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

Université Mouloud Mammeri De Tizi-Ouzou

Faculté De Génie Electrique Et D'Informatique
DEPARTEMENT D'Automatique

Mémoire de Fin d'Etude
de MASTER ACADEMIQUE
Spécialité : **Automatique**

Présenté par
Fatiha Doudjedid
Kamelia Berrouche

Mémoire dirigé par **Hamid Hamiche** et co-dirigé par **Saïd Djennoune**

Thème

Transmission sécurisée de données à base de systèmes chaotiques

Mémoire soutenu publiquement le 21/09/2014 devant le jury composé de :

M Kara Redouane
Maître de conférence classe A, UMMTO, Président

M Ahmed Maidi
Maître de conférence classe A, UMMTO, Examinateur

M^elle^ Ouerdia Megherbi
Magister, UMMTO, invité

Remerciements

Tout d'abord, nous tenons à exprimer toutes notre gratitude à ***Mr****.* ***DJENNOUNE*** *pour avoir proposé ce thème ainsi à* ***Mr****.* ***HAMICHE*** *pour accepter de nous encadrer.*

Nous les remercions pour leurs qualités de ses conseils, leurs disponibilités, leurs patiences et leurs aides tout au long de notre travail.

Nous remercions très sincèrement ***Mm. MEGHARBI OUERDIA*** *pour sont aide prestigieuse qui a contribué à la réalisation de ce modeste travail*

Nous exprimons notre remerciement à tous ceux qui ont contribué de prés ou de loin à l'élaboration de ce modeste travail.

Nous tenons aussi à remercier tout nos professeurs qui nous ont enseignés durant tout notre cursus d'étude qui nous ont enrichis de connaissances et de savoir qui nous guiderons vers un meilleur avenir professionnel qui soit.

Dédicaces

Je dédie ce modeste travail :

A mes très chers parents qui ont toujours été à mes côtés pour me soutenir, m'encourager, me conseiller et veiller à mettre tout à ma disposition pour pouvoir étudier dans les meilleures conditions possibles.

A mes frères, mes sœurs, ainsi M. Ali et a toute sa famille.

A tous mes amis qui seront se reconnaitre.

D. Fatiha

Dédicaces

Je dédie ce modeste travail :

A mes très chers parents qui ont toujours été à mes côtés pour me soutenir, m'encourager, me conseiller et veiller à mettre tout à ma disposition pour pouvoir étudier dans les meilleures conditions possibles.

A mon frère, mes deux sœurs, ma belle sœur et beau frère ainsi qu'à mes deux petits neveux Axel et Alicia.

A tous mes amis qui seront se reconnaitre.

B. kamelia

Sommaire

Liste des figures

Chapitre 3 : Synchronisation impulsive des systèmes chaotiques

Chapitre 4 : Application à la transmission sécurisée de données à base d'oscillateurs de Colpitts

Listes des figures

Introduction générale

Le chaos est défini généralement comme un comportement imprévisible particulier d'un système dynamique déterministe non-linéaire. En effet, le comportement chaotique a été considéré comme un phénomène exotique qui peut être seulement d'intérêt mathématique et ne serait jamais rencontré dans la pratique. Cependant, la possibilité de dynamique chaotique a été découverte dans de nombreux systèmes mécaniques, électroniques (oscillateurs chaotiques), physiques (laser), chimiques, biologiques, économiques et même en médecine.

Une des plus importantes des applications de l'ingénierie est la communication sécurisée grâce aux propriétés du comportement aléatoire et sensibilité aux conditions initiales des systèmes chaotiques. La sensibilité aux conditions et de l'imprévisibilité rend les systèmes chaotiques très convenable pour construire la cryptographie.

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

En générale, un « crypto-système » doit considérer plusieurs aspects, tels que l'intégrité des données, l'authentification, confidentialité, et bien d'autres. En effet les techniques de cryptographie classique basée sur la théorie des nombres et en particulier sur la décomposition d'un entier en éléments simples. Nous pouvons aussi citer les deux algorithmes bien connus : DES (Data Encryption Standard), RSA (Rivest Shamir-Adelman). Néanmoins avec la révolution de l'informatique, ces algorithmes proposés ne sont pas assez sécurisés, pour ces raisons, plusieurs chercheurs essayant de mettre en œuvre d'autre « crypto-systèmes » [11].

La synchronisation des systèmes chaotiques est une approche intéressante pour résoudre ce problème. Introduite en 1990 par Pecora et Carroll, Cette technique permet de reconstruire les états de l'émetteur à partir d'un signale transmis. A ce jour, différentes approches de synchronisation ont été proposés et explorées, parmi ces approches on trouve deux méthodes basés sur la notion maitre-esclave qui permettent d'établir la synchronisation et d'améliorer ce processus et de réduire l'erreur entre les états de l'émetteur et de récepteur. Tels que, il existe deux classes de la synchronisation, la synchronisation unidirectionnelle qui considère comme un problème de synthèse d'observateur et la synchronisation bidirectionnelle [2]. Afin d'assurer la synchronisation, on peut donc utiliser différents types d'observateurs non linéaires (Filtre de Kalman étendu, Luenberger étendu, grand gain, modes glissants, ..). Un autre type d'observateur utilisé est l'observateur impulsif. Pour ce type d'observateur, le signal d'injection qui permet de garantir la convergence de l'observateur, se présente comme un train d'impulsions. L'information est envoyée par impulsion à des instants discrets de manière aléatoire. Ce type d'observateur convient bien aux systèmes de

transmission puisqu'il permet de ne pas saturer le canal public et aussi de tenir compte de la disponibilité de routeurs dans un réseau informatique.

Dans ce mémoire notre objectif est l'emploi du chaos pour la transmission sécurisée de l'information, on exploitant d'une part sur les propriétés des systèmes dynamique chaotique, et d'une autre part sur la possibilité de synchronisation par observateur dans le but de la transmission sécurisée, en utilisant l'observateur impulsif pour garantit une bonne performance pour la condition de synchronisation.

Ce travail comporte quatre chapitres

Le premier chapitre est consacré aux généralités et les notions de base sur les systèmes chaotiques.

Dans le deuxième chapitre, nous présentons le principe des systèmes de transmission avec les méthodes de cryptage et décryptage, ainsi les généralités sur la synchronisation des systèmes chaotiques.

Le troisième chapitre est consacré à la synchronisation des systèmes chaotique par la commande impulsive.

Dans le dernier chapitre, nous exposons les résultats de simulation de la synchronisation impulsive de deux oscillateurs de Colpitts. Nous étudions aussi la robustesse du système de transmission face aux bruits, aux variations des paramètres et aux retards.

Enfin, nous terminons ce travail par une conclusion générale récapitulant nos principaux résultats et quelques perspectives.

Chapitre 1 : Généralités sur les Systèmes Chaotiques

1.1 Introduction

Le chaos est un phénomène qui se produit largement dans les systèmes dynamiques. Ce phénomène à été considéré complexe et n'a jamais été donné de l'importance parce qu'il n'y avait aucune analyse simple disponible qui pourrait aider les étudiants et les chercheurs à immerger dans ce phénomène intéressant.

En 1963, le météorologue Edward Lorenz expérimentait une méthode lui permettant de prévoir les phénomènes météorologiques. C'est par hasard qu'il observa qu'une modification minime des données initiales pouvait changer de manière considérable ses résultats. Lorenz venait de découvrir le phénomène de sensibilité aux conditions initiales [1].

Cependant, les travaux de certains scientifiques menés bien avant cette découverte vont être très utile à la compréhension de la dynamique chaotique. En effet le français Henri Poincaré fut l'un des premiers à entrevoir la théorie du chaos [2], qui avait déjà mis en évidence le phénomène de sensibilité aux conditions initiales [1].

Le chaos a aussi trouvé de nombreuses applications dans des déférents domaines. Ainsi, nous nous intéressons dans ce chapitre aux systèmes dynamiques chaotiques, ces caractéristiques, et la route (transition) ver le chaos.

L'objectif de ce chapitre est de donner quelques généralités sur le système chaotique, pour lesquels nous permettront de mieux comprendre le comportement de systèmes chaotique.

1.2 Système Dynamique

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

Un système dynamique est constitué d'un espace des phases, l'espace des états possibles du phénomène convenablement paramétré, muni d'une loi d'évolution qui décrit la variation temporelle de l'état du système.

1.3 Système Chaotique

Un système chaotique est un système complexe, régi par une grande variété de facteurs (comme la météorologie), dépendant de plusieurs paramètres et dont la caractéristique fondamentale est son extrême sensibilité aux conditions initiales.

Le comportement de tels systèmes est imprévisible, bien que leurs composantes soient gouvernées par des lois simples, connues et déterministes. Les méthodes théoriques et

mathématiques sont inadaptées à la prévision de tels systèmes, on en est réduit à tenir compte de la statistique, du seul calcul des probabilités.

1.4 Caractéristiques des systèmes chaotiques

1.4.1 La non-linéarité

Un système chaotique n'est produit que par des systèmes dynamiques non linéaires, par contre un système linéaire ne possède jamais de comportement chaotique.

1.4.2 Le déterminisme

C'est la capacité de prédire le futur d'un phénomène à partir d'un événement passé ou présent.

1.4.3 Sensibilité aux conditions initiales

Cette propriété à été observée pour la première fois par Edward Lorenz sur son modèle météorologique, il a découvert que deux conditions initiales infiniment proches dans l'espace de phase peuvent donner lieu à des évolutions futures qui divergent après un temps fini, cela empêche d'établir des prévisions à long terme du système, ainsi de là découle l'effet papillon : un événement en apparence insignifiant engendre une réaction en chaîne qui à terme donne un résultat totalement imprévisible [3].

- **Exemple de Lorenz** :

Cette sensibilité aux conditions initiales sera illustrée par le système de Lorenz régi par les équations différentielles suivantes :

$$\begin{cases} \dot{x} = \sigma(y - x) \\ \dot{y} = x(\gamma - z) - y \\ \dot{z} = xy - \beta z \end{cases} \qquad (1.1)$$

Les paramètres étant fixés aux valeurs suivantes : σ=10, γ=28, β=8/3.

La figure (1.1) représente deux trajectoires de l'état z avec une différence de 0.01% sur la troisième composante de l'état initial.

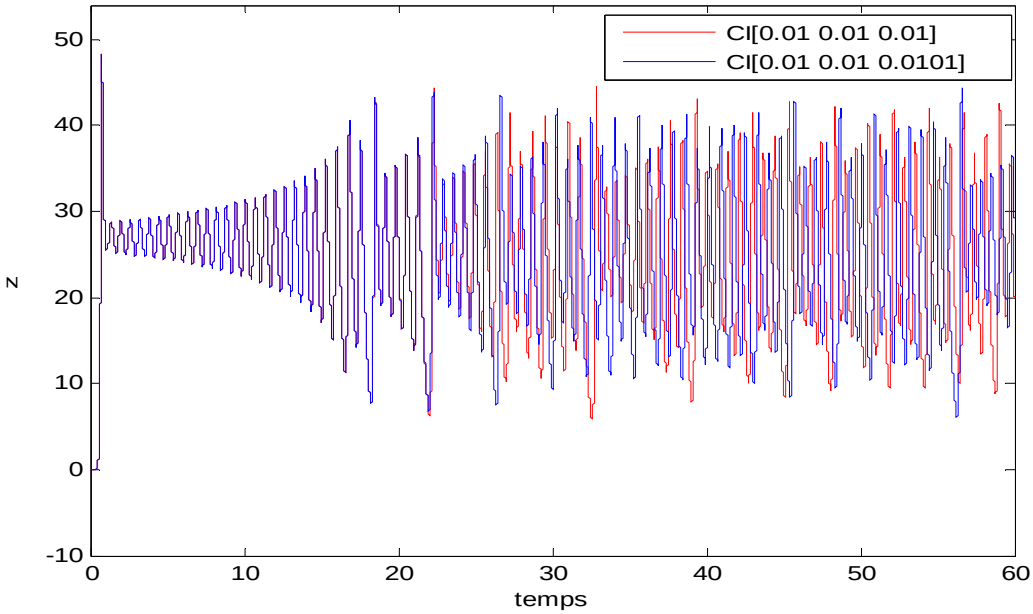
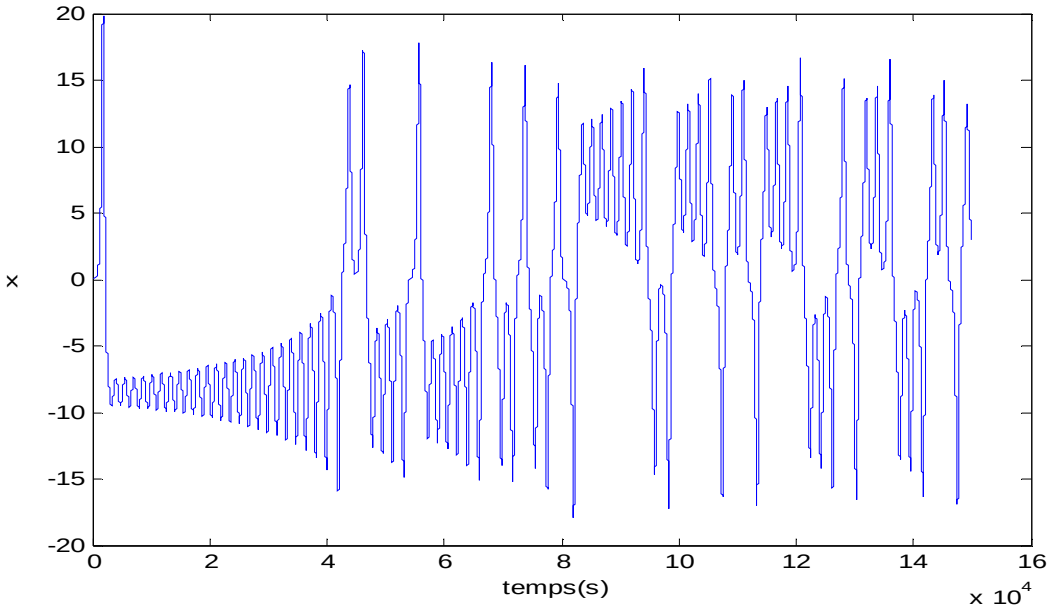


Fig1.1 : Sensibilité aux conditions initiales

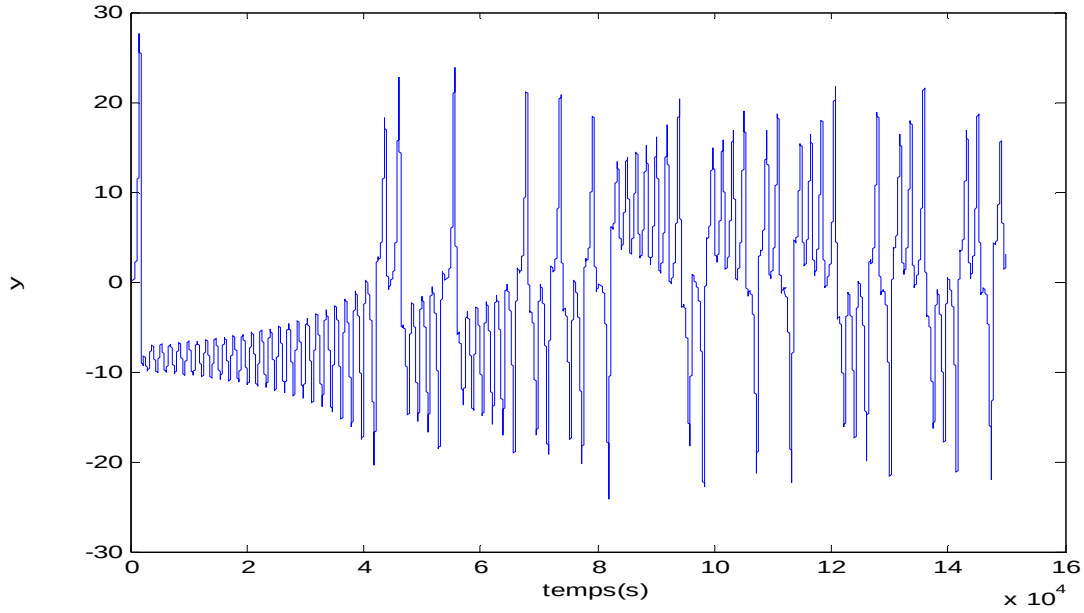
1.4.4 Le caractère pseudo aléatoire

Tous les états d'un système chaotique présentent des aspects aléatoires

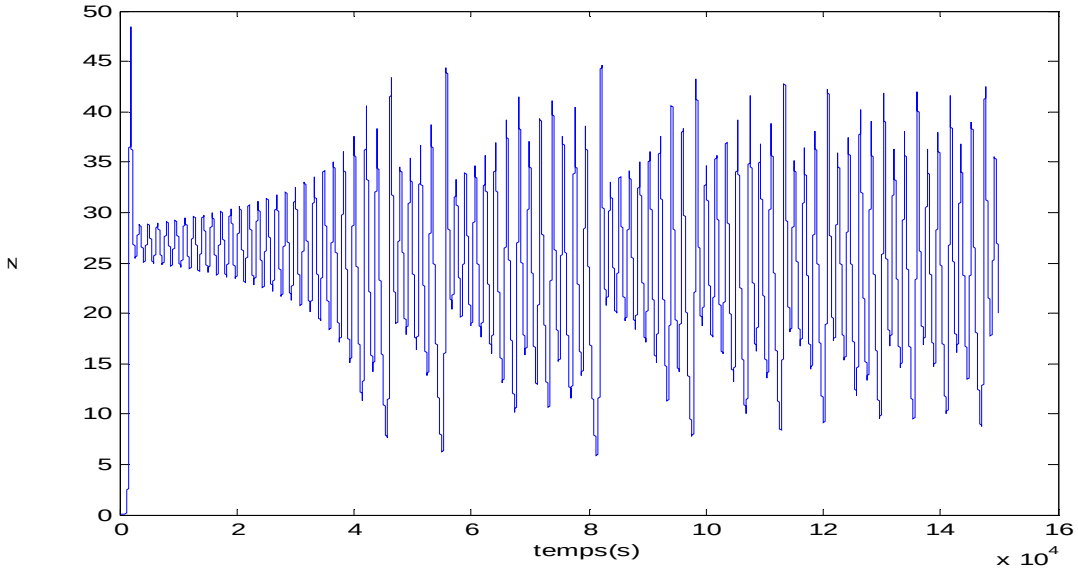
La figure (1.2) illustre l'aspect aléatoire des états du système de Lorenz.



a- Etat x du système de Lorenz



b- Etat *y* du système de Lorenz



c- Etat *z* du système de Lorenz

Fig1.2 : Aspects aléatoires des états du système de Lorenz

1.4.5 Attracteur étrange

Un attracteur est un objet géométrique vers le lequel tendent toutes les trajectoires des points de l'espace des phases.

Jusqu'en 1963 il ne fut connaissance que de trois types d'attracteurs: le point fixe, le cycle limite et le tore. Dans un système élémentaire, l'attracteur est représenté par un point fixe : l'exemple en est le pendule simple qui oscille en spirale en perdant de l'énergie et qui finit par s'arrêter sur un point final appelé « point fixe ». Ce point constitue un attracteur ponctuel.

D'autres systèmes ont une évolution cyclique est périodique, comme le pendule d'une horloge dont les oscillations sont entretenues. Dans ce cas, l'ensemble des trajectoires tendent vers un cycle, cette attracteur est appelé cycle limite.

On à aussi l'attracteur torique, dont la surface est en forme de chambre à air et qui représente les mouvements résultant de deux oscillations indépendantes dont les trajectoires s'enroulent autour d'un tore.

Ces trois formes d'attracteurs non chaotiques constituent des systèmes qu'on dit « prédictibles » car bien que leurs mouvements soient complexes, ils sont néanmoins prévisibles à long terme. C'est sur telles bases que des prédictions sont faites à l'avance des heures des marées et des éclipses dont l'arrivée dépend pourtant de plusieurs mouvements périodiques.

Dans le cas des systèmes plus complexes dont l'évolution est « imprédictible », l'état du système est alors représenté à chaque instant par un point dans cet espace appelé ″espace des phases″.

Ce point est attiré vers une courbe limite. Près de laquelle, il repasse régulièrement, les mathématiciens appellent ces courbes des ″attracteurs étranges″, ces derniers présentent une caractéristique bien particulière, une symétrie interne de sorte que si l'on procède à un zoom avant ou arrière, c'est toujours la même structure que l'on retrouve, donc il existe une formation préférentielle aux systèmes chaotiques, un ordre sous-jacent au désordre, les courbes fractales développées en premier par le mathématicien Benoit Mandelbrot sont des attracteurs étranges.

Un attracteur étrange est caractérisé par :

1- Un volume nul.
2- Une séparation exponentiellement rapide de trajectoire initialement proche.
3- Une dimension souvent fractale (non entière).

La naissance de cet attracteur est liée à l'existence de deux processus, à savoir l'étirement, responsable de l'instabilité et de la sensibilité aux conditions initiales, et le repliement, responsable du côté étrange, fractal de l'attracteur [4].

La figure (1.3) suivante illustre l'attracteur étrange de Lorenz.

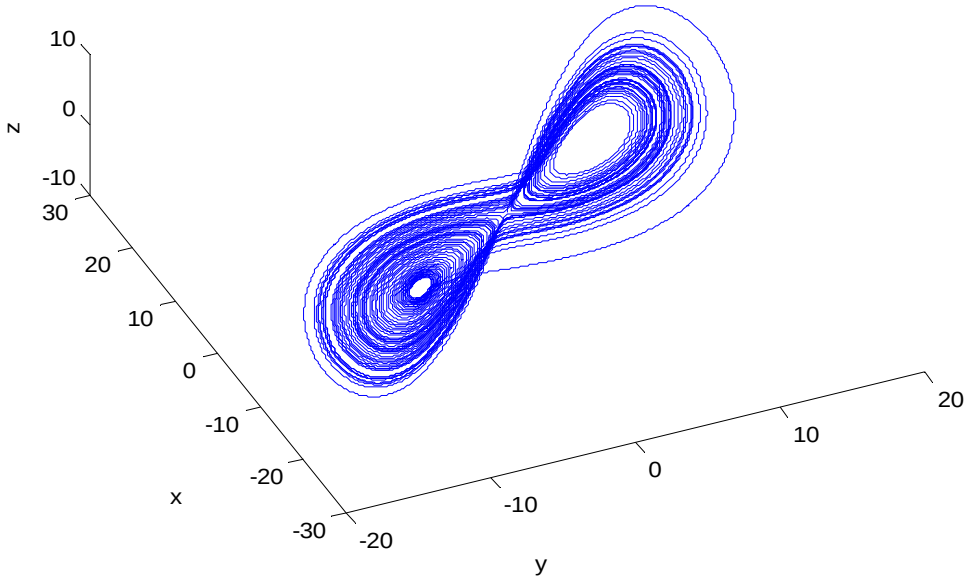


Fig1.3 : Attracteur de Lorenz

❖ **Exemple de Rossler**

Nous illustrons un autre exemple d'attracteur qui est celui de Rössler, régi par les équations différentielles suivantes :

$$\begin{cases} \dot{x} = -(y+z) \\ \dot{y} = x + ay + 0.01x\ln(z) \\ \dot{z} = c + z(x-b) \end{cases} \qquad (1.2)$$

Avec (x,y,z) est le vecteur d'état et a, b, c sont les paramètres du système
Se système montre un comportement chaotique pour les valeurs suivants
a=0.2, b=5.7, c=0.2 avec les conditions initiales$x(0) = 0.01, y(0) = 0.01, z(0) = 0.01$.

La figure (1.4) suivante illustre attracteur étrange de Rössler.

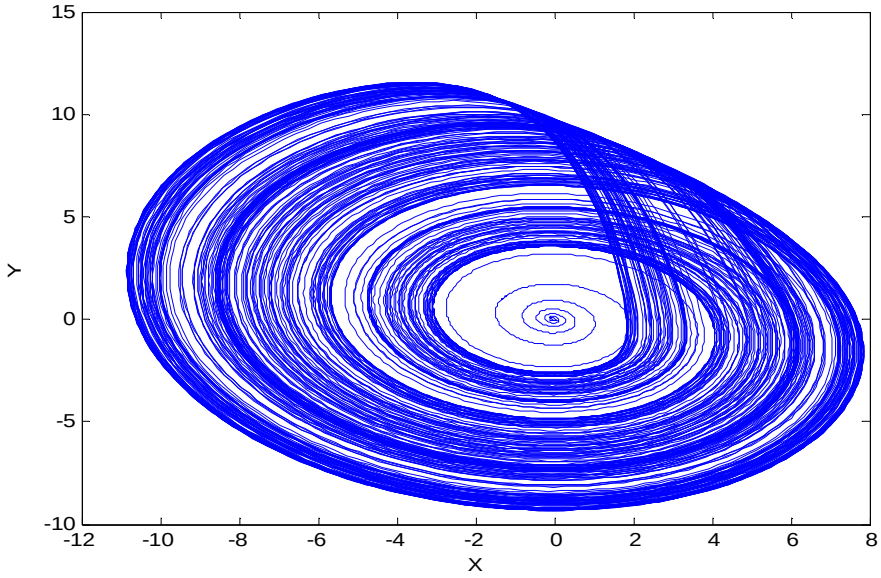


Fig1.4 : Attracteur de Rossler

1.4.6 Les exposants de Lyapunov

Les exposants de Lyapunov permettent de mesurer les taux de séparation exponentielle des trajectoires voisines, en partant de la caractérisation de la sensibilité aux conditions initiales d'un système dynamique.

Un exposant de Lyapunov positif est la signature d'une sensibilité extrême aux conditions initiales et d'une divergence exponentielle des trajectoires [5].

Pour un attracteur non chaotique, les exposants de Lyapunov sont tous inférieur ou égaux à zéro et leurs sommes est négative. Cependant, un attracteur étrange possède au moins trois exposants de Lyapunov, dont un au moins doit être positif.

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

Tableau : classification des régimes permanents en fonction du spectre Lyapunov.

1.5 Bifurcation

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

Une bifurcation survient lorsqu'une variation quantitative d'un paramètre du système engendre un changement qualitatif des propriétés d'un système telles que la stabilité, le nombre de points d'équilibre ou la nature des régimes permanents. Les valeurs des paramètres au moment du changement sont appelées valeurs de bifurcation [2].

