmission : il sert à véhiculer l'information sur une certaines distance.

En plus de ces trois éléments, des modules de codage et de décodage sont souvent nécessaires afin soit de sécuriser l'information ou bien de transformer le signal transmis en une forme adéquate au canal de transmission.

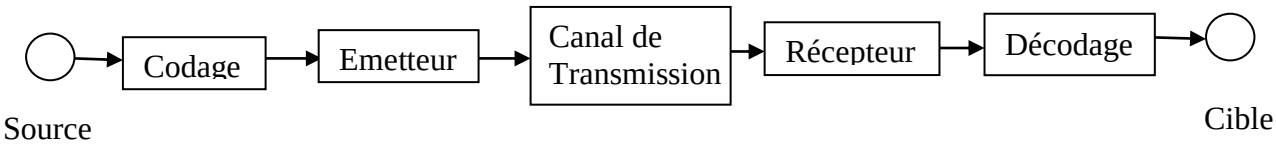


Fig. 2.1 Schéma synoptique d'un système de transmission

2.2.1 Les supports de transmission [1], [18], [19]

Les différents supports de transmission utilisés sont :

- Transmission par lignes
- Transmission par ondes rayonnées
- Transmission par antenne
- Guide d'ondes
- Fibre optique

2.2.2 Les caractéristiques des réseaux de transmission [18], [19]

L'évolution des besoins et des applications informatiques conduit à transporter sur un même système physique des flux d'information de natures différentes. Afin de qualifier ces différents flux vis-à-vis du système de transmission, nous définirons les caractéristiques essentielles d'un réseau de transmission.

2.2.2.1 Notion de débit binaire

Les systèmes de traitement de l'information emploient une logique à deux états dite «binaire». Pour y être traitée, l'information doit être traduite en symboles compréhensibles et manipulables par ces systèmes. Selon le type d'information à transformer, l'opération qui consiste à transformer les données en éléments binaires s'appelle le *codage* ou *numérisation*. On appelle débit binaire (D) le nombre d'éléments binaires, ou nombre de bits, émis sur le support de transmission pendant une unité de temps. Le débit binaire est généralement la grandeur utilisée en premier pour qualifier un système de transmission.

2.2.2.2 Notion de rapport signal sur bruit

Durant la transmission, les signaux électriques peuvent être perturbés par des phénomènes électriques ou électromagnétiques d'origine externe désignés sous le terme générique de *bruit*. Le bruit est un phénomène qui dénature le signal et qui est susceptible d'introduire des erreurs d'interprétation du signal reçu (figure 2.2).

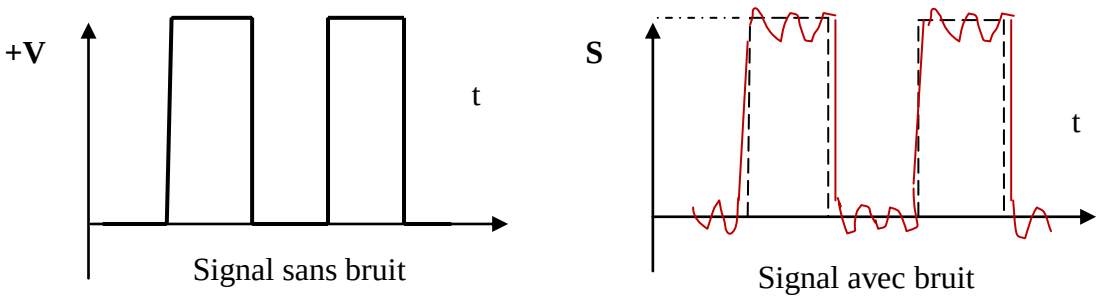


Fig. 2.2 Le signal pollué par le bruit

Il existe plusieurs sources de bruits [2]

- Le bruit *thermique*
- Le bruit *grenaille*
- Le bruit *impulsionnel*

2.2.2.3 Notion d'erreur et de taux d'erreur [18], [19]

Les capacités de transport d'information (débit) sont directement liées au rapport entre la puissance du signal utile et celle du signal de bruit. Ce rapport, appelé rapport signal sur bruit (SNR , Signal Noise Ratio que nous noterons S/N), s'exprime en dB (décibel), formule dans laquelle S représente la puissance électrique du signal transmis et N la puissance du signal parasite ou bruit affectant le canal de transmission .

$$S/N_{dB} = 10log_{10}(S/N) \text{ (en puissance)} \qquad \textbf{(2.1)}$$

On appelle taux d'erreur binaire(Te ou BER, Bit Error Rate) le rapport du nombre de bits reçus en erreur au nombre de bits transmis.

$$Te = \frac{Nombre\ de\ bits\ en\ erreur}{Nombre\ de\ bits\ transmis} \quad \textbf{(2.2)}$$

2.2.2.4 Notion de temps de transfert [18], [19]

Le temps de transfert, appelée aussi temps de transit ou temps de latence, mesure le temps entre l'émission d'un bit, à l'entrée du réseau et sa réception en sortie de ce dernier. Ce temps prend en compte le temps de propagation sur les supports et le temps de traitement par les éléments actifs du réseau (nœuds).

2.2.2.5 **Notion de spectre du signal [18], [19]**

Le mathématicien français **Joseph Fourier** (1768-1830) a montré que tout signal périodique de forme quelconque pouvait être décomposé en une somme de signaux élémentaires sinusoïdaux (fondamental et harmoniques) superposée à une valeur moyenne (composante continue) qui pouvait être nulle. L'ensemble de ces composantes forme le spectre du signal ou bande de fréquence occupée par le signal (largeur de bande).

2. 3 Notions générales sur la cryptographie [18], [19]

2.3.1 Principe

L'origine du mot cryptographie provient du grec kryptós (caché) et gráfein (écrire). On peut définir la cryptographie comme l'ensemble des techniques permettant de protéger une communication, par exemple l'assurance que l'information contenue dans un message ne soit révélée qu'au seul destinataire de ce message. La manière la plus simple de transmettre un message de manière sécurisée entre deux entités est d'utiliser un canal sécurisé, par exemple en faisant appel à un porteur en qui vous avez totale confiance et qui va aller porter votre message à votre correspondant. S'il se fait capturer par l'ennemi, ce porteur ne devra rien dire... Cependant, il est évident que les canaux sécurisés ont des contraintes trop importantes pour être couramment utilisés en pratique. La cryptographie permet de correspondre de manière sécurisée en utilisant des canaux non sécurisés. Pour cela, une fonction de chiffrement est appliquée au message à transmettre et le résultat de ce chiffrement, appelé texte chiffré, pourra être transmis à l'autre entité qui connait comment déchiffrer ce texte chiffré afin d'obtenir le texte clair. Bien sûr, aucune information ne devra être dévoilée sur le texte clair si le texte chiffré tombe entre les mains de l'ennemi. Pour cela, les fonctions de chiffrement et de déchiffrement doivent rester secrètes. Pour des raisons pratiques, ces fonctions sont décomposées en algorithmes paramétrés par une clé. Le fonctionnement de ces algorithmes est public et seule la valeur des clés est tenue secrète.

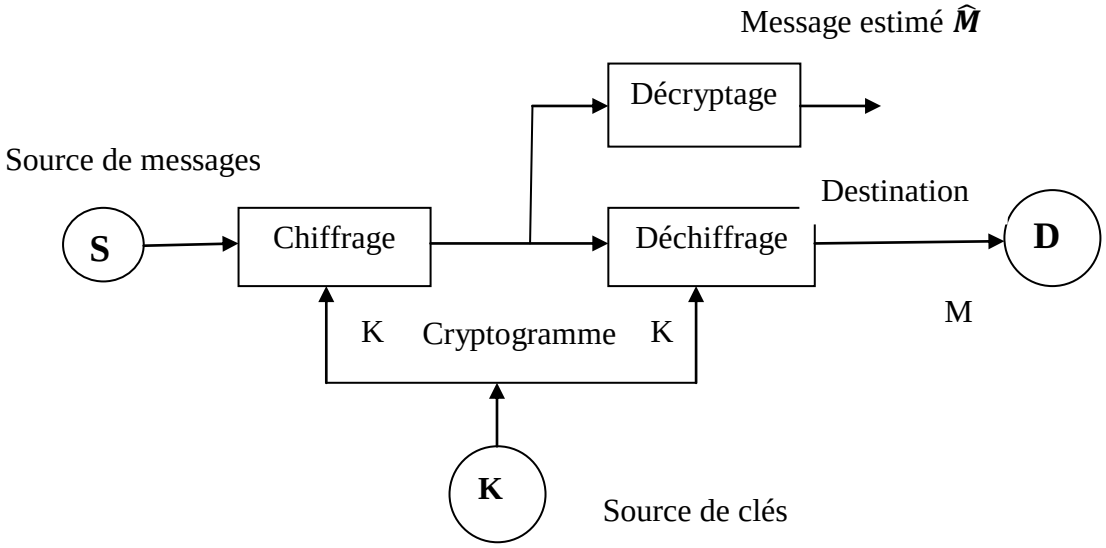


Fig. 2.3 Schéma générale du chiffrage

Le texte en clair est noté M, c'est le message à chiffrer. Il peut être une suite de bits, un fichier de texte, un enregistrement de voix numérisé, ou une image vidéo numérique. De toute façon M n'est rien d'autre que de l'information binaire, comme il peut être transmis ou stocké. Le texte chiffré est noté C. C'est aussi de l'information binaire, parfois de la même taille que M, parfois plus grand. Les deux fonctions de chiffrement et déchiffrement sont notées respectivement E (pour Encoder) et D (pour Décoder).

2.3.2 Définitions et concepts

Comme toute science, la cryptographie possède son propre langage :

- ***Cryptologie :*** est la science qui étudie les aspects scientifiques des méthodes de chiffrement et de déchiffrement d'information. Elle englobe donc la cryptographie et la cryptanalyse.
- ***Cryptographie :*** Discipline incluant les principes, les moyens et les méthodes de transformation des données, dans le but de masquer leur contenu, d'empêcher leur modification ou leur utilisation illégale.
- ***Stéganographie :*** contrairement à la cryptographie, la sténographie (en grec « écriture couverte » est l'art de dissimuler un message par l'intermédiaire d'un autre.
- ***Cryptanalyse :*** est l'art de déchiffrer un message dans le but de le rendre compréhensible.
- ***Chiffre* :** Ensemble de procédés et ensemble de symboles (lettres, nombres, signes…etc.) employés pour remplacer les lettres du message à chiffrer. On distingue généralement les chiffres à transposition et ceux à substitution.

