RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR
ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITÉ DE MOHAMMED SEDDIK BEN YAHIA-JIJEL
FACULTÉ DES SCIENCES ET DE LA TECHNOLOGIE
DÉPARTEMENT D'ELECTRONIQUE

Projet de fin d'études pour l'obtention du Diplôme de Master en télécommunication (LMD)

Option : systèmes des télécommunications

Thème :

Conception d'un système de chiffrement d'information à base d'un Memristor

Réalisé par :

M^{elle} : NourElhouda BOUKABACHE

M^{elle} : Hanane MERADJI

Proposé par :

Dr: Manel MESSADI

Année universitaire

2019-2020

بسم الله الرحمن الرحيم

وَمَا أُوتِيتُمْ مِنَ الْعِلْمِ إِلاَّ قَلِيلاً (85)

سورة الإسراء

وَقُلْ رَبِّ زِدْنِي عِلْماً (114)

سورة طه

Remerciements

Avant tout nous remercions Dieu tout-puissant de nous avoir guidés durant toutes ces années et de nous donner le courage, la volonté et la patience pour réaliser ce travail.

Nos sincères remerciements et notre profonde gratitude à notre promotrice estimée Dr. MESSADI Manel, pour nous avoir encadré et suivie également pour son aide, ces orientations, sa patience et sa correction sérieuse de ce travail.

Nos vifs remerciements vont également aux membres du jury, d'avoir accepté de examiner notre travail et de l'enrichir par leurs propositions.

Nous souhaitons également adresser nos remerciements à l'ensemble des enseignants du département d'électronique, qui ont contribué à notre formation durant cinq années d'études.

Enfin, nous remercions toutes les personnes qui ont participé, de près ou de loin, à la réalisation de ce modeste travail.

DEDICACES

Avec l'aide d'Allah le tout Puissant, j'ai pu achever ce modeste travail que je dédie :

À ma très chère mère ; quoi que je fasse ou que je dise, je ne saurai point te remercier comme il se doit, ton affection me couvre ta bienveillance me guide et ta présence à mes côtés a toujours été ma source de force pour affronter les différents obstacles.

À mon père décédé trop tôt toujours présent dans mon cœur j'espère que, du monde qui est sien maintenant il apprécie ce geste comme preuve de reconnaissance de la part d'une fille qui a toujours prié pour tout puissant l'avoir en sa sainte miséricorde.

À ma grand-mère (maman Zineb) ceci est ma profonde gratitude pour ton éternel amour que ce travail soit le meilleur cadeau que je puisse t'offrir.

À mes grands-parents, mes oncles, mes tantes merci pour leurs amours et leurs encouragements que dieu leur donne une longue et joyeuse vie.

À la femme de mon oncle et même temps ma copine Salima, merci pour ton soutien et ta patience et grâce à toi aussi j'ai pu réaliser ce travail.
À mes meilleurs amis, Mimi et Inass qui m'ont toujours encouragé et à qui je souhaite plus de succès.
Sans oublier mon binôme Hanan pour son soutien moral sa patience et sa compréhension

Nour Elhouda

DEDICACES

Avec l'aide d'Allah le tout Puissant, j'ai pu achever ce modeste travail que je dédie :

À ma mère et mon père,

Aucune dédicace ne saurait être assez éloquente pour exprimer ce que vous méritez, pour tous les sacrifices que vous n'avez cessé de me donner depuis ma naissance, durant mon enfance et même à l'âge adulte.

Puisse Dieu, le tout puissant, vous préservez et vous accordez santé, longue vie et bonheur.

Je t'aime maman, merci.

À mon frère adoré Housem que j'aime énormément.

À ma soeur adorée Naouel.

À Mes très chers frères et soeurs.

Karima, Aymen et Anis.

À mes meilleurs amies Abdel wahab, Hadjer et Besma.

Sans oublier mon binôme Nour Elhouda pour son soutien moral sa patience et sa compréhension

Hanan

Résumé

La cryptographie joue un rôle important dans la sécurité et la fiabilité des systèmes de transmission de données. Notre travail de fin d'études consiste à réaliser un système de transmission sécurisé à base du système chaotique de Memristor. Ce système se compose de deux oscillateurs chaotiques identiques du système Memristor liés par un canal de transmission publique. Le message à transmettre est injecté dans la dynamique de Memristor au niveau de l'émetteur, la commande prédictive est appliquée pour établir la synchronisation à la fin une démodulation chaotique est utilisée pour restituer le message transmis. Les résultats de simulations montrent clairement l'efficacité de l'approche proposée.

Mots clefs : chaos, sécurisation de la communication, synchronisation du chaos, Memristor chaotique, commande prédictive, démodulation chaotique.

ملخص

يلعب التشفير دورًا مهمًا في أمان وموثوقية أنظمة نقل البيانات. يتمثل عملنا في التخرج في بناء نظام نقل آمن يعتمد على نظام ممريستور الفوضوي. يتكون هذا النظام من مذبذبين فوضويين متطابقين لنظام ممريستور مرتبطين بقناة إرسال عامة. يتم حقن الرسالة المراد إرسالها في ديناميكيات ممريستور على مستوى المرسل، ويتم تطبيق التحكم التنبئي لإنشاء التزامن واستخدام إزالة التشكيل الفوضوي لتقديم الرسالة المرسلة. تظهر نتائج المحاكاة بوضوح فعالية النهج المقترح.

الكلمات الرئيسية: الفوضى، أمن الاتصالات، مزامنة الفوضى، ممريستور الفوضوية ، التحكم التنبئي ، إزالة التشكيل الفوضوي.

Abstract

Cryptography plays an important role in the security and reliability of data transmission systems. Our graduation work is to build a secure transmission system based on the Memristor chaotic system. This system consists of two identical chaotic oscillators of the Memristor system linked by a public transmission channel. The message to be transmitted is injected into the dynamics of Memristor at the transmitter, predictive control is applied to establish synchronization at the end a chaotic demodulation is used to render the transmitted message. The simulation results clearly show the effectiveness of the proposed approach.

Keywords: chaos, communication security, chaos synchronization, chaotic Memristor, predictive control, chaotic demodulation.

Liste des figures

Liste des Tableaux

SOMMAIRE

CHAPITRE 1

Etat de l'art sur le chaos

CHAPITRE 2

Etat de l'art sur la synchronisation et le chiffrement d'informations par le chaos

CHAPITRE 3

Synchronisation du système Memristor chaotique par la commande prédictive

CHAPITRE 4

Chiffrement d'information à base de la commande prédictive et de Memristor

Introduction générale

Depuis l'antiquité, l'homme n'a pas cessé de chercher les différents moyens pour transmettre un message à son correspondant et pouvoir ainsi communiquer avec lui en toute sécurité. Il a fourni, à travers des époques successives, des efforts autant physiques qu'intellectuels pour pouvoir trouver une technique de communication efficace et appropriée.

En effet, les modes de télécommunications sont en évolution continue avec la recherche permanente de meilleurs débits, de facilité d'utilisation, de mobilité améliorée et surtout d'une confidentialité élevée [1].

La cryptographie a depuis des siècles été une histoire de conflit qui oppose deux camps, un qui cherche à cacher une information et un autre qui essaie de trouver ce qu'on lui cache. Ainsi à chaque fois que le premier trouve un moyen de chiffrer ses messages le second essaie et, avec le temps et les moyens dont il dispose, réussit à trouver la méthode ou « l'astuce » pour le décrypter. La cryptographie ancienne utilisait différents outils pour dissimuler une information ou un texte secret. Certains remplaçaient des mots par des nombres, d'autres mélangeaient, décalaient ou permutaient les lettres, comme dans la substitution alphabétique inverse, pour rendre la lecture du message difficile voire impossible [2].

La cryptographie actuelle cherche à transformer de façon mathématique et algorithmique un message clair pour obtenir un autre chiffré et qui, à première vue, semble aléatoire. Plus l'inversion de la transformation est difficile plus la sécurité est élevée et vice versa. On cherche alors un phénomène d'apparence aléatoire mais qui est déterministe à l'origine pour le masquage d'information [1].

Il existe plusieurs systèmes présentant ce comportement, ils sont dits chaotiques, ils sont régis par des lois déterministes, dépendent d'un ou de plusieurs paramètres et leur évolution dans le temps est imprévisible. L'étude de tels systèmes est liée à la théorie du chaos qui a connu un grand essor à partir de 1960 grâce aux travaux de plusieurs chercheurs notamment ceux de Lorenz et à la découverte de nouveaux outils de calculs [3].

Le chaos est caractérisé par un certain nombre de caractéristiques telles la sensibilité aux conditions initiales et l'imprévisibilité, ce qui rend les systèmes chaotiques très intéressants dans le cryptage des données [4].

La cryptographie chaotique est ainsi née par inclusion du chaos dans les télécommunications et systèmes de transmission. L'idée consiste à noyer un message dans un signal chaotique pour faire face aux éventuelles tentatives de piratage [1].

La transmission chaotique est un mode de communication à clé secrète. La connaissance de cette clé est nécessaire du côté de l'émetteur du message ainsi que du récepteur pour le chiffrement et le déchiffrement du message. On doit alors disposer au niveau du récepteur, d'un signal chaotique identique synchrone pour pouvoir récupérer le message masqué [1].

La synchronisation des systèmes chaotiques est une approche intéressante pour résoudre ce problème. Introduite en 1990 par les travaux de Pecora et Caroll [5,6] cette technique permet de reconstruire les états de l'émetteur à partir du signal transmis. Différentes approches ont été proposées depuis pour améliorer ce processus et réduire l'erreur entre les états de l'émetteur et ceux restaurés au niveau du récepteur [7, 8, 9].

Ce travail de mémoire Master consiste à réaliser un système de transmission sécurisée à base du chaos, ce système se compose de deux oscillateurs chaotiques identiques à base de système Memristor (chaotique) liés par un canal de transmission publique. Un message sera crypté puis envoyé à partir de l'oscillateur émetteur en employant le cryptage par inclusion (injection). Au niveau du récepteur, l'objectif est de récupérer ce signal utile en utilisant une synchronisation chaotique de l'oscillateur émetteur.

Pour bien présenté notre travail, ,nous avons organisé notre mémoire de la maniére suivante:

Dans le premier chapitre, nous allons définir les systèmes dynamiques de manière générale et les systèmes chaotiques de manière un peu plus détaillé, en suite nous allons présenter les propriétés permettant de caractériser les dynamiques chaotiques.

Le second chapitre fait le lien entre les systèmes chaotiques et le domaine des télécommunications. Celui-ci est centré sur le phénomène de synchronisation des systèmes chaotiques, ainsi que les techniques de transmission sécurisée d'informations qui reposent sur le principe de synchronisation chaotique, car l'emploi d'un signal chaotique dans le domaine des télécommunications pose directement le problème de synchronisation du récepteur dans le but de dupliquer le signal chaotique employé à l'émetteur. Ensuite, des différentes méthodes de synchronisation sont exposées. Un des objectifs du chaos étant de protéger l'information transmise, nous citons les différentes techniques de cryptages par le chaos.

Le troisième chapitre est dédié à la synchronisation de deux systèmes Memristor chaotiques identiques (maitre /esclave) par la commande prédictive, et dans le quatrième et dernier chapitre, nous présenteront une approche pour le chiffrement d'information à base de la commande prédictive et la Modulation/démodulateur chaotique.

Enfin, on termine par une conclusion générale et quelques perspectives.

CHAPITRE 1

État de l'art sur le chaos

1.1. Introduction :

Depuis longtemps, le chaos était synonyme du désordre et de confusion. Il s'opposait à l'ordre et devait être évité car la science était caractérisée par le déterminisme, la prévisibilité et la réversibilité. Poincaré fut l'un des premiers à entrevoir la théorie du chaos, il découvrit la notion de sensibilité aux conditions initiales à travers le problème de l'interaction de trois corps Célestes [10,11]. Le terme chaos définit un état particulier d'un système dont le comportement ne se répète jamais qui est très sensible aux conditions initiales, et imprédictible à long terme. Des chercheurs d'horizons divers ont alors commencé à s'intéresser à ce comportement [11]. Le chaos a ainsi trouvé de nombreuses applications dans différents domaines tel que la physiques, la biologie, la chimie l'économie, les télécommunications (Cryptage de l'information)..etc. Nous nous intéresserons principalement dans ce chapitre aux systèmes dynamiques chaotiques sur leurs applications, aspect aléatoire, l'attracteurs étranges et les différentes propriétés de ces systèmes, ce qui nous permettra de mieux comprendre la nature du chaos [1].

1.2. Systèmes dynamiques :

Un système dynamique peut être représenté par un ensemble de variables, qui évoluent au cours du temps. Ces variables peuvent être destinées pour l'étude des fluctuations d'état d'un phénomène ou d'un objet quelconque.

Un système dynamique en temps continu peut être modélisé mathématiquement par un système d'équations différentielles, alors qu'en temps discret on parle d'un système d'équations aux différences finies.

Dans ces représentations mathématiques interviennent des paramètres qui vont conditionner l'évolution de ce système, ainsi il peut avoir un comportement périodique, pseudopériodique ou chaotique [12,13].