La figure suivante illustre le diagramme de bifurcation pour la fonction logistique

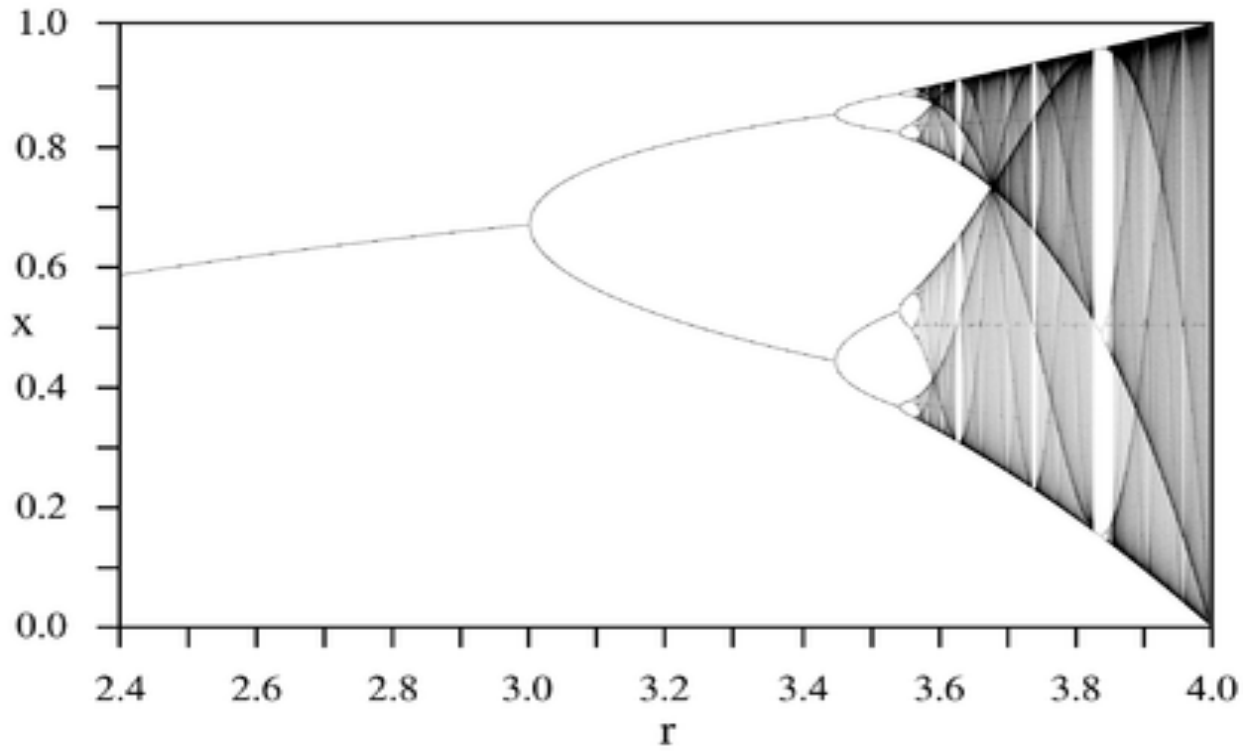


Fig1.5 : Diagramme de bifurcation de la fonction logistique

Ce diagramme permet de connaître tous les comportements de la suite logistique en fonction de r.

Pour r=3 on observe un doublement de période appelé ici bifurcation.

Avant de basculer dans le chaos il y a une cascade de doublement de période. Après un doublement de période l'orbite périodique précédent est toujours présente mais instable, ce qui explique qu'elle n'est pas visible sur le diagramme de bifurcation, un système chaotique a donc une infinité d'orbites périodiques.

1.6 Transition vers le chaos

On peut identifier le chaos par sa manière d'entrer en scène :

1.6.1 Le doublement de période

Ce phénomène se manifeste sur un oscillateur forcé, à mesure que la contrainte augmente, la période de l'oscillateur est multipliée par deux, puis par quatre, par huit, etc. Ces doublements de périodes sont de plus en plus rapprochés, lorsque la période est infinie, le système est chaotique [6].

1.6.2 L'intermittence

Ce scénario est caractérisé par un mouvement périodique stable entrecoupé par des mouvements chaotiques qui apparaissent de manière irrégulière.

Le système conserve pendant un certain laps de temps un régime périodique ou pratiquement quasi-périodique, c'est-à-dire une certaine « régularité », et il se déstabilise, brutalement, pour donner lieu à un comportement chaotique. Il stabilise de nouveau, pour donner lieu à une autre « explosion chaotique » plus tard [2].

1.6.3 La quasi-périodicité

Ce phénomène intervient quand un deuxième oscillateur perturbe un système initialement périodique. Si le rapport des périodes des deux oscillateurs en présence n'est pas rationnel, alors le système est dit quasi-périodique. L'influence des deux oscillateurs l'un sur l'autre conduit à un dérèglement de leur mouvement [6].

1.7 Conclusion

Dans ce chapitre nous avons présenté quelques généralités sur les systèmes chaotiques. Nous avons d'abord défini les systèmes chaotiques ; puis nous avons expliqué, en donnant chaque fois des exemples, leurs propriétés. Nous avons aussi présenté la bifurcation ensuite, cité les différentes situations pour qu'un système présente un comportement chaotique.

Dans le chapitre qui suit nous entamerons la cryptographie chaotique qui est une application intéressante des systèmes chaotiques. Il s'agit d'utiliser les propriétés du chaos pour assurer une transmission sécurisée de données.

Chapitre 2 : Transmission sécurisée de données à base d'oscillateurs chaotiques

2.1 Introduction

La nouvelle révolution industrielle en informatique et dans les télécommunications a abouti au stockage et à la transmission de grandes quantités de données confidentielles et à un souci croissant d'en protéger l'accès. La cryptologie est un moyen de sauvegarder le caractère confidentiel des informations. Elle ne protège pas les communications mais plutôt leurs contenus. Ils existent plusieurs méthodes de chiffrage qui sont connues depuis des milliers d'années. Mais le mathématicien C.E Shannon a été le premier à fournir ces méthodes de chiffrage.

Dans ce chapitre, nous allons présenter la cryptographie et la cryptanalyse où, nous allons expliquer d'une manière globale le principe de la transmission sécurisée. , Ensuite, nous allons présenter les méthodes de cryptage ainsi le décryptage par le chaos.

2.2 Cryptographie

C'est l'ensemble des processus de verrouillage (sécurité des données) visant à protéger l'accès à certaines données, à garantir la confidentialité et l'intégrité des informations. La cryptographie recouvre les méthodes rendant des informations inaccessibles aux personnes non autorisées. L'émetteur d'une information peut ainsi être certain de l'identité du destinataire et vice versa. La cryptographie repose sur l'emploi de formules mathématiques souvent complexes, ainsi que des algorithmes. Ceux-ci servent à coder des informations qui seront ensuite décodées avec une clé. En utilisant des algorithmes, on verrouille les données, c'est-à-dire qu'on les transforme, ou les inclut dans d'autres données pour les protéger [7].

Il existe deux classes de système de cryptographie :

- Les systèmes symétriques ou la clé secrète (la même clé est utilisée pour encoder et décoder).
- Les systèmes asymétriques où la clé publique (la clé qui sert à coder est totalement différente de celle utilisée pour le décodage).

2.3 Cryptanalyse

La cryptographie permet de préserver les données confidentielles [8] de l'indiscrétion des attaquants comme les adversaires, espions, décrypteurs, ou les ennemis. A l'inverse, la cryptanalyse est l'étude des probabilités de succès des attaques possible sur les systèmes cryptographiques dans le but de trouver leurs faiblesses.

La figure (2.1) représente le schéma de principe de chiffrage et déchiffrage.

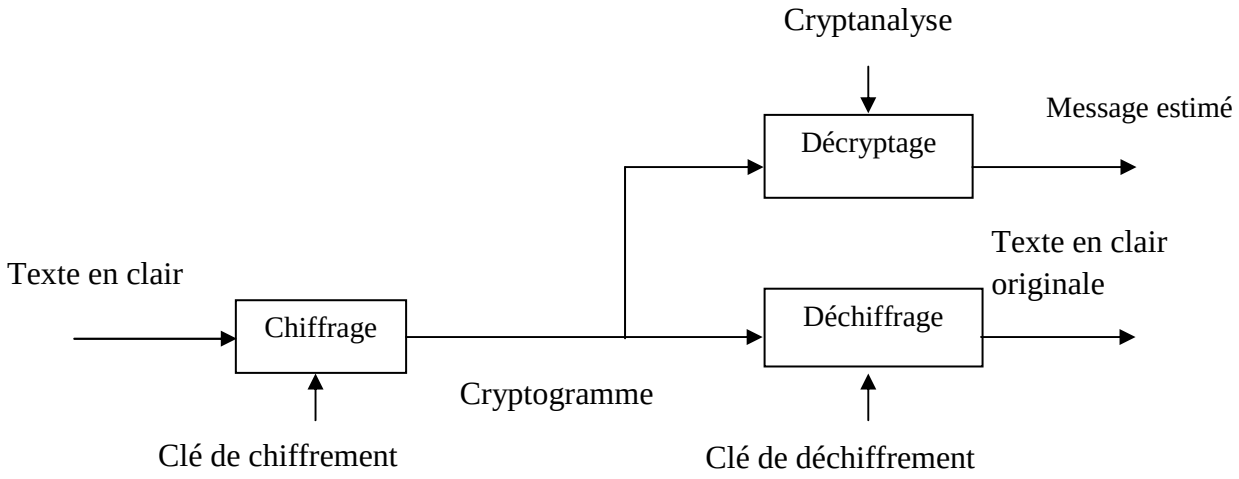


Fig2.1 : Principe de cryptographie et de cryptanalyse

❖ **Remarque**

- La clé de chiffrage : c'est l'opération par laquelle le message est rendu modifié.
- La clé de déchiffrage : la connaissance de la clé permet d'effectuer l'opération inverse, à savoir revenir de l'espace des cryptogrammes à l'espace des messages.
- Le cryptogramme : c'est le message chiffré.
- Clés : série de symboles commandant les opérations de chiffrement et déchiffrement.
- crypter : c'est transformer un texte clair en texte codé. L'opération ou son résultat s'appelle un chiffrement.
- La 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.
- La cryptanalyse (décrypter): le procédé par lequel on déduit le message du cryptogramme lorsque la clé n'est pas connue.
- La cryptologie: une science mathématique qui couvre en même temps la cryptographie et la cryptanalyse [7].

2.4 Généralités sur la synchronisation

A ce jour, différentes forme de synchronisation ont été proposés et explorées. Parmi ces formes, on trouve deux méthode basées sur la notion maitre-esclave qui permet de réaliser la synchronisation, et aussi nous citerons les différents régimes de synchronisation les plus évoqués et étudiés dans le domaine de la synchronisation.

2.4.1 Méthodes de synchronisation

Il existe deux classes de la synchronisation suivant la manière par laquelle les deux systèmes chaotique sont couplés. Supposons qu'ils sont identiques oscillant de façon totalement indépendante. Les deux systèmes finiront par présenter un comportement commun : il est possible de coupler les systèmes chaotiques dans un sens (couplage unidirectionnel) Ou dans les deux sens (couplage bidirectionnel). Dans le cas d'une synchronisation unidirectionnelle, le couplage entre les deux systèmes chaotiques identiques est réalisé à l'aide d'un élément fonctionnant dans un seul sens, comme par exemple un suiveur. Par contre, dans le cas de la synchronisation bidirectionnelle, le couplage entre les deux systèmes identiques est réalisé à l'aide d'un élément permettant l'échange d'énergie dans les deux sens, ceci peut être obtenu par exemple en utilisant une simple résistance [2].

Les deux méthodes de synchronisation expliquées sont basées sur l'utilisation de systèmes identiques. Toutefois, ceci n'est pas toujours réalisable en pratique. Un petit écart peut jouer sur les comportements des deux circuits et détériorer le phénomène de synchronisation [10].

2.4.2 Différents régimes de synchronisation

Plusieurs régimes de synchronisation ont été proposés dans la littérature, parmi lesquels nous citerons les plus évoqués et étudiés dans le domaine de la synchronisation.

2.4.2.1 Synchronisation généralisée

Cette méthode de synchronisation correspond à une généralisation du concept de synchronisation identique. On considère deux systèmes dynamiques tels que :

$$\dot{x}(t) = f(x(t)) \qquad (2.1)$$

et

$$\dot{\acute{x}}(t) = \acute{f}(\acute{x}(t)) \qquad (2.2)$$

Alors, les deux systèmes (2.1) et (2.2) sont synchronisés, s'il existe une transformation M telle que :

$$lim_{t\to\infty}\|\dot{x}(t) - M(x(t))\| = 0 \qquad (2.3)$$

Avec $x(t)$ est l'état du système émetteur et $x'(t)$ est l'état du système récepteur.
Et dans ce cas, les conditions initiales sont indépendante et ne sont pas tenues en compte. Si la fonction M est inversible, alors $M^{-1}(\dot{x})$ fournit une estimation de l'état x , par contre si M n'est pas inversible, il est impossible d'estimer x [4]. Ce qui présente un majeur inconvénient pour les techniques de communication utilisant l'état de l'émetteur pour décrypter le message transmis.

2.4.2.2 Synchronisation retardée

Avec cette méthode de synchronisation, l'état du système esclave converge vers l'état décalé dans le temps du système maître [4].

$$lim_{t\to\infty}\|\dot{x}(t) - x(t-\tau)\| = 0 \qquad (2.4)$$

Où τ est un retard positif.

2.4.2.3 Synchronisation en boucle fermée

Une autre technique de synchronisation est basée sur la boucle fermée (technique basée sur un bouclage par contre réaction) qui est illustré dans la figure (2.3) où nous utilisons l'erreur entre l'émetteur et le récepteur afin de réaliser la synchronisation [11]. L'idée de cette technique est d'appliquer une correction au système en fonction de l'erreur entre le signal transmis par le premier système (maître) et le signal généré par l'autre système (esclave).

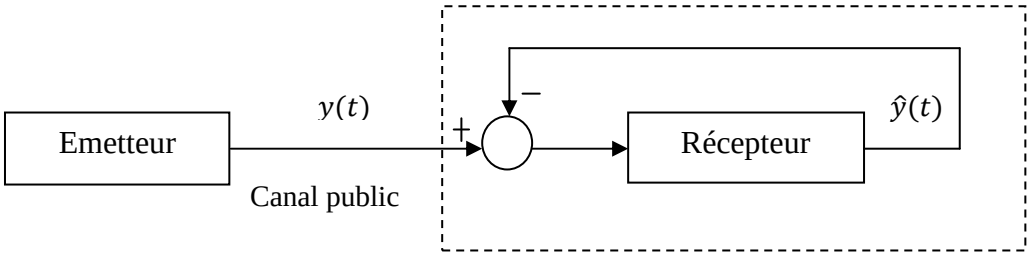


Fig2.2: Synchronisation par boucle fermée

2.4.2.4 Synchronisation projective

Dans cette méthode l'état du système récepteur se synchronise avec un multiple de l'état du système émetteur. Il existe donc α et τ tels que :

$$lim_{t\to\infty}\|\dot{x}(t) - \alpha x(t-\tau)\| = 0 \qquad (2.5)$$

Où α est le facteur d'échelle, $x(t)$ est l'état du système émetteur, $x'(t)$ est l'état du système récepteur et τ est un retard positif.
Ce type de synchronisation est utilisé pour les systèmes partiellement linéaires et permet de synchroniser, à un facteur prés, les états qui ne peuvent être synchronisés [4].

2.4.2.5 Synchronisation de phase

Pour deux systèmes périodiques de phase $\emptyset_1$ et $\emptyset_2$, la synchronisation peut être exprimé par la relation suivante :

$$|n\emptyset_1 - m\emptyset_2| < c \qquad (2.6)$$

Avec m, n sont des entiers naturels et c est une constante positive.
Ce mode de synchronisation permet de définir la phase d'un système chaotique. On peut mentionner le signal analytique et $\psi(t)$ une fonction complexe définie comme suit :

$$\Psi(t) = s(t) + j\tilde{s}(t) = A(t)e^{j\emptyset(t)} \qquad (2.7)$$

Où s(t) est la transformée de Hilbert de la série temporelle s(t), A(t) est l'amplitude du signal $\psi(t)$ et $\emptyset(t)$ sa phase [4].

2.4.3 Synchronisation par observateur

La première approche de synchronisation chaotique a été proposée par Pécora et Carroll, et elle est basée sur la partition du système. Dans cette approche, Le système maître est un système chaotique quelconque et le système esclave est un observateur d'état. D'une manière générale : Un observateur ou reconstructeur d'état est un système dynamique qui permet d'obtenir une estimation de la valeur courante de l'état non mesuré d'un système à partir de ses entrées et sorties ainsi de la connaissance de son modèle dynamique qui sont les seuls informations disponibles. Théoriquement, le problème de la conception d'un observateur pour un système (non linéaire) est défini comme suit :

$$\|x(t) - \hat{x}(t)\| \to 0 \quad \text{Quand} \quad t \to \infty \qquad (2.8)$$

Où x(t) est l'état du système et $\hat{x}(t)$ est l'état estimé
Ce principe est illustré par la figure (2.4) suivante :

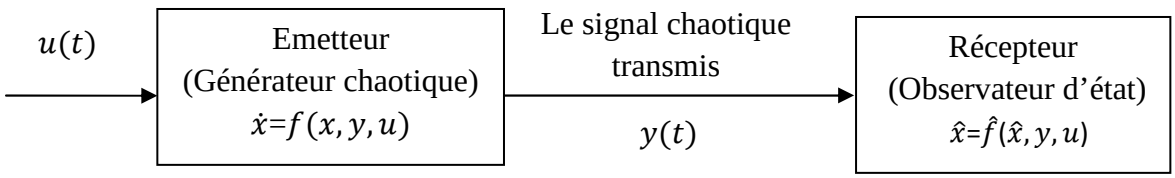


Fig2.3 : Principe de synchronisation à base d'observateurs

La synchronisation peut également être réalisée en employant un observateur. L'observateur est une méthode typique afin d'estimer les états inconnus d'un système dynamique qui ne peuvent pas être mesurés directement : soit inaccessible, soit pas économique.

Notre objectif consiste à concevoir un système de transmission sécurisée en utilisant les systèmes chaotique. L'émetteur est composé d'un système chaotique en temps continu. Au niveau de la réception, un observateur impulsif en temps continu est conçu pour reconstituer les états chaotiques et récupérer le message envoyé.

Une fois que la synchronisation entre le récepteur et l'émetteur est réalisée, il est possible d'utiliser ce phénomène pour transmettre une information m (t). Il existe pour cela plusieurs techniques qui permettent de plus une transmission sécurisée. Il s'agit donc d'une méthode de cryptage basée sur l'utilisation des signaux générés par des systèmes dynamiques.

2.5 Principe de système de transmission sécurisée

La transmission de données concerne toute communication d'un signal électromagnétique, qui transporte l'information sous forme analogique (par des fonctions continues) ou numérique (par une succession de bits 0 et 1).

Un système de communication est constitué globalement des trois éléments principaux : un émetteur, un canal de transmission et un récepteur utilisés pour transmettre une information sur une certaine distance.

L'émetteur : il met en forme une information selon un codage donné, pour 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.

2.5.1 Canal de transmission

On appelle canal de transmission tout milieu physique servant de support au transfert de l'information entre deux points distants, une source et une cible (figure 2.2)

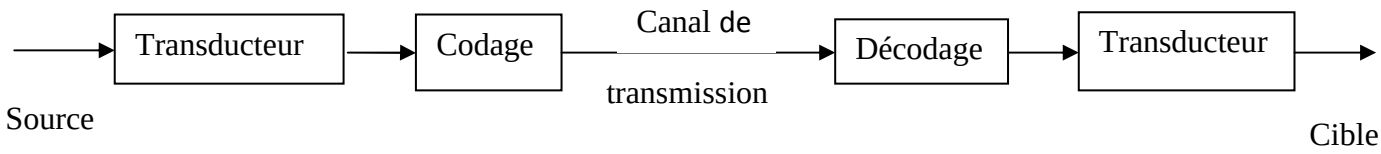


Fig2.4 : Schématisation d'un système de transmission

La transformation de cette information sous forme de signal analogique est effectuée par un transducteur. Le codage est une opération destinée à harmoniser le transfert entre la source et la cible de façon à ce qu'elles aient la même compréhension de l'information. En général, il permet d'adapter le type d'information à transmettre aux propriétés du canal. Il engendre en particulier une optimisation du système global.

Tout signal porteur d'informations est composé d'une suite de signaux élémentaires, appelés symboles (ou moments) dont les caractéristiques propres (amplitude, fréquence, phase) restent constantes pendant la durée du symboleT_s.

2.5.2 Cryptage

Le cryptage proprement dit, ou comment mélanger et séparer les données et le signal chaotique, est l'étape finale pour construire le système de communication chaotique. Un signal chaotique porteur d'information représente une généralisation des systèmes conventionnels de modulation. Ainsi, un message source à faible amplitude est masqué par un signal chaotique. Le signal chaotique est mélangé avec le message source de différentes façons [9].

2.6 Méthodes de cryptage

Un système de communications utilisant le chaos représente une application prometteuse de l'estimation d'état des systèmes non linéaires. A partir d'un message contenant l'information, l'émetteur génère un signal qui est transmis au récepteur par l'intermédiaire d'un canal. Le récepteur reconstruit alors le message original, grâce à une « clé» partagée avec l'émetteur. Parmi les méthodes de transmission chaotiques, on peut citer le cryptage par addition, le cryptage par modulation, cryptage par commutation, Cryptage par inclusion.

2.6.1 Cryptage par addition

Avec cette méthode, le message confidentiel est additionné à un signal chaotique (la sortie d'un système chaotique), et le signal résultant est envoyé au récepteur, et par exemple le système de Pecora et Carroll. Dans cette classe deux canaux de transmission sont nécessaires, l'un pour la synchronisation et l'autre pour le signal de transmission. En conséquence, après la synchronisation le message confidentiel peut être récupéré par une simple opération de soustraction entre la sortie du récepteur et le signal émis sur le canal public [11].

La figure (2.5) représente le schéma de principe du cryptage.

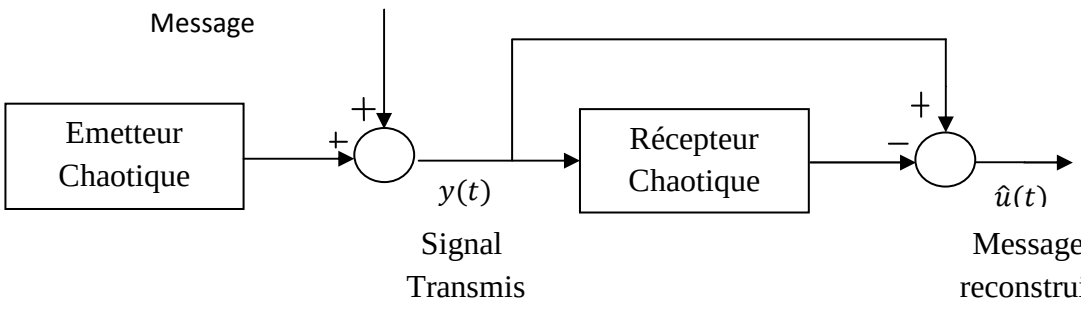


Fig2.5 : Principe de cryptage par addition.

2.6.2 Cryptage par modulation

Une autre méthode utilise le message pour modifier directement l'attracteur du système chaotique. Cette méthode s'appelle la modulation chaotique, et est décomposée en deux méthodes [11] : la modulation chaotique de paramètre, celle-ci modifie le paramètre du système chaotique, et la modulation chaotique d'état, qui modifie l'état du système chaotique. Cependant, la façon d'injecter le message et donc la fonction de modulation des paramètres ne doivent pas supprimer le caractère chaotique du signal envoyé au récepteur. Il est important de souligner que cette technique exploite pleinement les qualités des systèmes chaotiques [10].

2.6.3 Cryptage par commutation

Un autre schéma de transmission chaotique de données est la commutation chaotique dite CSK (Chaotic Switch Keying), qui exige que le message soit binaire, pour plus de simplicité. L'émetteur est constitué de deux systèmes chaotiques : ces deux systèmes peuvent avoir le même modèle dynamique, avec des paramètres différents, ou avoir deux modèles dynamiques totalement différents [4]. La figure (2.6) illustre le principe du cryptage par commutation : (selon la valeur de u(t) à l'instant t (C'est à dire u(t)=0 ou u(t)=1).

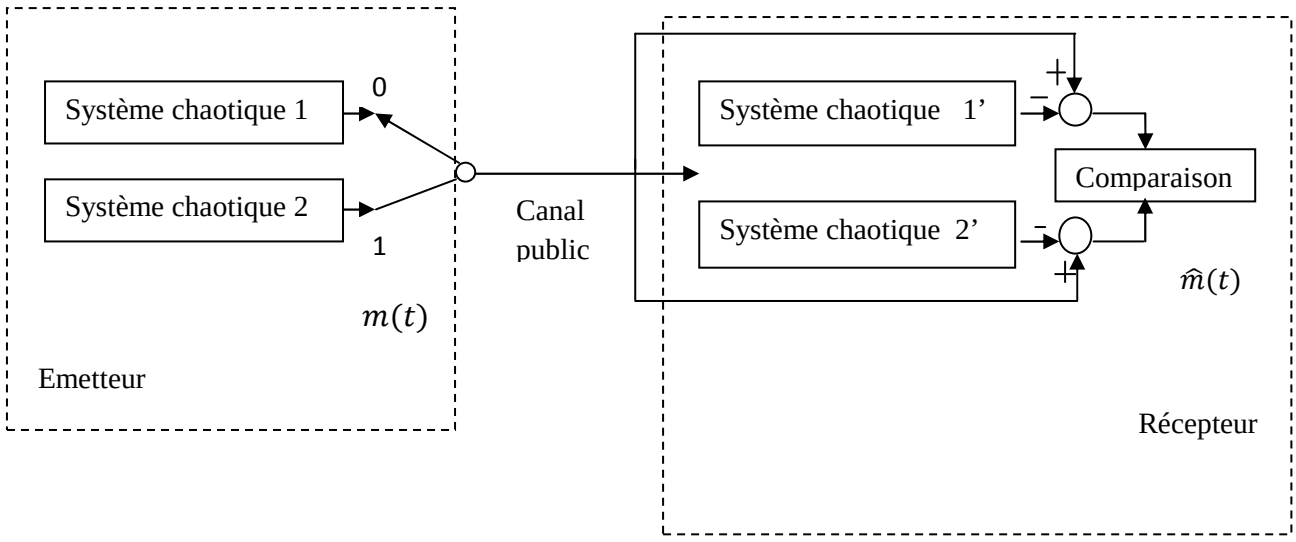


Fig2.6 : Principe de cryptage par commutation.

Si sa valeur est 0, le système chaotique 1 est choisi et le signal de sortie est transmis, sinon la sortie du système chaotique 2 transmis, dans ce sens, le message binaire commute l'émetteur entre deux attracteurs étranges correspondants aux deux systèmes chaotiques [11].
Cette méthode a d'énormes avantages, la robustesse au bruit en est un: en effet, au niveau du récepteur, on détermine la valeur exacte du message soit en évaluant l'erreur de synchronisation, soit par corrélation entre le signal envoyé et le signal récupéré [4].