- ***Chiffrer*= crypter :** c'est transformer un texte clair en texte codé. L'opération ou son résultat s'appelle un chiffrement.
- ***Clés* :** série de symboles commandant les opérations de chiffrement et déchiffrement.
- ***Déchiffrer* :** c'est traduire en clair en connaissant la clé. C'est donc le destinataire légitime du message qui déchiffre.
- ***Décrypter, cryptanalyser* :** c'est traduire un texte en clair en ne connaissant pas la clé. L'opération ou son résultat s'appelle un décryptement
- ***Message clair*:** désigne le message original n'ayant pas subi aucune modification.
- **Message chiffré, cryptogramme :** désigne le message ayant subi le chiffrement.
- ***Hachage :*** est une fonction qui convertit un grand ensemble en un plus petit ensemble, l'empreinte. Il est impossible de la déchiffrer pour revenir à l'ensemble d'origine, ce n'est pas donc une technique de chiffrement.

2.3.3 Les objectifs de la sécurité

De nos jours, la cryptographie consiste à mettre au point les systèmes cryptographiques afin d'assurer les piliers suivant :

- ***La confidentialité des données* :** il s'agit de s'assurer que l'information ne s'ébruite pas en dehors des personnes autorisées à l'obtenir, cela revient à garantir l'identité du destinataire. La principale idée présentée ici sera de communiquer une version transformée du message n'ayant aucun sens pour une personne n'étant pas en possession du mécanisme nécessaire pour retrouver le message original.

- ***L'authentification* :** il s'agit de s'assurer que les interlocuteurs sont bien ceux qu'ils prétendent être, cette fois cela revient à garantir l'identité de l'expéditeur. Il y a plusieurs implémentations possibles, certaines étant plus simples à mettre en œuvre, d'autres plus fiables. Cela peut aller de l'utilisation d'un mot de passe, à des méthodes plus travaillées, par exemple on peut se baser sur la cryptographie asymétrique que l'on verra plus loin : l'expéditeur envoie son message crypté avec une méthode dont il est le seul à avoir la clé secrète, si sa clé publique décrypte le message, alors on est sur que c'était bien de lui (le destinataire).

- ***La non-répudiation* :** il s'agit de s'assurer qu'un contrat ne peut être remis en cause par l'une des parties. Cela rejoint un peu le point précédent : on doit prouver la participation d'un interlocuteur dans un échange de données.

- ***L'intégrité des données* :** il s'agit de s'assurer que les données ne subissent aucune altération ou destruction volontaire ou accidentelle. D'un point de vu cryptographique, on cherche à vérifier que les données n'ont pas été modifiées. On peut par exemple utiliser une fonction de hachage selon le principe suivant. On se donne une fonction

dite de hachage qui prend en argument des données et dont le résultat est nommé empreinte (ou somme de contrôle). Ensuite l'expéditeur envoie des données et l'empreinte qui va avec, et lorsque le destinataire reçoit les données, il en calcule à son tour l'empreinte et la compare à celle qu'il a reçu. S'il observe une différence, les données ont été modifiées, sinon il y a peu de chance (selon la fonction et le protocole de communication utilisés) qu'il y ait eu une modification. En dehors de la cryptographie, on peut avoir besoin de détecter, et si possible de corriger, les altérations, il s'agit du rôle des codes correcteurs d'erreurs.

2.3.4 Les méthodes de cryptage [18], [19]

Il existe de nombreuses méthodes pour masquer et sécuriser la transmission d'informations. Les premières méthodes sont basées sur le chiffrement et font appel aux algorithmes informatiques décodage de l'information connus sous le nom d'algorithme de chiffrement. Plusieurs techniques de chiffrement sont proposées dans la littérature (chiffrement à clé secrète, chiffrement à clé public, chiffrement par blocs, chiffrement symétrique, chiffrement asymétrique …) et aussi plusieurs modes de chiffrement (algorithmes DES, RSA, AES, …). Actuellement, dans la transmission par fibre optique, on masque couramment l'information à sécurisée dans un signal chaotique généré par des dispositifs optoélectroniques en utilisant des techniques de modulation, le signal chaotique jouant le rôle de porteuse d'information. Une autre méthode récente de sécurisation de la transmission de données consiste à utiliser au niveau de l'émetteur et du récepteur des systèmes chaotiques réalisés par des oscillateurs électroniques (Colpitts, Chua, Qi, …). Le principe de transmission sécurisée à base de systèmes chaotiques et illustré par la figure 2.4 ci-dessous. Le signal à transmettre est « noyé » dans la dynamique chaotique est donc difficile à reconstruire. Les principales méthodes de cryptage à base d'oscillateurs chaotiques sont :

2.3.4.1 Cryptage par addition

Cette méthode appelée, masquage chaotique, est la première chronologiquement qui introduit la synchronisation du chaos. L'émetteur est un système chaotique autonome dont le signal de sortie $y(t)$ est ajouté au signal du message $m(t)$. La somme des 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 d'un simple soustracteur. Ainsi, après la synchronisation des deux systèmes chaotiques (émetteur et récepteur), le message est extrait à l'aide d'une opération de soustraction. Notons que dans cette méthode, l'attracteur étrange du système chaotique n'est pas modifié par le message. Le schéma représentant cette méthode est donné par la figure 1 suivante :

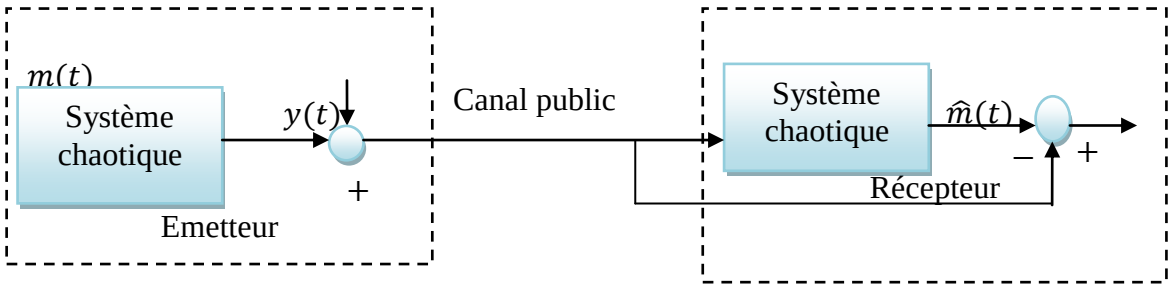


Fig. 2.4 Principe du cryptage par addition

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. Dans les deux cas, il est impératif que l'amplitude du message original soit significativement plus petite que celle de la porteuse chaotique, d'une part pour ne pas perturber l'établissement de la synchronisation au niveau du récepteur, et d'autre part pour garantir le secret de la transmission. Dans tous les cas, à cause de la présence du message, la synchronisation ne peut être parfaite. En outre, la fréquence du message doit être comprise dans le spectre du signal chaotique. Un autre problème qui se pose naturellement concerne la présence d'un bruit additif au niveau du canal de transmission. Dans ce cas, il faut que l'amplitude du message soit plus grande que celle du bruit. Il y a donc un compromis à trouver entre la sécurité de la transmission, et la robustesse au bruit.

En résumé cette technique de masquage nécessite deux conditions : la première est que le spectre du message soit entièrement recouvert par le spectre du chaos généré, sinon une simple opération de filtrage permet d'extraire au moins partiellement le message. La seconde condition concerne l'efficacité du masquage. Il est important que l'amplitude du message, $m(t)$, soit suffisamment faible devant les fluctuations chaotiques $c(t)$ de la porteuse. De manière empirique, cette condition est vérifiée lorsque $m(t) \leq 0.1\ c(t)$. Le message devient alors de taille comparable à celle qu'occupe le bruit sur le canal de transmission. Le message et le bruit deviennent donc confondus ce qui dégrade très rapidement la qualité de la communication. De fait, ce type d'encodage est très peut utilisé en communication à cause des problèmes liés au bruit.

2.3.4.2 Cryptage par inclusion

Cette technique de cryptage consiste à injecter le message dans la dynamique de l'émetteur, sans toutefois réaliser une modulation de paramètres. 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.

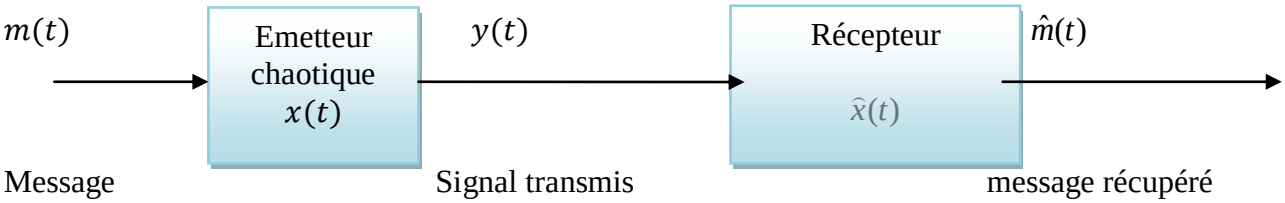


Fig. 2.5 Cryptage par inclusion

Remarque

D'autres méthodes de cryptage ont été proposées comme celle de cryptage par modulation.

2.4 Synchronisation des systèmes dynamiques [20], [21], [22]

2.4.1 Position du problème

Le terme « synchronisation » vient de grec « συγ » (syn) qui signifie « avec », et « χρονος » (chronos) qui signifie, « temps ». On peut donner une première définition de la synchronisation, à savoir : la synchronisation est un phénomène qui caractérise deux systèmes se comportant de la même façon en même temps. En fait, les manifestations de la synchronisation sont observées depuis le XVII^{ème} siècle. Le mathématicien hollandais Huygens (1629-1695) remarqua ce phénomène en étudiant deux horloges de fréquences légèrement différentes. Il constata qu'en les reliant l'une à l'autre avec un morceau de bois, elles affichaient toutes les deux la même heure : elles se synchronisaient. Des exemples de synchronisation existent dans la nature, dans le domaine de la science de la vie et de la terre, ainsi que dans les domaines techniques. En neurobiologie, la notion de synchronisation apparaît pour expliquer le fonctionnement du cerveau : chaque activité est produite par un ensemble de neurones dont les signaux électriques oscillent de manière synchrone. Dans le domaine de la transmission sécurisée, les procédés utilisés pour transmettre l'information exigent, en général, un synchronisme précis entre certaines fonctions du récepteur et les fonctions correspondantes de l'émetteur. Donc le principe de la synchronisation ici, est le suivent. L'émetteur génère un signal $x(t)$ et l'envoie au récepteur qui génère lui aussi un signal $\hat{x}(t)$. Le récepteur est dit synchronisé lorsque $x(t)$ et $\hat{x}(t)$sont identiques.

D'une façon générale, la synchronisation peut être décrite par la définition suivante **[23]**. Considérons les deux systèmes suivants :

$$\begin{cases} \dot{x} = f_1(x, m) \\ \dot{\hat{x}} = f_2(\hat{x}, \hat{m}) \end{cases} \quad \textbf{(2.3)}$$

Avec $x \in IR^n, \hat{x} \in IR^n$, dans lesquels $f_i: IR^n \times IR^n \to IR^n$ sont des champs de vecteurs non linéaires, les deux systèmes dit synchronisés si $e = \hat{x}(t) - x(t) \to 0 \ quand \ t \to \infty$ où (e) représente l'erreur de synchronisation.