1.2.1. Temps continu [14] **:**

Les systèmes à temps continu sont caractérisés par l'utilisation d'équations différentielles décrivant l'évolution des variables dans le temps.

Les équations utilisées, reposant sur une approximation au premier ordre, possèdent la forme suivante :

$$\dot{x} = \dot{x}_{(t)} = f_{(x;t;\upsilon)} \tag{1.1}$$

Avec $x_{(t)}$ représentant l'évolution du système dans le temps et $\dot{\mathbf{x}}_{(t)}$ correspondant à l'état instantané du système. La fonction f dépend du temps, ainsi que des paramètres du système $\boldsymbol{\upsilon}$.

Dans un système à N variables, l'expression (1.2) devient :

$$\begin{aligned} \dot{x}_1 &= f_1(x_1, x_2, \dots, x_N; t; \upsilon) \\ \dot{x}_2 &= f_2(x_1, x_2, \dots, x_N; t; \upsilon) \\ &\vdots \\ \dot{x}_N &= f_N(x_1, x_2, \dots, x_N; t; \upsilon) \end{aligned} \tag{1.2}$$

Dont le système X_1,...,X_N possèdent des conditions initiales connues $X1_0$,..., XN_0.

1.2.2. Temps discret [14]:

Pour les systèmes à temps discret, le système est décrit en utilisant une modélisation dont les instants sont répartis dans le temps de façon équidistante.

Afin de répondre aux critères de discrétisation du système dans le temps, deux possibilités s'offrent à nous :

1. les caractéristiques du système imposent leurs caractères discrets.
2. le système est une version échantillonnée d'un système en temps continu.

Mais dans les deux cas, leurs représentations mathématiques utilisent des fonctions

De récursivité. Une mise en équation via un système de premier ordre, est caractérisée.

De la façon suivante :

$$X_{(n+1)} = f_{(X_n)} \text{ , } n \geq 0 \tag{1.3}$$

Avec une condition initiale connue $X_{(0)}$=x_0.

Dans le cas d'un système d'ordre supérieur (r ≥ 2) :

$$X_{(n+r)} = f_{(X_n, X_{n+1}, \dots, X_{n+r-1})}, \text{ n}\geq 0 \quad (1.4)$$

1.3.Système dynamique chaotique :

La théorie du chaos traite des systèmes dynamiques déterministes qui présentent un phénomène fondamental d'instabilité appelé «sensibilité aux conditions initiales », ce qui les rend non prédictibles en pratique sur le «long » terme. Le chaos est défini généralement comme un comportement semblant aléatoire (ou imprévisible) d'un système dynamique défini par des équations déterministes [15].

Un système dynamique est défini à partir d'un ensemble de variables qui forment le vecteur d'état $X = \{xi \in R\}$, i = 1…n où n représente la dimension du vecteur. Nous appelons état d'un système l'ensemble des variables qui, étant connues à l'instant initial, permettent de décrire l'évolution de ce système. L'ensemble de tous les états pouvant être pris par le système s'appelle l'espace des phases. Le processus évolue de manière déterministe si ses états futurs sont caractérisés par la connaissance de ses états présents et passés. La loi d'évolution dans le temps de ce système dynamique est généralement désignée par "dynamique ". En somme, la notion de déterminisme provient du fait que le système est caractérisé par son état initial et sa dynamique [15].

1.4.Propriétés des systèmes chaotiques

Pour qu'un système dynamique soit classifié en tant que chaotique, il doit comporter les propriétés suivantes :

- Non-linéarité.
- Déterminisme.
- Aspect aléatoire.
- Sensibilité aux conditions initiales.
- Notion d'attracteur.
- Exposants de Lyapunov.

1.4.1. Non-linéarité

Un système chaotique est un système dynamique non linéaire. Un système linéaire ne peut pas être chaotique. Le comportement chaotique d'un système dynamique non linéaire est dû aux non linéarités. En général, pour prévoir des phénomènes générés par les systèmes dynamiques, la démarche consiste à construire un modèle mathématique qui établit une relation entre un ensemble de causes et un ensemble d'effets. Si cette relation est une opération de proportionnalité, le phénomène est linéaire. Dans le cas d'un phénomène non linéaire, l'effet n'est pas proportionnel à la cause [11].

1.4.2. Déterminisme

La notion de déterminisme signifie la capacité de « prédire » le futur d'un phénomène à Partir d'un évènement passé ou présent. L'évolution irrégulière du comportement d'un Système chaotique est dû aux non linéarités [1].

Dans les phénomènes aléatoires, il est absolument impossible de prévoir la trajectoire D'une quelconque particule. À l'opposé, un système chaotique a des règles fondamentales Déterministes et non probabilistes [1].

1.4.3. L'aspect aléatoire

Tous les états d'un système chaotique présentent des aspects aléatoires, la figure suivante illustre l'aspect aléatoire du système de Lorenz :

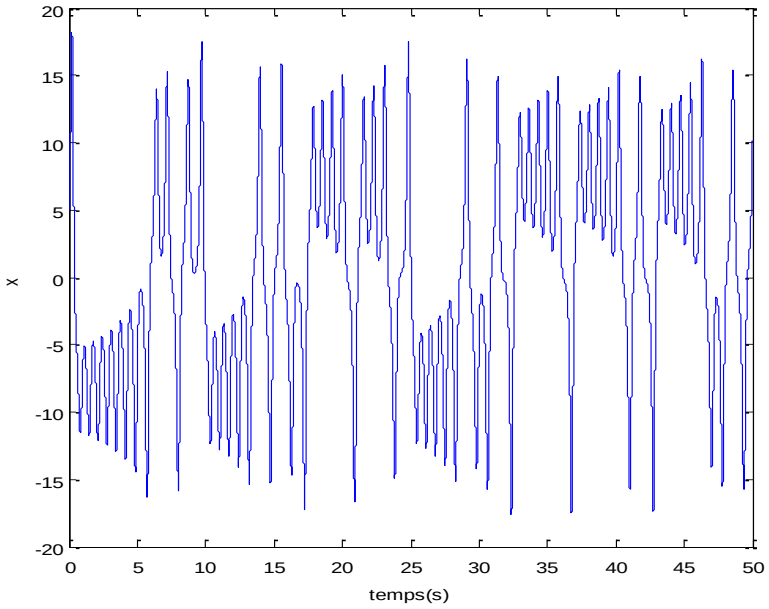


Figure (1.1) : Système chaotique de Lorenz.

1.4.4. Sensibilité aux conditions initiales (SCI)

Les systèmes chaotiques sont extrêmement sensibles aux perturbations. On peut illustrer ce fait par *l'effet papillon*, popularisé par le météorologue *Edward Lorenz.* L'évolution d'un système dynamique chaotique est imprédictible dans le sens qu'elle est sensible aux conditions initiales. Ainsi, deux trajectoires de phases initialement voisines s'écartent toujours l'une de l'autre, et ceci quelle que soit leur proximité initiale. Il est clair que la moindre erreur ou simple imprécision sur la condition initiale empêche de décider à tout temps qu'elle sera la trajectoire effectivement suivie et, par conséquence, de faire une prédiction autre que statistique sur le devenir à long terme du système. Ainsi, bien que l'on traite de systèmes déterministes, il est impossible de prévoir à long terme leurs comportements. La seule manière est d'opérer effectivement l'évolution du système. Si cette simulation se fait informatiquement, un problème de précision sur les conditions initiales se pose alors : de petites erreurs d'arrondissement dues à la précision du type de la variable Codant ces conditions initiales peuvent exponentiellement s'amplifier de telle sorte que la trajectoire de phases obtenue n'est pas représentative de la réalité [16].

Illustrons ce phénomène de SCI par une simulation numérique. On affecte à un système chaotique de Lorenz deux conditions initiales très proches. Dans un premier temps, les deux systèmes évoluent de la même manière ; mais, très vite, leur comportement devient différent [16]. Ceci est illustré sur la figure suivante :

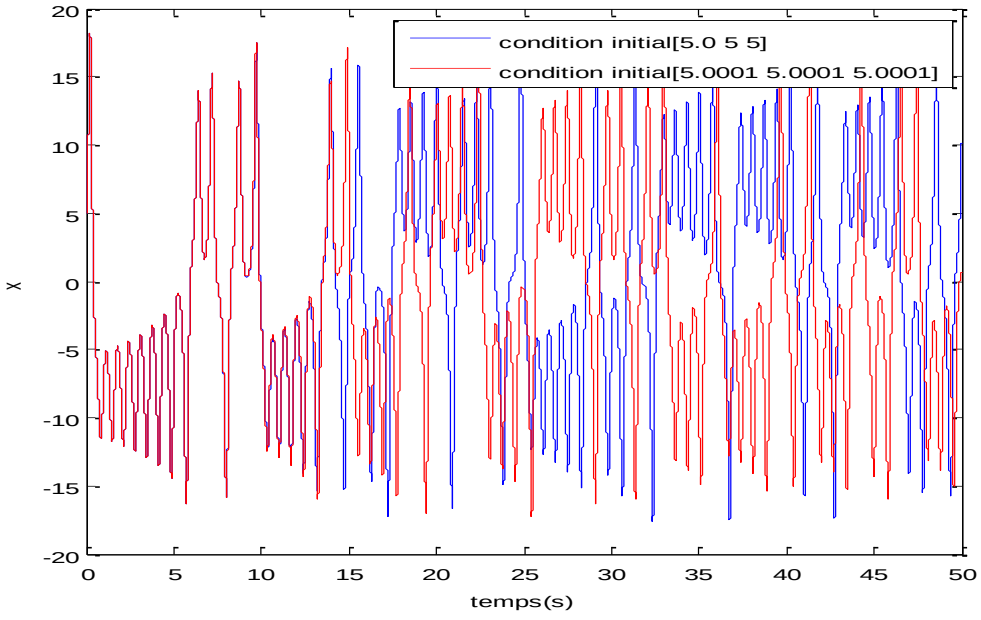


Figure (1.2) : Sensibilité aux conditions initiales (Système de Lorenz).

1.4.5. Notion d'attracteur

La région de l'espace de phases vers laquelle convergent les trajectoires d'un système dynamique dissipatif s'appelle « attracteur ». Les attracteurs sont des formes géométriques qui caractérisent l'évolution à long terme des systèmes dynamiques [1].

Il y a deux types d'attracteurs : les attracteurs réguliers et les attracteurs étranges ou chaotiques **:**

1.4.5.1. Attracteurs réguliers

Les attracteurs réguliers caractérisent l'évolution des systèmes non chaotiques, et peuvent être de deux sortes :

- **Un point fixe** : la trajectoire du pendule dissipatif simple (dans l'espace des phases représentant son altitude et sa vitesse), par exemple, tend vers l'origine du repère, quelles que soient la position et la vitesse initiales [17].
- **Un cycle limite** : la trajectoire du pendule idéal dans ce même espace des phases, par exemple. Pour tous les attracteurs réguliers, c'est-à-dire pour tous les systèmes non chaotiques, des trajectoires qui partent de « points » proches l'un de l'autre dans l'espace de phase 1 restent indéfiniment voisines. On sait donc prévoir l'évolution de ces systèmes, à partir d'une situation connue [17].

1.4.5.2. Attracteurs étranges [18]

Les attracteurs étranges sont des formes géométriques complexes qui caractérisent l'évolution des systèmes chaotiques : au bout d'un certain temps, tous les points de l'espace des phases donnent des trajectoires qui tendent à former l'attracteur étrange.

L'attracteur étrange se caractérise par :

1. Sensibilité aux conditions initiales (deux trajectoires de l'attracteur initialement voisines finissent toujours par s'éloigner l'une de l'autre, ceci traduit un comportement chaotique).
2. La dimension de l'attracteur est fractale et non entière (ce qui justifie l'adjectif étrange).
3. L'attracteur est de volume nul dans l'espace des phases**.**

Ci-dessus la figure (1.3) montre l'attracteur de Lorenz.

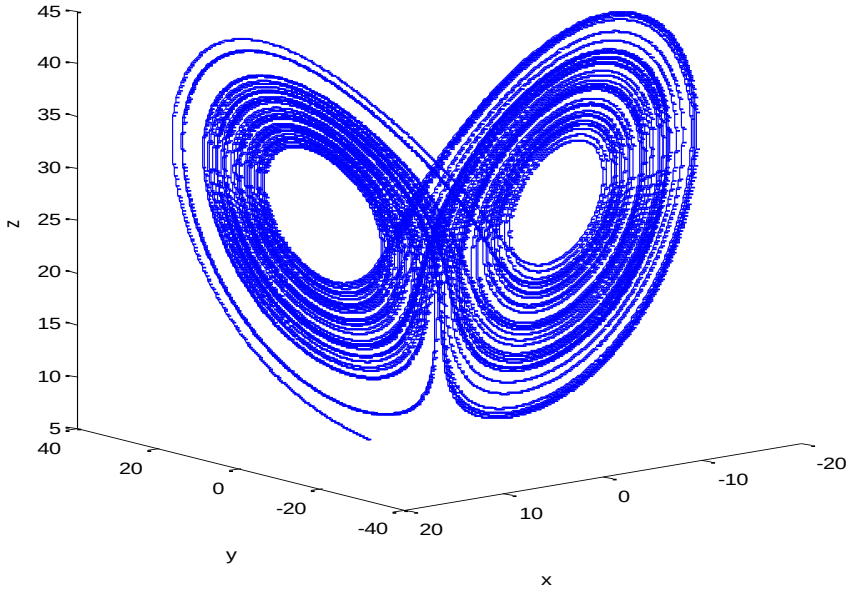


Figure (1.3) : Attracteur de Lorenz.