2.6.4 Cryptage par inclusion

Dans le cryptage par inclusion, le message source est inclus dans la structure du système chaotique du côté de l'émission. Dans ce cas, un observateur doit être utilisé à la réception pour récupérer le message original. Cette classe de méthode nécessite un seul canal de transmission ; Ainsi elle présente beaucoup d'avantages et reste très utilisée en pratique [10].

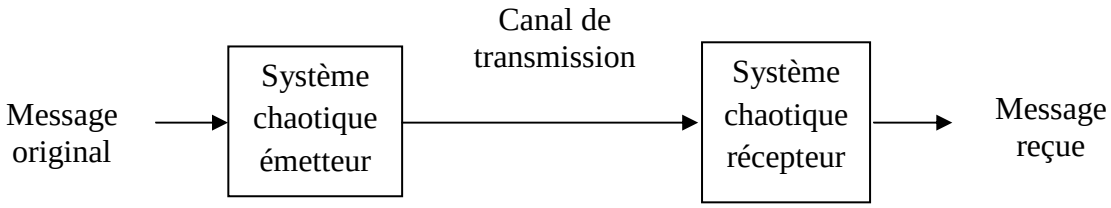


Fig2.7: Cryptage par la méthode d'inclusion

2.6.5 Transmission par deux voies

Le principe de la transmission par deux voies est illustré dans la figure (2.8). L'idée de base consiste à séparer les tâches de synchronisation et de cryptage en utilisant deux voies de communication [12]. L'´emetteur chaotique génère un signal chaotique $y(t)$ transmis dans le premier canal de communication (Canal 1) vers le récepteur qui doit se synchroniser avec le système maître. L'´emetteur génère également un autre signal chaotique utilisé dans une fonction de cryptage qui produit le signal chiffré $C(t)$ transmis dans un deuxième canal de transmission (Canal 2).

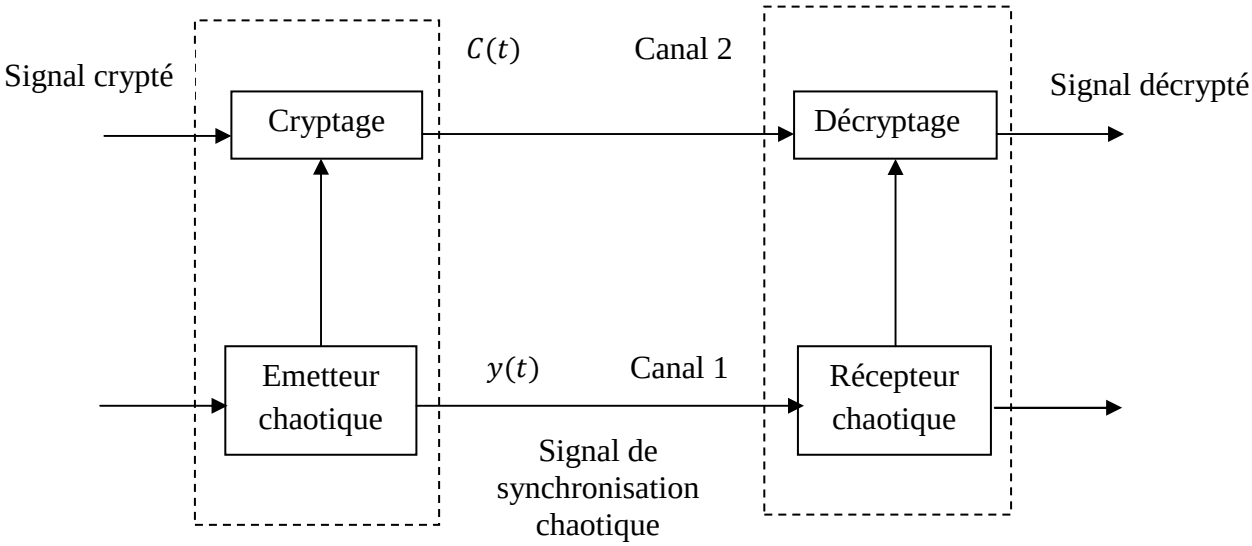


Fig2.8: Transmission à deux voies.

Cette méthode garantit un meilleur niveau de sécurité par rapport aux autres techniques puisque la séparation entre les opérations de cryptage et de synchronisation permet de concevoir une fonction de cryptage de plus en plus complexe sans se soucier de détériorer l'aspect chaotique de l'émetteur ou de perdre la synchronisation entre les systèmes maître et esclave. Cependant, cette technique présente de mauvaises performances en présence du bruit de transmission puisque l'effet du bruit est doublé en agissant à la fois sur le signal transmis $y(t)$ dans la première voie et également sur le signal du texte chiffré $C(t)$ présent dans la deuxième voie de transmission [13].

2.8 Conclusion

L'objectif de ce chapitre est de présenter les concepts fondamentaux de la cryptographie qui permettent de protéger la communication, les notions de cryptanalyse, clé de cryptage et cryptogramme. Ensuite, nous avons présenté quelques principes de système de la transmission sécurisé. Nous avons également cités, quelques généralités sur la synchronisation où nous avons démontré la possibilité de coupler les systèmes chaotiques que ce soit dans un sens (couplage unidirectionnel) et dans les deux sens (couplage bidirectionnel) ainsi que les déférents régimes de synchronisation, Par la suite nous avons présenté la synchronisation à base d'observateurs. Enfin, nous avons terminé ce chapitre par les différentes méthodes de cryptage et le décryptage, en donnant les avantages et les inconvénients de chacune de ces méthodes de synchronisation.

Dans le chapitre suivant, nous nous intéresserons à la méthode de synchronisation en utilisant des observateurs de types impulsive où les concepts de base seront énoncés avec plus de détails.

Chapitre 3 : La synchronisation impulsive des systèmes chaotiques

3.1 Introduction

On définit un système impulsif, un système dont toutes ou quelques variables d'état changent d'évolution brusquement par un saut instantanée d'une valeur à une autre. Ce saut peut être dû soit à un événement extérieur par une commande par exemple ou par un événement intérieur. L'étude des systèmes impulsifs a suscité ces dernières années un intérêt grandissant du fait de leur importance en pratique, [22]. Ceci a conduit à la mise en œuvre de tout un arsenal théorique pour l'analyse (existence et forme de solution, stabilité, commandabilité, observabilité) et la commande de tels systèmes. Cette théorie a permis aussi de mieux expliquer certaines notions qu'on croyait, il y a bien longtemps, bien connaitre comme la commandabilité lorsque la commande est générée en temps discret par un calculateur ou encore l'observabilité lorsque les mesures sont prises à des instants discrets.

La synchronisation de deux systèmes (émetteur et récepteur) par la technique des observateurs nécessite un signal d'injection généré par l'émetteur et transmis au récepteur afin que ce dernier se synchronise avec l'émetteur. L'envoi d'un signal d'injection à des instants discrets et de manière parcimonieuse sous forme d'impulsion est un grand avantage pour la transmission de données. En effet, ceci permet de ne pas saturer le canal public. D'autre part, l'envoi d'impulsion est souvent imposé par les réseaux de communications sur lesquels de nombreux usagers ou applications sont connectées. Les routeurs sont forcés de partager la transmission des informations à des instants discrets et aléatoires pour satisfaire tous les clients [2][10][23].

Dans ce chapitre, nous allons étudier le problème de synchronisation des systèmes chaotiques par un observateur impulsif. Dans un premier temps, nous rappelons les définitions de la notion d'observabilité des systèmes non linéaires. Ensuite, nous donnerons les types les plus importants des observateurs non linéaires dont l'observateur impulsif. La convergence de l'observateur impulsif est prouvée sur la base des résultats de stabilité des systèmes impulsifs. A cet effet, nous présentons les résultats principaux de stabilité des systèmes impulsifs.

3.2 Observabilité

L'observabilité est la possibilité de reconstruire l'état initial d'un système uniquement à partir de la connaissance des signaux d'entrées et de sorties.

3.2.1 Observabilité des systèmes linéaires

Soit le système linéaire temps invariant d'ordre n donné par sa représentation d'état suivante :

$$\begin{cases} \dot{x}(t) = Ax(t) + Bu(t) \\ y(t) = Cx(t) + Du(t) \end{cases} \tag{3.1}$$

Où les vecteurs$x(t)\epsilon\mathbb{R}^n$, $u(t)\epsilon\mathbb{R}^m$ et $y(t)\epsilon\mathbb{R}^q$ représentent respectivement l'état, la commande et la sortie du système. Les matrices A ,B,C et Dsont des matrices constantes de dimensions appropriées. L'observabilité du système non linéaire (3.1) est garantie si et seulement si :

$$rang(O) = rang\begin{pmatrix} C \\ CA \\ CA^2 \\ \vdots \\ CA^{(n-1)} \end{pmatrix} = n \tag{3.2}$$

Le système linéaire (3.1) est observable si le rang de la matrice d'observabilité O est égale à la dimension n de ce système, dans le cas où le rang de la matrice O est inferieure à n on parle alors d'observabilité partielle.

3.2.2 Observabilité des systèmes non linéaires

Soit le système non linéaire donné sous la forme suivante :

$$\begin{cases} \dot{x}(t) = f\big(x(t)\big) + g\big(x(t)\big)u(t) \\ y(t) = h\big(x(t)\big) \end{cases} \tag{3.3}$$

Où $x(t)\epsilon\mathbb{R}^n$, $u(t)\epsilon\mathbb{R}^m$sont respectivement les vecteurs d'état et de commande.

❖ **Définition 1 : Indiscernabilité**

Soient x_0 et $x_1$deux conditions initiales du système (3.3) et $x_u(t,x_0)$, $x_u(t,x_1)$ désignent les solutions à l'instant t de l'équation (3.3) correspondant aux états initiaux x_0 et x_1 respectivement.

La paire (x_0, x_1) est dite indiscernable si :

$\forall u\epsilon\mathbb{R}^m$, $\forall t \geq 0$,$h\big(x_u(t,x_0)\big) = h(x_u(t,x_1))$

Un état x est indiscernable de x_0 si la paire (x, x_0) est indiscernable [13].

❖ **Définition 2 : Observabilité**

Un système non linéaire est dit observable s'il n'admet pas de paires indiscernables.

❖ **définition 3 : Observabilité au sens du rang**

On dit que la paire (f, h) est observable au sens du rang si :

$$Rang\{dh, Ld_f h \dots dL_f^{(n-1)}h\}^T = n \tag{3.4}$$

$dL_f^k h$ est donnée par le vecteur :

$$dL_f^k h = \left(\frac{\partial L_f^k h}{\partial x_1}, \frac{\partial L_f^k h}{\partial x_2}, \ldots \frac{\partial L_f^k h}{\partial x_n}\right) \tag{3.5}$$

❖ **Remarque**

L'indiscernabilité entre deux solutions d'un système non linéaire ne peut être vérifiée pour un temps infini et aussi dans tout l'espace d'état. En général, on se borne à un intervalle de temps fini et à une région d'espace d'état limitée au voisinage d'un point considéré. De ces restrictions, découlent les notions d'observabilité faible et d'observabilité locale.

3.3 Différents types d'observateurs non linéaires

Plusieurs observateurs d'état ont été proposés. Dans cette partie du mémoire, nous présenterons les observateurs non linéaires les plus étudiés et appliqués par la communauté scientifique.

3.3.1 Filtre de Kalman étendu

Le filtre de Kalman étendu est l'une des techniques d'estimation des systèmes dynamiques non linéaires. Le principe consiste à utiliser les équations du filtre de Kalman classique au modèle non linéaire, qui est linéarisé par la formule de Taylor au premier ordre. Comme pour les systèmes linéaires, le filtre de Kalman étendu permet de prendre en compte l'influence du bruit de sortie sur la qualité de l'estimateur en synthétisant un gain optimal de l'observateur minimisant la variance de l'erreur d'estimation. Il faut noter que le filtre de Kalman étendu souffre d'une insuffisance théorique. La convergence des erreurs d'estimation vers zéro n'est pas démontrée.

3.3.2 Observateur de Luenberger étendu

Cette classe d'observateurs s'applique à des systèmes non linéaires faiblement localement observables. Ils interviennent soit au niveau du système original avec un gain constant, soit par le biais d'un changement de coordonnées avec un gain dépendant de l'état à estimer, dans le premier cas, un modèle linéarisé est nécessaire et le gain de l'observateur est calculé par placement de pôles. Cet observateur peut être compromis par des instabilités si on s'éloigne du point de fonctionnement, car il ne peut être utilisé que lorsqu'on est sûr que l'état restera au voisinage de son état d'équilibre. Dans le deuxième cas l'utilisation de solutions approchées est envisageable car les approches utilisant les changements de coordonnées nécessitent l'intégration d'un ensemble d'équations aux dérivées partielles non linéaires, ce qui est très délicat à réaliser [17].

3.3.3 Observateur à grand gain

Les techniques dites « grand gain » peuvent être appliquées sans transformation du système initial : dans ce cas, la conception de l'observateur se fait directement à partir de la structure du système [11]. Considérons la classe des systèmes non linéaires décrits par le modèle suivant :

$$\begin{cases} \dot{x} = f(x) = Ax + g(x,u) \\ y = h(x) = cx \end{cases} \tag{3.6}$$

La dynamique de l'état comporte une partie linéaire non commandée et une partie non linéaire commandée, vérifiant en général la condition de Lipschitz par rapport à x (au moins localement).

Condition de Lipschitz : une fonction $f : R^{n} \rightarrow R^{m}$ est dite K-Lipchitzien s'il existe $K > 0$ Tel que pour tout $(x, y) \in (R^{n})^{2}$:

$$\|f(x) - f(y)\| \leq k\|x - y\| \tag{3.7}$$

L'observateur à grand gain possède la structure suivante:

$$\begin{cases} \dot{\hat{x}} = f(\hat{x}) = A\hat{x} + f(\hat{x}) + K(y - \hat{y}) \\ \hat{y} = h(\hat{x}) = C\hat{x} \end{cases} \tag{3.8}$$

L'appellation à grand gain provient de la structure de l'observateur : lorsque la fonction non linéaire f possède une grande constante de Lipschitz, la moindre erreur entre l'état réel et l'état estimé va se répercuter et croître. Par conséquent, le gain de l'observateur doit être important pour compenser cet amplificateur de l'erreur.

Avec la dynamique de l'erreur d'estimation $e = x - \hat{x}$, nous pouvons obtenir :

$$\dot{e} = (A - KC)e + f(x) - f(y) \tag{3.9}$$

Il a été démontré dans [8] que si le gain k vérifie :

$$k < \frac{\lambda\min(Q)}{\lambda\max(P)}$$

Où k est la constante de Lipschitz de $f(x,u)$ telle que $\lambda\min(Q)$ et $\lambda\max(P)$ sont les valeurs propres maximale et minimale, Q est une matrice symétrique définie positive, et P est une matrice définie positive, solution de l'équation de Lyapunov est :

$$(A - KC)^{T}P + (A - KC) = -Q \tag{3.10}$$

Alors le système (3.8) est un observateur asymptotique du système non linéaire. Ces techniques dites à grand gain sont très répandues dans la littérature, il s'agit principalement de techniques de vérification qui permettent d'établir des conditions suffisantes de convergence

de l'état estimé vers l'état réel. Alors dans ce cas le problème de synchronisation entre l'émetteur (système maître) et le récepteur (système esclave) peut être réalisé.

3.3.4 Observateur à mode glissant

Un observateur à mode glissant est un observateur dont le terme correcteur est une fonction ***sign***. Le principe de cet observateur consiste à contraindre les trajectoires de l'observateur à évoluer, après un temps fini, sur une surface de glissement qui dépend généralement de l'erreur d'observation de la sortie mesurable. À l'aide des fonctions discontinues, l'attractivité de cette surface est assurée par des conditions appelées conditions de glissement. Si ces conditions sont vérifiées, le système converge vers la surface de glissement et y évolue selon une dynamique d'ordre $(n - p)$. Soit le système d'état non linéaire affine d'ordre *n*:

$$\begin{cases} \dot{x} = f(x) + g(x)u \\ y = h(x) \end{cases} \tag{3.11}$$

L'observateur à mode glissants pour ce système s'écrit de la façon suivante :

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

(3.12)

Ou λ est une matrice de gain de dimension $n \times p$. Notons que p désigne le nombre de commandes et aussi le nombre de surfaces jouant ici le rôle de sorties. Dans ce cas, on impose l'évolution des dynamiques du système sur une variété, sur laquelle l'erreur d'estimation de la sortie
$e_y = y - \hat{y}$ est nulle. Ainsi, cette erreur converge vers zéro à l'infini, et la dynamique du système se réduit de n à $n - p$. Ces critères permettent la synthèse de l'observateur à mode glissant et déterminent son fonctionnement [18].

3.3.5 Observateur à entrée inconnue

Le schéma de la figure (3.1) 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 [10] comme ceci est illustré par la figure 3.1 ci-dessous.

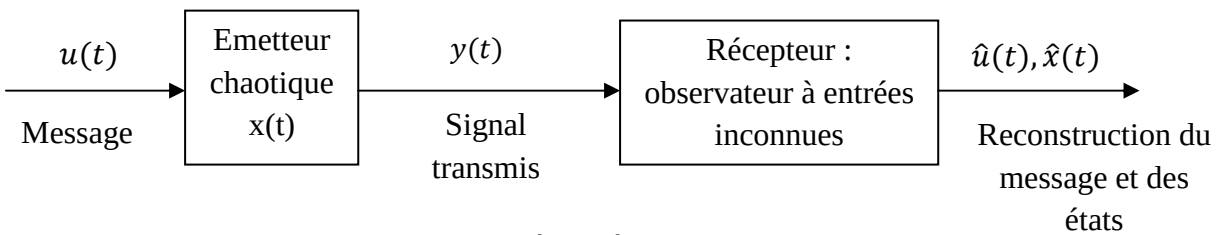


Fig3.1 : Observateurs à entré inconnues

3.4 Observateur impulsifs

Considérons la classe des systèmes suivants :

$$\begin{cases} \dot{x}_1(t) = f_1(x_1, x_2, t) \\ \dot{x}_2(t) = f_2(x_1, x_2, t) \\ y(t_k) = x_1(t_k) \end{cases} \quad (3.13)$$

Où $x(t) = (x_1(t)^T, x_2(t)^T)^T \in \mathbb{R}^n$ est le vecteur d'état, avec $x_1(t) \in \mathbb{R}^p$, $x_2(t) \in \mathbb{R}^{n-p}$ et $y(t_k) = \mathbb{R}^p$ est le vecteur de sortie. L'écriture (3.13) permet de mettre en évidences les états mesurables $x_1(t)$ et les états non mesurables $x_2(t)$. Les fonctions f_1 et f_2 sont continûment différentiables et lipchitziennes. De plus, les états évoluent dans un espace borné.
L'observateur impulsif du système (3.13) est donné comme suit :

$$\begin{cases} \dot{\hat{x}}_1(t) = f_1(\hat{x}_1, \hat{x}_2, t) \\ \dot{\hat{x}}_2(t) = f_2(\hat{x}_1, \hat{x}_2, t) \\ \hat{x}_1(t_k^+) = x_1(t_k) \end{cases} \quad (3.14)$$

A partir des systèmes (3.13) et (3.14), on obtient le système d'erreurs d'observation :

$$\begin{cases} \dot{e}_1(t) = f_1(x_1(t), x_2(t)) - f_1(\hat{x}_1(t), \hat{x}_2(t)) \\ \dot{e}_2(t) = f_2(x_1(t), x_2(t)) - f_2(\hat{x}_1(t), \hat{x}_2(t)) \\ e_1(t_k^+) = 0 \end{cases} \quad (3.15)$$

Le système d'erreur (3.15) est un système impulsif. Pour démontrer la convergence de l'observateur, on utilise les résultats de stabilité des systèmes impulsifs dont nous donnons l'essentiel ci-dessous [2].

3.4.1 Théorie des systèmes impulsifs

Considérons le système non linéaire suivant :

$$\dot{x} = f(t, x) \quad (3.16)$$

Où $f : R_+ \times R^n \to R^n$ est continue.

$x \in R^n$ est le vecteur d'état.

Soit l'ensemble discret $\{\tau_i\}$ des instants de temps, tel que

$$0 < \tau_1 < \tau_2 < \cdots < \tau_i < \tau_{i+1} < \cdots,$$

$\tau_i \to \infty$ quand $i \to \infty$

On définit le saut $U\ (i,x)$ dans la variable d'état à un instant τ_i comme suit [2] :

$$U(i,x) = \Delta x|_{t=\tau_i} \triangleq x(\tau_i^+) - x(\tau_i^-) \tag{3.17}$$

Le système d'équations différentielles impulsif est décrit par la relation suivante :

$$\begin{cases} \dot{x} = f(t,x) \quad t \neq \tau_i \\ \Delta x = U(i,x) \quad t = \tau_i \\ x(\tau_i^+) = x \quad t \geq 0, i = 1,2,\ldots \end{cases} \tag{3.18}$$

et $$\Delta x_{t=\tau_i} \triangleq x(\tau_i^+) - x(\tau_i^-) \tag{3.19}$$

$x(\tau_i^+)$, et $x(\tau_i^-)$ représente les instants de mesure, τ_i^+ est le temps juste après la i^{eme} mesure et τ_i^- le temps juste avant [20].

Où $\quad x(\tau_i^+) = \lim_{t\to\tau_i^+} x(t), \qquad x(\tau_i^-) = \lim_{t\to\tau_i^-} x(t) \tag{3.20}$

Dans cette section, nous allons rappeler la définition de base pour le système dynamique non linéaire impulsif. Ensuite, de nouvelles conditions suffisantes de stabilité de système impulsif seront données.

3.4.2 Stabilité des systèmes impulsifs

Dans cette section, nous donnerons quelques définitions et théorème de stabilité des systèmes impulsifs [2][19].
Considérons de nouveau le système dynamique (3.16)

❖ **Définition 1: (attractivité d'une boule)**

La boule $B_\in = \{x \in \frac{\mathbb{R}}{\|x\|} < \epsilon\}$ est attractive sur $B_\rho = \{x \in \mathbb{R}^n / \|x\| < \rho\}$ pour la dynamique (3.16), s'il existe une fonction β de classe L^1 telle que

$\forall x(0) = x_0 \in B_p$ le flux $\varphi(t,x_0)$ du système vérifie :

$$\forall t > 0, \|\varphi(t,x_0)\|_\epsilon \leq \beta(t) \tag{3.21}$$

❖ **Définition 2: (stabilité asymptotique d'une boule)**

La boule $B_\epsilon = \{x \in \mathbb{R}^n / \|x\| < \epsilon\}$ est asymptotiquement stable sur $B_\rho = \{x \in \mathbb{R}^n / \|x\| < \rho\}$ pour la dynamique (3.16) si elle est stable et attractive sur β_p [2].

❖ **Définition 3: (Stabilité asymptotique globale d'une boule)**

La boule $B_\epsilon = \{x \in \mathbb{R}^n / \|x\| < \epsilon\}$ est globalement asymptotiquement stable pour la dynamique (3.16) si elle asymptotiquement stable sur$\mathbb{R}^n$.
Dans cette partie du mémoire on considère la classe de dynamiques impulsives suivante :

$$\begin{cases} \dot{x}_1(t) = f_1(x_1(t), x_2(t), t) & t \neq t_k \\ \dot{x}_2(t) = f_2(x_1(t), x_2(t), t) & t \neq t_k \\ x_1(t_k^+) = 0 \\ x_2(t_k^-) = x_2(t_k) \end{cases} \qquad (3.22)$$

avec $x_1(t) \in \mathbb{R}^p$,$x_2 \in \mathbb{R}^{n-p}$, $f_1 : \mathbb{R}^n \to \mathbb{R}^p$ et $f_2 : \mathbb{R} \to \mathbb{R}^{n-p}$

La séquence $T = \{t_k : k \in \mathbb{N}\} \sqsubset \mathbb{R}^+$ vérifie qu'il existe τ_{min} et τ_{max} avec

$0 < \tau_{min} < \tau_{max}$ tel que $\forall k > 0 \quad t_{k+1} \geq t_k + \tau_{min}$ et $\quad t_{k+1} \leq t_k + \tau_{max}$

On suppose que :

$$t_i + \tau_{min} < t_{i+1} \qquad \text{et} \qquad t_i + \tau_{max} > t_{i+1} \qquad (3.23)$$

A partir de la définition de la stabilité asymptotique globale d'une boule, il est possible de présenter des conditions de stabilité suffisantes pour le système (3.16), pour cela, on doit supposer quelques hypothèses [2][20].

➢ **Hypothèse 1:**

f_1 Est au moins lipchitzienne localement où l_1 et l_2 sont les constante de Lipchitz par rapport à $x1$ et $x2$.

➢ **Hypothèse 2:**

$$F(x_1, x_2, t) = Ax_2 + B(t)x_1 \qquad \text{Où } \forall t \geq 0 \; B(t) < M \qquad (3.24)$$

▪ **Théorème :**

Si le système (3.22) vérifie les Hypothèses 1 et 2 et s'il existe une fonction définie strictement positive $V_2 : \mathbb{R}^{n-p} \to \mathbb{R}^+$ $V_2 \in C^1$ telle que

1. $\forall x_2 \neq 0 \; \left.\frac{\partial v_2}{\partial x_2}\right|_{x_2(.)} Ax_2 < -l_v \|x_2\|_2$
2. $\left.\frac{\partial v_2}{\partial x_2}\right|_{x_2(.)}$ est lipchitzienne où k_v est sa constante de Lipchitz.

Alors il existe un $\square_{max} > 0$ tel que pour toute séquence $\square_k \leq \square_{max}$, $x_2(t_k)$ converge globalement et asymptotiquement vers 0 pour tout $k \to +\infty$ [21].

❖ **Corollaire 1 :**

Supposons que les condition et hypothèses du Théorème sont vérifiées pour le système (3.22) alors : $x_1(t)$, $x_2(t)$ convergent vers 0 pour t→ ∞ .

❖ **Corollaire 2 :**

Si le système (3.15) vérifie les deux Hypothèses 1 et 2, alors il existe un $\square_{max}$ tel que pour chaque séquence impulsive$\square_k \leq \square_{max}$, les états de l'observateur (3.14) convergent vers les états du système (3.13).
Ces résultats de stabilité seront utilisés pour synchroniser impulsivement deux oscillateurs chaotiques de Colpitts [2].

3.6 CONCLUSION

Dans ce chapitre, nous avons proposé un schéma de synchronisation en utilisant les observateurs de type impulsifs. Pour cela, nous avons d'abord défini l'observabilité des systèmes linéaires et non linéaires dont les systèmes chaotiques que nous utilisons en est un cas.