2.4.2 Les méthodes de synchronisation

Plusieurs méthodes de synchronisation ont été proposées dans la littérature, selon la nature de connexion entre le système émetteur et le système récepteur. Parmi les quels on peut retenir quelques notions de base.

2.4.2.1 Synchronisation identique, ou complète

L'état du récepteur converge asymptotiquement vers l'état de l'émetteur. On considère deux systèmes dynamiques

$$\begin{cases} \dot{x} = f_1(x) \\ \dot{\hat{x}} = f_2(\hat{x}) \end{cases} \quad \textbf{(2.3)}$$

Alors les deux systèmes sont identiquement synchronisés si, quelles que soient leurs conditions initiales :

$$\lim_{t\to\infty} \| \hat{x}(t) - x(t) \| = 0 \quad \textbf{(2.4)}$$

2.4.2.2 Synchronisation généralisée [24]

Cela correspond à une généralisation du concept de synchronisation identique. Les systèmes se synchronisent, au sens généralisé, s'il existe une transformation M telle que :

$$\lim_{t\to\infty} \| \hat{x}(t) - Mx(t) \| = 0 \quad \textbf{(2.5)}$$

Et ce, indépendamment des conditions initiales. Si la fonction (M) est inversible, alors $M^{-1}(\hat{x})$ fournit une estimation de l'état (x). Si cette transformation n'est pas inversible, on ne peut pas estimer (x). Cela représente un inconvénient majeur pour certaines techniques de communication, qui utilisent l'état de l'émetteur pour décrypter le message transmis.

2.4.2.3 Synchronisation de phase

Pour deux systèmes périodiques de phases (ϕ_1) et (ϕ_2) , la synchronisation est exprimée par la relation $|n\emptyset_1 - m\phi_2| < c$, où (m), (n) sont des entiers naturels et (c) est une constante positive. Cette notion classique de synchronisation à été étendue aux systèmes chaotiques.

2.4.2.4 **Synchronisation projective**

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

$$\lim_{t\to\infty} \| \hat{x}(t) - ax(t-\tau) \| = 0 \quad \textbf{(2.6)}$$

Ce type de synchronisation est utilisé pour les systèmes "partiellement linéaires", et permet de synchroniser, à un facteur près, les états qui ne peuvent être synchronisés.

2.4.2.5 Synchronisation retardée

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

$$\lim_{t\to\infty} \| x'(t) - x(t-\tau) \| = 0 \qquad \textbf{(2.7)}$$

2.4.2.6 Synchronisation par la boucle fermée

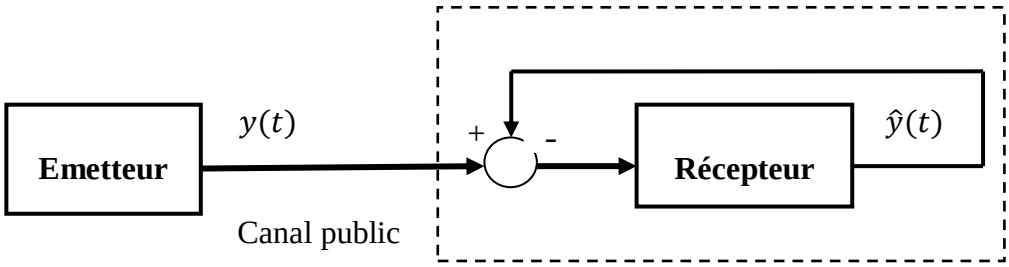


Fig. 2.6 Synchronisation par un contrôle en boucle fermée

La synchronisation basée sur la boucle fermée qui est illustrée en figure 2.6 où nous employons l'erreur entre l'émetteur et le récepteur pour corriger le comportement du récepteur afin de réaliser la synchronisation.
Supposons que l'émetteur s'écrit comme suit :

$$\begin{cases} \dot{x}\,(t) = f(x) \\ y = h(x) \end{cases} \qquad \textbf{(2.8)}$$

Et que le récepteur peut être décrit comme suit :

$$\begin{cases} \dot{\hat{x}} = f(\hat{x}\,) + g(y - \hat{y}) \\ \hat{y} = h(\hat{x}) \end{cases} \qquad \textbf{(2.9)}$$

Où (g) est une fonction de l'erreur entre (y) et ($\hat{y}$), et que cette fonction est choisie afin de garantir la synchronisation entre l'émetteur et le récepteur. En faite, ce genre de récepteur peut être considéré comme la conception d'un observateur. Ensuite, nous pouvons également appliquer quelques stratégies adaptatives quand nous employons l'erreur entre l'émetteur et le récepteur pour piloter le récepteur.

2.4.2.7 Synchronisation par l'inversion du système

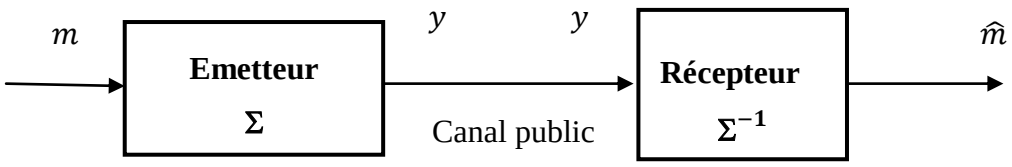


Fig. 2.7 Synchronisation par l'inversion du système

Jusqu'à présent, toutes les approches mentionnées ont dans le but de synchroniser seulement les états du système, et elles 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 sécurisée de données puisque l'entrée inconnue est généralement le message confidentiel. Naturellement, il existe également certains observateurs à entrée inconnue qui permettent d'accomplir l'estimation de ces dernières.

Une autre méthode proposée est basée sur la solubilité du problème d'inversion à gauche afin d'achever la synchronisation des états à entrées inconnues du système, où l'émetteur peut être écrit de la façon suivante :

$$\begin{cases} \dot{x} = f(x) + g(x)u \\ y = h(x) \end{cases} \quad \textbf{(2.10)}$$

Où $x \in R^n$ est le vecteur des états du système, $u \in IR^n$ (m) est le vecteur des entrées inconnues, $f: R^n \to IR^n$, $g: R^n \to IR^{n\times m}$, $h: IR^n \to IR^p$ sont des vecteurs des fonctions analytiques.

Pour le récepteur, son vecteur d'entrée est le vecteur de sortie de l'émetteur. Nous essayons de concevoir un récepteur tel que son vecteur de sortie convergera au moins asymptotiquement vers le vecteur d'entrée de l'émetteur. Ce problème s'appelle l'inversion à gauche du système.

2.4.2.8 Synchronisation impulsive

Dans un schéma 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, c-à-d, envoyer le signal minimum possible.

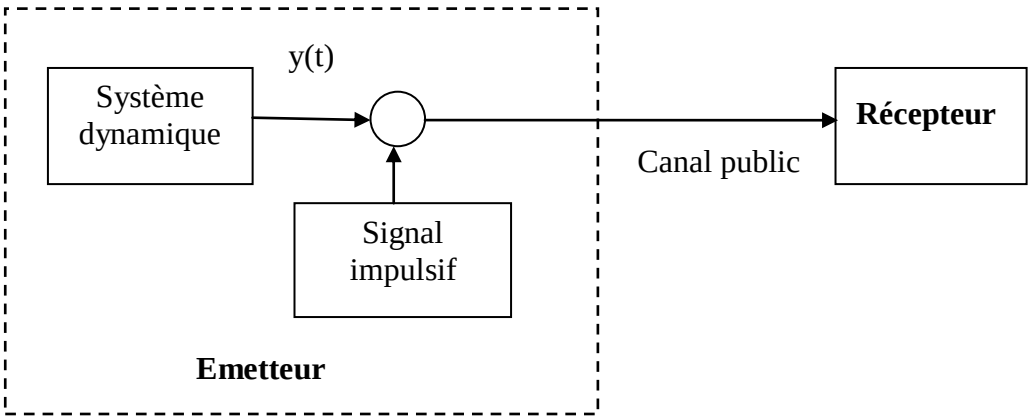


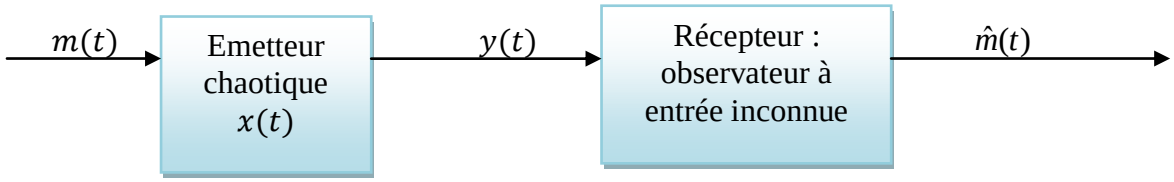
Fig. 2.8 Synchronisation impulsive

Dans cette approche, en raison de l'introduction d'un opérateur de Dirac, le problème de synchronisation entre l'émetteur et le récepteur devient celui de stabiliser un système impulsionnel.

2.5 Synchronisation par observateur à entrée inconnue

2.5.1 Observateur à entrées inconnues

Le schéma de la figure (2.9) illustre un problème classique d'estimation d'état non linéaire à entrées inconnues : il faut reconstruire l'état $x(t)$ du système émetteur et également l'entrée inconnue $u(t)$. Différentes techniques de synthèse d'observateurs à entrées inconnues ont été utilisées dans la littérature, et peuvent être utilisées à des fins de décryptage.



Message Signal transmis reconstruction du message et états

Fig. 2 .9 Observateur à entrée inconnue

Dans cette méthode de décryptage (décryptage par observateur à entrée inconnue) le signal d'injection nécessaire par la synthèse de l'observateur contient aussi le message transmis (c'est le principe de transmission à une voix).

2.5.2 Transmission et décryptage à deux voies

Dans le schéma présenté à la figure (2.10), l'émetteur envoie deux signaux au récepteur. Le premier(y_1), est une fonction à valeurs réelles de l'état (x) du système émetteur chaotique, dont l'unique but est de permettre la synchronisation du récepteur. Le second,(y_2) envoyé éventuellement sur un autre canal est un signal chaotique qui contient l'information à transmettre. Parmi les avantages de cette méthode, on peut souligner d'une part que le signal (y_1) ne contient aucune information, par conséquent la synchronisation peut s'établir de façon optimale. D'un autre côté, le second signal (y_2) contient l'information qui peut être soit cryptée par une fonction non linéaire de l'état(x), soit simplement masquée par un signal chaotique généré par l'émetteur, qui sert de porteuse. On peut noter également que les deux étapes de synchronisation et de cryptage étant totalement indépendantes, le décryptage n'est pas nécessairement effectué, au niveau du récepteur, en même temps que la synchronisation.