1.4.6. Exposants de Lyapunov

L'exposant de Lyapunov sert à mesurer le degré de stabilité d'un système et permet de quantifier la sensibilité aux conditions initiales d'un système chaotique.

L'évolution d'un flot chaotique est difficile à appréhender, parce que la divergence des trajectoires sur l'attracteur est rapide, C'est pourquoi on essaye d'estimer ou même de mesurer la vitesse de divergence ou convergence, Cette vitesse s'appelle l'exposant Lyapunov qui caractérise le taux de séparation de deux trajectoires très proches [19, 20].

Donc deux trajectoires dans le plan de phase initialement séparées par un taux Z1 divergent après un temps $\Delta t = t_2 - t_1$ vers Z_2 tel que [11] **:**

$$|Z_2| \approx \exp(\lambda . \Delta t)|Z_1| \qquad (1.5)$$

Où λ est l'exposant de Lyapunov**.**

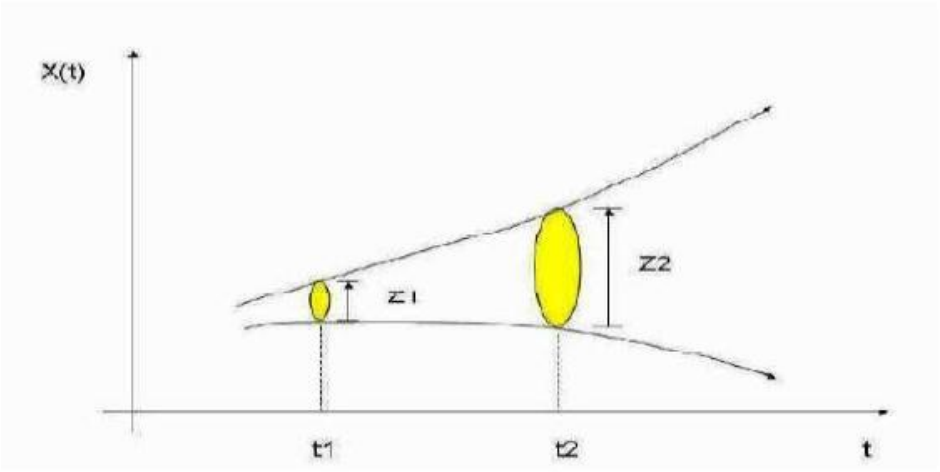


Figure (1.4) : Divergence de deux trajectoires dans le plan de phase [11].

Pour un attracteur non chaotique, les exposants de Lyapunov sont tous inférieurs ou égaux à zéro et leur somme est négative. Un attracteur étrange possèdera toujours au moins trois exposants de Lyapunov, dont un au moins doit être positif [11].

Le tableau suivant résume les différentes configurations d'exposants de Lyapunov [11].

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

Tableau (1.1) : Attracteurs et exposants de Lyapunov [11].

1.5. Exemples de systèmes chaotiques

Les exemples les plus connus et les plus étudiés des systèmes chaotiques.

1.5.1. Systèmes chaotiques à temps continu

C'est un système dont les variables évoluent de manière continue. On peut alors déterminer les valeurs de différentes coordonnées à tout moment et cela en fonction des autres valeurs. Pour les systèmes chaotiques à temps continu, on peut considérer : le système de Lorenz, le système de Rössler. [21].

1.5.1.1. Système de Lorenz

En 1963, le météorologue Edward Lorenz est le premier à mettre en évidence le caractère vraisemblablement chaotique de la météorologie.

Le modèle de Lorenz, appelé aussi système dynamique de Lorenz ou oscillateur de Lorenz, est une modélisation simplifiée de phénomènes météorologiques basée sur la mécanique des fluides. L'oscillateur de Lorenz est un système dynamique tridimensionnel qui engendre un comportement chaotique dans certaines conditions [22].

Il s'agit d'un système dynamique non linéaire en temps continu de dimension 3, obtenu des équations de transfert de la chaleur dans un liquide. Le système de Lorenz est défini par :

$$\begin{cases} \dot{x} = a\,(y - x) \\ \dot{y} = x(b - z) - y \\ \dot{z} = xy - cz \end{cases} \tag{1.6}$$

Les variables x, y et z représentent l'état du système à chaque instant. Et a, b, c les paramètres du système. Le système présente un comportement chaotique pour a=10, b=28, c=8/3 [23].

1.5.1.2. Système de Rossler

En 1976, un biochimiste allemand, Otto Rössler a essayé de construire un attracteur chaotique semblable à celui de Lorenz, mais plus facile à analyser. Il a tenté de concevoir le système le plus simple possible, capable de générer du chaos. Le modèle dynamique résultant est donné ci-dessous [24] :

$$\begin{cases} \dot{x} = -(y + z) \\ \dot{y} = x + a\,y + 0.01.x.ln(z) \\ \dot{z} = c + z(x - b) \end{cases} \tag{1.7}$$

Les paramètres étant fixés aux valeurs suivantes : a = 0.2, b = 5.7, c = 0. 2 [24].

L'attracteur étudié par Rössler est tracé à la figure (1.5).

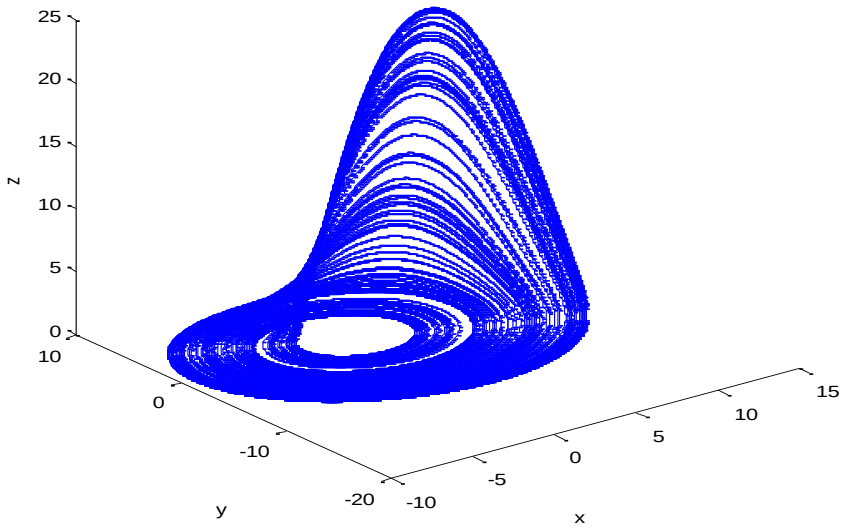


Figure (1.5) : Attracteur de Rossler.

1.5.2. Système chaotique à temps discret

Système dont les variables n'évoluent pas de manière continue. Pour les systèmes chaotiques à temps discret on peut considérer le système bidimensionnel de Hénon et de Lozi [21].

1.5.2.1. Système de Hénon

Ce système est un modèle proposé en 1976 par le mathématicien Michel Hénon [16], L'intérêt de ce modèle est l'étude de certaines propriétés d'une section de Poincaré de l'attracteur de Lorenz par l'introduction d'itérations dans le plan. Le Modèle mathématique de ce système est donné par [16]:

$$\begin{cases} x_{k+1} = a - x_k^2 + by_k \\ y_{k+1} = x_k \end{cases} \tag{1.8}$$

Avec *k*, le nombre d'itérations.

Les valeurs des paramètres proposées par Michel Hénon pour observer le

Phénomène chaotique sont : *a* =1.4 *et b* =0.3 [16].

Pour simuler l'attracteur de Hénon on a Pris pour conditions initiales (1,3). Ainsi la figure (1.6) représente l'attracteur de Hénon.

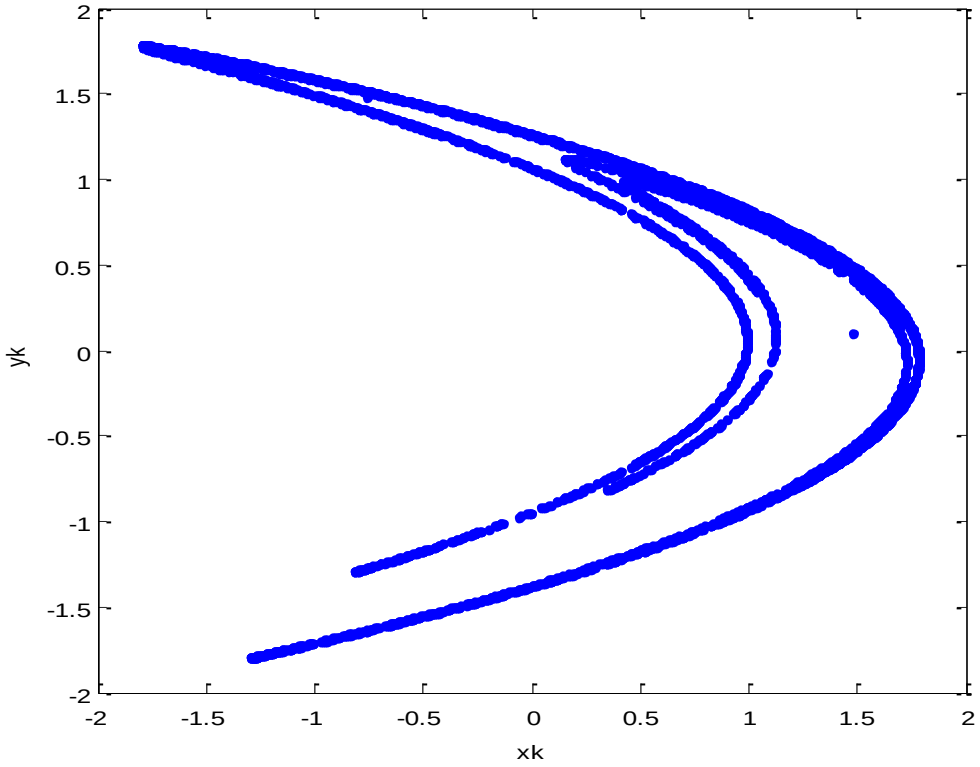


Figure (1.6) : Attracteur de Henon.

1.5.2.2. Système de Lozi

Le système de **Lozi** qui consiste en le système de **Henon** pour lequel la non-linéarité x_k^2 est remplacée par$|x_k|^2$[21].

1.6. Conclusion :

Dans ce chapitre, nous avons défini les systèmes dynamiques de manière générale et les systèmes chaotiques de manière un peu plus détaillé, en suite nous avons présenté les propriétés permettant de caractériser les dynamiques chaotiques, telle que la sensibilité aux conditions initiales, Attracteurs étranges, le calcul des exposants de Lyapunov...etc.

Cela a été illustré par des exemples de calcul et de simulation effectués sur des systèmes chaotiques à temps continu (système de Lorenz et le système de Rössler) et à temps discret (système de Hénon).

Cependant l'usage du chaos pour la sécurisation de la communication pose directement le problème de synchronisation du récepteur afin de suivre le signal chaotique employé à l'émetteur. Ce qui sera l'objet du second chapitre.

CHAPITRE 2

Etat de l'art sur la synchronisation et le chiffrement d'informations par le chaos

2.1. Introduction :

L'usage du chaos pour la sécurisation de la télécommunication a été rendue possible depuis la maîtrise de la synchronisation des systèmes chaotiques. En effet le problème de synchronisation du récepteur dans le but de dupliquer le signal chaotique utilisé au niveau du récepteur se pose directement. Alors c'est quoi la synchronisation [25,26]

La synchronisation existe depuis le $16^{ième}$siècle, elle caractérise l'évolution de deux systèmes qui se component des mêmes façons en même temps.

Grace à l'expérience réalisée par Huygens (1629- 1695), qui a fait L'étude de deux horloges de Fréquence, dont la différence est très petite a constaté, par la suite il a relié les deux horloges avec un morceau de bois, ce qui a donné un mouvement complètement identique dit synchronisation.

Les domaines d'utilisation de la synchronisation sont vastes, elle existe en technologique et en diverses sciences.et principalement en télécommunication. Dont elle est une clé importante pour une transmission réussie. Dans le domaine de la transmission sécurisée à base du chaos, la synchronisation chaotique au niveau du récepteur cherche à dupliquer le signal chaotique envoyé de l'émetteur malgré l'hypersensibilité aux conditions initiales. Cela vent dire que deux signaux chaotiques sont dits synchronises, seulement s'ils sont asymptotiquement identiques quand le temps tend vers l'infini [27].

Dans ce chapitre nous allons présenter les deux types de synchronisation. Ensuite, nous proposons différentes méthodes de synchronisation et on termine avec quelques techniques de cryptage à base du chaos.

2.2. Synchronisation des systèmes chaotiques

Parallèlement aux grandes avancées réalisées dans la théorie du chaos, les perspectives de l'utilisation du chaos dans diverses applications, notamment en télécommunication, ont motivé les chercheurs à étudier la question de l'éventuelle possibilité de synchroniser le chaos [28].