Nous avons, par la suite, présenté les différentes classe d'observateurs de système linéaire et non-linéaire par exemple : l'observateur à grand gain, à mode glissant, Luenberger étendu, et le filtre de Kalman.

Après cela, nous avons présenté les observateurs impulsifs en expliquant le principe et en donnant la condition sur la période T assurant la stabilité de l'erreur d'observation

Dans ce qui suit nous allons présenter la partie simulation, où seront illustrés les résultats de synchronisation des oscillateurs de Colpitts, ainsi que les résultats de transmission sécurisée à base des deux oscillateurs.

Chapitre 4 : Application à la transmission sécurisée de données à base d'oscillateurs de Colpitts

4.1 Introduction

Il existe plusieurs oscillateurs électroniques générateurs du chaos. Chaque circuit diffère de l'autre par leur structure, et par leurs éléments électriques. L'oscillateur que nous avons choisi et celui de Colpitts. Ce dernier à une structure simple, il comporte un non linéarité intrinsèque liée à la caractéristique exponentielle du transistor. Dans ce chapitre, nous présenterons un schéma de transmission sécurisée pour transmettre une information cryptée. Par la suite nous avons présenté l'oscillateur de Colpitts utilisé dans notre système de transmission, en donnant le circuit électronique, les conditions d'oscillations et le modèle d'état du circuit. Nous nous intéresserons aux différents régimes d'oscillation pour des valeurs particulières des paramètres du circuit. Nous expliquerons par la suite comment synchroniser impulsivement deus oscillateurs chaotiques de Colpitts pour les utiliser en transmission de données. Le chapitre sera clos par les différents résultats de simulation de la synchronisation et de la transmission sécurisée.

4.2 Présentation du système de transmission sécurisée de données à base d'oscillateurs de Colpitts

Dans cette partie de ce chapitre nous allons expliquer le diagramme bloc de la synchronisation impulsive à base d'oscillateurs de Colpitts pour concevoir un schéma de transmissions sécurisée constitué de deux blocs, un bloc pour l'émission et un autre bloc pour la réception.

La figure (4.1) illustre le schéma de transmission que nous avons conçu dans notre mémoire.

L'émetteur contient un oscillateur chaotique de Colpitts et un module pour le cryptage du message à transmettre.

Le récepteur contient également un oscillateur de Colpitts identique à celui de l'émetteur ; un module pour le décryptage est conçu pour récupérer le message envoyé.

Les blocs émetteur et récepteur sont reliés par deux canaux :

- Le canal1 sert à envoyer successivement les impulsions de synchronisation (signal de synchronisation échantillonné) de période T. Nous avons choisi le signal y=x2 comme signal de synchronisation échantillonné par la période T assurant la stabilité de l'erreur de synchronisation et envoyé pour synchroniser les deux oscillateurs de Colpitts au niveau de l'émetteur et du récepteur.
- Le canal2 contient l'information secrète cryptée envoyée par l'émetteur.

L'information (message envoyer) est cryptée par une des méthodes de cryptage. La clé du cryptage secrète est l'ensemble des paramètres de l'oscillateur Colpitts.

La Figure (4.1) illustre le diagramme bloc de la transmission utilisant la synchronisation impulsive.

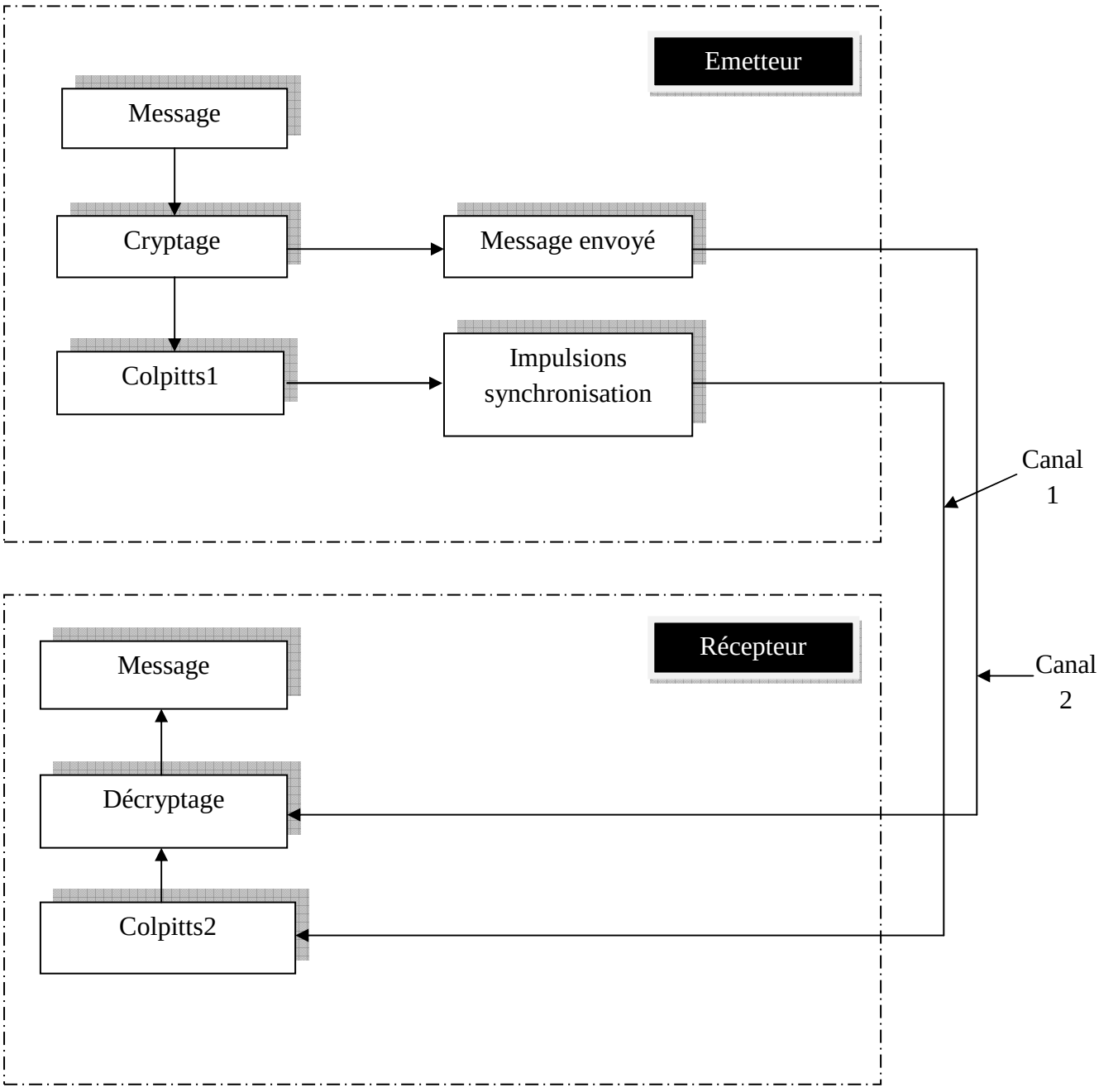


Fig4.1 : Diagramme bloc de la transmission utilisant la synchronisation impulsive

4.3 Les oscillateurs de Colpitts

Tout système oscillant est composé d'un élément passif qui dissipe de l'énergie : le résonnant, et d'un élément actif qui apporte de l'énergie : l'amplificateur. Dans le cas d'un oscillateur électronique, le résonateur est en général un filtre et l'amplificateur est souvent un amplificateur opérationnel ou bien un transistor [16].

4.3.1 Circuit électronique

Le circuit en basses fréquences de l'oscillateur Colpitts utilisé dans ce mémoire est un montage en base commune. Cette structure permet d'obtenir un gain plus élevé en autorisant une bande passante plus large. L'oscillateur comporte un transistor bipolaire classique, un circuit résonnant LC connecté entre le collecteur et la base du transistor. Une partie de la tension est retournée à l'émetteur [3]. Le point de fonctionnement du transistor est déterminé par les tensions d'alimentation V1 et V2

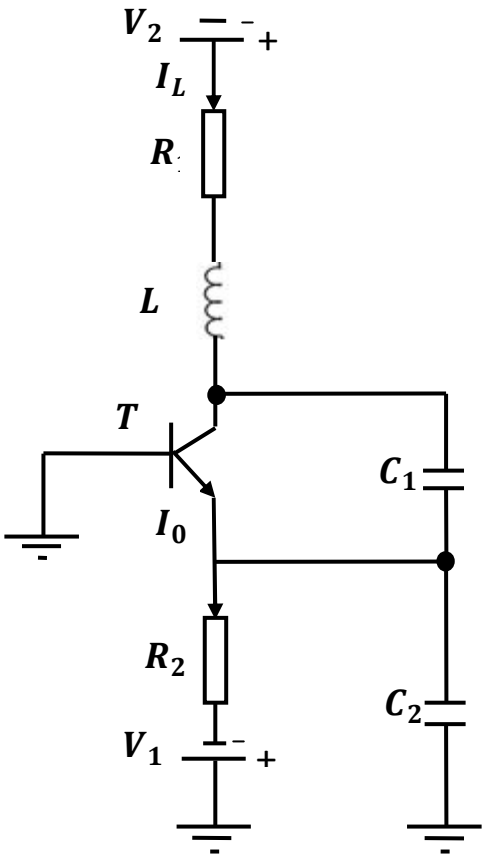


Fig4.2: Oscillateur de Colpitts avec **R1=47Ω, R2=1k, C1=C2=470nf, L=1mH, T : 2N2222**

4.3.2 Le critère d'oscillation de Barkhausen

La figure (4.3) montre la représentation la plus élémentaire d'un oscillateur électronique, l'élément A est un amplificateur et l'élément R est un filtre [2].

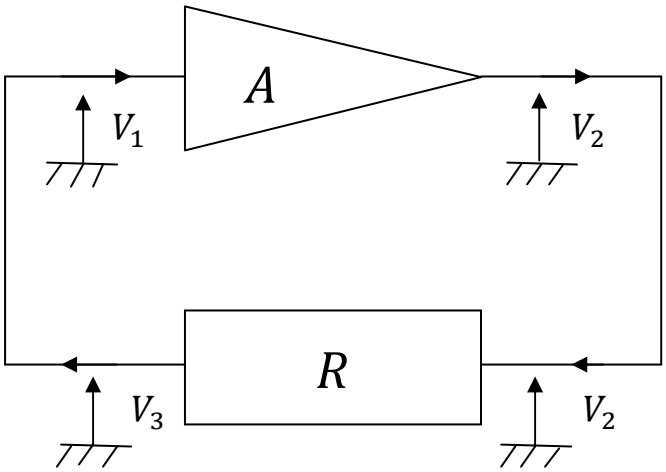


Fig4.3 : Oscillateur électronique : modèle de Barkhausen.

Supposons que les différentes grandeurs du montage soient sinusoïdales c'est-à-dire :

$V_2 = |A| \exp(j\Phi_A)\, V_1$ et $V_3 = |R| \exp(j\Phi_R) V_2$ et donc $V_3 = |A||R| \exp(j(\Phi_A + \Phi_R))$.

Le critère de Barkhausen impose que V_3 soit l'unité, ce qui nécessite deux conditions :

$$\begin{cases} |A|.|R| = 1 \\ \Phi_A + \Phi_R = 0 + 2k\pi, k \in \mathbb{Z} \end{cases} \quad (4.1)$$

la figure (4.4) présente le principe de l'oscillateur de colpitts.

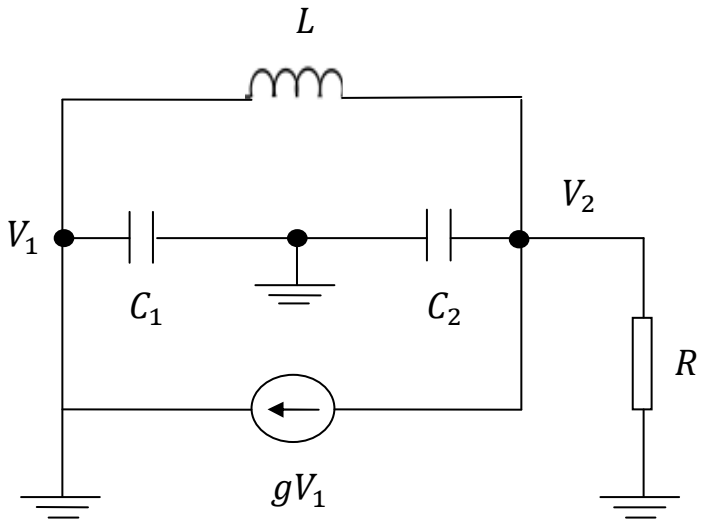


Fig4.4 : Principe de l'oscillateur de Colpitts

En appliquant la loi de Kirchhoff, nous aurons les équations du courant aux deux extrémités de l'inductance comme suit :

$$\begin{cases} -gV_1 - \frac{V_2}{R} - jC_2wV_2 + \frac{V_1 - V_2}{jLw} = 0 \\ \frac{V_2 - V_1}{jLw} - jC_1wV_1 + gV_1 = 0 \end{cases} \quad (4.2)$$

En remplaçant la valeur de V_2dans la première équation on aura :

$$\left[-g + \frac{1}{jLw}\right] - \left[jC_1w + \frac{1}{jLw}\right]\left[\frac{1}{R} + jC_2w + \frac{1}{jLw}\right] = 0 \quad (4.3)$$

Par annulation de la partie imaginaire dans l'équation (4.3), on obtient la fréquence w

$$C_1C_2RLw^2 - (C_1 + C_2)Rw = 0 \Rightarrow w = \frac{1}{\sqrt{L\frac{C_1C_2}{C_1+C_2}}} \quad (4.4)$$

En annulant la partie réelle, nous obtenons la condition d'oscillation de l'oscillateur Colpitts :

$$-Rg + LC_1w^2 - 1 = 0 \Longrightarrow R = \frac{LC_1w^2 - 1}{g} \Rightarrow gR > \frac{C_1}{C_2} \quad (4.5)$$

4.3.3 Représentation d'état

En utilisant la loi des mailles et des nœuds au circuit de Colpitts, nous obtenons les équations suivantes :

$$\begin{cases} \frac{dV_{C1}}{dt} = -\frac{1}{C_1}f\left(-V_{C_2}\right) + \frac{1}{C_1}I_L \\ \frac{dV_{C_2}}{dt} = \frac{1}{C_2}I_L - \frac{1}{C_2}I_0 \\ \frac{dI_L}{dt} = -\frac{1}{L_1}V_{C_1} - \frac{1}{L_1}V_{C_2} - \frac{R_1}{L_1}I_L - \frac{V_2}{L_1} \end{cases} \quad (4.6)$$

Le terme f(.) décrit la relation courant tension du transistor T, elle est fonction du courant de l'émetteur

$$I_E = f(V_{BE}) = f(-V_{C2}) \cong I_S\left[\exp\left(\frac{V_{BE}}{V_T}\right)\right] \cong I_S\left[\exp\left(\frac{-V_{C2}}{V_T}\right)\right] \quad (4.7)$$

I_S désigne le courant de la saturation inverse de la jonction base-émetteur [14][3].
Le système (4.6) peut être normalisé comme suit :

$$\begin{cases} z_1(t) = \frac{1}{V_T}\left[V_{C1}(w_0t) - V_{C_{10}}\right] \\ z_2(t) = \frac{1}{V_T}\left[V_{C2}(w_0t) - V_{C_{20}}\right] \\ z_3(t) = \frac{1}{I_0}\left[I_L(w_0t) - I_{L0}\right] \end{cases} \quad (4.8)$$

$$\begin{cases} \dot{z}_1 = \frac{g}{q(1-k)}(-\eta(z_2) + z_3) \\ \dot{z}_2 = \frac{g}{qk} z_3 \\ \dot{z}_3 = -\frac{qk(1-k)}{g}\left([z_1 + z_2] - \frac{1}{q} z_3\right) \end{cases} \quad (4.9)$$

Avec : $\eta(z_2) = \exp(-z_2) - 1$ et $k = \frac{c_2}{c_1 + c_2}$

q représente le facteur de qualité du circuit résonnant LC :

$$q = \frac{Lw_0}{R} \quad (4.10)$$

g est le gain de la boucle de réaction vérifient le critère de Barkhausen :

$$g = \frac{LI_0}{(C_1 + C_2)R_1 V_T} \quad (4.11)$$

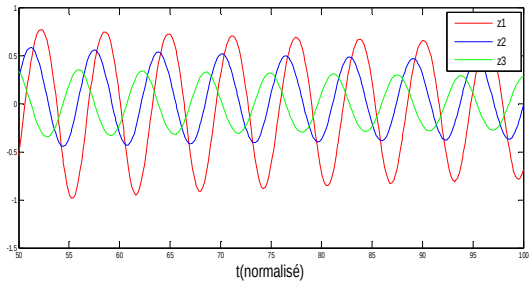
En posant $a_1 = \frac{g}{q(1-k)}$, $a_2 = \frac{g}{qk}$, $a_3 = \frac{qk(1-k)}{g}$, $a_4 = \frac{1}{q}$, $y = z_2$

La représentation du système se simplifie :

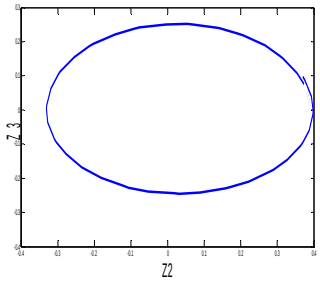
$$\begin{cases} \dot{z}_1 = a_1(-\exp(-z_2) + 1 + z_3) \\ \dot{z}_2 = a_2 z_3 \\ \dot{z}_3 = -a_3(z_1 + z_2) - a_4 z_3 \\ y = z_2 \end{cases} \quad (4.12)$$

4.4 Comportement chaotique

Pour obtenir les différents types d'oscillations. On fait varier le paramètre **g** du système (4.12). La figure (4.5) représente les résultats de simulation sous **Matlab/Simulink** du système de Colpitts (4.12) pour différentes valeurs de g.

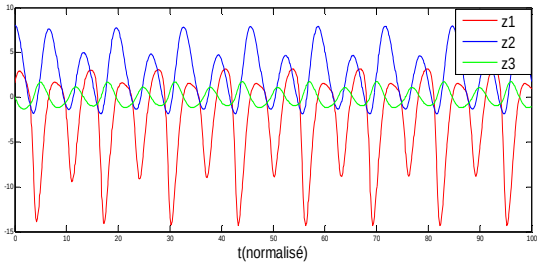


Réponses temporelles

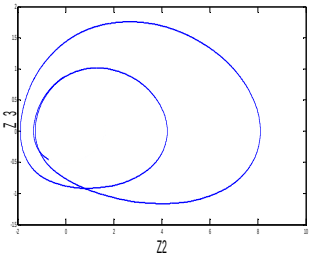


Plan de phase

***(a)* Pour g=1.0029**

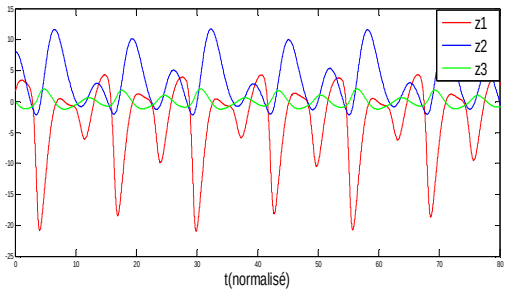


Réponses temporelles

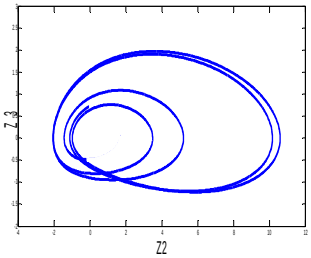


Plan de phase

(b) Pour g=2.13

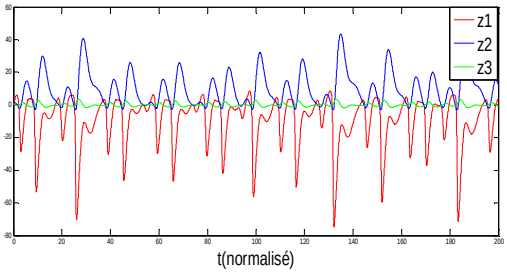


Réponses temporelles

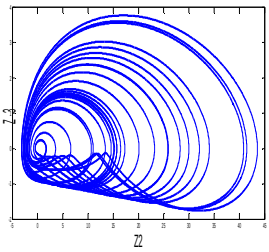


Plan de phase

(c) pour g=2.4



Réponses temporelles



Plan de phase

(d) pour g=4.46

Fig4.5 : Différents régimes de l'oscillateur de Colpitts.

Interpretation des resultats de simulations

Les résultats de la figure (4.5) montrent qu'à partir la valeur de **g** égale à 1.0029, Le système présente des oscillations sinusoidales, celà implique que la condition de Barkaussen est vérifée, par conséquent il ya apparition d'un cycle limite dans le plan de phase de la fig(4.5.a). En augmentant la valeur de **g** à 2.13, le système présente des oscillations sinusoidales à deux périodes qui corespondent à deux cycles limites dans le plan de phase fig(4.5.b). Pour **g** égale à 2.4 le système oscille avec quatre périodes correspondant à 4 cycles

limites dans le plan de phase fig(4.5.c).et pour **g** égale à 4.46, le système devient chaotique, cela se traduit par l'apparition d'un attracteur chaotique étrange dans le plan de phase fig(4.5.d).

4.5 Synchronisation impulsive de deux oscillateurs

Dans cette partie, nous allons présenter un observateur impulsif pour l'oscillateur de Colpitts. Le système Colpitts-observateur sera utilisé pour la transmission de données.

4.5.1 Modèle d'observateur impulsif

Dans cette section, un observateur impulsif est représenté comme suit :

$$\begin{cases} \dot{\hat{z}}_1 = a_1(-\exp(-\hat{z}_2) + 1 + \hat{z}_3) \\ \dot{\hat{z}}_2 = a_2 z_3 \\ \dot{\hat{z}}_3 = -a_3(\hat{z}_1 + \hat{z}_2) - a_4\hat{z}_3 \\ \hat{z}_2(t_k^+) = z_2(t_k) \end{cases}$$

Où : $E = (e1, e2, e3)^T$ définit le vecteurs d'erreur d'observation de système.

Telles que : $e_1 = z_1 - \hat{z}_1,\ e_2 = z_2 - \hat{z}_2, e_3 = z_3 - \hat{z}_3$ sont les erreurs sur les états des systèmes.

Le système d'erreurs dynamiques est alors donné comme suit :

$$\begin{cases} e_1 = a_1\exp(-z_2)(\exp(e_2) - 1) + a_1 e_3 \\ e_2 = a_2 e_3 \\ e_3 = -a_3(e_1 + e_2) - a_4 e_3 \\ e_2(t_k^+) = 0 \end{cases}$$

En négligeant les termes d'ordre supérieur dans la série de Tylor de l'expression de $exp(e2)$ le système devient [2]:

$$\begin{cases} e_1 = a_1(-\exp(-z_2)\, e_2 + e_3) \\ e_2 = a_2 e_3 \\ e_3 = -a_3(e_1 + e_2) - a_4 e_3 \\ e_2(t_k^+) = 0 \end{cases}$$

Ou: $f1(e_1, e_2, e_3) = a_2 e_3$

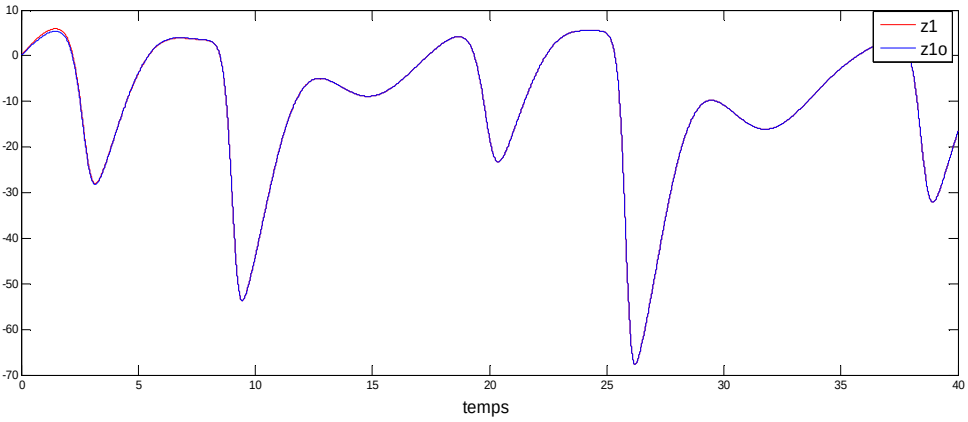
$$f2(e_1, e_2, e_3) = \begin{pmatrix} 0 & a_1 \\ -a_3 & -a_4 \end{pmatrix}\begin{pmatrix} e_1 \\ e_2 \end{pmatrix} + \begin{pmatrix} a_1 exp(-x z_2(t)) \\ -a_3 \end{pmatrix} e_2$$

Donc les erreurs sont bornées car les états évoluent dans un espace borné, par conséquent $f1$ est lipchitzienne.

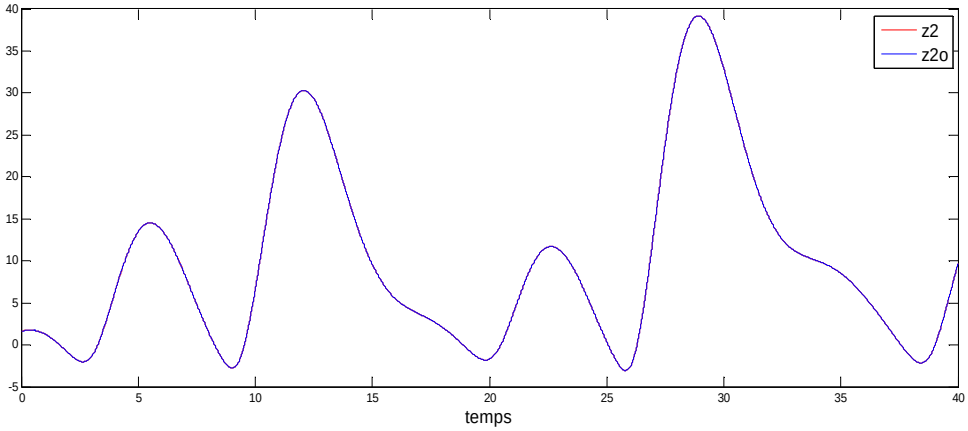
4.5.2 Résultats de simulation

Les résultats de simulation sous matlab montrent que la synchronisation chaotique par la commande impulsive peut illustrer les performances du système de transmission. Nous avons réalisé la simulation avec le logiciel Matlab/Simulink, qui est effectuée en utilisant la méthode numérique Runge-Kutta pour la résolution des équations différentielles avec un temps de calcul égale à 0.0004. La période des impulsions de synchronisation est fixée à T=0.04, avec la durée de chaque impulsions d=T/10. La grandeur de temps est normalisée. Afin d'avoir un régime chaotique, les paramètres du système de Colpitts sont pris comme suit: g=4.46, q=1.38, k=0.5 avec les conditions initiales $x_1(0)$=0.1, $x_2(0)$=1.6, $x_3(0)$=0.1. La figure (4.6) présente les états de synchronisation de l'oscillateur de Colpitts et de son observateur correspondant.