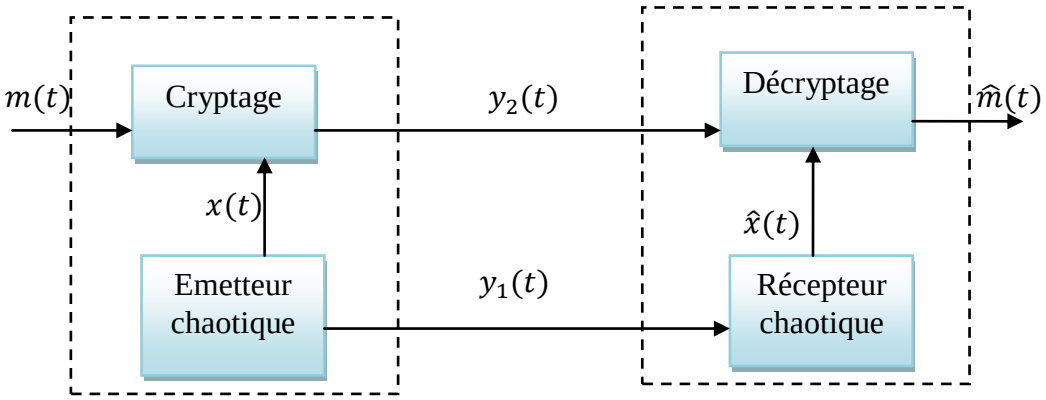


Fig. 2.10 Transmission à deux voies

2.6 Conclusion

L'objectif de ce chapitre a été de donner un aperçu de quelques notions de base sur la théorie et les techniques habituellement utilisées pour résoudre des problématiques de la transmission sécurisée.

Dans un premier temps et sans entrer dans les détails, on a présenté quelques principes de la transmission sécurisée qui se fait au travers de deux fonctions de base : la théorie de l'information qui a pour rôle de mieux transmettre l'information en évitant toute dégradation (bruit et perturbation) et la cryptographie qui consiste à mettre en œuvre les méthodes et les moyens permettant de protéger une communication. Une classification des méthodes de chiffrement a été donné, deux approches ont été distinguées celles à clé privée et celles à clé public, et chaque algorithmes à présenté ses avantages et ses inconvénients. En dernier, on a présenté les principales méthodes de synchronisation. Dans le cadre de ce projet, notre choix s'est porté sur la transmission à base de systèmes chaotiques et sur la méthode de synchronisation à base d'observateur à modes glissant à entrée inconnue. Nous développons dans le chapitre suivant ces différents points autour du circuit chaotique de **Chua**.

Chapitre 3

Synchronisation de circuits de Chua par observateur à modes glissants : Résultats de simulation

3.1 Circuit de Chua [23]

Lors d'une visite au Japon en 1983, **Leon Chua** fut témoin d'une tentative infructueuse de génération de chaos à partir d'une réalisation électrique inspirée des équations de Lorenz. Ceci le poussa à développer son propre circuit électronique.

Le circuit de **Chua** est un circuit électronique qui se compose de cinq éléments : une résistance R, une inductance L, deux condensateurs C_1 , C_2 et une résistance non linéaire NR appelée diode de **Chua** comme représenté dans la figure ci-dessous.

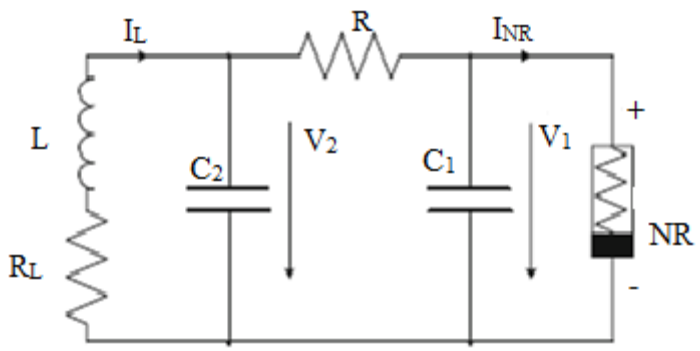


Fig. 3.1 Circuit de Chua

La résistance non-linéaire peut s'obtenir avec deux amplificateurs opérationnels et des résistances.
En utilisant la loi des mailles et la loi des noeuds, nous pouvons établir trois équations différentielles aux variables indépendantes, caractéristiques du circuit :

$$\begin{aligned} \frac{dV_1(t)}{dt} &= \frac{1}{C_1}[G\big(V_2(t)-V_1(t)\big)-f(V_1(t))] \\ \frac{dV_2(t)}{dt} &= \frac{1}{C_2}[G\big(V_1(t)-V_2(t)\big)+I_L(t)] \\ \frac{dI_L(t)}{dt} &= \frac{1}{L}[-V_2(t)-R_L I_L(t)] \end{aligned} \qquad \textbf{(3.1)}$$

Avec la conductance $G=\frac{1}{R}$, $I_L(t)$ le courant qui traverse l'inductance L, $V_1(t)$ et $V_2(t)$sont les tensions respectivement aux borne des capacités (C_1) et (C_2) et $f\big(V_1(t)\big)$ la fonction non-linéaire qui caractérise la diode de **Chua** a pour expression :

$$I_{NR}(t)=f\big(V_1(t)\big)=G_bV_1(t)+\frac{1}{2}(G_a-G_b)(|V_1(t)+E|-|V_1(t)-E|) \qquad \textbf{(3.2)}$$

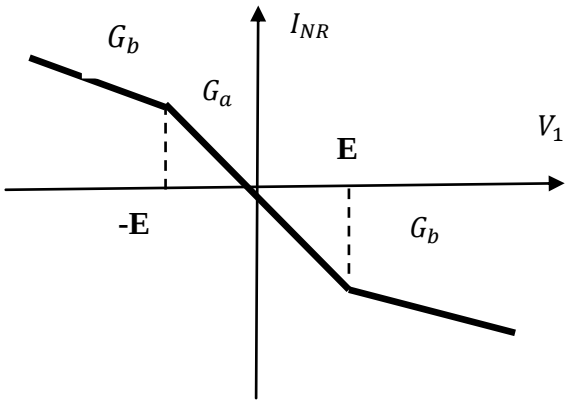


Fig. 3.2 La caractéristique de la non-linéarité de la diode de Chua

Avec (E) est la tension de palier de la diode. $G_a < 0$; $G_b < 0$ sont les pentes de la non-linéarité

En effectuant les changements de variables suivants :

$x = \frac{v_1}{E}$, $y = \frac{v_2}{E}$, $z = \frac{I_L}{E.G}$, $\alpha = \frac{C_2}{C_1}$, $\beta = \frac{C_2}{(LG)^2}$, $\gamma = \frac{C_2.R_L}{L.G}$

$m_1 = \frac{G_b}{G}$, $m_0 = \frac{G_a}{G}$ .L'échelle de temps est remplacé par $\tau = t(\frac{G}{C_2})$.

Le modèle (3.2) prend alors la forme suivante, appelée modèle sans dimension du circuit de **Chua** :

$$\begin{cases} \dot{x} = -\propto x + \propto y - \propto f(x) \\ \dot{y} = x - y + z \\ \dot{z} = -\beta y - \gamma z \end{cases} \quad \textbf{(3.3)}$$

$f(x)$ Représente la non-linéarité du circuit figure (3.2) et décrite par l'équation :

$$f(x) = m_1 x(t) + \frac{1}{2}(m_0 - m_1).(|x(t) + 1| - |x(t) - 1|) \quad \textbf{(3.4)}$$

Avec

$$f(x) = \begin{cases} m_1 x + (m_0 - m_1) & si\ x \geq 1 \\ m_0 x & si\ |x| < 1 \\ m_1 x - (m_0 - m_1) & si\ x \leq 1 \end{cases} \quad \textbf{(3.5)}$$

Les points fixes du système sont donnés par :

$C_0 = (0,0,0)$, ainsi que deux points fixes :

$$C_1 = \left(\frac{m_1 - m_0}{m_1 + 1}, 0, \frac{m_0 - m_1}{m_1 + 1}\right); \quad C_{-1} = \left(\frac{m_0 - m_1}{m_1 + 1}, 0, \frac{m_1 - m_0}{m_1 + 1}\right)$$

Pour certaines valeurs des différents paramètres $(\propto, \beta, \gamma, m_0, m_1)$ et différentes conditions initiales imposées aux variables d'états $x(t), y(t)\ et\ z(t)$, ce circuit présente des régimes de fonctionnement oscillatoires chaotiques.

3.2 Circuit de Chua modifié

Le modèle de **Chua modifié** est obtenu en remplaçant la fonction non linéaire discontinue (continue par morceaux) par une fonction non linéaire cubique continue.

Modèle de Chua modifié

$$\begin{cases} \dot{x} = -\alpha x + \alpha y - \alpha f(x) \\ \dot{y} = x - y + z \\ \dot{z} = -\beta y \end{cases} \qquad \textbf{(3.6)}$$

Où la non-linéarité cubique est

$$f(x) = \frac{x - 2x^3}{7} \qquad \textbf{(3.7)}$$

3.3 Comportement chaotique du circuit de Chua modifié

Nous avons simulé le modèle de Chua modifié sous **MATLAB/SIMULINK** (méthode de résolution de Runge-Kutta 45, fonction ode45 avec un pas variable) avec les paramètres suivant : $\alpha = 9.5$, $\beta = -100/7$. Les conditions initiales sur les variables d'état sont les suivantes $(x(0), y(0), z(0)) = (0.5, -0.1, -0.1)$. Les figures (3.3), (3.4) et (3.5) illustrent les réponses temporelles des variables d'état alors que les figures (3.6), (3.7) et (3.8) visualisent les attracteurs étranges obtenus sur les différents plans. La figure (3.9) donne les trajectoires de phase sur les trois dimensions (x, y, z). Au vu de ces figures, nous remarquons que les valeurs des paramètres choisie, le modèle de Chua modifié présente bien un comportement chaotique.