La synchronisation des oscillateurs non linéaires est un phénomène qui a attiré l'attention des chercheurs depuis le constat et la description de ce phénomène par Huygens en 1673, dans un exemple de deux systèmes mécaniques couplés. Depuis les années 90, de nombreux ouvrages ont été publiés au sujet de la synchronisation chaotique [29, 30] etc. Le phénomène de synchronisation est manifesté lorsque deux systèmes dynamiques évoluent d'une manière identique en fonction du temps. L'une des configurations de synchronisation les plus populaires est la configuration maître-esclave pour laquelle un système dynamique, appelé système esclave suit le rythme et la trajectoire imposés par un autre système dynamique, appelé système maître.

La synchronisation de deux systèmes dynamiques signifie que chaque système évolue en suivant le comportement de l'autre système. Ce concept repose sur le fait qu'un système chaotique est déterministe et possède un ou plusieurs exposants de Lyapunov positifs et qu'il est instable, si par un moyen quelconque, deux systèmes puissent échanger de l'énergie, action que l'on nomme couplage, ils finiront par se synchroniser [1].

Ainsi la synchronisation peut être définie comme suit :

$$\begin{cases} \dot{x} = f_1(x) \\ \dot{y} = f_2(\mathrm{y}) \end{cases} \tag{2.1}$$

Avec x(t), y(t) ∈ $\mathbb{R}^n$, f_1 et f_2 des fonctions non linéaires définies de $\mathbb{R}^n \rightarrow \mathbb{R}^n$.

Les deux systèmes sont synchronisés si :

$$Lim_{t\rightarrow\infty}\|y(t) - x(t)\|=0 \tag{2.2}$$

Où y(t)- x(t) représente l'erreur de synchronisation.

2.3. Types de synchronisation

On distingue deux types de synchronisation: la synchronisation par couplage unidirectionnel et la synchronisation par couplage bidirectionnel**.**

2.3.1. Synchronisation par couplage unidirectionnel

Dans le cas d'une synchronisation unidirectionnelle, le couplage entre deux systèmes identiques a et b est réalisé à l'aide d'un élément fonctionnant dans un seul sens, par exemple l'utilisation d'un circuit électrique suiveur [31].

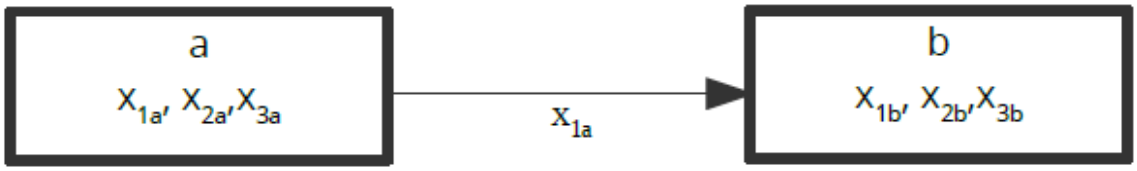


Figure (2.1):Couplage unidirectionnel.

2.3.2. Synchronisation par couplage bidirectionnel

Dans le cas d'une synchronisation bidirectionnelle, le couplage entre deux systèmes identiques a et b est réalisé à l'aide d'un élément permettant l'échange d'énergie dans les deux sens, par exemple l'utilisation d'une simple résistance [31].

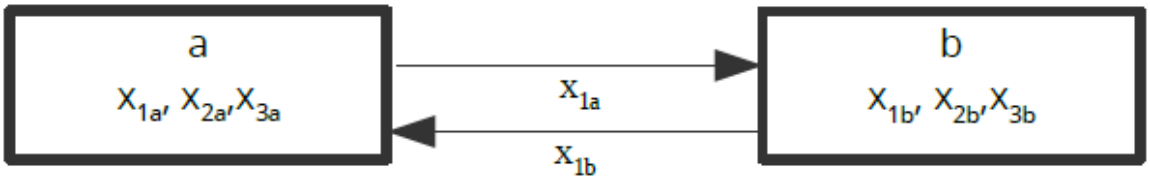


Figure (2.2) : Couplage bidirectionnel.

2.4. Méthodes de synchronisation des systèmes chaotiques

Le concept de synchronisation repose sur le constat qu'un système chaotique est déterministe et possède un ou plusieurs exposants de Lyapunov positifs et qu'il est instable. Il est donc possible de construire une réplique identique à ce système et d'essayer de synchroniser de façon que les deux signaux chaotiques issus des deux exemplaires soient identiques [1].

2.4.1. Synchronisation par Décomposition Du Système

La synchronisation identique proposée par Pecora et Carroll [32] a l'avantage de représenter une solution simple et performante de la synchronisation dont l'objectif est que l'esclave reproduit le plus fidèlement possible l'état du maître, après un régime transitoire [33].

Ce concept repose sur le constat qu'un système chaotique possède un ou plusieurs exposants de Lyapunov positifs et qu'il est instable. Il est donc impossible de construire une réplique identique à ce système et d'essayer de synchroniser. L'idée consiste à diviser

le système d'origine en deux sous-systèmes de telle sorte que les variables dynamiques de départ soient réparties de part et d'autre de chacun des sous-systèmes [32,34]. Il s'agit ensuite de reproduire les sous-systèmes à l'identique et de les mettre en cascade. Le signal issu du système de départ (système maître) sert à piloter (synchroniser) le premier des deux sous-systèmes dupliques mis en cascade qui lui-même permet de synchroniser le second sous-système dupliqué .Considérons un système dynamique autonome, en temps continu, de dimension « n » représenté par la relation suivante [32, 34,35].

$$\dot{x} = f(u) \tag{2.3}$$

$U \in R^n$

$Avec\ \ U(t) = \big(U_1(t) \dots \dots \dots \dots U_n(t)\big)\ et\ F(u) = \big(F_1(u) \dots \dots \dots \dots F_n(u)\big).$

Ce système est divisé arbitrairement en deux sous-systèmes [33]:

$$x = G(x, y_1)\ et\ \dot{y} = H(x_1, y) \tag{2.4}$$

$$\text{Avec : } x(t) = u_1(t) \dots\ u_m(t) = \ x_1(t) \dots x_m(t)\ ,$$
$$y(t) = u_{m+1}(t) \dots\ u_n(t) = (y_1(t) \dots y_p(t))$$

Tel que : $m + p = n$

Soient :

$$\begin{cases} \dot{x}_1 = G_1(x, y_1) \\ \quad\quad . \\ \quad\quad . \\ \dot{x}_m = G_m(x, y_1 \end{cases} \tag{2.5}$$

$$\begin{cases} \dot{y}_1 = H_1(x_1, y) \\ \quad\quad . \\ \quad\quad . \\ \dot{y}_p = H_P(x_1, y) \end{cases} \tag{2.6}$$

La figure (2.3) illustre plus en détails le processus de séparation de deux sous-systèmes [33] :

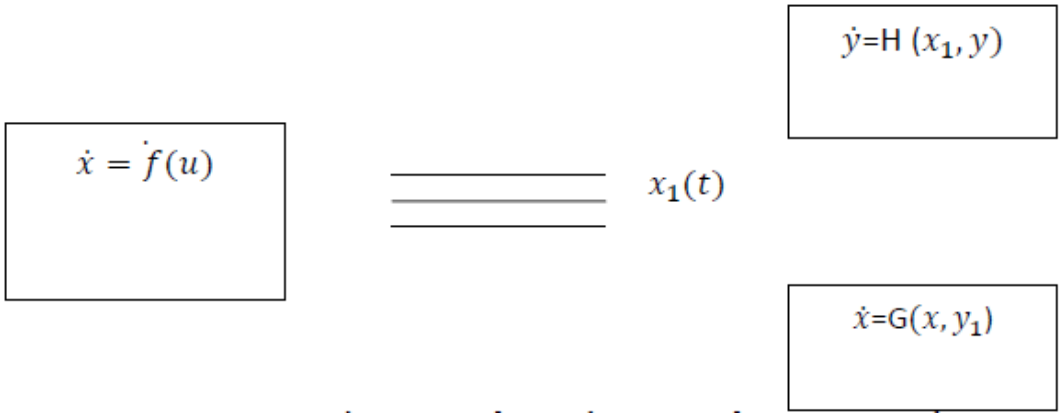


Figure (2.3)*: Séparation du système F en deux sous-systèmes G et H.*

2.4.2. Synchronisation complète :

On considère un système maitre représenté par les équations suivantes [36] :

$$\begin{cases} \dot{x} = f(t,x) \\ y = h(x) \end{cases} \quad (2.7)$$

Où $x \in R^n$ et $h: R^n \to R^n$, x est le vecteur d'état et f est la fonction de sous –système.

Et un système esclave donné par :

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

Avec $\hat{x} \in R^p$ et $\hat{h}: R^p \to R^q$

Où $(x, \hat{x})$ sont les états des systèmes et $(y, \hat{y})$ sont les sorties.

Soit φ une fonction continue, qui décrit la relation entre le maître et l'esclave lors de la synchronisation.

$$\hat{y} = \varphi(y) \; ; \varphi: R^m \to R^q \quad (2.9)$$

La synchronisation est dite complète si :

$$\hat{x}(t) = x(t) \quad (2.10)$$

Ce qui implique que : $m = q$ et φ est une identité [1].

Si $\hat{f} = f$, la relation devient une synchronisation complète identique.

Si $\hat{f} \neq f$ c'est une synchronisation complète non identique.

La synchronisation complète est donc une coïncidence complète entre les variables d'état des deux systèmes synchronisés .Les méthodes de synchronisation complète sont typiquement associées avec la synchronisation des systèmes identiques.

La majorité des concepts de synchronisation complète utilise un schéma de rétroaction et la synchronisation considérée comme étant bidirectionnelles, car les deux systèmes sont à la fois source et destination [1].

2.4.3. Synchronisation généralisée :

Les systèmes chaotiques identiques synchronisent en suivant la même trajectoire chaotique. Cependant, dans le monde réel, les systèmes ne sont en général pas identiques. Par exemple, lorsque les paramètres de deux systèmes identiques couplés ne sont pas les mêmes ou quand ces systèmes couplés appartiennent à des classes différentes**.**

Pour les systèmes non identiques, il faut examiner différents types de synchronisation.

Il a été montré que lorsque deux systèmes différents sont couplés avec une valeur de couplage assez forte, une relation synchrone générale entre leurs états peut exister et peut être exprimée par une fonction régulière inversible : y(t) = $\psi(x(t))$.

Ce phénomène s'appelle la **synchronisation généralisée**, c'est donc une forme plus générale que la synchronisation identique pour des systèmes non identiques.

La synchronisation généralisée a été introduite pour des systèmes couplés unidirection-nellement par Rulkov et al en 1995 [37].

$$\begin{cases} \dot{x} = \mathrm{F}(x) \\ \dot{y} = \mathrm{G}(\mathrm{y}, \mathrm{u}(\mathrm{t})) \end{cases} \tag{2.11}$$

Où $x \in \mathbb{R}^n$,y $\in \mathbb{R}^m$.

F:$\mathbb{R}^n \to \mathbb{R}^n$, G: $\mathbb{R}^m \times \mathbb{R}^k \to \mathbb{R}^m$, $u(t) = (u_1(t),\ldots, u_k(t))$, $u_i(t)=h_i(x(t, x_0)$.

Le premier et le deuxième système (2.11) sont appelés maître et esclave, respectivement.

2.4.4. Synchronisation par la contre-réaction (couplage diffusif)** [38]

Les recherches qui ont suivies celles de Pecora et Carroll ont montré que la synchronisation par remplacement complet n'était qu'un cas très particulier de la méthode que nous allons maintenant présenter dans ce paragraphe.

Dans la globalité on garde les mêmes notations pour le système chaotique étudié mais sans le séparer en sous-systèmes. Pour que la synchronisation ait lieu, on prend au moins un des signaux x_{ri} et on ajoute un facteur amortissant qui a pour valeur la différence x_{ci} -x_{ri}au système de réponse. On a alors :

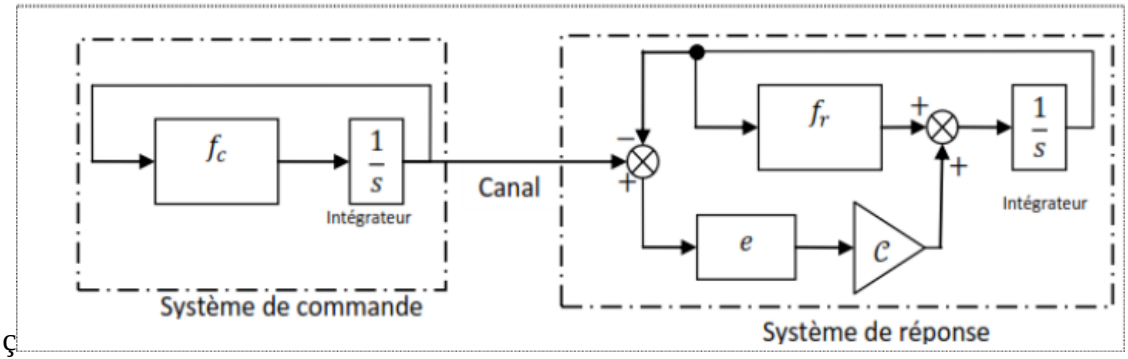
$$\dot{x}_c = f(x_c) \text{ et } \dot{x}_r = f(x_r) + \mathcal{C}\, \mathrm{e}(x_c - x_r) \tag{2.12}$$

Où $\mathcal{C}$ est le facteur de couplage et e est une fonction linéaire qui définit la combinaison linéaire des signaux qui seront utilisés pour l'amortissement. Puis, similairement, on pose $\boldsymbol{\varepsilon} = x_c - x_r$ et on a :

$$\dot{x}_c = f(x_c) \text{ et } \dot{x}_r = f(x_r) + \mathcal{C}\, \mathrm{e}(x_c - x_r) \tag{2.13}$$

Pour avoir la stabilité asymptotique, on calcule les exposants de Lyapunov correspondants à l'équation variation elle sur $(J_f - \mathcal{C}.e)$ en fonction de $\mathcal{C}$ et on choisit ce facteur de manière à avoir les exposants les plus négatifs possibles. Si le facteur de couplage tend vers $+\infty$ alors on se retrouve dans le cas de la synchronisation par remplacement complet car la matrice $\boldsymbol{e}$remplacera dans $\boldsymbol{f}$ toutes les x_{ri} par x_{ci} Mais les exposants de Lyapunov des signaux utilisés ne seront pas forcement négatifs dans le cas limite.