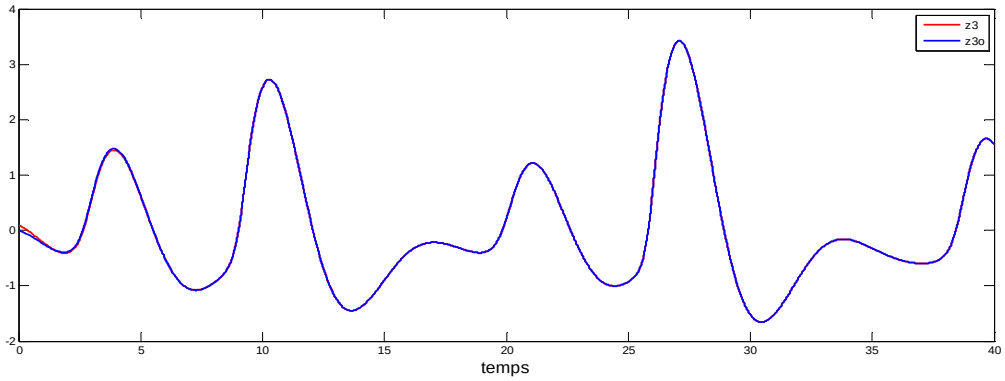
D'après les résultats obtenus dans la figure (4.6), nous pouvons constater que tous les états sont bien synchronisés à partir de la valeur t=13 (t normalisé).



(a) Etats z1 et z1o



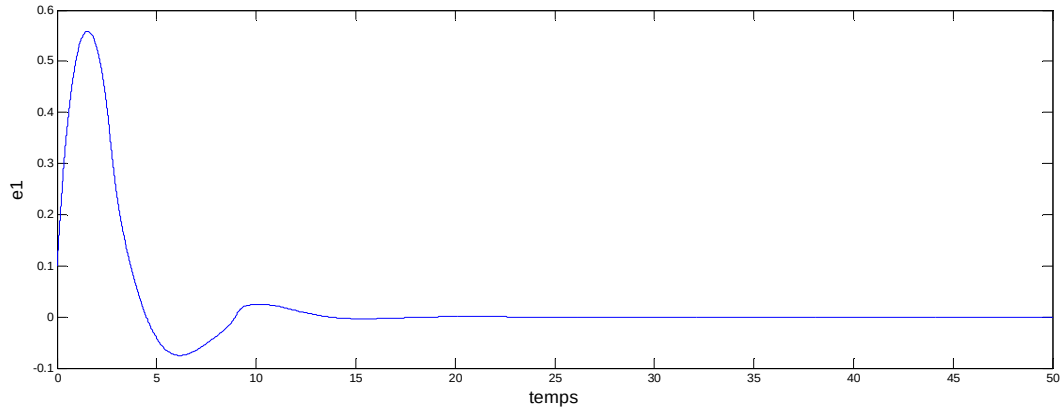
(b) Etats z2 et z2o



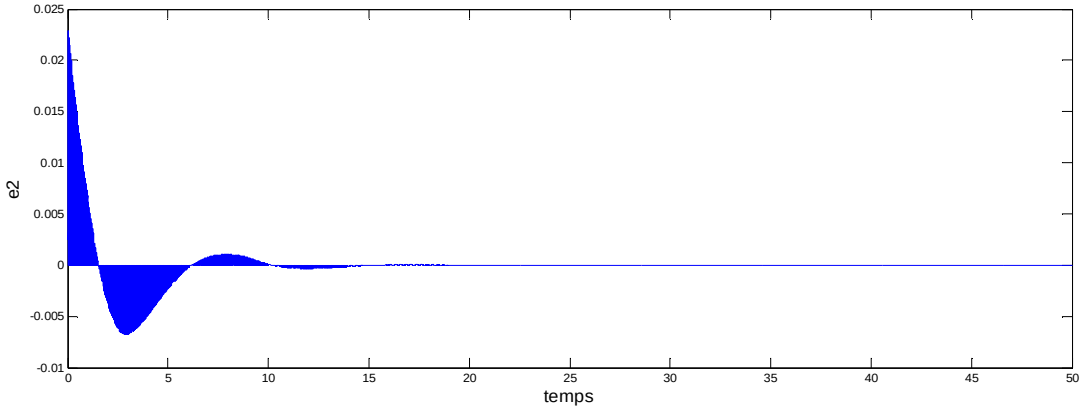
(c) Etats z3 et z3o

Fig4.6 : résultats de synchronisation des états

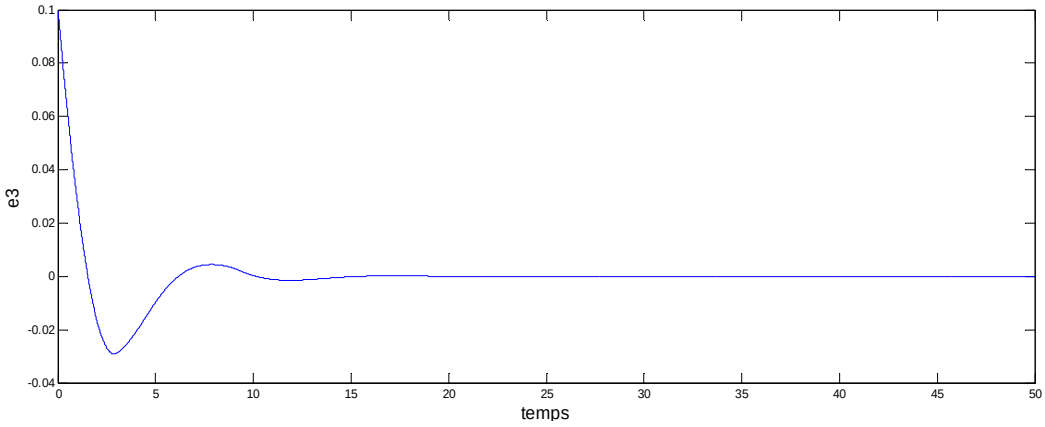
La figure (4.7) montre les erreurs de synchronisation des trois états, et d'apprêt les résultats obtenu nous constatant que touts les états converge ver zéro.



$$e_1 = z_1 - \hat{z}_1$$



$$e_2 = z_2 - \hat{z}_2$$



$$e3 = z_3 - \hat{z}_3$$

Fig4.7 : Erreurs de synchronisation des états.

La figure (4.8) nous montre le plan de phase des deux signaux z_2 et $\hat{z}_2$. Le plan de phase des deux signaux z_2 et $\hat{z}_2$ montre une droit de 45°. Ceci implique que les deux oscillateurs sont bien synchronisés.

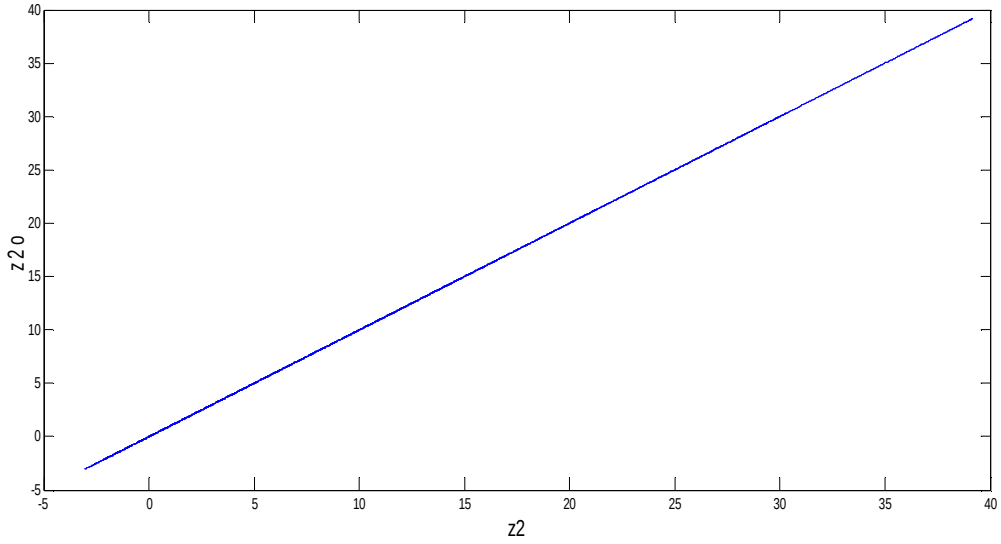
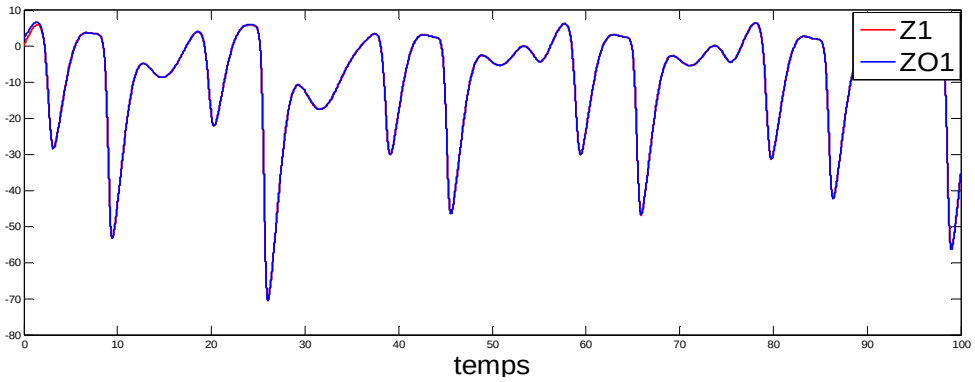


Fig4.8 : plan de phase de deux signaux synchronisés $z2$ et $\hat{z}2$

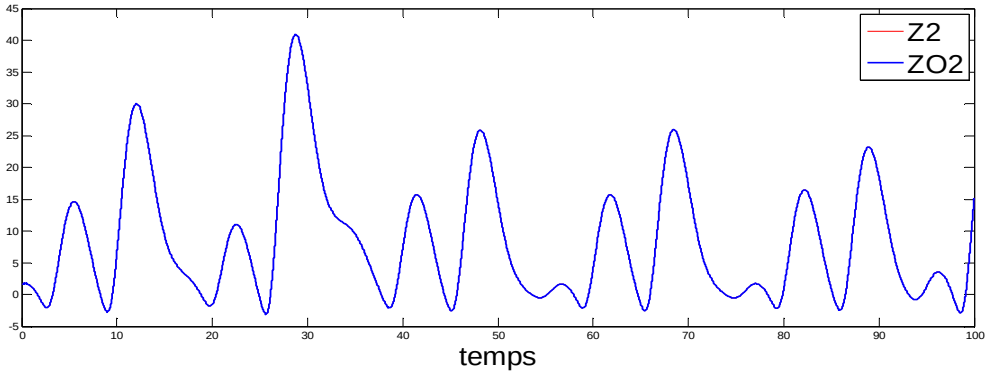
4.6 Transmission sécurisée à base de circuits de Colpitts

4.6.1 Transmission a une seule voie

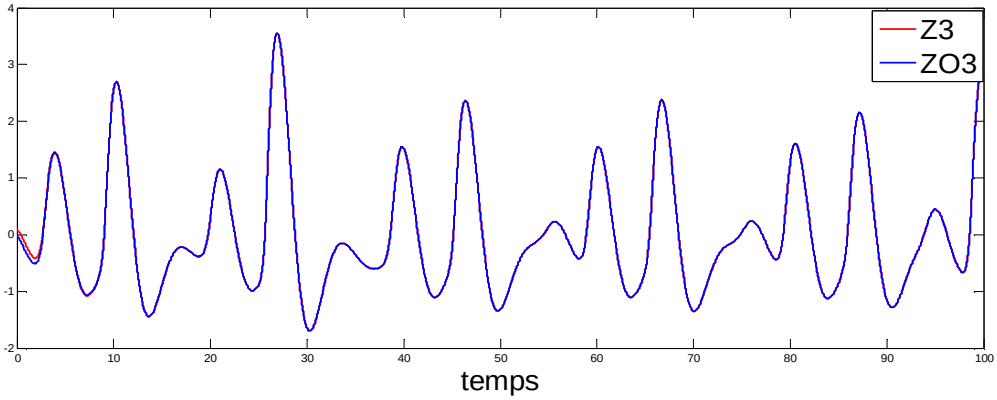
Résultats de la synchronisation des états



a- L'état z_1 et $\hat{z}_1$



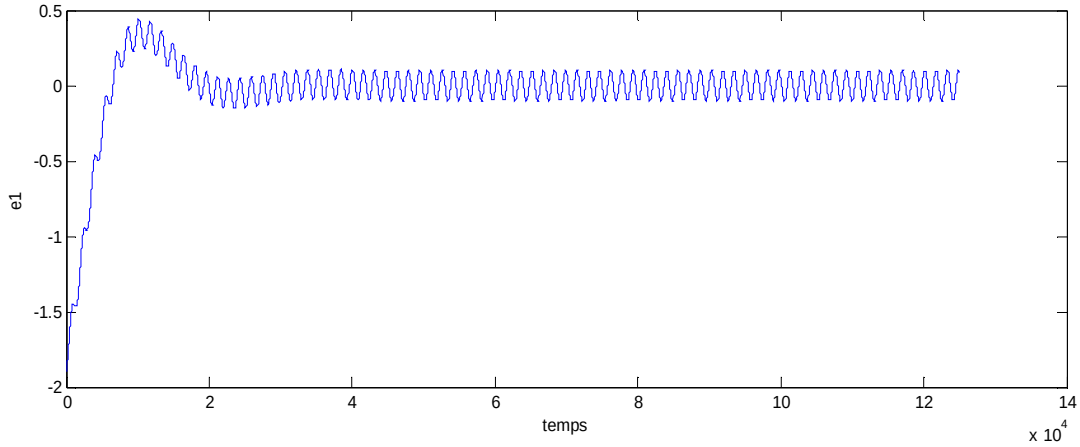
b- Les états z_2 et $\hat{z}_2$



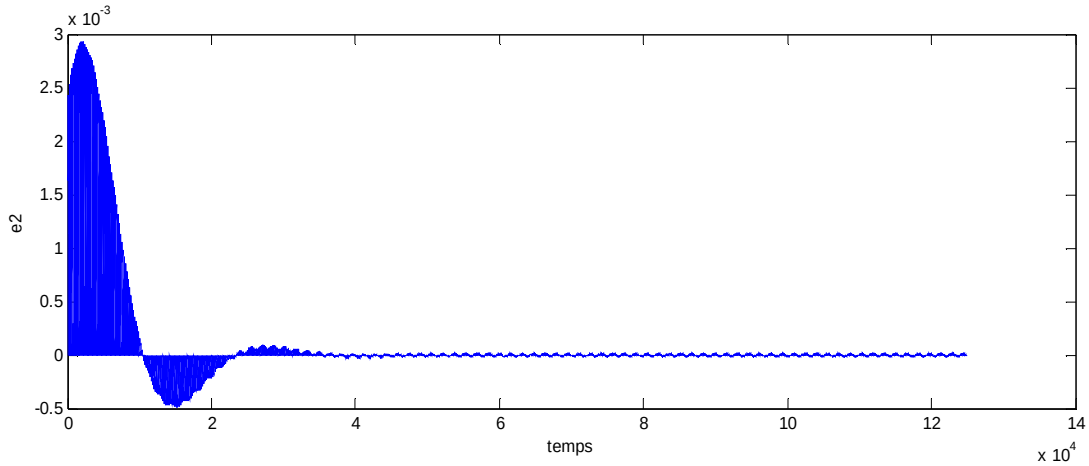
c- Les états z_3 et $\hat{z}_3$

Fig4.9 résultat de synchronisation des états

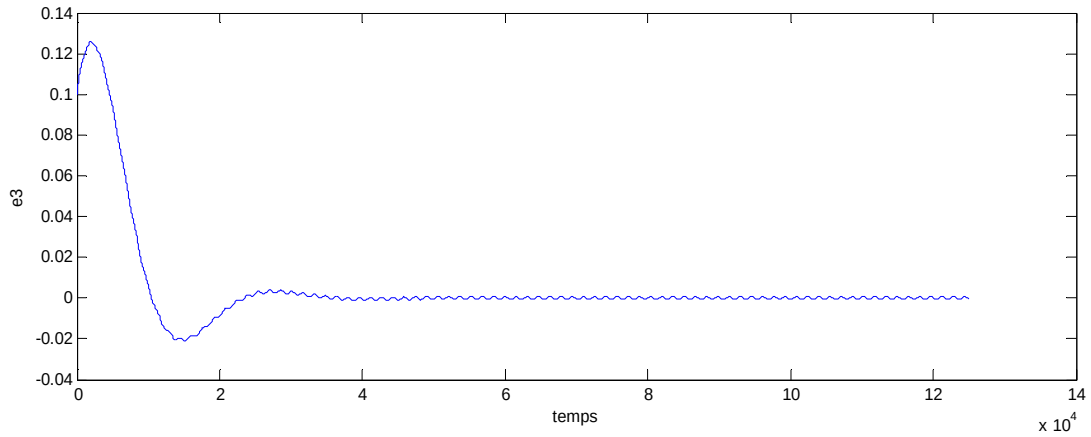
La figure (4.10) nous donne les Résultats des erreurs de synchronisation des états



a- Erreur de synchronisation $e_1 = z_1 - \hat{z}_1$



b- Erreur de synchronisation $e_2 = z_2 - \hat{z}_2$



c- Erreur de synchronisation $e_3 = z_3 - \hat{z}_3$

Fig4.10 : résultats des erreurs de synchronisations des états

En observant les résultats, on constate qu'il y a apparition des oscillations très petites au niveau des erreurs de synchronisation, les états ne sont pas bien synchronisés, cela est dû au message qu'on a inclus dans la première dynamique du système de Colpitts.

La figure (4.11) nous montre le portait dans plan de phase des deux signaux z_2 et $\hat{z}_2$ qui est une droit de pente 45°

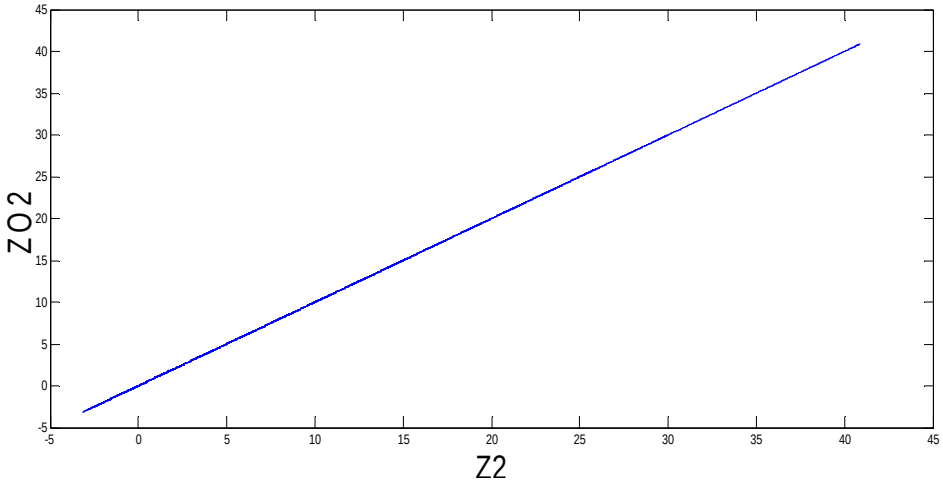
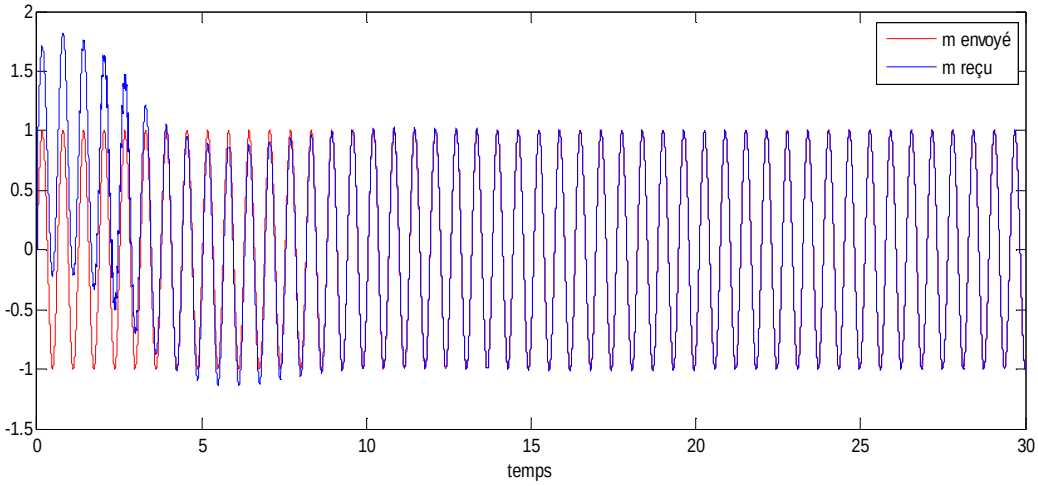
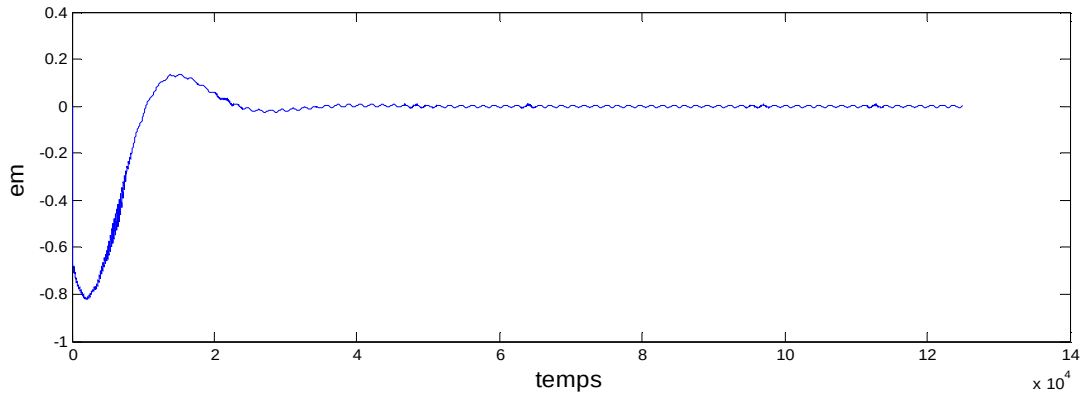


Fig4.11 : Plan de phase de deux signaux synchronisés z_2 et $\hat{z}_2$

Pour masquer le message nous avons appliqué le cryptage par inclusion. Le message a été inclus dans la dynamique z_1 de l'oscillateur de Colpitts au niveau de l'émetteur. La figure (4.12) illustre les résultats de la récupération du message m ainsi l'erreur de synchronisation sur le message.



a-Message envoyé et reçu



b-Erreur de synchronisation sur le message $e_m = m - \hat{m}$

Fig4.12 : Récupération de message m par la méthode de cryptage par inclusion

D'après les résultats nous constatons que l'erreur e_m ne converge pas vers zéro donc la synchronisation n'a pas eu lieu le message n'est pas bien récupéré. Les résultats de simulation obtenue pour la méthode de cryptage par inclusion, montrent que la synchronisation impulsive des deux oscillateurs de Colpitts n'est pas réussie, ainsi le message n'a pas été bien récupéré.

Pour remédier a ce problème nous avons fait plusieurs essais afin d'annuler les oscillations qui apparaissent au niveau des erreurs de synchronisations cela en variant les paramètres du système. Mais nous n'avons pas eu d'améliorations.

4.6.2 Transmission à deux voies

Pour le cryptage par la méthode d'addition, on à ajouté le message sur la ligne de transmission y2 (canal 2), et (y1 (canal 1) permet la synchronisation des états), tell que :

$$\varphi = y2 + m = x_1 + x_3 + m$$

Où φ est le message crypté.

Et pour décrypté le message transmis, nous utilisons l'observateur impulsive, donc l'équation du message décrypté devient :

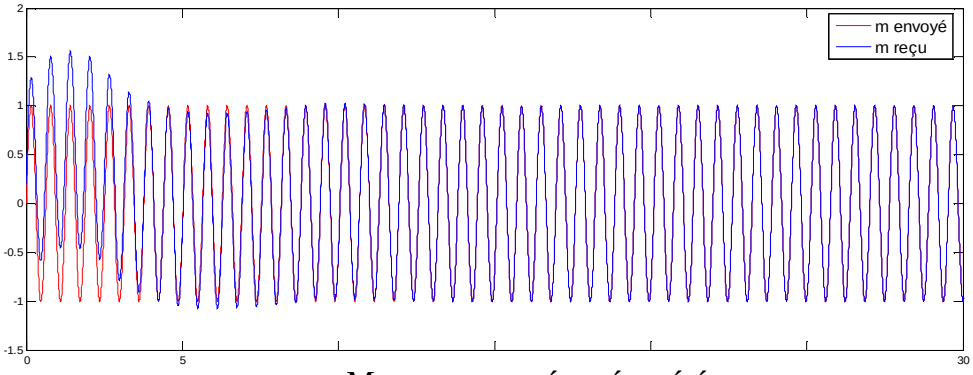
$$\varphi_d = \varphi - \hat{x}_1 - \hat{x}_3$$

Où φ_d est le message décrypté.