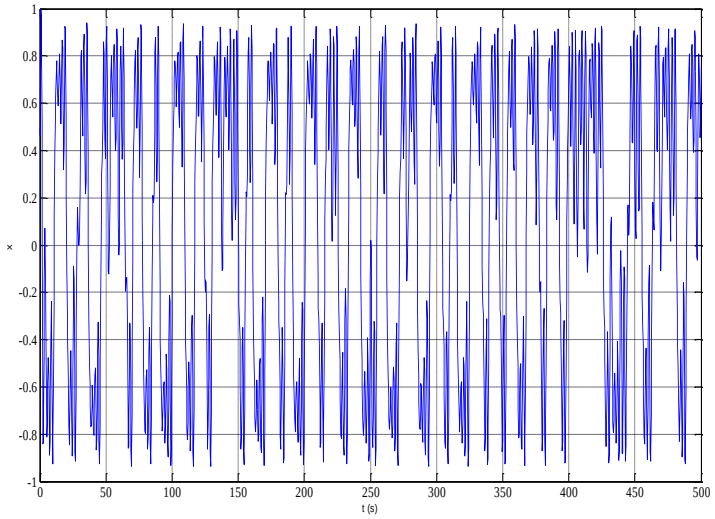


Fig. 3.3 Réponse temporelle de l'état (x)

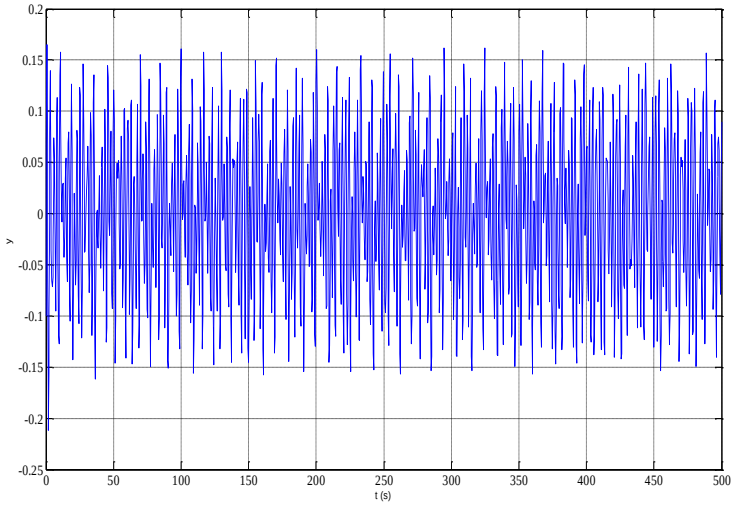


Fig. 3.4 Réponse temporelle de l'état (y)

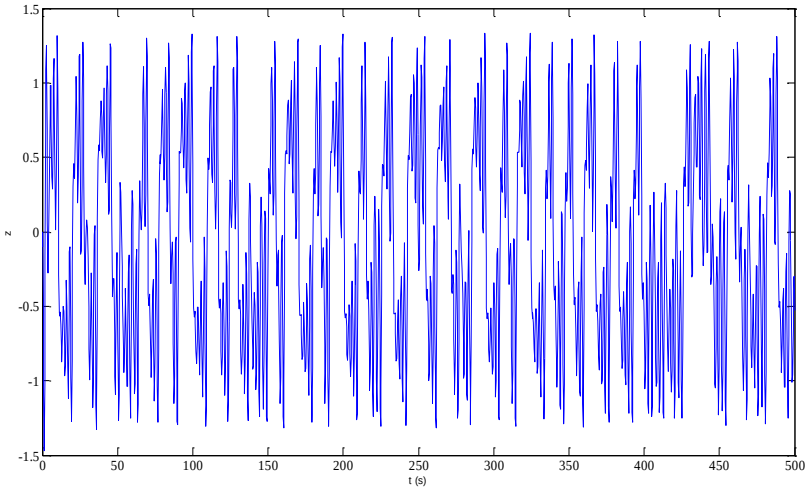


Fig. 3.5 Réponse temporelle de l'état (z)

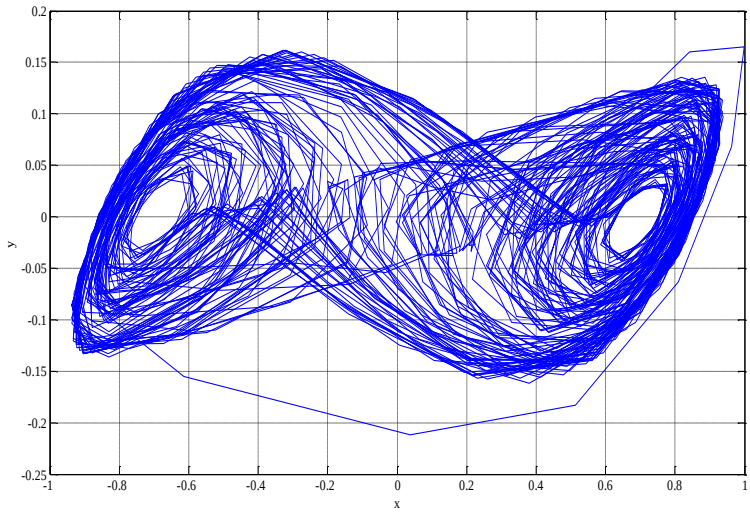


Fig. 3.6 Attracteur étrange sur le plan (x y)

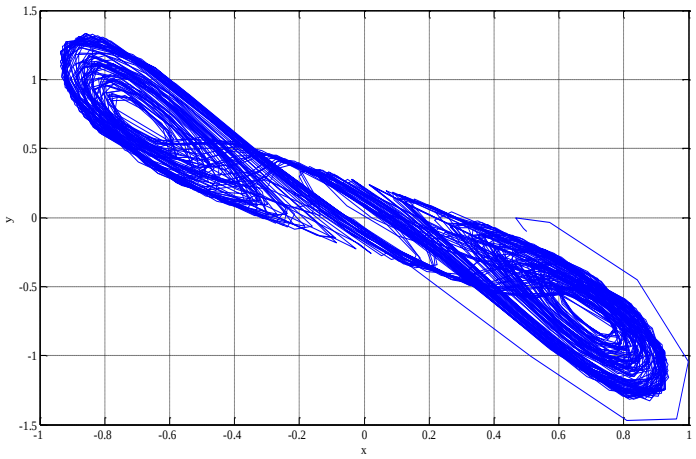


Fig. 3.7 Attracteur étrange sur le plan (x z)

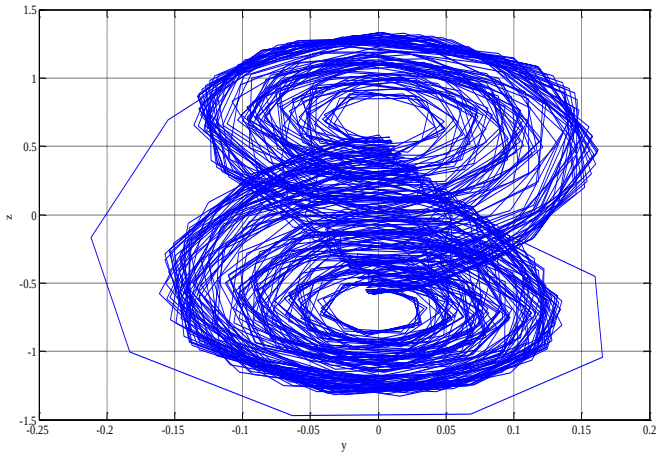


Fig. 3.8 Attracteur étrange sur le plan (y z)

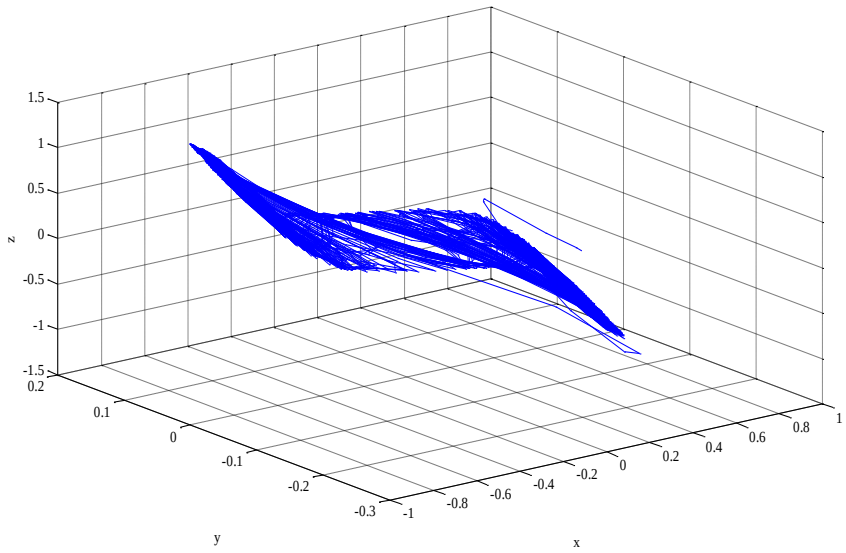


Fig. 3.9 Trajectoires de phase dans le trièdre (x y z)

3.4 Schéma de transmission sécurisé à base du système chaotique de Chua

Les systèmes chaotiques sont utilisés dans la sécurisation de la transmission d'information en raison du comportement imprévisible de leurs réponses. En effet, il est souvent difficile d'extraire une information secrète si celle-ci est noyée dans un signal chaotique. Le schéma de principe est représenté par la figure (3.10). L'émetteur, générateur de signaux chaotiques est formé par le circuit de Chua. La méthode de cryptage que nous avons adoptée est celle par inclusion. Le message m(t) à sécurisée est ajouté à la dynamique du système chaotique. Le choix de la variable sur laquelle est ajoutée le message secret doit répondre aux conditions d'observabilité et de recouvrement à gauche afin de garantir la construction de l'observateur. Le récepteur est justement formé par un observateur du système chaotique afin de réaliser la synchronisation entre l'émetteur et le récepteur. Dans notre étude, nous avons opté pour une transmission à une voie. Ceci est avantageux car il permet de ne pas encombrer le canal de transmission. Le signal cryptant le message servira aussi comme l'entrée d'injection à l'observateur.

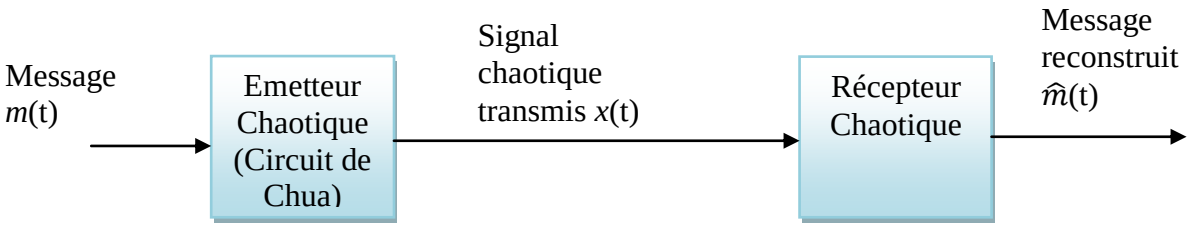


Fig. 3.10 Schéma de transmission à base de circuit chaotique de Chua

L'émetteur est régi par le système non linéaire de Chua suivant :

$$\begin{cases} \dot{x} = -\alpha x + \alpha y - \alpha f(x) \\ \dot{y} = x - y + z \\ \dot{z} = -\beta y + m(t) \end{cases} \quad \textbf{(3.8)}$$

Le message est ajouté à la dérivée de la troisième variable d'état *z*(t) par inclusion. Nous avons décidé de transmettre la variable *x*(t) vers le récepteur à travers le canal public. Avant de mettre en œuvre l'observateur (récepteur), nous devons vérifier si le système chaotique de l'émetteur vérifie les deux conditions d'observabilité et d'inversion à gauche.

- **Observabilité de l'émetteur chaotique**

L'émetteur peut s'écrire sous la forme analytique suivante :

$$\begin{cases} x(t) = F(x)^{\cdot} + G(x)m(t) \\ y(t) = H(x) \end{cases} \quad \textbf{(3.9)}$$

Avec $$F(x) = \begin{bmatrix} -\alpha x + \alpha y - \alpha f(x) \\ x - y + z \\ -\beta y \end{bmatrix}; G(x) = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}; \quad H(x) = x \quad \textbf{(3.10)}$$

La matrice d'observabilité s'écrit donc

$$O = \begin{bmatrix} dH \\ dL_F H \\ dL_F^2 H \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ \alpha\left(\frac{1-6x^2}{7}\right) & \alpha & 0 \\ \alpha\rho\left(\frac{1-6x^2}{7}\right) + \alpha & \alpha(\rho - 1) & \alpha \end{bmatrix} \quad \textbf{(3.11)}$$

Où $\rho = \alpha\left(\frac{1-6x^2}{7}\right)$.