Montage de synchronisation :



ç

Figure (2.4) : Synchronisation par contre-réaction.

2.5. Transmission basée sur la synchronisation de systèmes chaotiques

Depuis quelques années, les chercheurs s'intéressent à la possibilité d'utiliser des signaux chaotiques dans les systèmes de transmission de données, en particulier pour transmettre des quantités importantes d'informations sécurisées. L'intérêt d'utiliser des signaux chaotiques réside dans deux propriétés du chaos.

Un signal chaotique est un signal à large spectre et permet donc de transmettre des signaux très variés, d'autre part, un signal chaotique est obtenu à partir d'un système déterministe, il est donc possible de le reconstituer en se plaçant dans les mêmes conditions que celles qui ont contribué à le créer et, ainsi, de récupérer l'information de départ [39].

La Figure (2.5) [40] illustre d'une façon qualitative le principe de la transmission sécurisée de données à base de systèmes chaotiques.

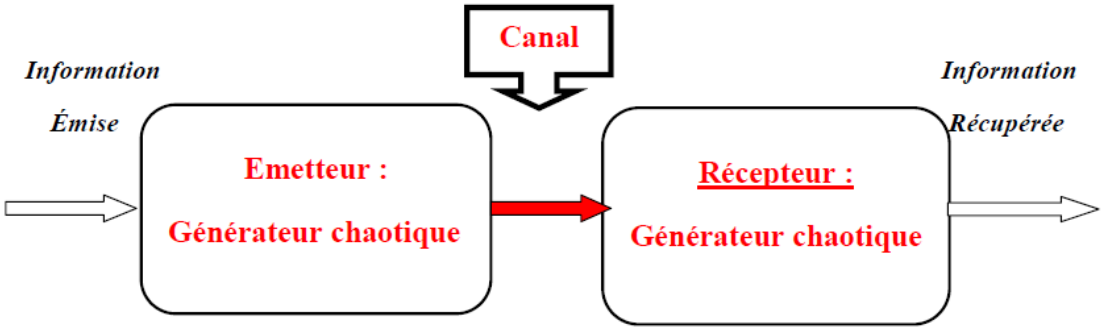


Figure (2.5) : Fondement de la transmission sécurisée à base du chaos

La confidentialité du message, son intégrité et son authenticité, constituent généralement les caractéristiques fondamentales d'une communication sûre et performante. On trouve ainsi différentes méthodes de synchronisation de systèmes et différentes techniques de cryptage [40].

2.6. Techniques De Cryptage Par Le Chaos

Le chiffrement d'un message par le chaos s'effectue en superposant à l'information initiale un signal chaotique. Nous envoyons par la suite le message noyé dans le chaos à un récepteur qui connaît les caractéristiques du générateur de chaos. Il ne reste alors plus au destinataire qu'à soustraire le chaos de son message pour retrouver l'information [41].
Différentes techniques d'injection de l'information dans un système chaotique, tels que le Cryptage additif et la modulation paramétriques, Cryptage par inclusion présentés ci-dessous.

2.6.1. Cryptage par addition

La première et la plus simple des méthodes de cryptage, illustrée dans la figure (2.6), développé en 1993 [42]. Elle consiste en deux systèmes chaotiques identiques, l'émetteur et le récepteur. Le signal chaotique c(t) est l'une des variables d'état du système dans l'émetteur. Le message d'information (le signal utile qui doit être crypté) m(t), qui est typiquement très faible devant c(t), est ajouté au signal c(t) et donne le signal transmis s(t). Comme c(t) est très complexe et m(t) est beaucoup plus petit que c(t), alors il est difficile de séparer m(t) du signal s(t) sans connaître c(t).

Le récepteur est constitué d'un système chaotique identique à l'émetteur et d'un simple soustracteur. Ainsi, après la synchronisation des deux systèmes chaotiques (émetteur et récepteur), le message est extrait à l'aide d'une opération de soustraction [40].

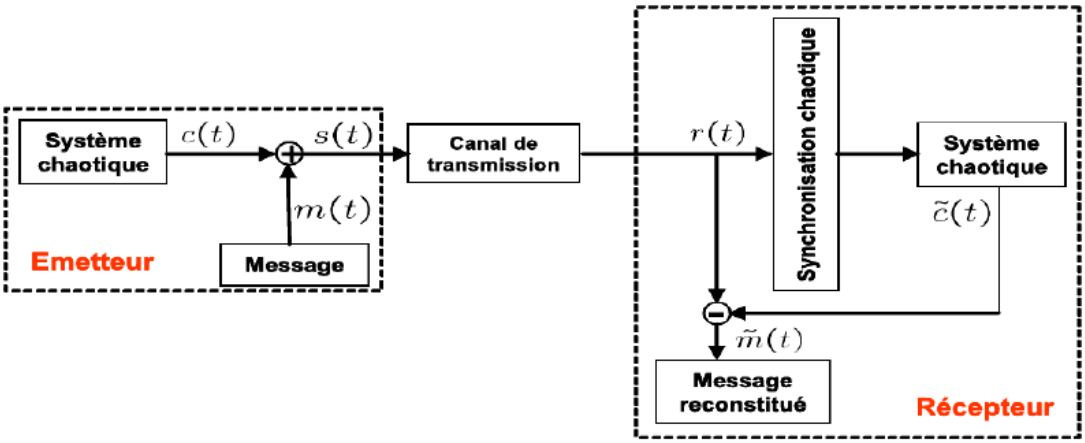


Figure (2.6): Schéma de communication par addition.

Le principal avantage de cette méthode réside dans la simplicité du cryptage, et aussi qu'elle est applicable à des systèmes continus ou discrets. L'inconvénient est qu'il est impératif que l'amplitude du message original soit significativement plus petite que celle de la porteuse chaotique afin d'éviter de perturber l'établissement de la synchronisation et de garantir la sûreté de la transmission [40].

2.6.2. Cryptage par commutation [28]

Dans cette méthode, l'information est binaire et le principe consiste à transmettre un signal chaotique durant la transmission d'un bit "0" et un autre signal chaotique différent du premier pour un bit "1". Les deux signaux chaotiques peuvent soit provenir de deux systèmes différents, soit de deux systèmes possédant la même structure mais avec des paramètres modifiés. De cette façon, chaque bit est représenté par un attracteur étrange distinct.

Le schéma de principe de cette technique est représenté par la figure (2.7) Au niveau de l'émetteur, on dispose de deux oscillateurs générant les signaux chaotiques A(t) et B(t). Le signal d'information de type binaire M(t) est utilisé pour commuter entre A(t) encodant le bit 1 et B(t) encodant le bit 0. Le signal résultant X(t) est transmis à travers le canal de transmission vers le système récepteur constitué de deux systèmes esclaves. Le premier système esclave synchronise exclusivement avec le premier oscillateur (correspondant au signal chaotique A(t)) de telle façon que le bit 1 est détecté par la convergence de l'erreur de synchronisation vers zéro et par conséquent le signal d'information peut être enfin restauré à la fin du processus de détection.

Schéma représentatif d'un système de transmission CSK :

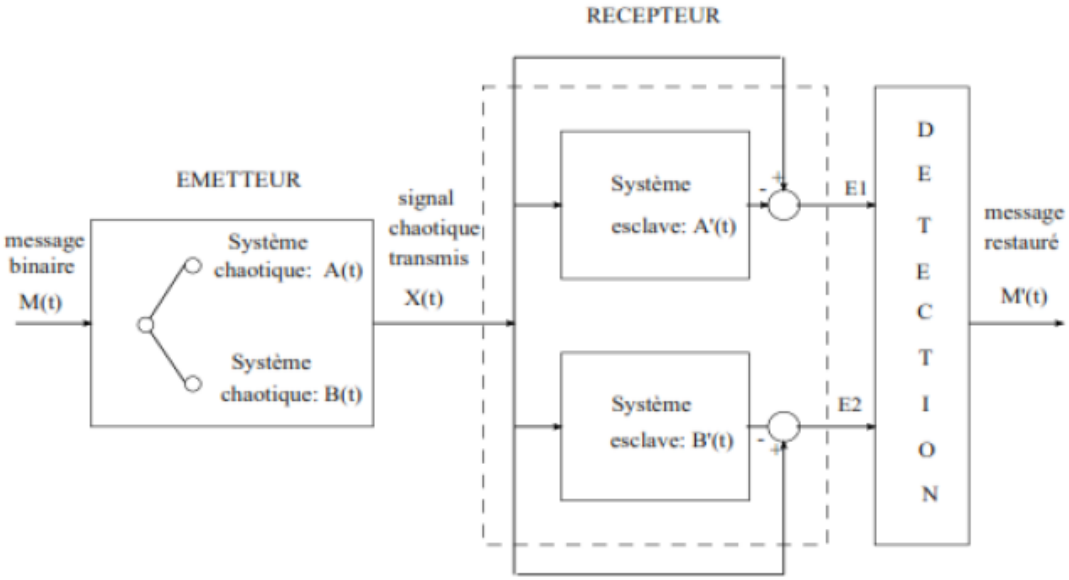


Figure (2.7) : Architecture d'un système de transmission CSK.

Comparée à la technique de masquage chaotique, la commutation chaotique présente relativement plus de robustesse au bruit de canal ; néanmoins, les crypto systèmes utilisant cette technique possèdent une faible vitesse de transmission car à chaque changement de bit on doit tenir compte du temps de convergence nécessaire pour la mise en place de la synchronisation. Cette méthode est caractérisée par un faible niveau de sécurité puisqu'à chaque changement du niveau binaire, on peut observer la modification du signal du texte chiffré, surtout lorsque les deux oscillateurs utilisés au niveau de l'émetteur possèdent deux attracteurs très différents.

2.6.3. Cryptage par modulation paramétriques

Cette technique, développée dans [43, 44,45], utilise le message contenant l'information, généralement de nature binaire, Pour moduler un paramètre de l'émetteur chaotique. Un contrôleur adaptatif est chargé de maintenir la synchronisation au niveau du récepteur, tout en suivant les changements du paramètre modulé.

Le schéma correspondant est présenté à la figure (2.8) au niveau de l'émetteur, le fait de moduler un/plusieurs paramètre(s) impose à la trajectoire de changer continûment d'attracteur, et de ce fait, le signal transmis est plus complexe qu'un signal chaotique "normal".

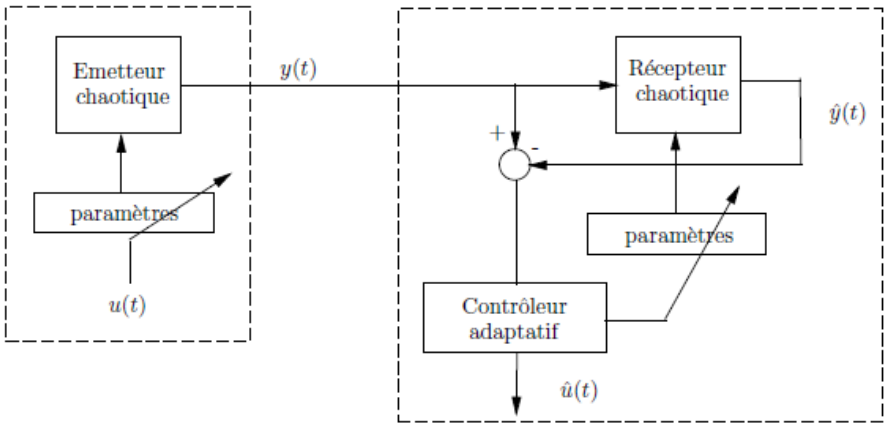


Figure (2.8): Principe de Cryptage par modulation paramétriques

Cependant, la façon d'injecter le message et donc la fonction de modulation des paramètres ne doivent pas supprimer le caractère chaotique du signal envoyé au récepteur. Il est important de souligner que cette technique exploite pleinement les qualités des systèmes chaotiques. Elle n'a pas d'équivalent parmi les systèmes de communications classiques. Cependant, le cryptage par modulation s'est avéré sensible à certaines attaques détaillées dans les références [46, 47].