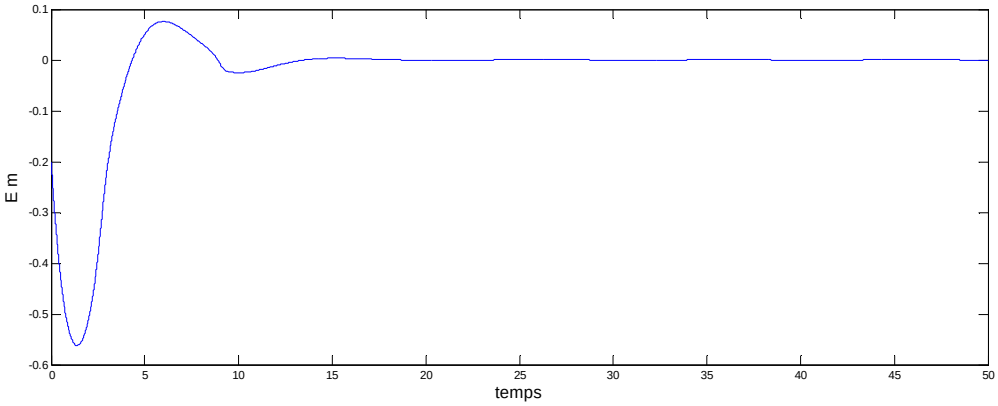
Les figures suivantes illustrent les résultats de la récupération de différents messages m

1) m est un signal sinusoïdal :

La figure (4.13) représente l'envoi et la récupération du message sinusoïdal par la méthode par addition



a-Message envoyé et récupéré

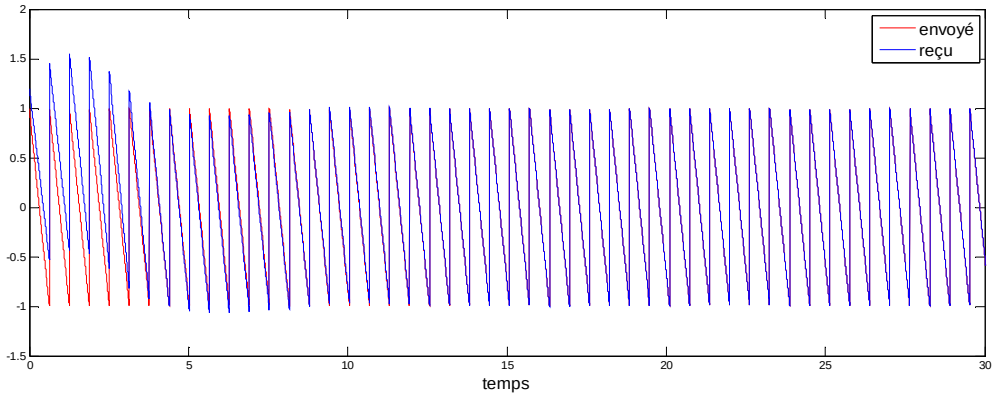


b-Erreur de synchronisation sur le message e_m

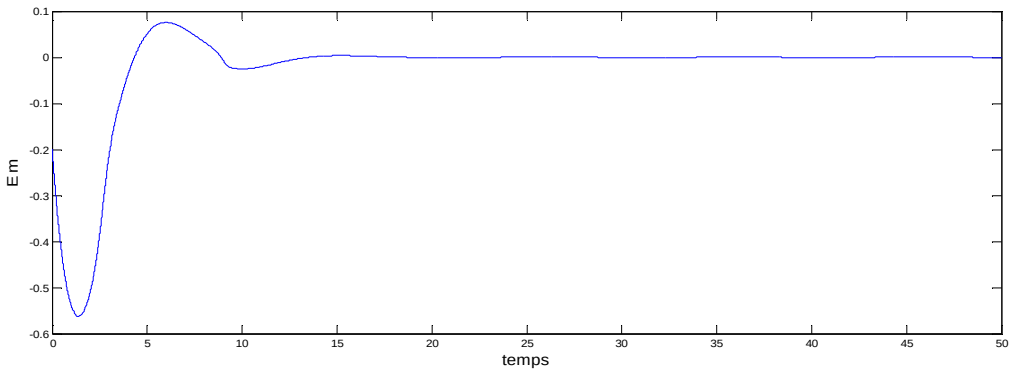
Fig4.13 : Récupération du message sinusoïdal par la méthode d'addition

2) m est un signal triangulaire

La figure (4.14) représente la synchronisation du message triangulaire.



a-Message envoyé et récupéré

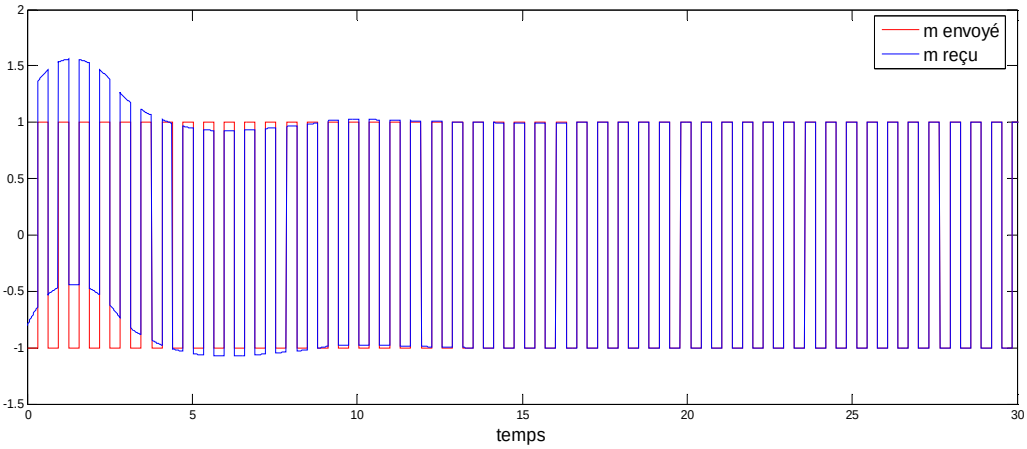


b-Erreur de synchronisation sur le message e_m

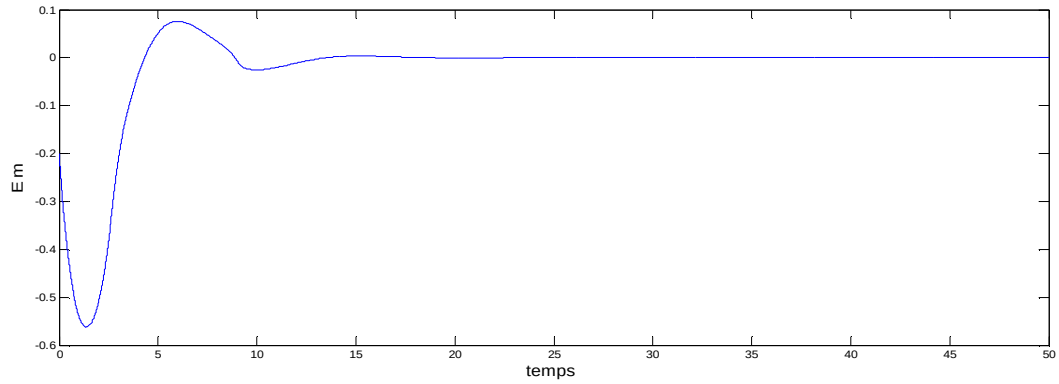
Fig4.14 : Récupération du message triangulaire par la méthode d'addition

3) m est un signal carré

La figure (4.15) représente la synchronisation du message en signal carré.



a-Message envoyé et récupéré



b-Erreur de synchronisation sur le message e_m

Fig4.15 : Récupération du message carré par la méthode d'addition

A travers les résultats de synchronisation des états du système, nous ne constatons que toutes les erreurs de synchronisation convergente vers zéro à partir de l'instant t= 13.

4.7 Robustesse aux bruits de transmission et aux variations des paramètres

4.7.1 Robustesse aux bruits de transmission

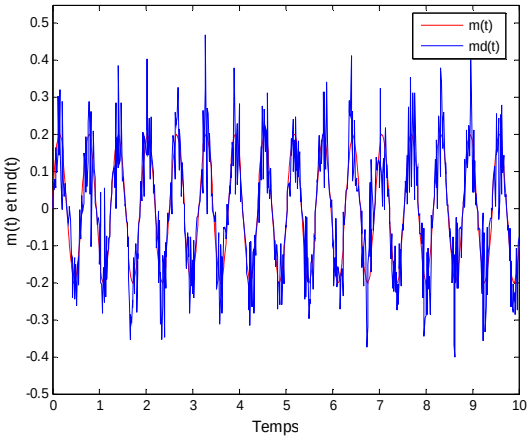
La robustesse aux bruits se pose pour tout système de communication analogique ou numérique : l'émetteur est relié au récepteur par un canal, l'élément physique qui permet de transmettre les informations. Quel que soit le canal utilisé, le bruit modifie le signal en lui ajoutant une grandeur qui peut perturber la transmission.

Dans ce qui suit nous étudierons l'impact du bruit affectant le signal dévolu à la synchronisation sur la qualité de la restauration du message (signal sinusoïdal et carré). On considère un bruit additif b(t) gaussien, normal centré perturbant le signal transmis y(t).Pour quantifier le rapport entre l'amplitude du signal et celle du bruit qui l'affecte, on rappelle la définition du rapport signal sur bruit SNR, exprimé en décibel.

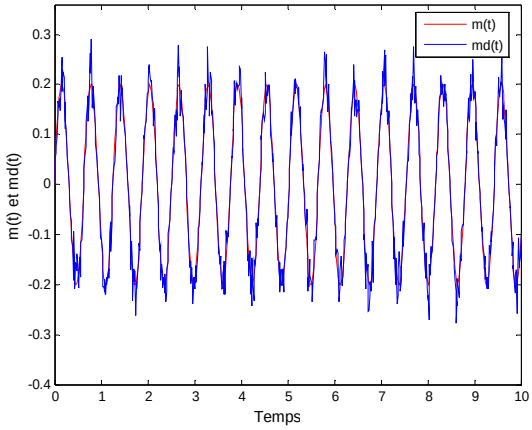
$$SNR(y,b) = 20log_{10}\left\|\frac{y(t)}{b(t)}\right\|$$

Plus ce rapport est grand, moins le bruit perturbe le signal original. Ceci est illustré dans les figures (4.16) et (4.17).

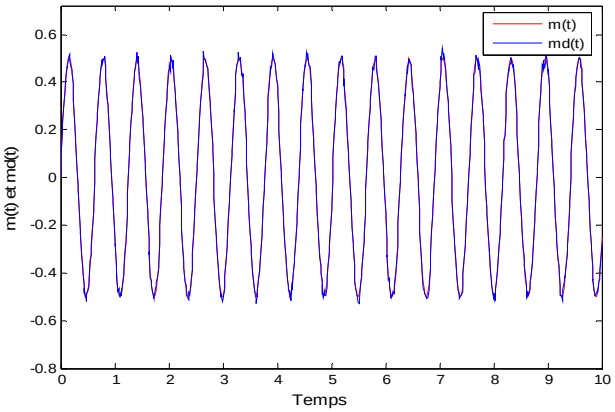
1) m est un signal sinusoïdal



$(a)\ SNR = 5dB$



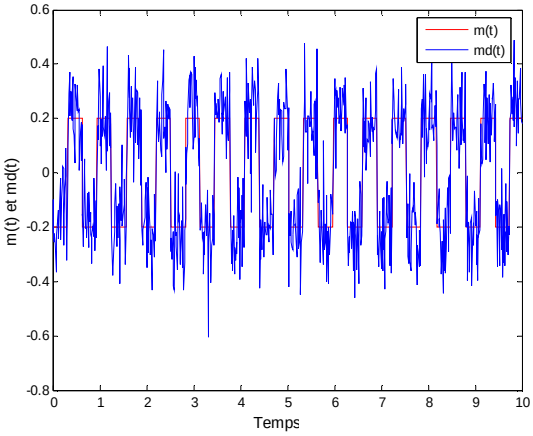
$(b) SNR = 15dB$



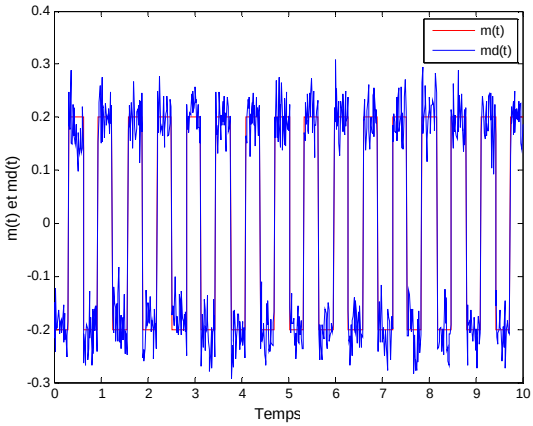
$(c) SNR = 30dB$

Fig4.16 : Les messages décryptés en présence de bruits, pour différents SNR

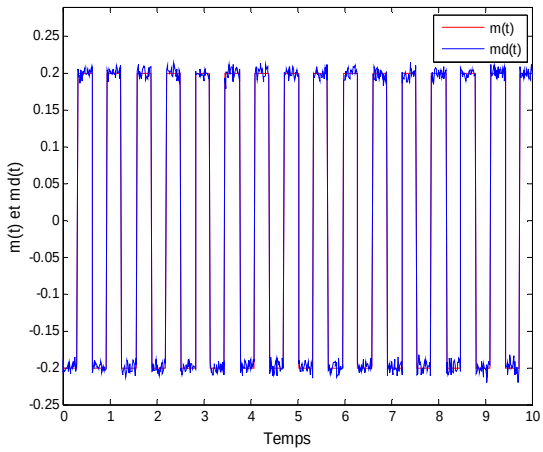
2) m est un signal carré



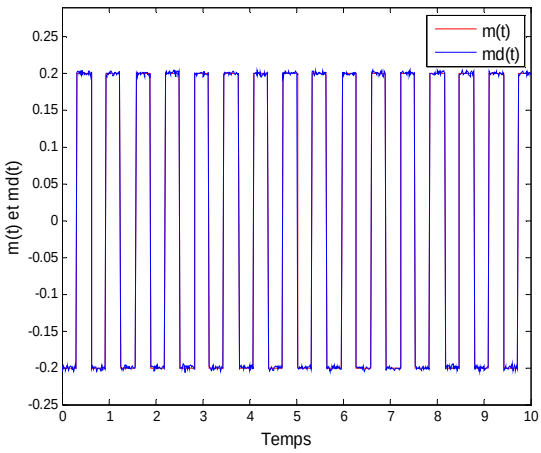
$(a)\ SNR = 5dB$



$(b)\ SNR = 15dB$



$(c)\ SNR = 30dB$



$(d)\ SNR = 40dB$

Fig4.17 : Les messages décryptés en présence de bruits, pour différents SNR

Interprétation des résultats obtenus

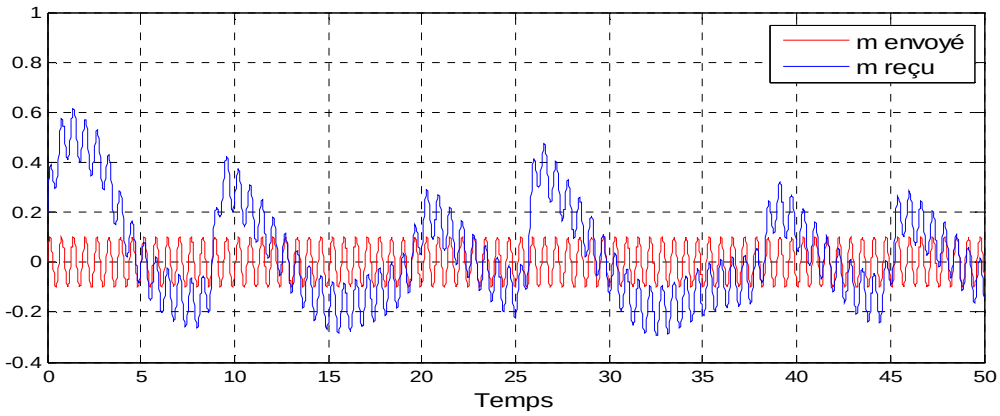
La présence du bruit sur le signal transmis, engendre des erreurs dans l'estimation des états de l'émetteur, par conséquence le message est complètement perdu. On arrive à voir cela pour une valeur$SNR = 5db$qui corespand à un grand niveau de bruit. Une bonne restauration du message a eu lieu pour la valeur $SNR = 30db$ pour le signal sinusoïdal et $SNR = 40db$ pour le signal carré.

D'après ces résultats, nous constatons bien que notre système est insensible au bruit. Ceci illustre sa robustesse vis-à-vis aux bruits de canal.

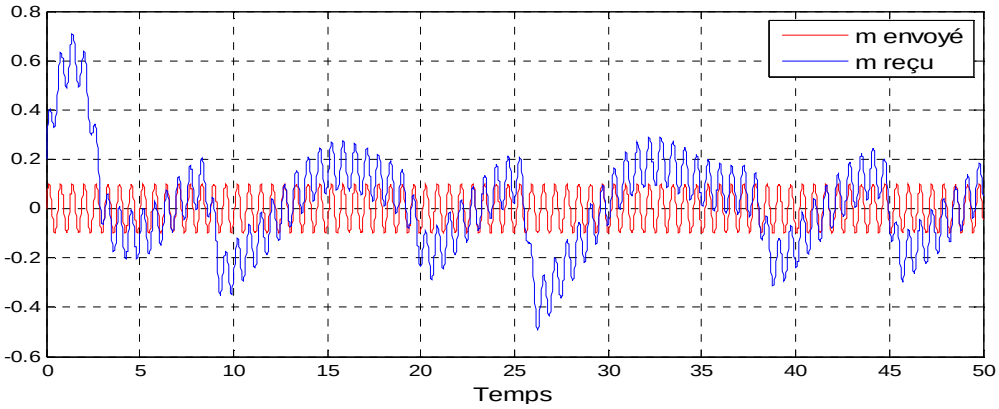
4.7.2 Robustesse aux variations des paramètres

Dans ce qui suit, nous testons la robustesse et la capacité d'adaptation du système de communication face à un pirate possédant des paramètres proche des valeurs réels du système. Dans le système (4.12) les paramètres (g, q, k) constituent les clés de sécurité. Il est à noter que plus le nombre de paramètres est grand, plus la transmission est plus sécurisée. Nous allons varier en premier lieu le paramètre q uniquement, $g = 4.46$ et $k = 0.05$ restent constants. Dans cette partie, nous considérons le cas d'une transmission d'un signal sinusoïdal.

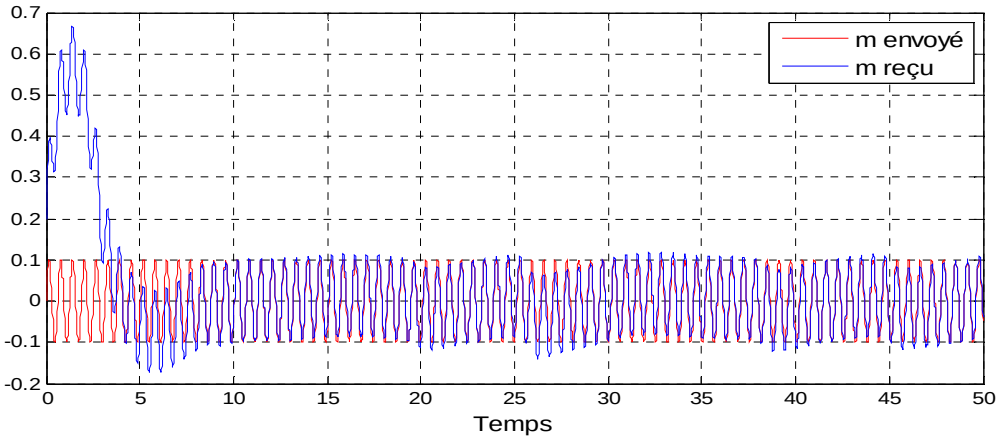
Nous allons transmettre trois fois le même message, mais pour des valeurs de q différentes : $q = 1.379$, $q = 1.39$, $q = 1.381$. Les résultats obtenus sont montrés par la figure (4.17)



(a) $q = 1.379$



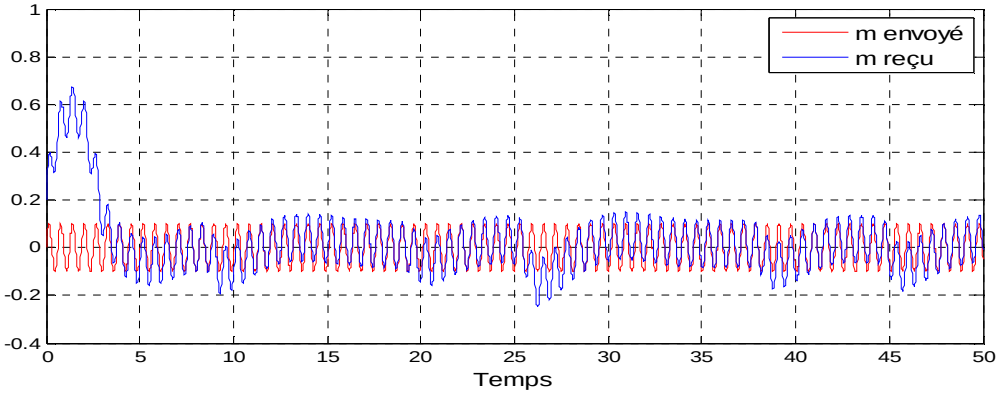
(b) $q = 1.39$



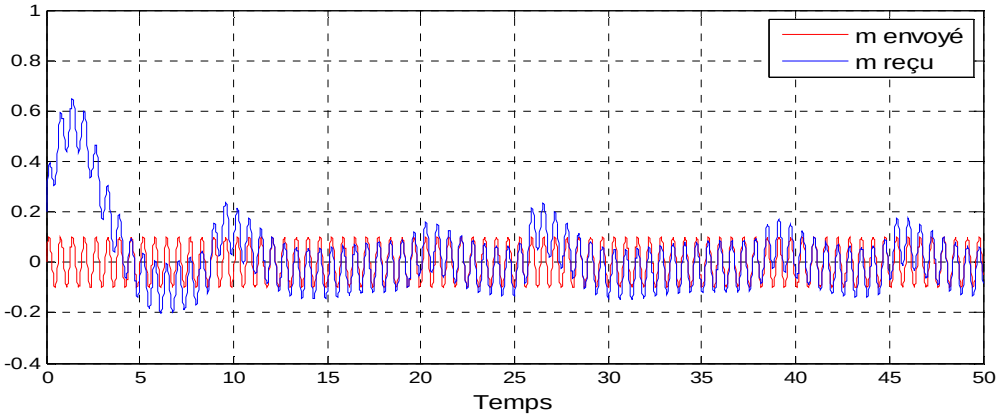
(c) $q = 1.381$

Fig4.18 : la reconstruction du message m pour différentes valeurs de q

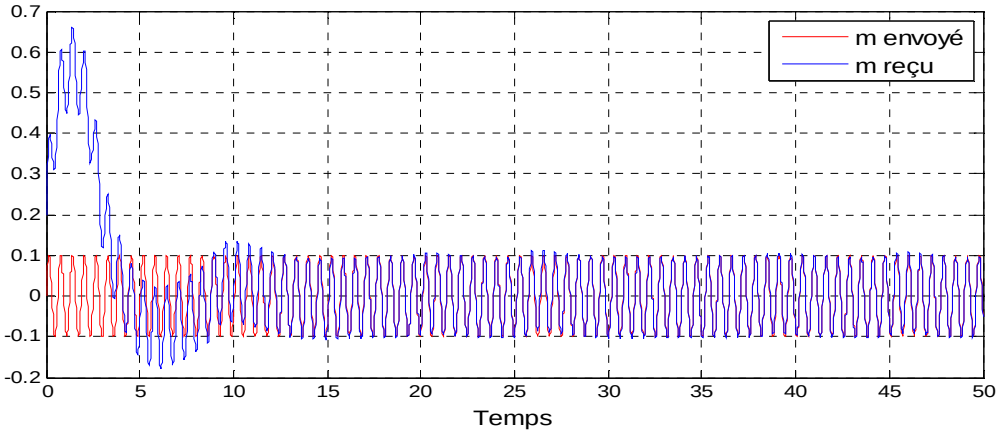
Ensuite, nous fixerons les paramètres q=1.38, k=0.5, et nous varierons seulement le paramètre$g$, les résultats obtenus sont présenté par la figure suivante



(a) $g = 4.45$



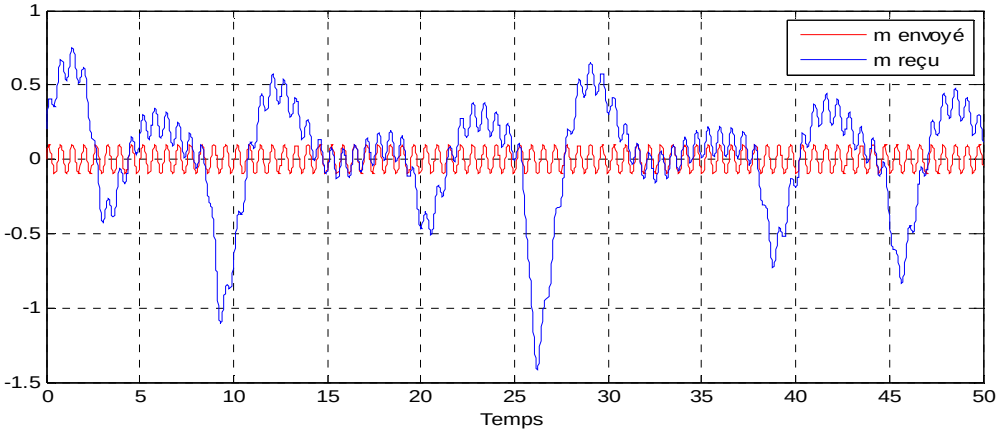
(b) $g = 4.47$



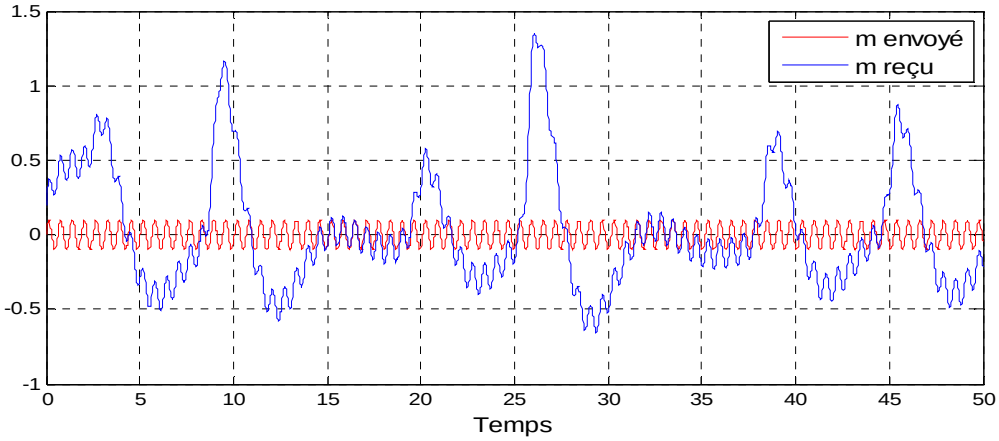
(c) $g = 4.461$

Fig4.19 : la reconstruction du message m pour différentes valeurs de g

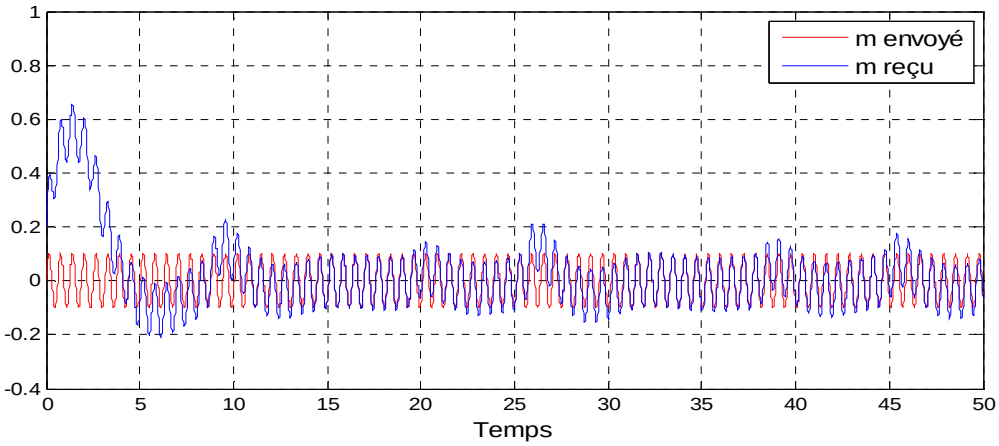
En dernier nous varierons le paramètre k uniquement, les paramètres g=4.46 et q=1.38 restent constants, la figure suivant illustre les résultats obtenus



(a) $k = 0.49$



$(b)\ k = 0.56$



$(c)\ k = 0.501$

Fig4.20 : la reconstruction du message m pour différentes valeurs de k

Interprétation des résultats obtenus

D'après les résultats obtenus on peut conclure que notre système est robuste face aux variations des paramètres.