On déduit que *det* (*O*) = $\alpha \neq 0$ car le coefficient (α) est un réel strictement positif donc le rang de (*O)* est égal à n=3. Le système de Chua vérifie donc bien la condition d'observabilité.

- **Inversion à gauche de l'émetteur chaotique**

Le calcul de

$$((dH)^T\ (dL_F H)^T\ (dL_F^2 hH)^T)^T . G(x)$$

Donne

$$(O) * g(x) = \begin{bmatrix} 1 & 0 & 0 \\ \alpha(\frac{1-6x_1^2}{7}) & \alpha & 0 \\ \alpha\rho\left(\frac{1-6x_1^2}{7}\right)+\alpha & \alpha(\rho-1) & \alpha \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \alpha \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \theta \end{bmatrix} \quad \textbf{(3.12)}$$

Comme $\alpha \neq 0$ alors $\theta \neq 0$. Donc la condition de recouvrement d'observabilité (l'inversibilité à gauche) de l'émetteur chaotique est vérifiée ainsi que Il est possible d'extraire le message (m) à l'aide d'un observateur à mode glissants si l'entrée du système reste bornée et $\alpha \neq 0$.

3.5 Mise en œuvre du récepteur par un observateur à modes glissants [23], [24]

L'observateur à modes glissant étape par étape s'écrit :

$$\begin{cases} \dot{\hat{x}} = \alpha\left(\hat{y} + \frac{x-2x^3}{7}\right) + \lambda_1 sgn(x-\hat{x}) \\ \dot{\hat{y}} = x - \hat{y} + \hat{z} + E_1\lambda_2 sgn(\tilde{y}-\hat{y}) \\ \dot{\hat{z}} = -\frac{100}{7}\hat{y} + E_2\lambda_3 sgn(\tilde{z}-\hat{z}) \end{cases} \quad \textbf{(3.13)}$$

Où $\hat{x}, \hat{y}$ et $\hat{z}$ sont les estimées des variables *x*, *y* et *z*, respectivement.
Les états auxiliaires sont :

$$\begin{cases} \tilde{y} = \widehat{\hat{x}_2} + \frac{1}{\alpha}\lambda_1 E_1 sgn(x-\hat{x}) \\ \tilde{z} = \hat{z} + E_2\lambda_2 sgn(\tilde{y}-\hat{y}) \end{cases}$$

Le message estimé est donné par :

$$\tilde{m} = E_3\lambda_3 sgn(\tilde{z}-\hat{z}) \quad \textbf{(3.14)}$$

Les fonctions de commutation E_i , $i = 1, 2, 3$ obéissent à la logique suivante :

- $E_1 = 1$ si $x = \hat{x}$, et $E_1 = 0$ si $x \neq \hat{x}$
- $E_2 = 1$ si $E_1 = 1$ et $y = \hat{y}$; $E_2 = 0$ sinon. **(3.15)**

- $E_3 = 1$ si $E_1 = 1$ et $E_2 = 1$ et $z = \hat{z}$; $E_3 = 0$ sinon.

Les paramètres de synthèse λ_i, i = 1, 2, 3 sont des réels positifs pour assurer la convergence de l'observateur. On démontre **[16]** sous l'hypothèse de la bornitude des états et du message, qu'on peut choisir ces paramètres pour assurer la convergence en temps finie des variables d'état estimées vers les variables d'état réelles et du message estimé vers le message transmis. La démonstration repose sur une construction étape par étape de la méthode de **Lyapunov**. Notons aussi que ce la méthode des modes glissant utilisée est d'ordre un. Le choix des paramètres(λ_i) doit d'un côté assurer une convergence rapide mais d'un autre côté éviter d'introduire un chaterring important. Nous avons essayé de satisfaire ce dilemme en remplaçant la fonction discontinue (***signe)*** par une signoïde qui est la fonction (**tangente hyperbolique)**. Il est clair que l'utilisation de cette fonction réduit la précision de la méthode des modes glissant et diminue la robustesse ; L'utilisation des modes glissants d'ordre deux (supertwisting) donnerait des résultats nettement meilleurs.

3.6 Résultats de simulation

Nous avons considéré pour le message à transmettre, un signal sinusoïdal d'amplitude (0.5) et de pulsation (1rad/s), (Figure 3.11).

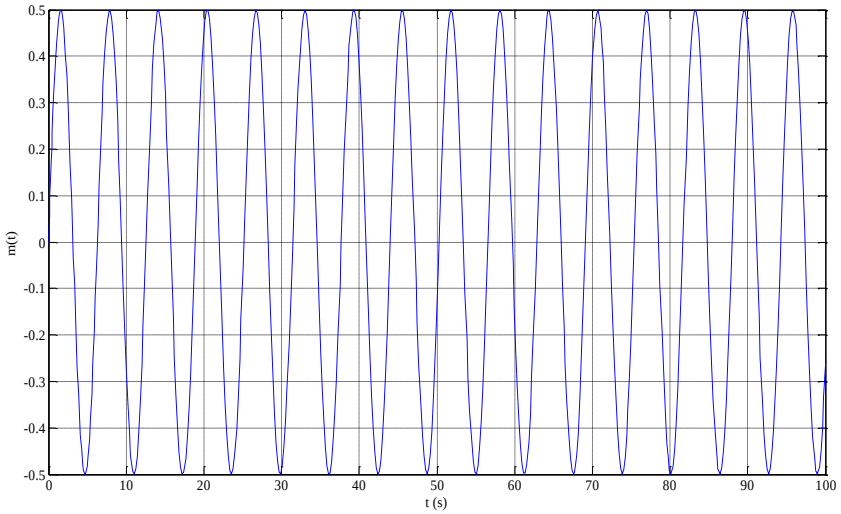


Fig. 3.11 Message *m*(t) transmis

Les conditions initiales pour l'émetteur sont $(x(0), y(0), z(0)) = (0.5, -0.1, 0.1)$ et les conditions initiales pour le récepteur sont prises toutes égales à (0). Les coefficients des surfaces de glissement sont ajustés tous à la valeur $\lambda_1 = \lambda_2 = \lambda_3 = 3.5$, Sur les courbes (3.12)-(3.14) sont portées les réponses temporelles des variables d'état (*x*, *y*, *z*) et de leurs estimées. Nous constatons que le récepteur est bien synchronisé avec l'émetteur car les variables d'état estimées convergent rapidement vers les variables réelles.