2.6.4. Cryptage par inclusion (injection)

Cette technique de cryptage consiste à injecter le message dans la dynamique de l'émetteur, sans toutefois réaliser une modulation de paramètre. Le récepteur a pour but de synchroniser avec l'émetteur et de reconstruire le signal d'information, La restauration de l'information se fait principalement par deux techniques, reposant soit sur les **observateurs à entrées inconnues**, soit sur **l'inversion du système émetteur** [31].

Le schéma de principe de cette technique est représenté dans la figure **(2.9)** [48].

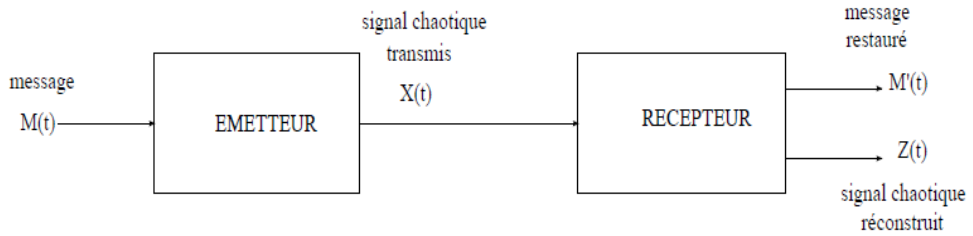


Figure (2.9): Schéma représentatif de la technique de cryptage par injection.

Cette technique est valable pour transmettre un message de nature binaire ou analogique, mais la puissance de ce dernier doit être suffisamment petite pour ne pas détériorer le comportement chaotique du système maître. Cette technique présente un niveau de sécurité nettement élevé par rapport aux techniques précédentes puisque le signal d'information est masqué dans la dynamique du système maître et que le signal chaotique disponible dans le canal public ne porte pas l'information d'une manière directe comme dans le cas de la technique de masquage chaotique [49].

2.6.4.1. Observateurs à entrées inconnues :

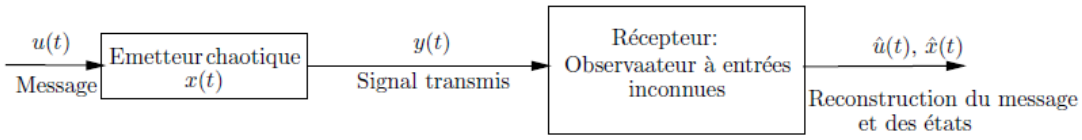


Figure (2.10): Observateurs à entrées inconnues.

Le schéma de la figure (2.10) 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. Parmi les articles utilisant ces types d'observateurs pour décrypter l'information [50,51].

2.6.4.2. Décryptage par inversion :

Le schéma présente un processus de décryptage par inversion c'est à dire, le récepteur est conçu en inversant le modèle de l'émetteur. La figure (2.11) présente le principe général de cette approche [52].

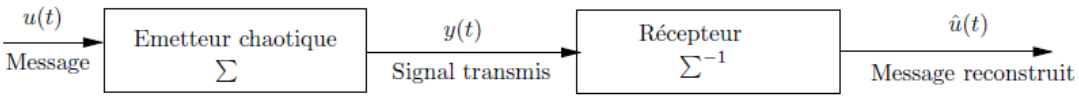


Figure (2. 11): Principe du cryptage par inversion

2.7. Conclusion :

Dans ce chapitre, nous avons expliqué le concept et les classes de synchronisation des systèmes chaotiques (unidirectionnelle, bidirectionnelle), ainsi que quelques méthodes de synchronisation (identique, complète, généralisée et par la contre-réaction). Enfin, nous avons vu un schéma général de la transmission sécurisée à base du chaos et donné des

techniques de chiffrement par le chaos (Cryptage par addition, Cryptage par commutation, Cryptage par modulation paramétriques, Cryptage par inclusion).

CHAPITRE 3

Synchronisation du système Memristor chaotique par la commande prédictive

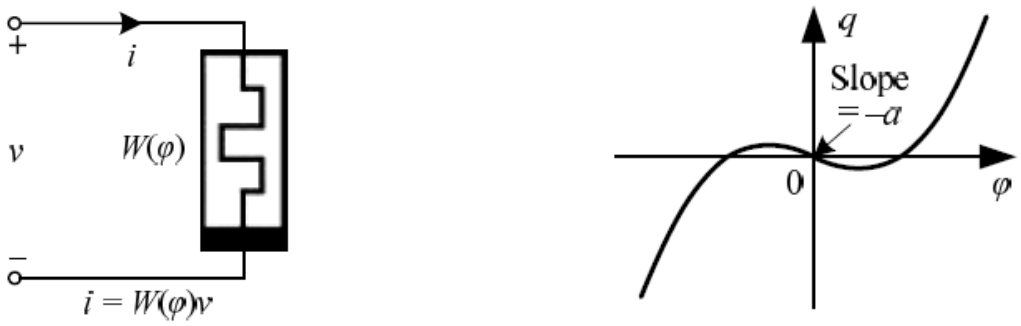
3.1. Introduction

En électronique, le Memristor (ou Memristance) est un composant électronique passif. Il a été décrit comme le quatrième composant passif élémentaire, aux côtés du condensateur, de la résistance et de la bobine. Le nom est constitué du rapprochement des deux mots anglais memory resistor. Un Memristor stocke efficacement l'information car la valeur de sa résistance électrique change, de façon permanente, quand un courant est appliqué. À l'endroit où une résistance classique apporte une valeur stable de résistance, un Memristor peut avoir une valeur élevée de résistance interprétable dans un ordinateur comme un "1" en termes logiques, et une faible valeur qui peut être interprétée comme un "0. " Ainsi, une donnée peut être enregistrée et réécrite par un courant de contrôle. Dans un certain sens, un Memristor est une résistance variable qui, par la valeur de sa résistance, reflète sa propre histoire. Le Memristor a été prédit et décrit en 1971 par Leon Chua de UC Berkeley, dans un écrit de IEEE Transactions on Circuit Théorie. Depuis 1971, le Memristor était un composant hypothétique, aucun exemple physique n'étant connu.

3.2. Circuit chaotique Memristor simple

3.2.1. Memristor actif à flux contrôlé

La non-linéarité des systèmes dynamiques est nécessaire pour générer des phénomènes chaotiques. Les caractéristiques non linéaires du système dynamique déterminent directement les comportements chaotiques et les mécanismes générateurs de chaos. Dans ce chapitre, un nouveau modèle de Memristor à flux contrôlé à deux terminaux avec une non-linéarité active comme le montre la figure (3.1) (a) est présentée, ce qui est très important pour la conception d'un circuit chaotique basé sur un Memristor [53].



(a) **(b)**

Figure (3.1) : Memristor actif à flux contrôlé.

Un memristor actif défini sur la figure (3.1) (b) peut être caractérisé par une non-linéarité cubique continue lisse comme [53] :

$$q(\varphi) = -a\varphi + b\varphi^3 \tag{3.1}$$

Où $a, b > 0$. A partir de cette équation, la memductance $W(\varphi)$ est obtenu comme :

$$W(\varphi) = \frac{dq(\varphi)}{d\varphi} = -a + 3b\varphi^2 \tag{3.2}$$

La puissance instantanée dissipée par le Memristor ci-dessus est donnée par [53]:

$$p(t) = W\big(\varphi(t)\big)v(t)^2 \tag{3.3}$$

Le flux d'énergie dans le Memristor du temps t_0 à t satisfait [53]:

$$w(t_0, t) = \int_{t_0}^{t} p(\tau)d\tau \tag{3.4}$$

Pour tout $t \geq t_0$. Comme la memductance $W(\varphi)$ peut devenir négative dans certaines plages de fonctionnement, la puissance $p(t)$ et l'énergie $w(t_0, t)$ varieront entre positive et négative avec l'évolution temporelle. Ainsi, la relation constitutive du memristor sur la figure (3.1) (b) devient active. Un Memristor actif peut être équivalent à un circuit memristive constitué d'un Memristor passif avec une résistance négative [54,55].

Considérons une entrée de tension sinusoïdale avec une amplitude et une fréquence unitaires ω, c'est-à-dire sin (ωt), connectée aux bornes du Memristor contrôlé par le flux comme indiqué sur la figure (3.1) (a), et définissez v et i comme tension aux bornes de l'appareil et du courant circulant à travers le dispositif respectivement [53]:

$$v = \sin(\omega(t))$$

$$i = W(\varphi)v = (-a + 3b\varphi^2)v$$

$$\frac{d\varphi}{dt} = v$$

3.2.2. Modélisation du circuit chaotique memristor :

Le circuit avec une configuration alternative du circuit de Chua, analysé pour la première fois par Barboza et Chua [2008], comprend les mêmes éléments que le circuit original de Chua, dans un nouvel agencement où trois d'entre eux sont caractérisés par des valeurs négatives. En remplaçant la diode de Chua dans ce circuit chaotique par le Memristor contrôlé par flux caractérisé par (3.1), un circuit chaotique basé sur un Memristor lisse comme le montre la figure (3.2) est facilement conçu, dont la topologie diffère de celles des circuits chaotiques à base de Memristor analysés dans [56, 57, 55, 58,59].

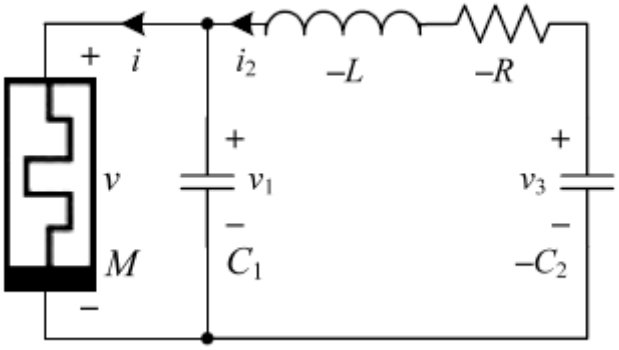


Figure (3.2) : Circuit chaotique simple memristor.

En appliquant les lois de circuit de Kirchhoff au circuit de la figure (3.2), nous obtenons un ensemble de quatre équations différentielles du premier ordre, qui définissent la relation entre les quatre variables de circuit (φ, v_1, i_2, v_3) [53] :

$$\begin{cases} \frac{d\varphi}{dt} = v_1 \\ C_1 \frac{dv_1}{dt} = i_2 - W(\varphi)v_1 \\ L\frac{di_2}{dt} = v_1 - Ri_2 - v_3 \\ C_2 \frac{dv_3}{dt} = i_2 \end{cases} \tag{3.5}$$

La courbe caractéristique $\varphi - q$ du memristor contrôlé par flux est donnée par (3.1) et$W(\varphi) = \frac{dq(\varphi)}{d\varphi}$.

En laissant $x_1 = \varphi$,$x_2 = v_1$, $x_3 = i_2$, $x_4 = -v_3$, $\alpha = 1/C_1$, $\beta = 1/C_2$, $\gamma = R$, $L = 1$, et définir les fonctions non linéaires $q(x)$et $W(x)$ comme [53]:

$$\begin{cases} q(x) = -ax + bx^3 \\ W(x) = \frac{dq(x)}{dx} = -a + 3bx^2 \end{cases} \quad (3.6)$$

Respectivement, les équations d'état de (3.5) peuvent être réécrites sous forme adimensionnelle comme [53]:

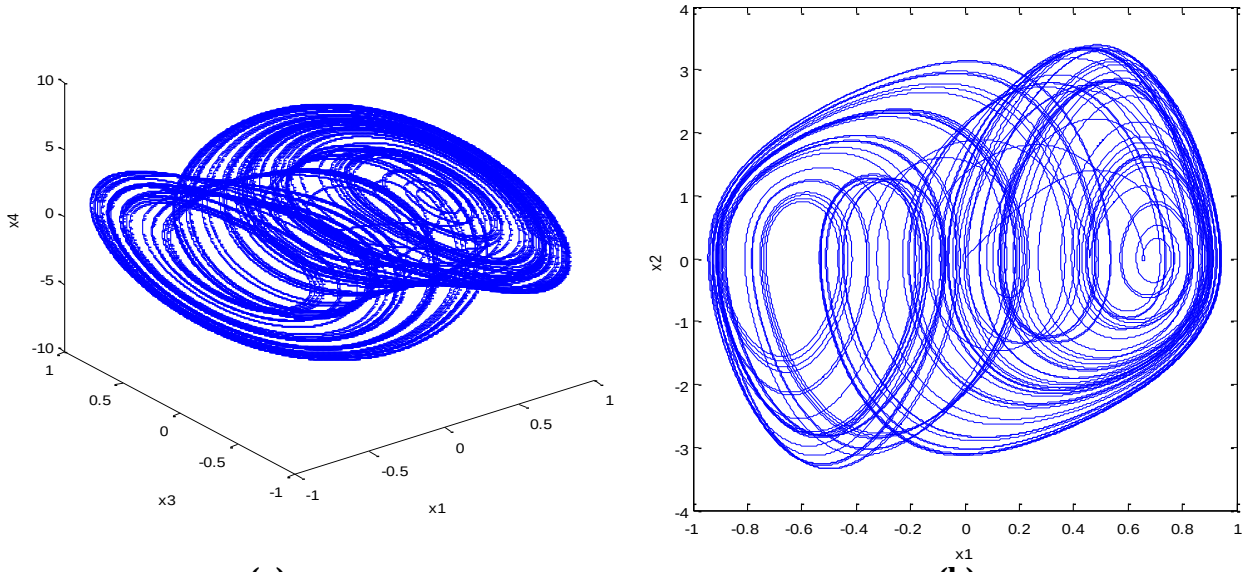
$$\begin{cases} \dot{x}_1 = x_2 \\ \dot{x}_2 = \alpha[x_3 - W(x_1)x_2] \\ \dot{x}_3 = x_2 - \gamma x_3 + x_4 \\ \dot{x}_4 = -\beta x_3 \end{cases} \quad (3.7)$$

Où α, β et γ sont des constantes réelles positives. Il convient de noter qu'à l'exception de la première équation, le modèle de circuit basé sur les Memristors décrit par équations (3.5) et (3.7) sont assez similaires au modèle de circuit de [60]. De même, pour les

Paramètre : $\alpha = 21, \beta = 48, \gamma = 0{,}6, a = 1/7 \; et \; b = 2/7,$

$W(x_1) = -a + 3bx_1{}^2$ [60].