- **Remarque**

Une étude a été réalisé auparavant est ce avec une variation de paramètres au niveau de l'émetteur, ce qui s'avère robuste.

Nous avons opté pour des variations au niveau du récepteur, les résultats obtenus confirment sa robustesse aussi.

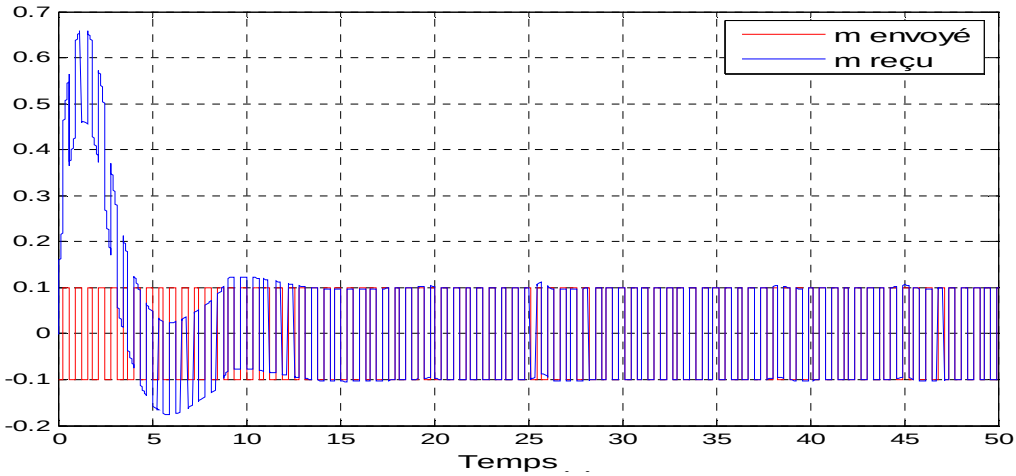
4.8 Etude du retard

Dans ce qui suit nous avons introduit des petits retards dans notre système chaotique pour voir leurs influences au niveau de la réception du message. Pour cela nous avons en premier lieu introduit un retard sur la ligne de transmission du message seulement, puis sur la ligne de la synchronisation. Les résultats obtenus sont illustrés par les figures suivantes.

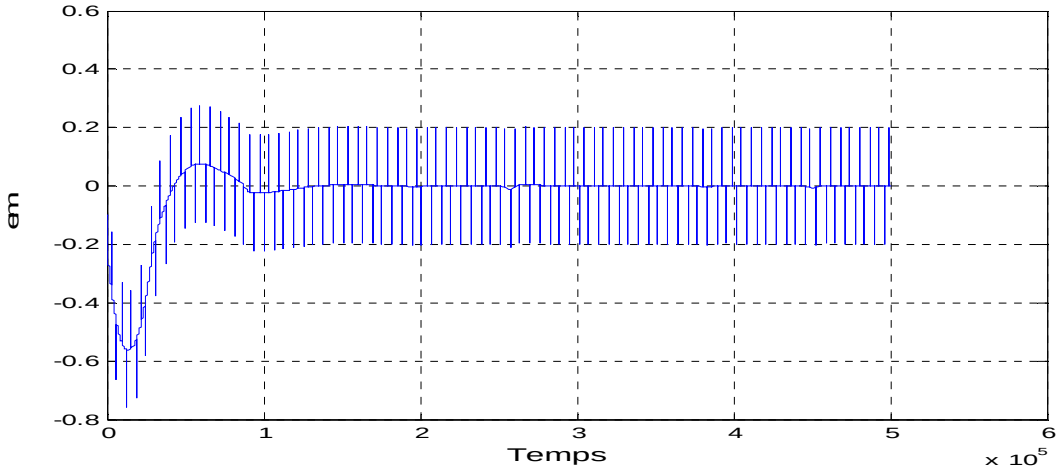
4.8.1 Retard sur le message

- **Pour $\tau = 10^{-4}$**

a- Signal carré

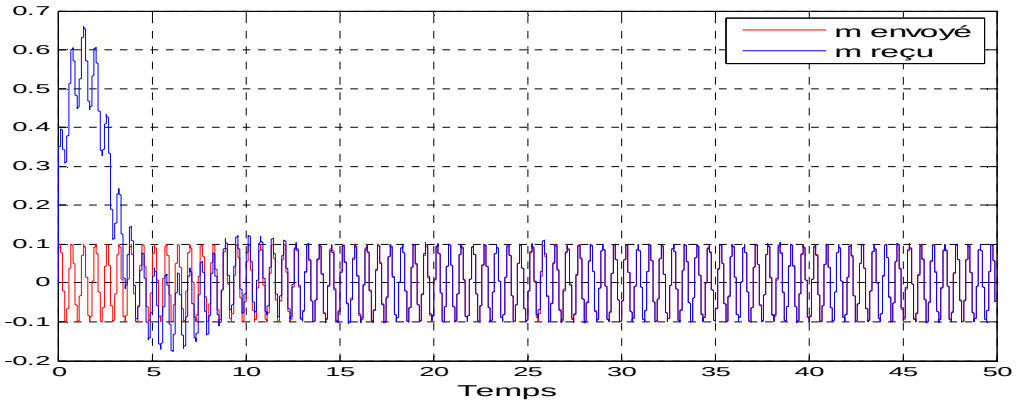


a1- Message envoyé et récupéré

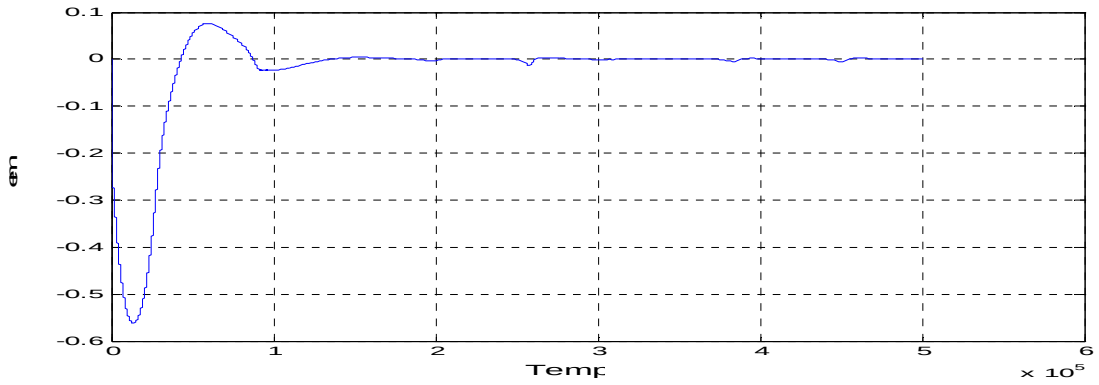


a2- Erreur de synchronisation sur le message

b- Signal sinusoïdal



b1- Message envoyé et récupéré

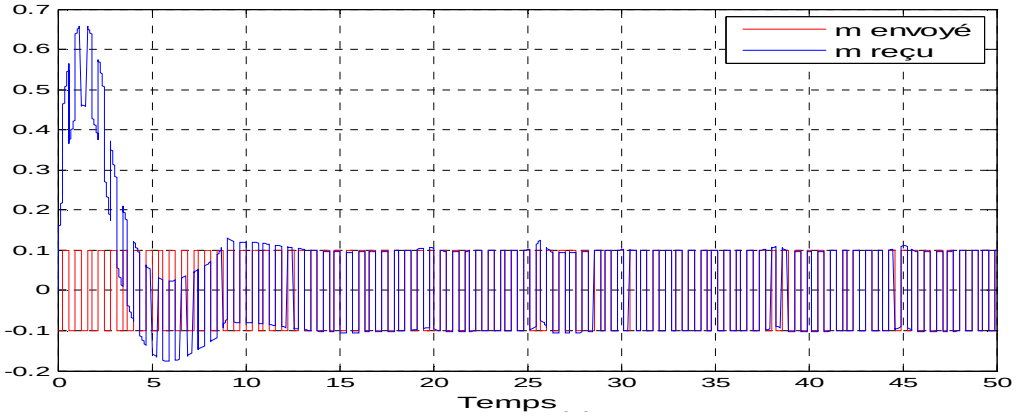


b2- Erreur de synchronisation sur le message

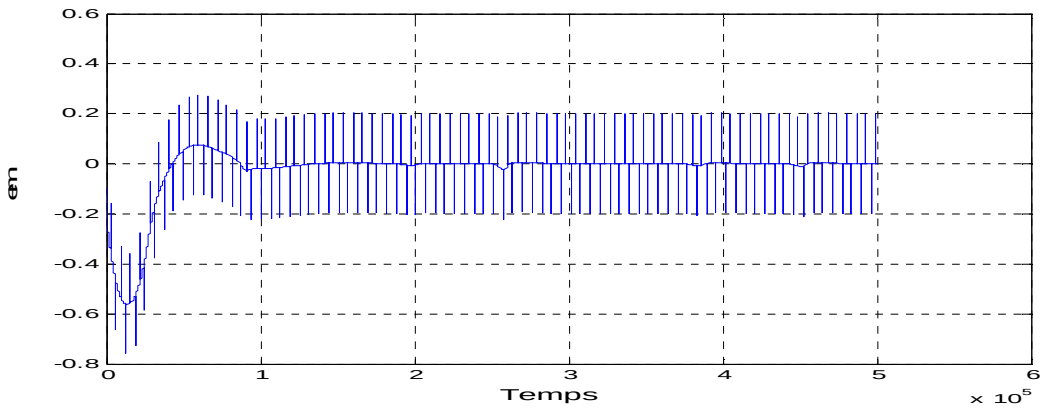
Fig4.21 : Résultat de simulation pour un signal carré et sinusoïdal à $\tau = 10^{-4}$

➢ **Pour** $\tau = 2 * 10^{-4}$

a- Signal carré

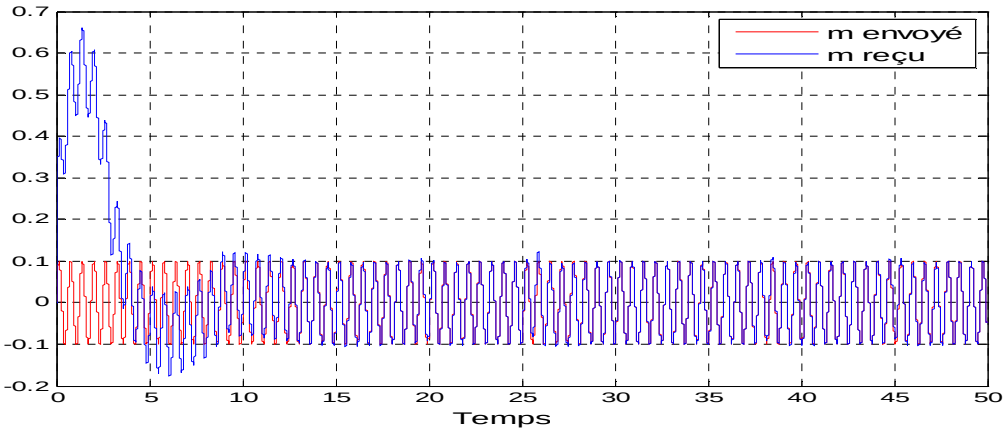


a1- Message envoyé et récupéré

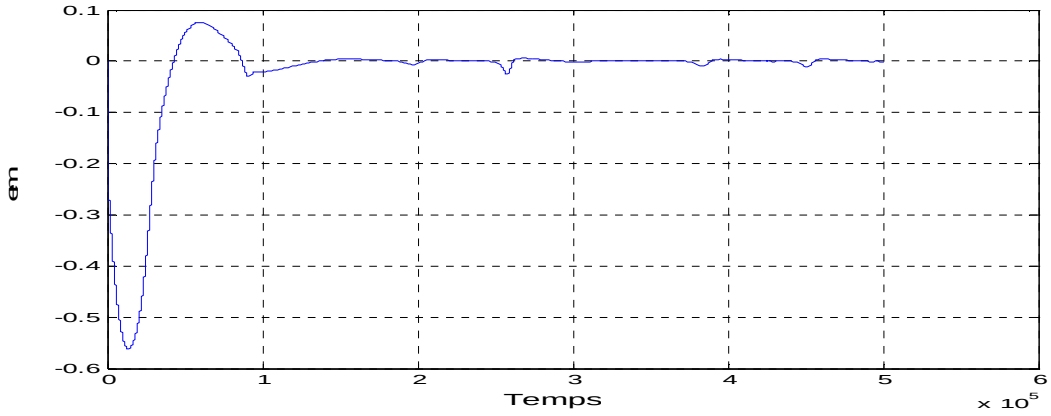


a2- Erreur de synchronisation sur le message

b- Signal sinusoïdal



b1- Message envoyé et récupéré

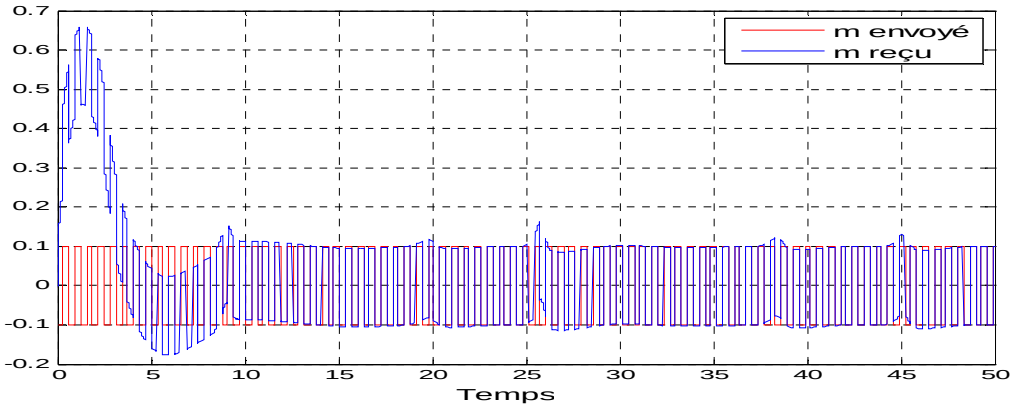


b2- Erreur de synchronisation sur le message

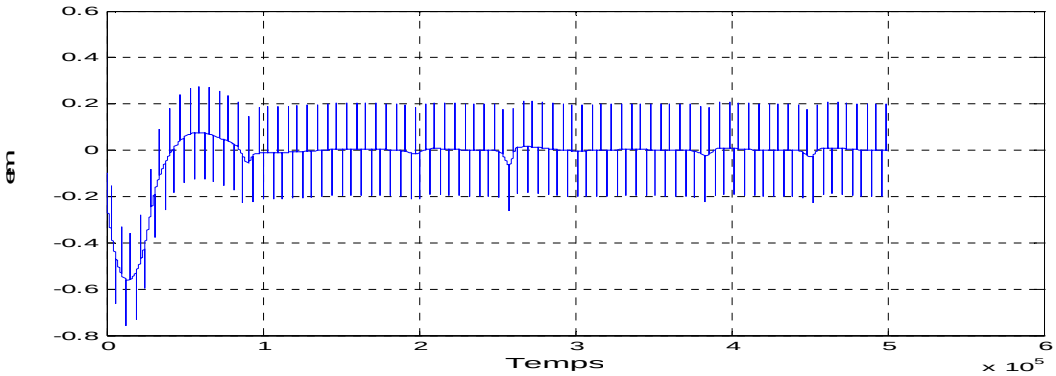
Fig4.22 : Résultat de simulation pour un signal carré et sinusoïdal à $\boldsymbol{\tau = 2 * 10^{-4}}$

➢ **Pour $\tau = 5 * 10^{-4}$**

a- Signal carré

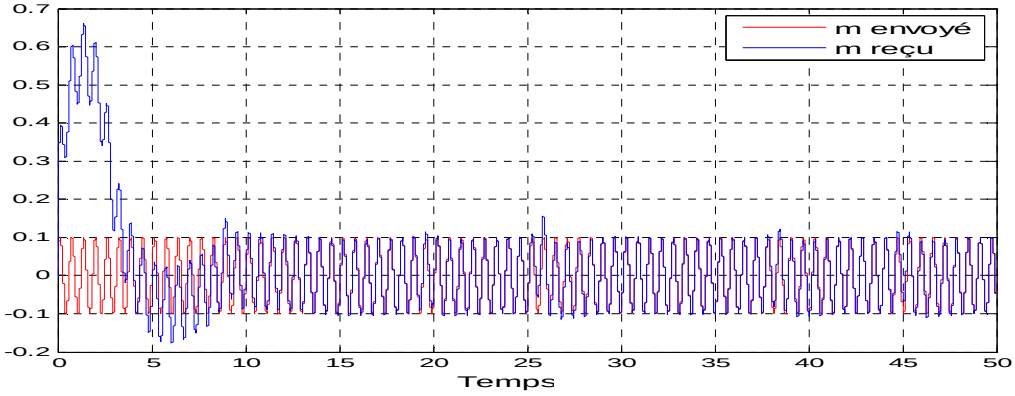


a1- Message envoyé et récupéré

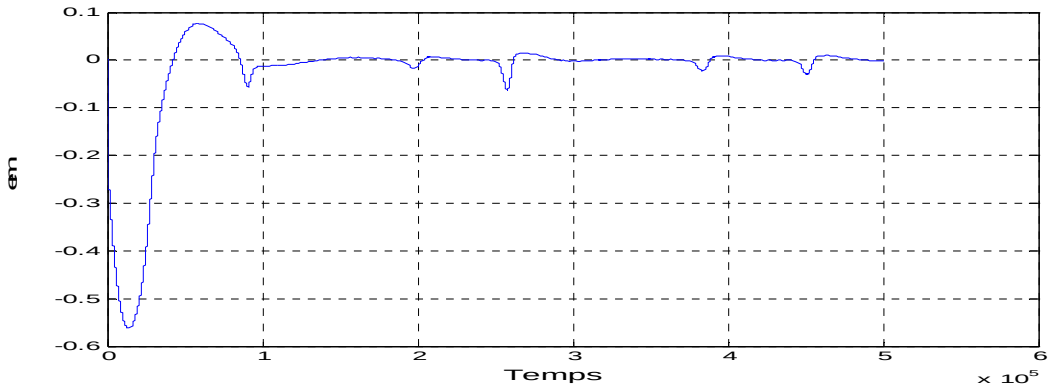


a2- Erreur de synchronisation sur le message

b-Signal sinusoïdal



b1- Message envoyé et récupéré

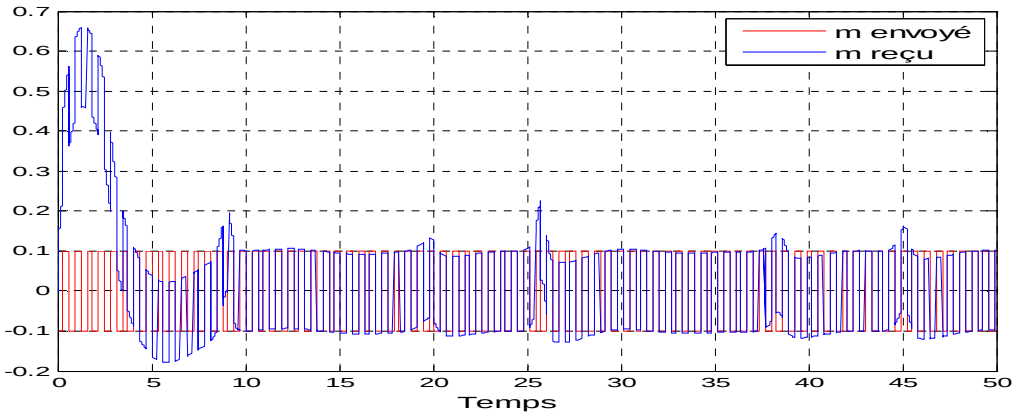


b2- Erreur de synchronisation sur le message

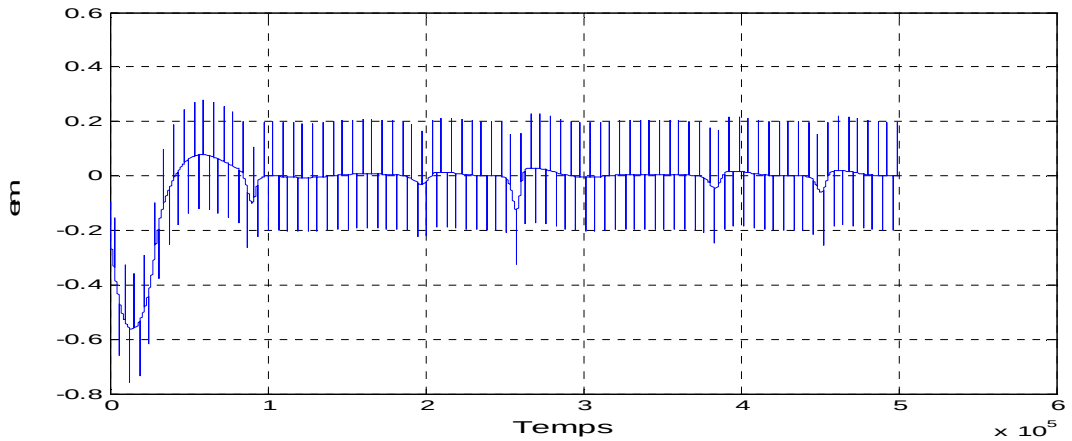
Fig4.23 : Résultat de simulation pour un signal carré et sinusoïdal à $\boldsymbol{\tau = 5 * 10^{-4}}$

- **Pour $\boldsymbol{\tau = 10^{-3}}$**

a- Signal carré

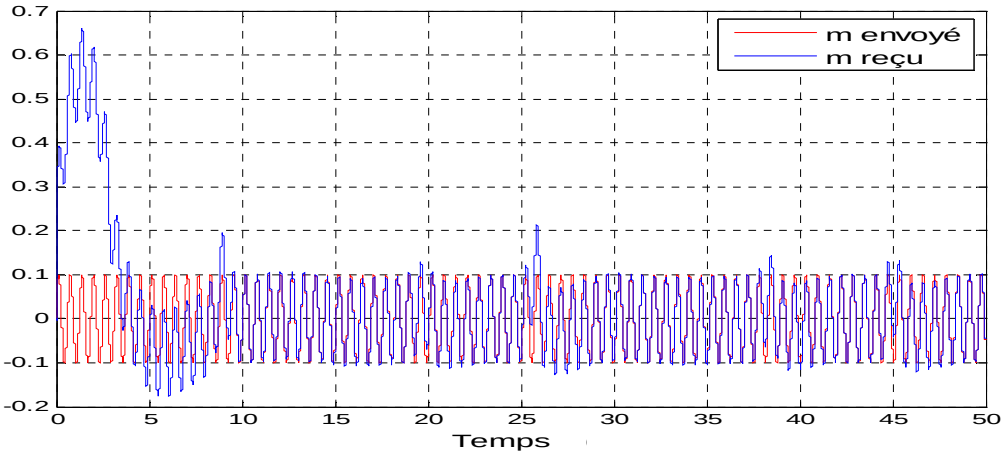


a1- Message envoyé et récupéré

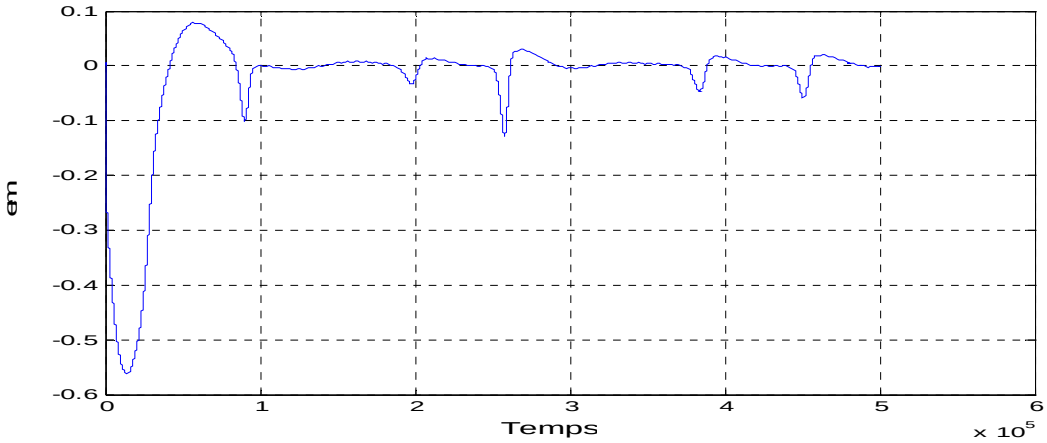


a2- Erreur de synchronisation sur le message

b-Signal sinusoïdal



b1- Message envoyé et récupéré

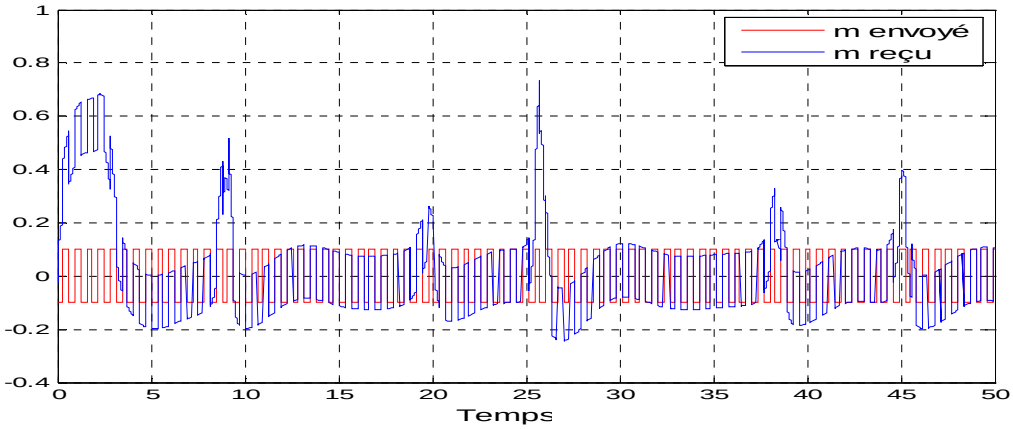


b2- Erreur de synchronisation sur le message

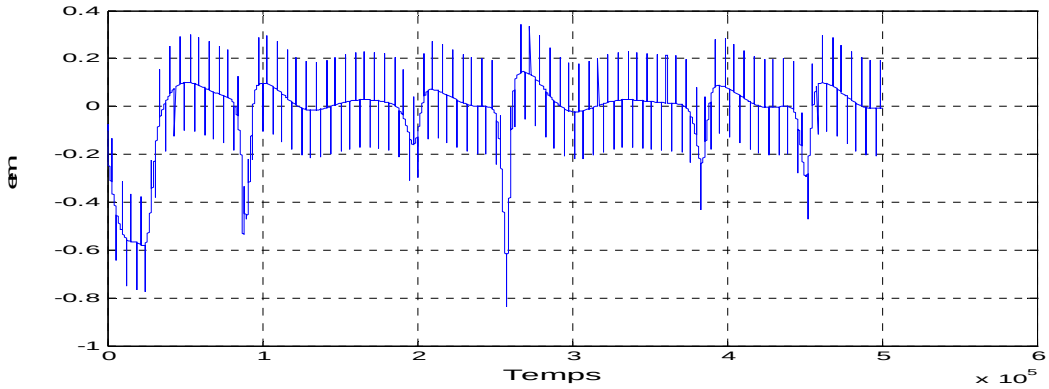
Fig4.24 : Résultat de simulation pour un signal carré et sinusoïdal à $\tau = 10^{-3}$