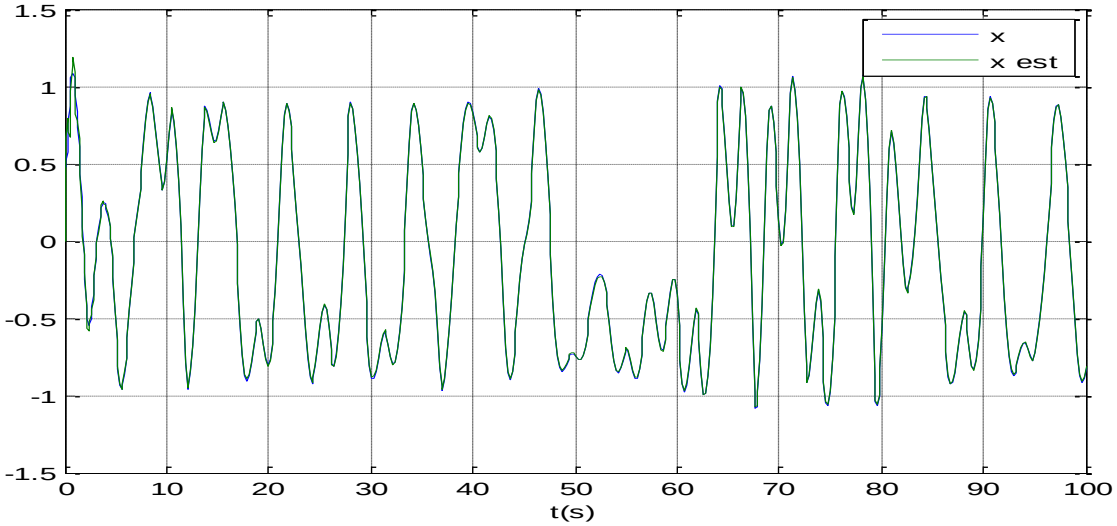


Fig. 3.12 Etat x et son estimé $\hat{x}$

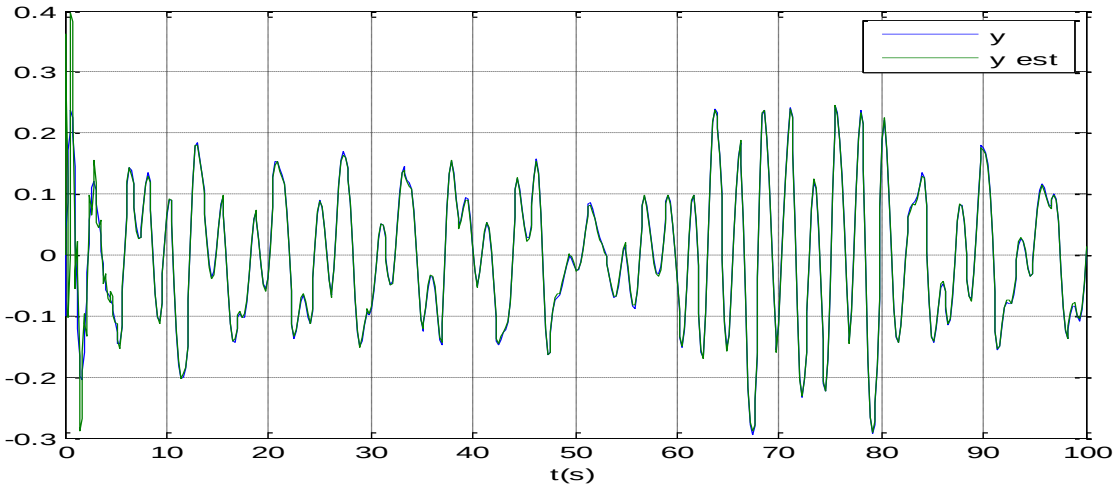


Fig. 3.13 Etat y et son estimé $\hat{y}$

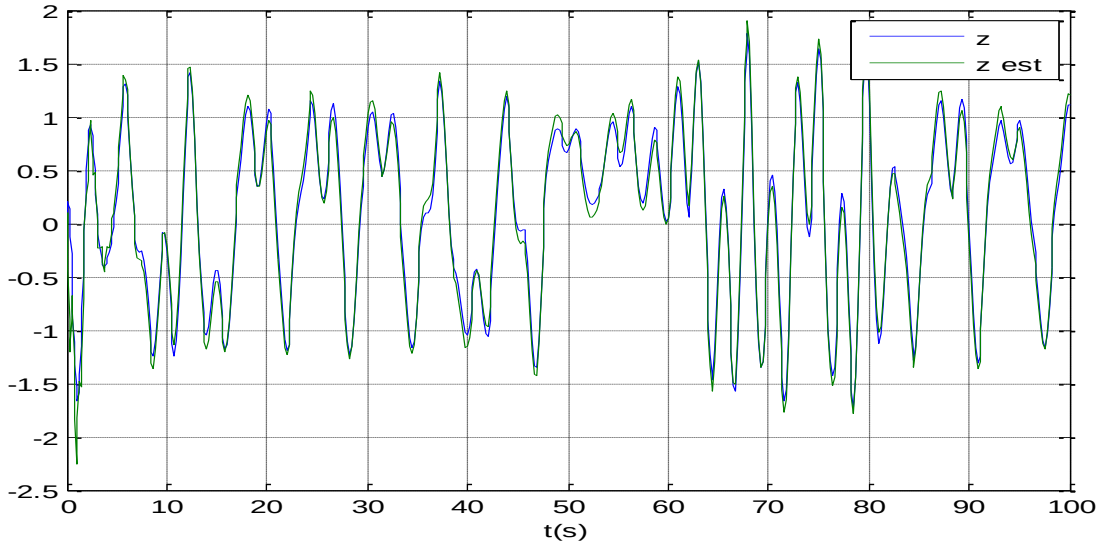


Fig. 3.14 Etat z et son estimé $\hat{z}$

La figure (3.15) illustre le message transmis et le message estimé. Le message transmis est plus ou moins récupéré avec des imperfections. Nous avons aussi tracé dans le plan (m, m estim) le message récupéré en fonction du message transmis, Figure (3.16) et la figure (3.17) donne l'évolution de l'erreur d'estimation sur le message. Ces courbes montrent bien qu'après un certain instant, les deux messages sont presque identiques néanmoins avec là aussi des imperfections. Nous avons essayé d'augmenter les paramètres (λ_i) afin d'améliorer la précision, cependant, nous avons constaté beaucoup de chattering comme le montre la figure (3.18) pour $\lambda_i = 10$. La diminution des (λ_i) introduit un écart important entre le message transmis et le message récupéré comme le montre la figure (3.19) pour $\lambda_i = 2.5$.

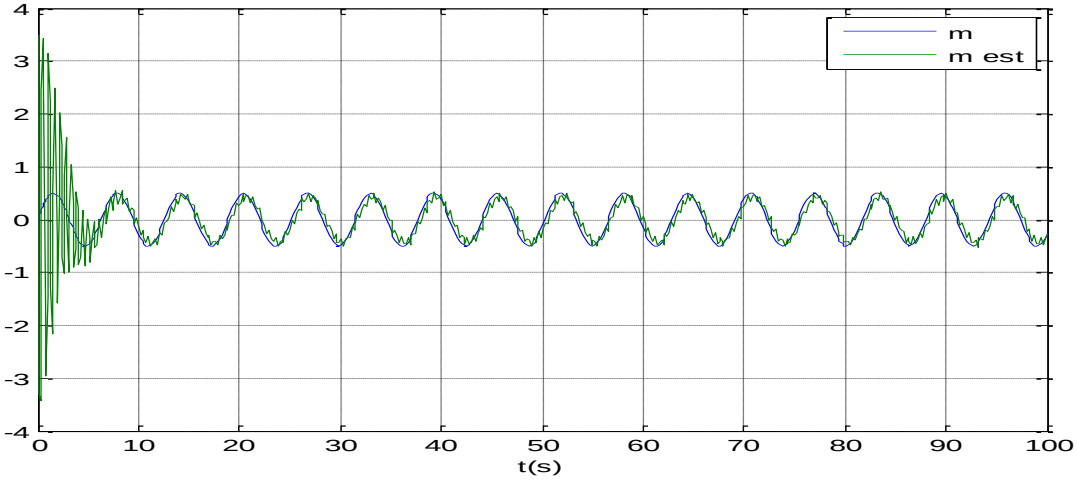


Fig. 3.15 Message m et son estimé $\hat{m}$

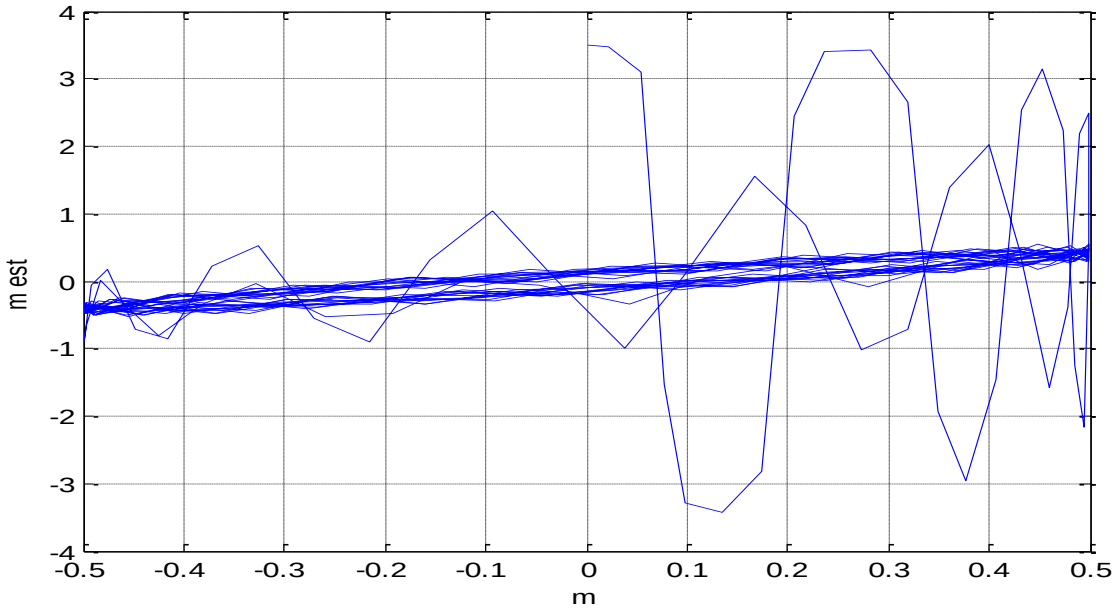


Fig. 3.16 Message m et son estimé $\hat{m}$

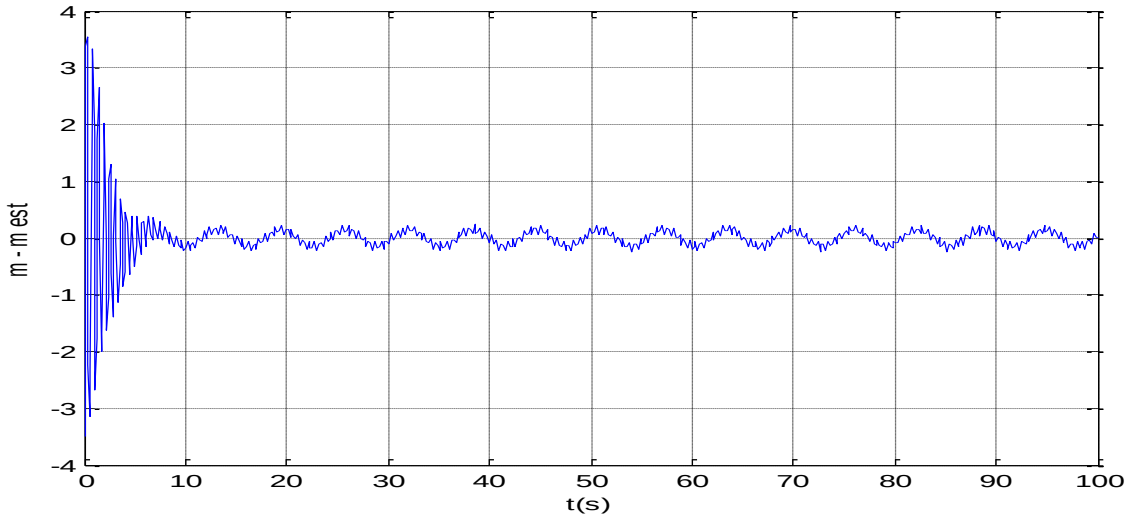


Fig. 3.17 Erreur d'estimation sur le message

Valeur prise : $\lambda = 10$

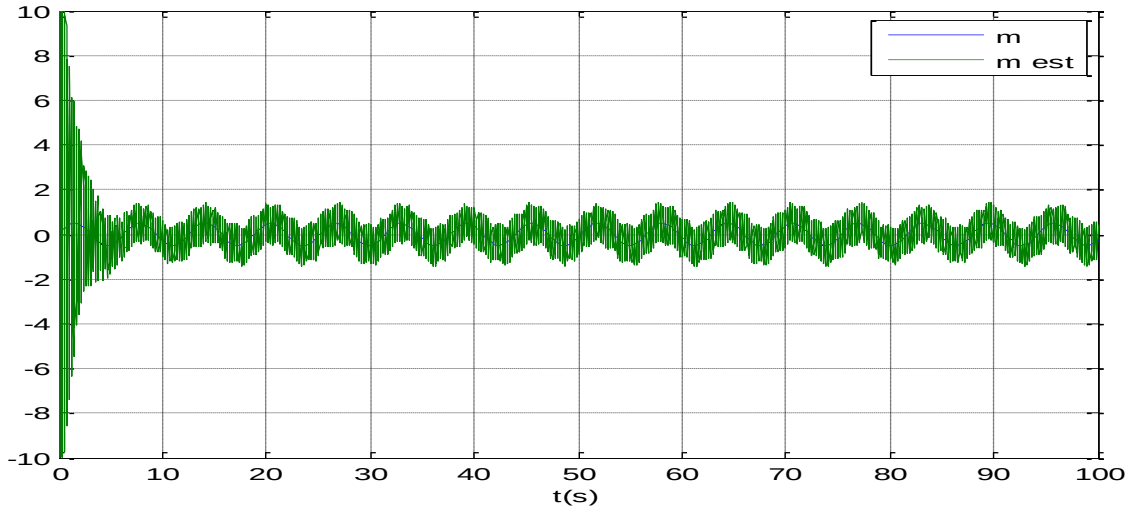


Fig. 3.18 Evolution du message et son estimé

Ici $\lambda = 2.5$ (Chattering diminué)

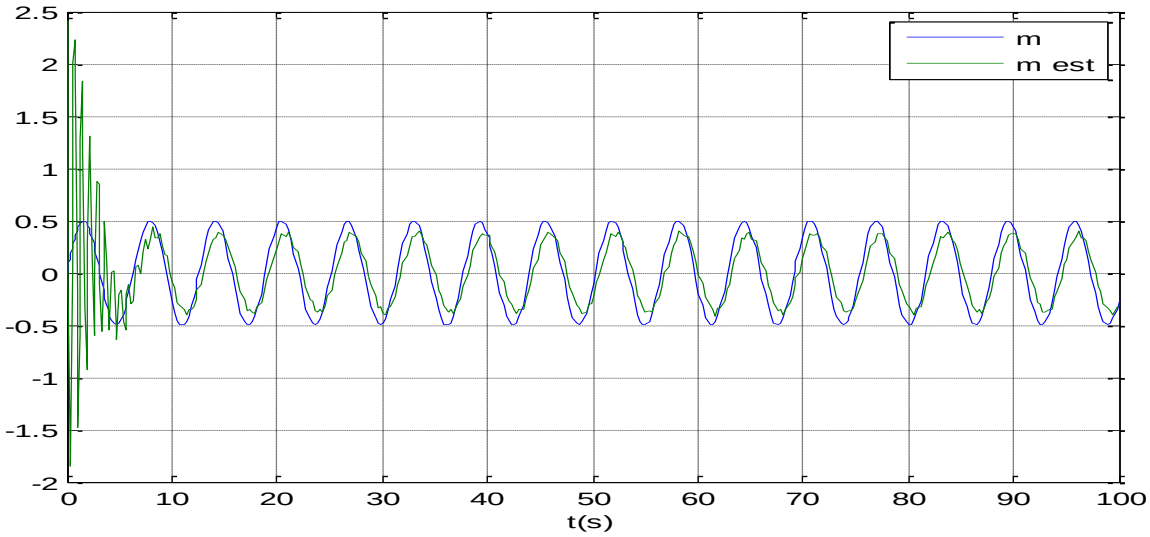


Fig. 3.19 Evolution du message et son estimé

- **Analyse de la robustesse**

Pour assurer une meilleure sécurisation de la transmission contre d'éventuels pirates, il faut qu'une légère modification des paramètres de l'observateur implique la perte du message. Nous avons procédé au test suivant. Dans la figure (3.20) nous traçons le message transmis et le message récupéré lorsque au niveau de l'observateur la valeur de (α) est prise égale à 12.5 au lieu de 9.5, Nous remarquons que le message n'est bien récupéré. Ceci montre bien l'intérêt d'utiliser les systèmes chaotique dans les dispositifs de transmission de données. Le changement des valeurs d'autres paramètres à la fois entrainerait inévitablement toute la perte du message.

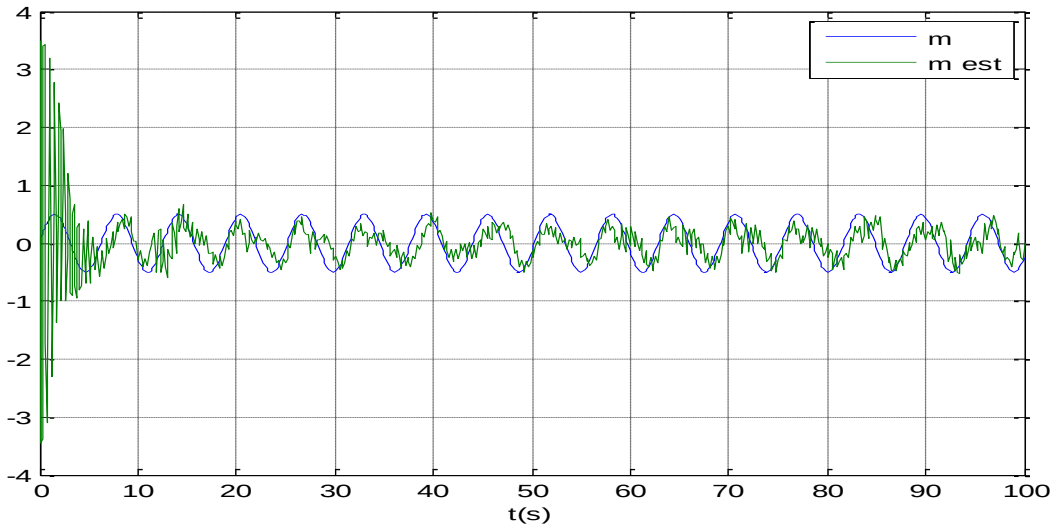


Fig. 3.20 Evolution du message transmis et le message récupéré

3.7 Conclusion

Ce chapitre avait comme objectif principal la synchronisation de deux circuits de Chua par observateur à mode glissant. Nous avons présenté le modèle de Chua modifié et étudié son comportement chaotique obtenue pour certaines valeurs des paramètres. Ensuite, nous avons construit l'observateur à mode glissant étape par étape à entrée inconnue. L'insertion de système chaotique dans un dispositif de transmission sécurisée de donnée a été illustrée par le circuit de **Chua**. Après avoir testé la convergence de l'observateur, nous avons montré que le message transmis considéré comme l'entrée inconnue est bien récupéré pour un choix adéquat des paramètres de l'observateur. Néanmoins, les résultats ne sont pas parfaits et le compromis entre la précision de l'estimation du message et l'importance du chattering (qualité du message récupéré) est difficile à satisfaire même avec l'utilisation de la fonction (**sigmoide**) à la place de la fonction (**signe**). L'amélioration des résultats nécessiterait, à notre avis, soit l'ajout de filtre ou bien l'utilisation de la technique des modes glissant du second ordre.

Conclusion générale

Conclusion générale

L'objectif de ce travail de mémoire était l'étude des observateurs et la transmission sécurisée par l'effet du chaos.

Afin de bien situer le travail, un état de l'art à été proposé dans le premier chapitre. Il s'articule autour des systèmes chaotiques, et les observateurs non linéaires, Le deuxième chapitre avait comme objectif d'élaborer quelques notions de base sur la synchronisation de systèmes chaotiques à base d'observateur à mode glissant en a rappeler les différents aspects fondamentaux et application à la transmission sécurisée de donnée.

Dans le troisième chapitre, nous avons présenté tous les résultats de simulations, pour cela nous avons choisi un circuit simple et bien connu de « **Chua** ».

On peut conclure que :

- L'observateur à mode glissant converge étape par étape et les erreurs de synchronisation tendent vers zéro en temps fini.
- Les crypto-systèmes proposés avec la technique de cryptage exploitent au mieux les propriétés fondamentales des systèmes chaotiques, et le principe de leur synchronisation. Les résultats de sécurité ont montré que la technique de cryptage par inclusion présente une bonne sécurité.
- Le chattering apporte des erreurs dans la récupération du message reconstruit.

Le problème de la synthèse et de la cryptanalyse des schémas de chiffrement restera toujours un problème ouvert. Les technologies informatiques (ressources mémoires, processeur,…) évoluant constamment, elles permettent une analyse plus poussée de la robustesse des schémas de chiffrement et obligent donc de concevoir des schémas de plus en plus sophistiqués. Les perspectives de ce travail sont :

- Etude de la possibilité d'utilisation d'un observateur à mode glissant d'ordre supérieur afin de diminuer l'effet du chattering.
- Utilisation d'une modulation-démodulation de fréquence entre l'émetteur et le récepteur afin d'éviter en partie les problèmes posés par le canal de transmission (le bruit)
- L'utilisation d'un filtre passe bas serait une solution pour remédier au phénomène de chattering.
- Ce travail ouvre la voie à d'autres développements qui restent ouverts notamment en ce qui concerne la synthèse d'observateur.

Références bibliographiques

Références bibliographiques

[1] L. Kocarev et S. Lian, *Chaos-Based Cryptography: Theory, Algorithms and Applications,* Springer, 2011.
[2] T. Kapitaniak, *Chaos for Engineers, Theory, Application and Control,* Springer, 2000.
[3] G. Chen, X. Yu, *Chaos Control: Theory and Applications,* Springer, 2003.
[4] E. N. Lorenz, *Deterministic non-periodic flow*, Journal of the Atmospheric Sciences, Vol. 20, no. 2, 1963.
[5] H. Poincaré, *Problème des trois corps*, Acta Math, vol 13, pp. 1–270, 1890.
[6] D. Ruelle et F. Takens, *On the nature of turbulence,* Commun. Math. Phys., vol. 20, pp. 167-192, 1971.
[7] R. E. Kalman et R. S. Bucy, New Results in Linear Filtering and Prediction Theory
[8] D. Luenberger, *Observers for multivariable systems,* IEEE Trans. Auto. Contr., Vol. 11, pp. 190-197, 1966.
[9] A.J. Krener and A. Isidori, *Linearisation by output injection and nonlinear observers,* Systems and Control Letters, vol. 3, pp. 47–52, 1983.
[10] M.Fliess et I Kupka, *A finiteness criterion for nonlinear input-output differential systems.* SIAM J. Control Optim, Vol. 21, pp. 721-728, 1983.
[11] A.J. Krener et W. Respondek , *A nonlinear observer with linearizable error dynamics*. SIAM J. Control Optim, 30 : 1985, 197-216.
[12] M. Zeitz, *The extended Luenbeger observer for nonlinear systems*, Syst. And Contr. Letters, Vol. 9, pp. 149-156, 1987.
[13] A. H. Jazwinski . *Filtering for nonlinear dynamical systems.* IEEE Trans. Auto. Contr., Vol. 11, pp. 765-766, 1966.
[14] B. Bonnard and H. Hammouri, *A high gain observer for a class of uniformaly observable systems*, 30 th IEEE Conference on Decision and Control CDC'91, Brighton ,UK, 1991.
[15] A. Isidori, *Nonlinear control systems*, Springer, 1995.
[16]W. Perruquetti et J.P . Barbot, *Sliding mode control in engeneering* , Edition Marcel Deeker , New York, 2002.
[17] B. L Walcott et S. H Zak , *State observation of nonlinear uncertain dynamical systems.* IEEE Trans. Auto. Contr. Vol. 32 , pp . 166-170, 1987.
[18] L. Kocarev, *Chaos-based cryptography*, Springer, 2011.
[19] W. Stallings, *Cryptography and Network security*, Prentice Hall, 2011.
[20] H. Hamiche, *Inversion à gauche des systèmes dynamiques hybrides chaotiques : Application à la transmission sécurisée de données*, Thèse de Doctorat, UMMTO, 2011.
[21] G. Kaddoum, *Contribution à l'amélioration des systèmes de communication multiutilisateurs par chaos : synchronisation et analyse des performances,* Thèse de Doctorat, Université Paul Sabatier de Toulouse, 2008.
[22] L. M Pecora et T. L. Carrol, *Synchronization in chaotic systems,* Physical Review Letters, Vol.64, pp. 821-824, 1990.
[23] M. L'Hernault, J. De Leon, J. P. Barbot et A. Ouslimani, *Comparaison d'un observateur à modes glissants et un observateur adapatatif pour la synchronisation de systèmes chaotiques,* téléchargeable sur http://www.nonlineaire.univ-lille.fr/SNL/media/2006LCR/Lhenault.pdf
[24] N. Djeghali, *Observation, diagnostic et commande de la machine asynchrone, Thèse de Doctorat,* UMMTO, 2013.