- **Pour $\tau = 5 * 10^{-3}$**

a- Signal carré

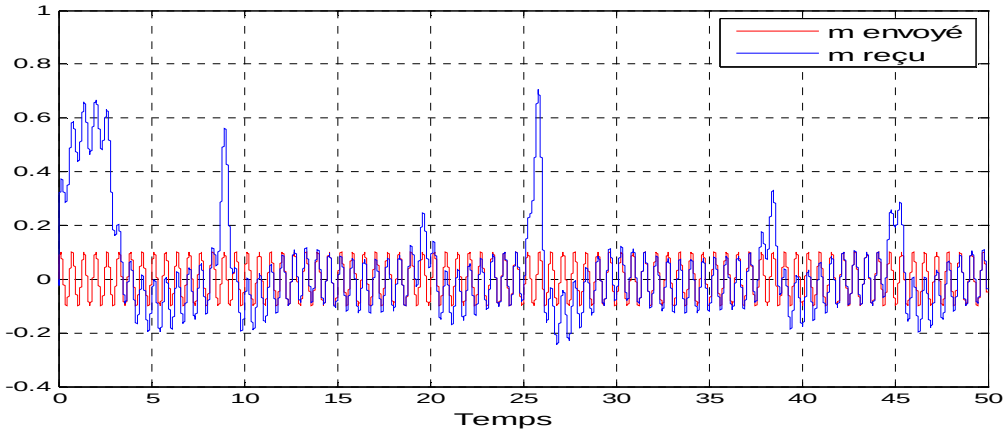


a1- Message envoyé et récupéré

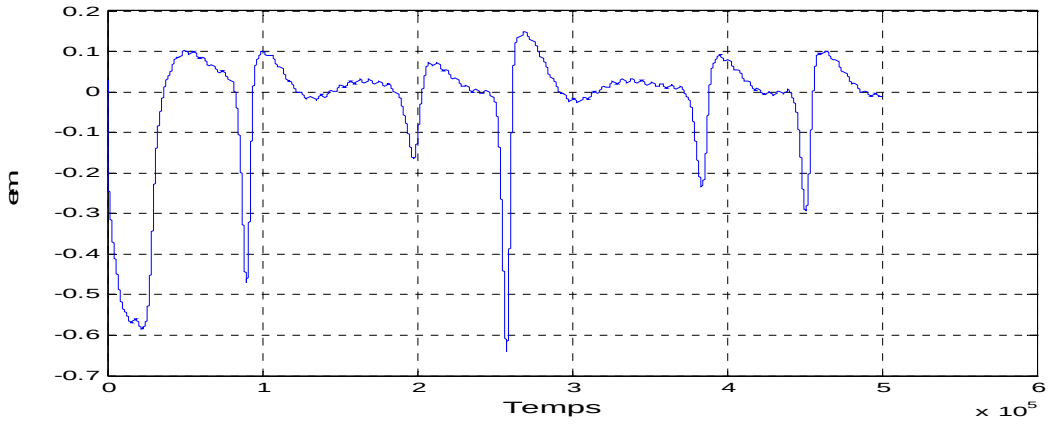


a2- Erreur de synchronisation sur le message

b- Signal sinusoïdal



b1- Message envoyé et récupéré



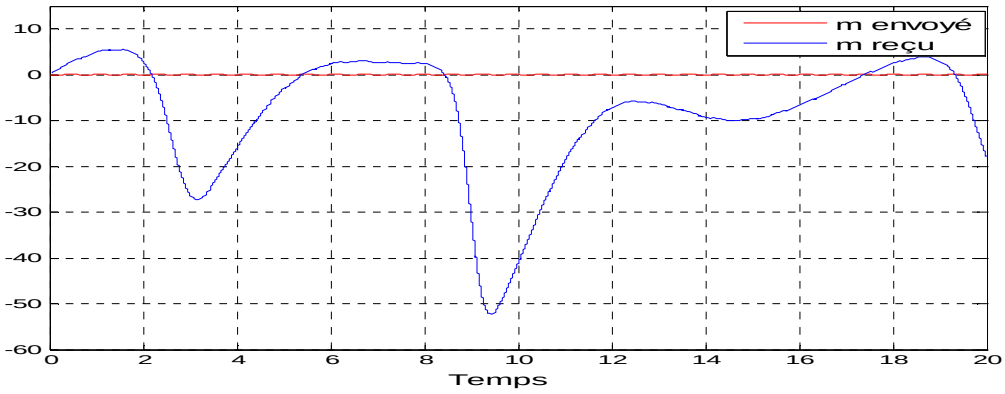
b2- Erreur de synchronisation sur le message

Fig4.25 : Résultat de simulation pour un signal carré et sinusoïdal à $\boldsymbol{\tau = 5 * 10^{-3}}$

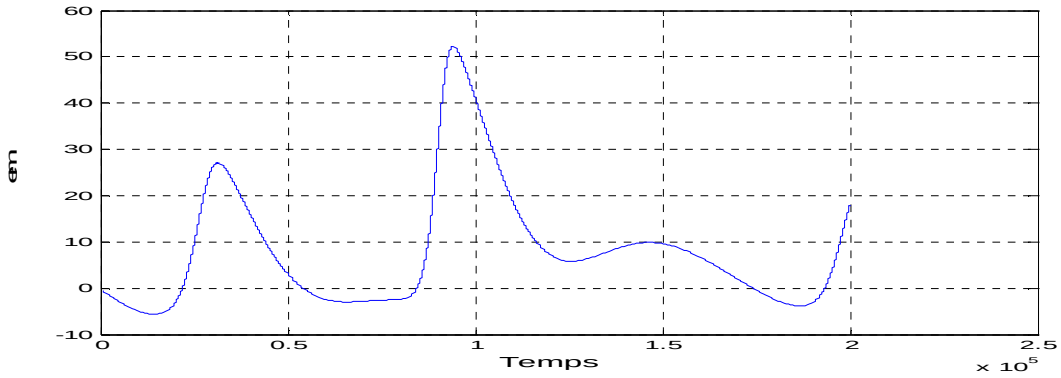
4.8.2 Retard sur la synchronisation

- **Pour $\tau = 10^{-4}$**

a- Signal carré

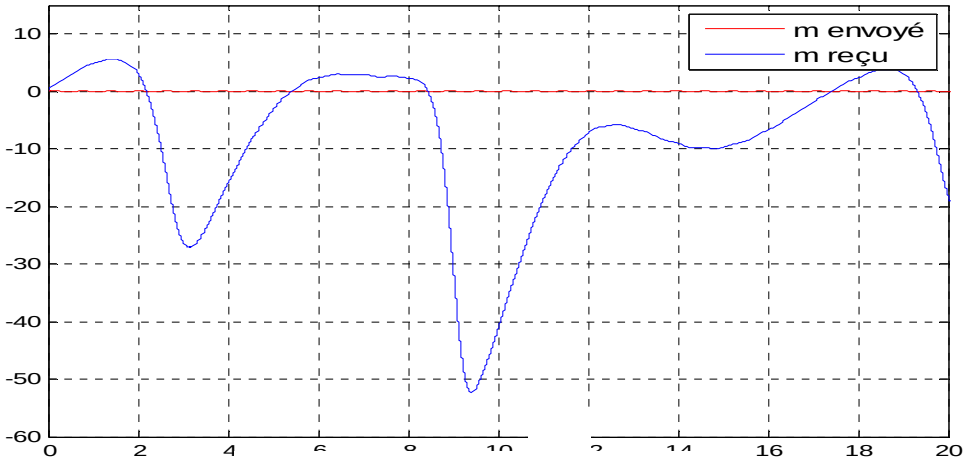


a1- Message envoyé et récupéré

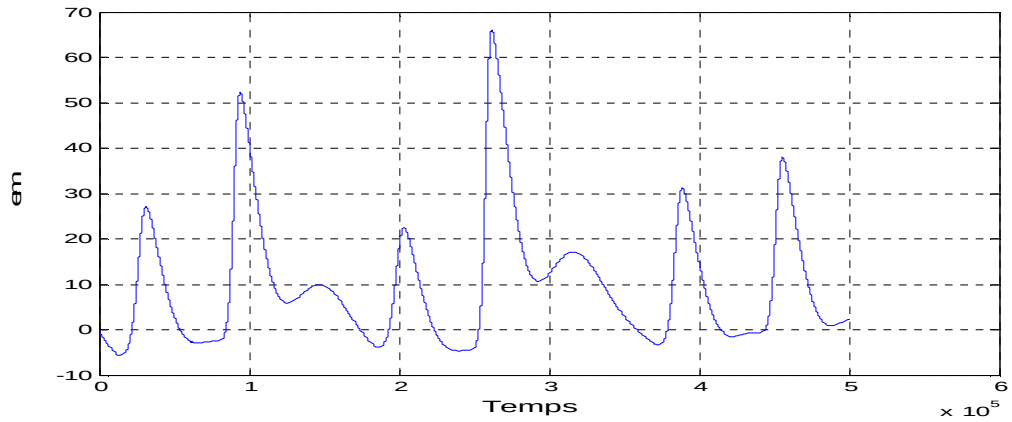


a2- Erreur de synchronisation sur message

b-Signal sinusoïdal



b1- Message envoyé et récupéré

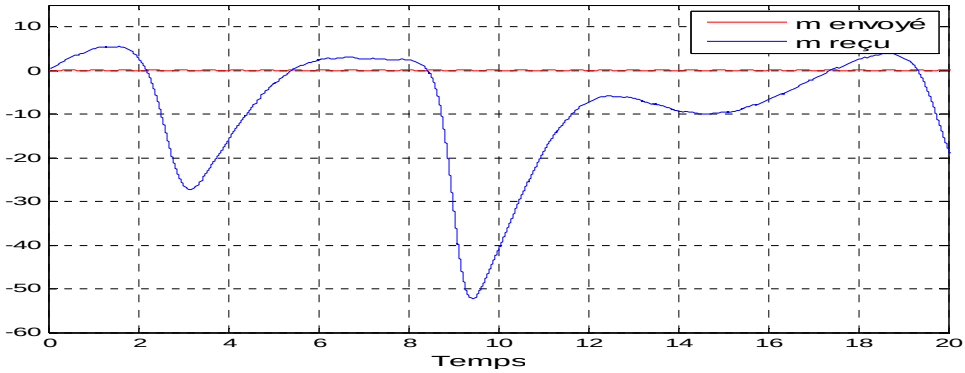


b2- Erreur de synchronisation sur le message

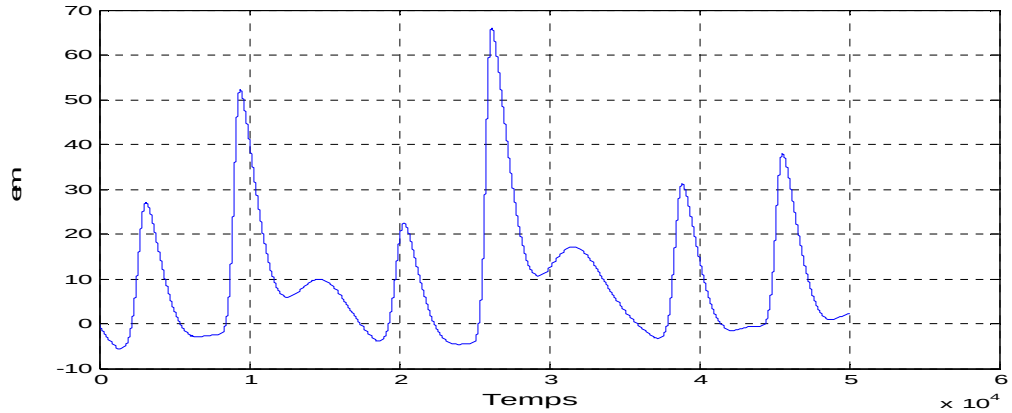
Fig4.26 : Résultat de simulation pour un signal carré et sinusoïdal à $\tau = 10^{-4}$

➢ **Pour $\tau = 10^{-3}$**

a- Signal carré

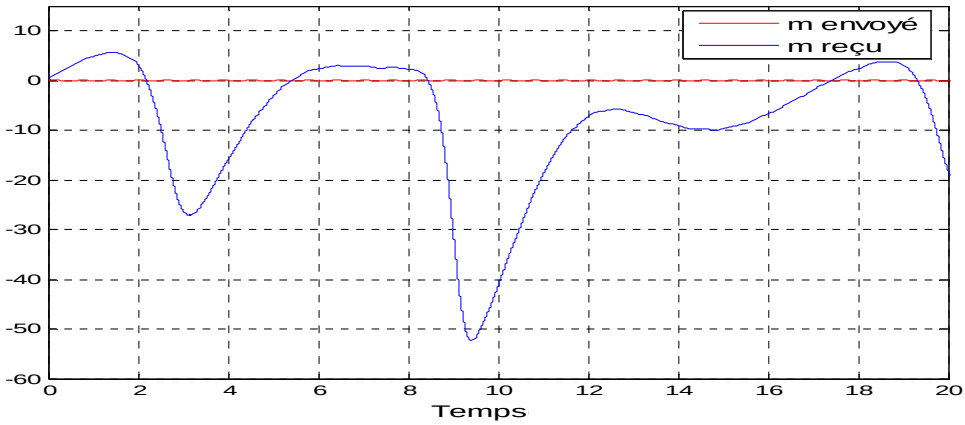


a1- Message envoyé et récupéré

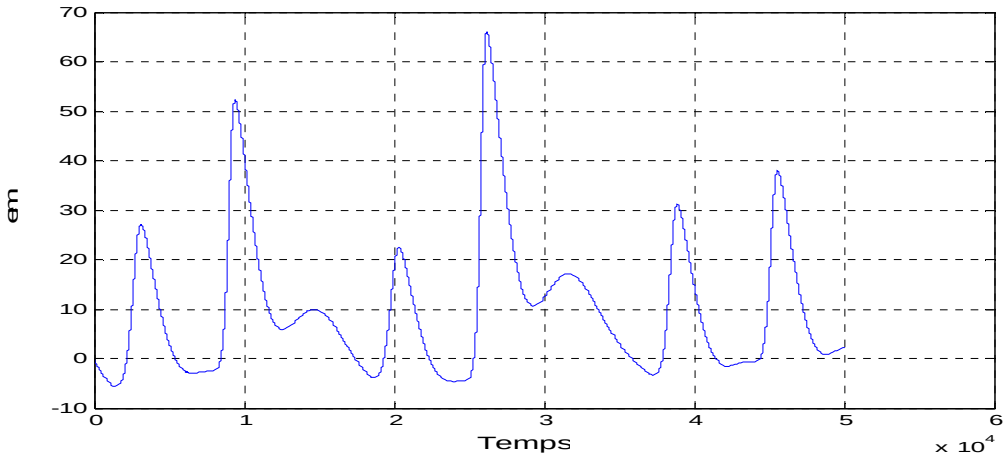


a2- Erreur de synchronisation sur le message

b- Signal sinusoïdal



b1- Message envoyé et récupéré



b2- Erreur de synchronisation sur le message

Fig4.27 : Résultat de simulation pour un signal carré et sinusoïdal à $\boldsymbol{\tau = 10^{-3}}$

Interprétation des graphes

On constate que pour n'importe quelle valeur du retard, la synchronisation n'a pas eu lieu, le message obtenu est complètement déformé.

La récupération du message est impossible, et cela même en introduisant un retard très petit. Pour remédier à ce problème, il faut chercher un autre type d'observateur qui peut compenser ce retard. Peu de travaux ont été réalisés sur ce problème, par exemple, on peut citer le travail de Liu [24].

Saïd

4.9 Conclusion :

Dans ce dernier chapitre, nous avons donné les résultats de simulation du système de transmission à base de la synchronisation impulsive de deux oscillateurs chaotiques de Colpitts. Nous avons d'abord exposé le schéma synoptique du dispositif de transmission et de synchronisation impulsive à base de systèmes chaotiques de Colpitts. Ensuite, nous avons présenté l'oscillateur chaotique de Colpitts en donnant son circuit électronique et son modèle d'état. Enfin, nous avons donné la structure de l'observateur impulsif.

La synchronisation impulsive a été appliquée pour synchroniser deux oscillateurs chaotiques de Colpitts, pour deux cas de transmission : une transmission à une seule voie et une transmission à deux voies. Les résultats de simulations montrent que l'erreur de synchronisation converge vers zéro lorsque nous utilisons deux voies de transmission, ce qui n'est pas le cas avec une transmission à une seule voie.

La robustesse du schéma de transmission sécurisé à partir de deux circuits de Colpitts impulsivement synchronisés est étudiée à la fin de ce chapitre pour connaitre la réaction du système cryptographique face aux bruits et aux variations des paramètres. Les différents résultats de simulations obtenus montrent les performances du système de transmission proposé. Néanmoins, il est à noter que l'observateur proposé présente l'inconvénient de ne pas tenir compte des retards sur la ligne de tranmission.

Conclusion générale

L'objectif de ce mémoire est d'étudier un système de transmission sécurisé à base de deux oscillateurs chaotiques de Colpitts en utilisant un observateur de type impulsif. Ce système de transmission exploite les propriétés des systèmes chaotiques pour transmettre des données d'un système émetteur vers un système récepteur comportant un observateur impulsif.

Dans le premier chapitre de ce mémoire, nous avons défini les systèmes chaotiques en donnant leurs propriétés les plus connues et les plus intéressantes pour notre système comme l'aspect aléatoire d'un signal chaotique, le déterminisme et la sensibilité aux conditions initiales. Nous avons ensuite développé les différents cas qui peuvent mener au chaos dans un système dynamique.

Dans le deuxième chapitre, nous avons introduit la cryptographie chaotique et les concepts de base d'un schéma de cryptage. Nous avons expliqué le cryptage par le chaos et les différentes manières de masquer l'information utile à transmettre par un signal chaotique. Dans la deuxième partie de ce chapitre, nous avons abordé la synchronisation chaotique, une étape essentielle dans un système de transmission a base du chaos. Nous avons aussi présenté les différents régimes de synchronisation.

Dans le troisième chapitre de ce mémoire, nous avons étudié particulièrement une méthode de synchronisation récente qui consiste à utiliser de simples impulsions de commande pour synchroniser deux systèmes chaotiques. Il s'agit de la synchronisation impulsive en utilisant un observateur impulsif.

Dans le dernier chapitre de ce mémoire, nous avons donné le circuit de l'oscillateur chaotique de Colpitts ainsi que son modèle d'état. Un observateur impulsif a été également proposé pour reconstituer les états de l'oscillateur de Colpitts. Nous avons illustré la méthodologie par des résultats des simulations effectuées sous MATLAB/SIMULINK.

Le système oscillateur de Colpitts-observateur impulsif a été utilisé dans un système cryptographique pour transmettre un message d'un émetteur contenant l'oscillateur de Colpitts vers un récepteur contenant l'observateur impulsif. Des résultats de simulations sont donnés pour deux cas : un cryptage à une seule voie et un cryptage à deux voies. La synchronisation des états et des messages envoyés et reçus est bien établie dans le cryptage à deux voies, ce qui n'est pas le cas dans le cryptage à une seule voie où l'erreur de synchronisation des messages envoyé et reçu n'est pas convergente.

La robustesse du système de transmission proposé est étudiée face aux bruits du canal, aux variations des paramètres et aux retards. Les résultats montrent que le système est sensible aux retards et aux variations des paramètres des oscillateurs. Dans le cas des bruits sur le canal de transmission, la transmission est sensible aux bruits ayant un rapport signal/bruit (SNR) inférieur à 30db pour un message sinusoïdal et 40db pour un message carré.

Les résultats de synchronisation impulsive sont très bons, et nous motivent à essayer de concevoir des systèmes de transmission plus complexes et encore plus robustes aux bruits, aux retards et aux variations des paramètres.

Comme perspectives à notre travail, nous pouvons envisager d'aborder les points suivants :

-sur le plan théorique

- explorer le phénomène du retard, étudier de manière approfondie son influence sur la synchronisation et proposer de nouvelles structures d'observateurs impulsifs tenant compte du retard sur le signal de synchronisation
- étudier un observateur à modes glissant impulsif avec la fonction de discontinuité.

- sur le plan pratique

- réaliser le dispositif de transmission complet (circuit émetteur, circuit récepteur, circuit de synchronisation) afin de valider les résultats théoriques et d'effectuer des tests sur le retard.

Bibliographie

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

[2] O. Megherbi « Etude et Réalisation d'un Système Sécurisé à Bas de Systèmes Chaotiques ». Mémoire de Magister, UMMTO, 2013.

[3] T. Hamaizia, «Systèmes Dynamiques et Chaos 'Application à l'Optimisation a l'aide d'Algorithme Chaotique' », Docteur en sciences, Univ Constantine, 2013.

[4] E. Cherrier, « Estimation de l'Etat et des Entrées Inconnues pour une Classe de Systèmes non Linéaires », Thèse Doctorat, Nancy, France, 2006.

[5] T. Yang, « A Survy of Chaotic secure Communications Systems, International Journal of Computational cognition» vol 2, pp 81–130, 2004.

[6] E D S. Goncalves, « Introduction aux Systèmes Dynamique et Chaos », Ecole d'ingénieur, 2004.

[7] A. Ali Pacha, N. Hadj Said « la Cryptographie et ses Principaux Systems : R.S.A et D.E.S» Vol 12, No 1, USTO-BP 1505,2002.

[8] N. Hamri, «La Synchronisation et le Contrôle du Chaos dans un Système Tridimensionnel», Proceedings Fractales 98, Séminaire National sur les Fractales dans la Compression des Images, pp. 48-57, 1998.

[9] A. Abdoul Rahuman « Analyse des Systèmes Non-Linéaires à Dynamique Complexes » Thèse Magister, Univ Tlemcen, 2014.

[10] H. Hamiche, «Inversion à Gauche des Systèmes Dynamique Hybrides Chaotique. Applications à la Transmission Sécurisée de Données», Thèse de Doctorat, UMMTO, 2011

[11] G. Zheng, « Forme Normales d'Observabilité Paramétrées par les Sorties : Application au Cryptage par Synchronisation de Système Chaotiques », Thèse Doctorat, Cergy-Pontoise, France, 2006.

[12] G. Millérioux and C. Mira. «Coding scheme based on chaos synchronization from noninvertible maps», "Int. J. of Bifurcate and Chaos", Vol 8, No 10, pp 2019–2029, 1998.

[13] H. Dimassi, « Synchronisation des Systèmes Chaotique par Observateurs et Application à la Transmission d'Information », Thèse de Doctorat, Paris Sud, 2012.

[14] U. Feldmann, M. Hasler and W. Schwarz, «Communication par Chaotic Signals: The Inverse System Approach», International Journal of Circuit Theory and Applications vol 24, pp 551-579, 1996.

[15] D. Benzemam, « Systèmes Chaotiques et Hyperchaotiques pour la Transmission Sécurisée de Données », Mémoire de Magister, Univ Tlemcen. .

[16] C. Li, X. Liao & K.W Wong, « Chaotic lag Synchronization of Coupled Time-Delay Systems and its Application in Secure Communication. Systems & Control Letters», pp 133–142, 1986.

[17] S. Alexandru, « Fondements de la Théorie de la Transmission de l'Information », Pesses Polytechniques romandes, 1987.

[18] M. L'Hernault, A. Ouslimani, J.P.Barbot, « Conception et Réalisation d'un Observateur à Modes Glissants pour un Oscillateur de Colpitts Chaotique » vol 55, No 2, 2008

[19] M. Strok, J. Hrusak, D. Mayer, « Discrete Time Chaotique Systems Impulsive Synchronization and Data Transmission» Conference on Systems. ISSN: 1790-2769 ISBN: 978-960-474-097-0.

[20] T. Yang, «Impulsive Stabilization for Control and Synchronization of Chaotic Systems: Theory and Application to Secure Communication», Vol 44, No 10, 1997.

[21] Y. Khaled, J.-P. Barbot, D. Benmerzouk, K. Busawon and M. Ghanes, « Strange Attractor Identification and State Observation under Sparse Measurements», 2nd International Symposium on Environment Friendly Energies and Applications, 2012.

[22] W. M. Haddad, V. Chellaboina, S. G. Nersesov. «Impulsive and Hybrid Dynamical Systems. Stability, Dissipativity and Control», Princeton University Press, Princeton, NJ, 2006.

[23] Y. Khaled, « Contribution à la Commande et l'Observation des Systèmes Dynamiques Continus sous Mesures Clairsemées » Docteur de l'Université de Cergy-Pontoise en Automatique.

[24] L. Guangmin, W. Ding, «Impulsive Synchronization for a Chaotic system with Channel time-delay», Communication in Nonlinear Science and Numerical Simulations, Volume 16, pp. No 2, 2011