Pour les conditions initiales (0, 0, 0,0001, 0), le système (3.7) est chaotique et affiche un attracteur chaotique à 2 volutes dans un intervalle de temps fini, comme le montrent les Figure (3.3) a et b:



(a) **(b)**

Figure (3.3) : attracteur chaotique d'un simple circuit de Memristor, (a) : attracteur à trois dimensions, (b) : attracteur à deux dimensions.

Et La figure (3,4) montre les trajectoires des quatre états du circuit de Memristor :

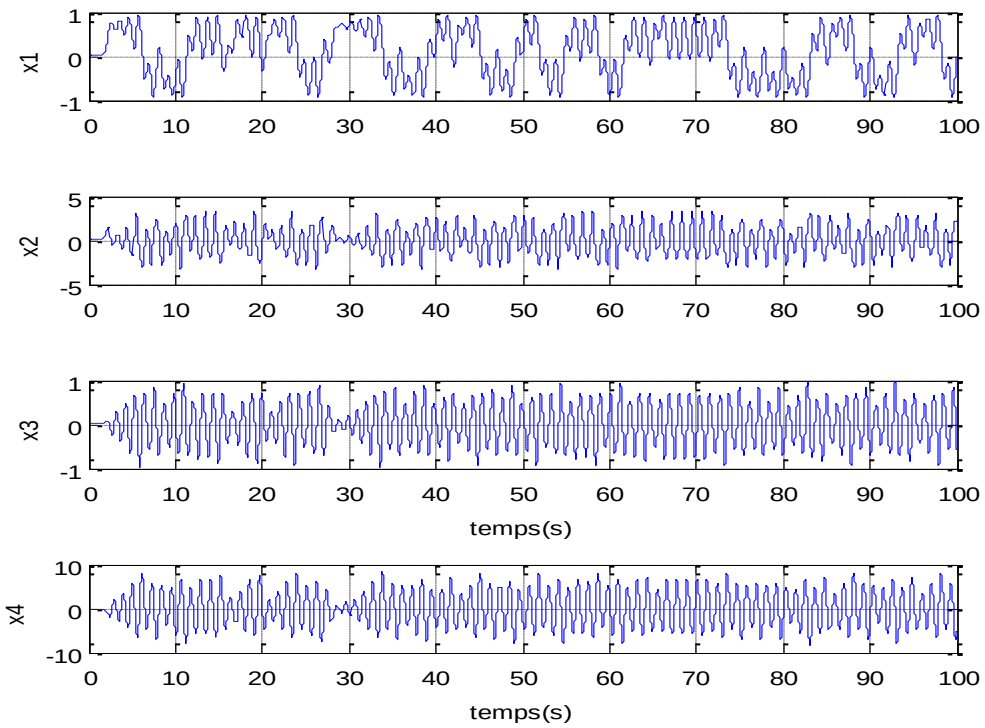


Figure (3.4) : Etats chaotique x_1, x_2, x_3, x_4 de circuit Memristor.

3.3. Théorie de la commande prédictive :

Considérons le système non linéaire décrit par [61] :

$$\dot{x}(t) = f\big(x(t)\big) + u(t) \tag{3.8}$$

Où $x \epsilon R^n$ est le vecteur d'état, $u \in R^n$ la commande et f: $R^n \times R^+ \rightarrow R^n$ est une fonction continue non-linéaire.

On appelle x_f point fixe ou point d'équilibre du système (3.8) :

$$\dot{x} = f\big(x_f\big) = 0 \tag{3.9}$$

Dans le cadre de la commande prédictive, la forme de la commande $u(t)$ est choisi tel que proposé par Boukabou et al [61,62] :

$$u(t) = K(x_p(t) - x(t)) \tag{3.10}$$

Où : *K* représente le gain.

$x(t)$Représente l'état actuel du système et $x_p(t)$représente l'état prédit.

En utilisant une prédiction d'un pas en avant, on obtient [61,62]:

$$u(t) = K(\dot{x}(t) - x(t)) \tag{3.11}$$

Le système chaotique contrôlé devient [63]:

$$\dot{x}(t) = f\big(x(t)\big) + K\big(\dot{x}(t) - x(t)\big) \tag{3.12}$$

La linéarisation autour de ce point revient à prendre la formule suivante : $x = x_f + \delta x$

Par dérivation.

$$\dot{x} = \dot{x}_f + \delta\dot{x} \tag{3.13}$$

En remplaçant dans (3.8), on obtient :

$$\dot{x}_f + \delta\dot{x} = f(x_f + \delta x) \tag{3.14}$$

Et, par développement de Taylor du premier ordre de $F(x)$, on obtient :

$$f\big(x_f + \delta x\big) = f\big(x_f\big) + f'\big(x_f\big)(x - x_f) \tag{3.15}$$

Remplaçant dans (3.14) :

$$\dot{x}_f + \delta\dot{x} = f\big(x_f\big) + f'\big(x_f\big)(x - x_f) \tag{3.16}$$

D'après la définition du point fixe :

$$\dot{x} = f\big(x_f\big) = 0 \tag{3.17}$$

On en déduit :

$$\delta\dot{x} = f'\big(x_f\big) * (x - x_f) \tag{3.18}$$

De (3.13) on a :

$$\delta x = x - x_f \tag{3.19}$$

D'où la forme générale :

$$\delta\dot{x} = Df\big(x_f\big) * \delta x \tag{3.20}$$

Ou DF représente la matrice jacobienne de $f(X)$par rapport à x, tel que :

$$DF = \left\{\frac{df_i}{dx_j}\right\}, i = 1,2,\dots,N \;\; j = 1,2,\dots,N \tag{3.21}$$

En linéarisant le système précédent, on obtient :

$$\begin{aligned}
\delta\dot{x}(t) &= Df\big(x_f\big)\delta x(t) + \delta u(t) \\
\delta\dot{x}(t) &= Df\big(x_f\big)\delta x(t) + K\left(Df\big(x_f\big)\delta x(t) - \delta x(t)\right) \\
\delta\dot{x}(t) &= Df\big(x_f\big)\delta x(t) + K * Df\big(x_f\big)\delta x(t) - K\delta x(t) \\
\delta\dot{x}(t) &= \big(Df\big(x_f\big) + K(Df\big(x_f\big) - I)\big)\delta x(t)
\end{aligned} \tag{3.22}$$

Les références [61,62] supposent que le gain *K* est un constant dans un intervalle, par contre dans notre travail, on le suppose sous forme d'une matrice, qu'il faut le calculer à partir des LMIs [64].

3.4. Application de la commande prédictive pour la synchronisation de deux systèmes chaotiques Memristor

L'objectif principe de ce chapitre est de synchroniser deux systèmes chaotiques à base de la commande prédictive pour cela :

Considérons les deux systèmes chaotique Memristor identiques suivants, où le système d'émetteur et le système de réception sont désignés par x et y, respectivement :

Système émetteur :

$$\begin{cases} \dot{x}_1 = x_2 \\ \dot{x}_2 = \alpha[x_3 - W(x_1)x_2] \\ \dot{x}_3 = x_2 - \gamma x_3 + x_4 \\ \dot{x}_4 = -\beta x_3 \end{cases} \quad (3.23)$$

Système récepteur :

$$\begin{cases} \dot{y}_1 = y_2 + u_1 \\ \dot{y}_2 = \alpha[y_3 - W(y_1)y_2] + u_2 \\ \dot{y}_3 = y_2 - \gamma y_3 + y_4 + u_3 \\ \dot{y}_4 = -\beta y_3 + u_4 \end{cases} \quad (3.24)$$

Avec $\alpha = 21, \beta = 48, \gamma = 0{,}6, a = \frac{1}{7}, b = \frac{2}{7}$,

$W(x_1) = -a + 3b{x_1}^2, W(y_1) = -a + 3b{y_1}^2$ [60].

Le système est synchronisé asymptotiquement dans le sens où :

$$\lim_{t\to\infty} e(t) \to 0 \quad (3.25)$$

Tout d'abord nous commençant par calculer l'erreur entre le système émetteur/récepteur.

$$e(t) = [e_1(t) \quad e_2(t) \quad e_3(t) \quad e_4(t)]^{\mathrm{T}} \quad (3.26)$$

$$= [y_1(t) - x_1(t) \quad y_2(t) - x_2(t) \quad y_3(t) - x_3(t) \quad y_4(t) - x_4(t)]^{\mathrm{T}}$$

Ensuite, la dynamique du système d'erreur est déterminée, directement en soustrayant Système de récepteur de Système d'émetteur :

$$\dot{e}(t) = [\dot{e}_1(t) \quad \dot{e}_2(t) \quad \dot{e}_3(t) \quad \dot{e}_4(t)]^{\mathrm{T}} \quad (3.27)$$

$$= [\dot{y}_1(t) - \dot{x}_1(t) \quad \dot{y}_2(t) - \dot{x}_2(t) \quad \dot{y}_3(t) - \dot{x}_3(t) \quad \dot{y}_4(t) - \dot{x}_4(t)\ ]^{\mathrm{T}}$$

$$\begin{cases} \dot{e}_1 = e_2 + u_1 \\ \dot{e}_2 = \alpha[e_3 - W(y_1)y_2 + W(x_1)x_2] + u_2 \\ \dot{e}_3 = e_2 - \gamma e_3 + e_4 + u_3 \\ \dot{e}_4 = -\beta e_3 + u_4 \end{cases} \quad (3.28)$$

A base de l'équation (3.27) et en appliquant les LMIs on obtient la valeur de la matrice K comme suit :

$$K = \begin{bmatrix} 4.7238 & -1 & -1 & -2.3619 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 9 \end{bmatrix}$$

Et la commande aura la formule suivante :

$$u(t) = K\big(\dot{e}(t) - e(t)\big)$$

$$u(t) = \begin{bmatrix} 4.7238 & -1 & -1 & -2.3619 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 9 \end{bmatrix} * \begin{bmatrix} \dot{e}_1(t) - e_1(t) \\ \dot{e}_2(t) - e_2(t) \\ \dot{e}_3(t) - e_3(t) \\ \dot{e}_4(t) - e_4(t) \end{bmatrix}$$

$$u(t) =$$

$$\begin{cases} u_1 = 4.7238\big(\dot{e}_1(t) - e_1(t)\big) - \big(\dot{e}_2(t) - e_2(t)\big) - \big(\dot{e}_3(t) - e_3(t)\big) - 2.3619\big(\dot{e}_4(t) - e_4(t)\big) \\ u_2 = 0 \\ u_3 = 0 \\ u_4 = 9\big(\dot{e}_4(t) - e_4(t)\big) \end{cases} \quad (3.29)$$

Les résultats obtenus de la synchronisation entre les deux systèmes suite à l'application de la loi de contrôle prédictif sont représentés par les figures suivantes:

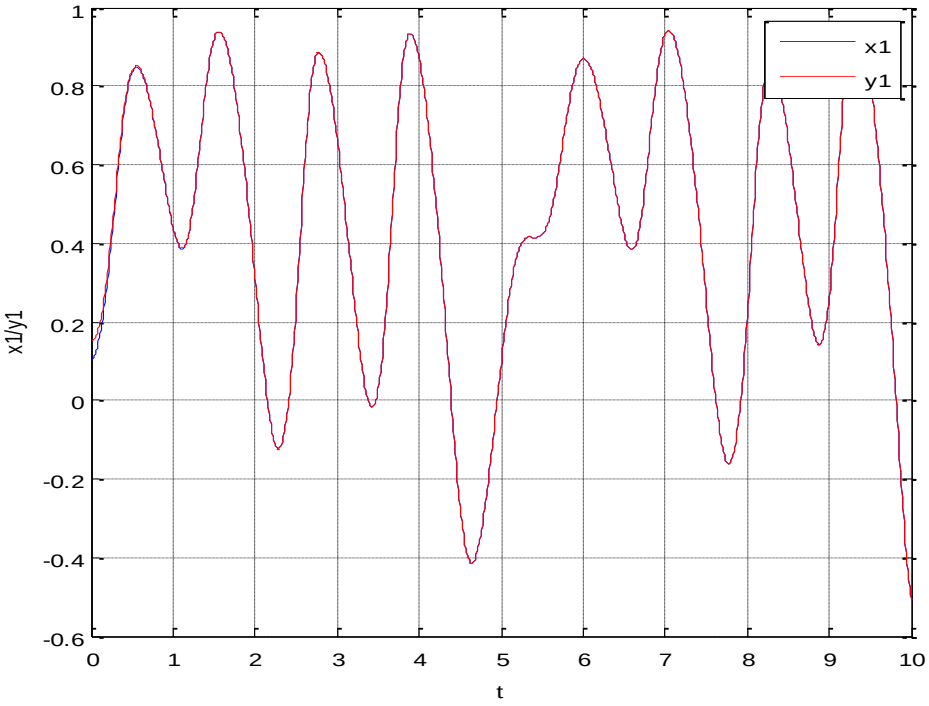


Figure (3.5) : la synchronisation entre l'état $x_1 \text{et} y_1$

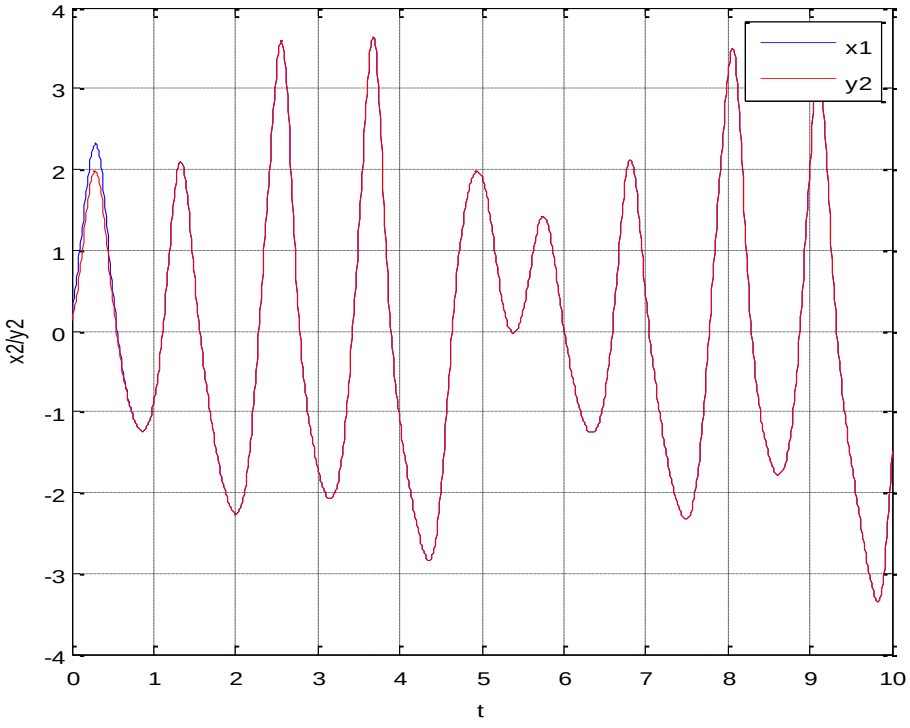


Figure (3.6) : la synchronisation entre l'état $x_2 \text{et} y_2$.

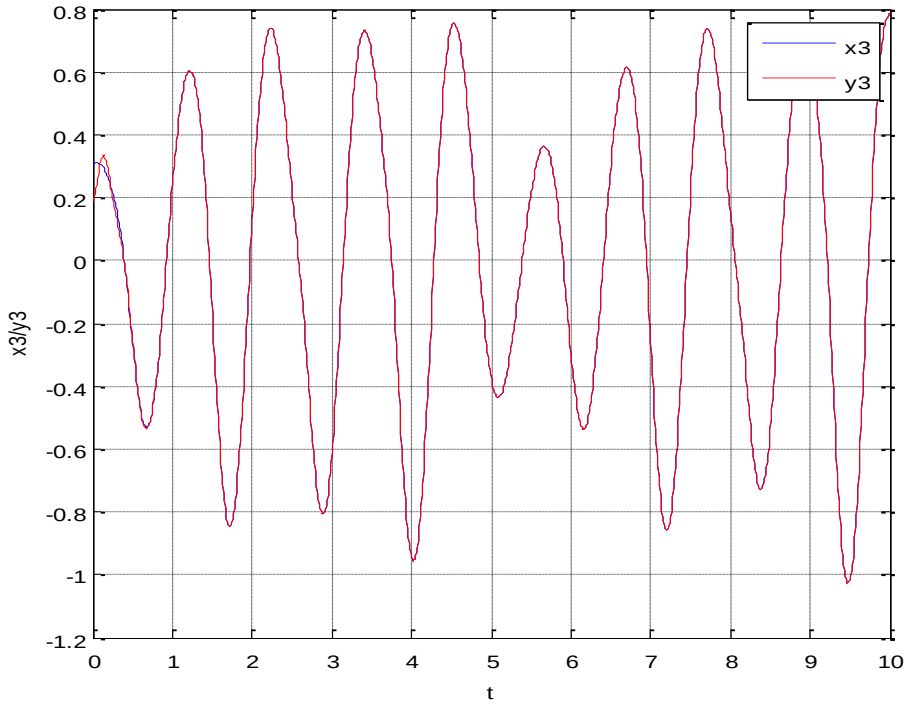


Figure (3.7) : la synchronisation entre l'état $x_3 et y_3$.

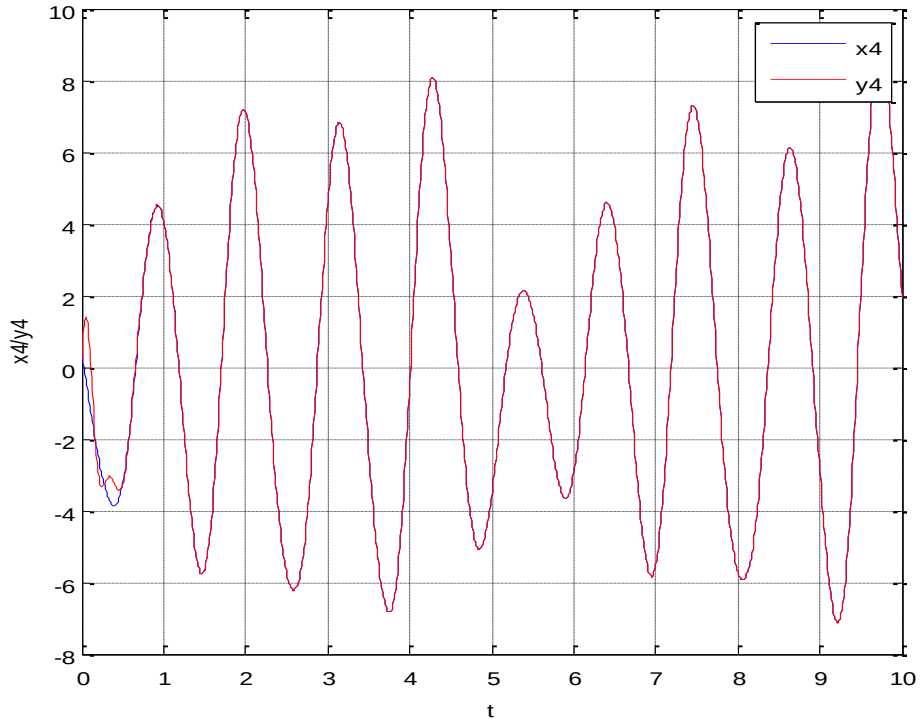


Figure (3.8) : la synchronisation entre l'état $x_4 et y_4$.

Et le figure (3.9) représente l'erreur de synchronisation prédictive entre les deux systèmes :

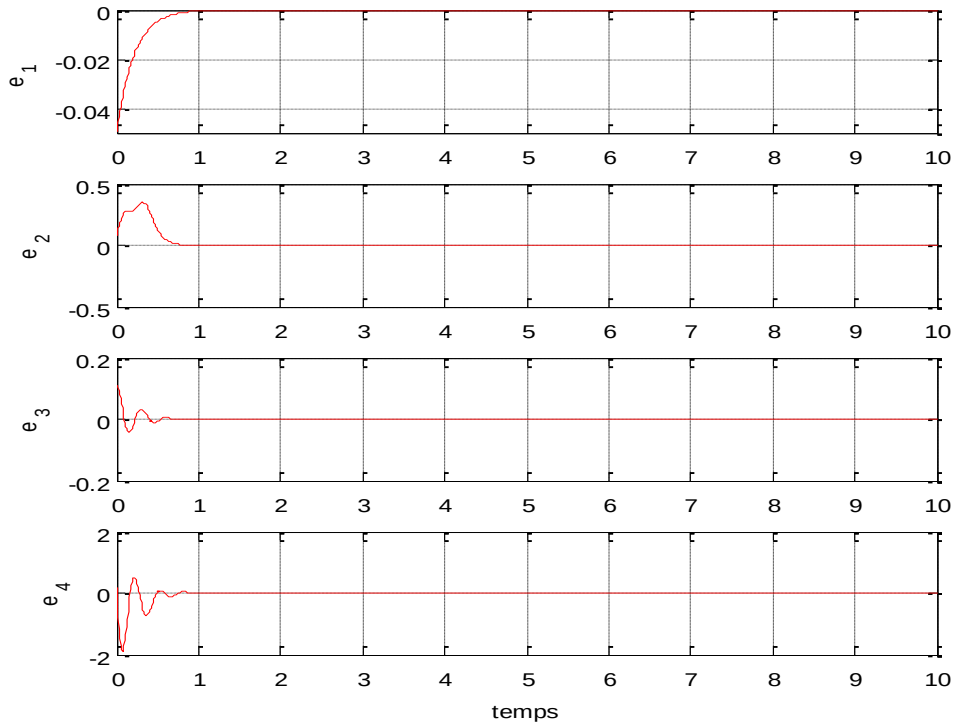


Figure (3.9) : Erreur de synchronisation prédictive

D'après les résultats de simulation, on remarque que les deux systèmes se synchronisent parfaitement et rapidement; ce qui signifie l'efficacité de l'approche proposée.

3.5. Conclusion :

Dans ce chapitre, nous avons appliqué la commande prédictive pour la synchronisation de deux systèmes Memristor chaotiques. Les résultats de simulation obtenus, montrent clairement l'efficacité de la stratégie de commande, ce qui sollicite son application pour le chiffrement d'informations

CHAPITRE 4

Chiffrement d'information à base de la commande prédictive et de Memristor

4.1. Introduction

L'idée d'utiliser des signaux chaotiques pour transmettre des informations dans les systèmes de communication est apparue au début des années 1990, après avoir réalisé que deux systèmes chaotiques pourraient être synchronisés [65]. Différentes méthodes ont été proposés pour transmettre des informations à l'aide de signaux porteurs chaotiques [66, 67].

4.2. Modulation/ Démodulation chaotique

Considérons un oscillateur chaotique à n dimensions de la forme [68] :

$$\begin{cases} \dot{x} = f(x, y) \\ \dot{y} = g(x, y) \end{cases} \tag{4.1}$$

Où $x \epsilon R^n$ et $y \in R^{n-1}$ sont les états du système. $f: R^n \to R$ et $g: R^n \to R^{n-1}$ Sont des fonctions continues. Le signal d'information analogique $s(t) \in R$est injecté dans l'oscillateur comme suit [68]:

$$\begin{cases} \dot{x} = f(x, y) + cs(t) \\ \dot{y} = g(x, y) \end{cases} \tag{4.2}$$

Où $c > 0$ est une constante, choisit de telles façons que le terme additionnel $cs(t)$ ou le message à transmettre doit se comporter correctement afin de ne pas détruire la caractéristique chaotique du système d'origine, et inclut par injection dans la dynamique du système [68].

Dans le schéma de communication, nous prenons $x(t)$ dans (4.2) comme signal transmis.

Au niveau du récepteur, nous pouvons construire un sous-système synchrone [68] :

$$\dot{\hat{y}} = g(x, \hat{y}) \tag{4.3}$$

La stabilité du sous-système y implique que [68]:

$$\hat{y}(t) \to y(t), \text{quand } t \to \infty \tag{4.4}$$

La démodulation peut facilement être effectuée comme suit [68]:

$$\lambda(t) = \frac{\dot{x} - f(x,y)}{c} \tag{4.5}$$

[68] Propose un nouvel algorithme robuste pour récupérer le signal d'information et éviter la différenciation du signal transmis, qui est définit comme suit:

$$\begin{cases} \hat{s}(t) = ckx(t) + w(t) \\ \dot{w} = -ck[f(x,y) + c\hat{s}(t)] \end{cases} \tag{4.6}$$

Où le gain $k > 0$ est une constante, $c > 0$ est une constante et $\hat{s}(t)$représente le signal récupéré. La figure (4.1) montre le schéma du système de communication proposé [68].

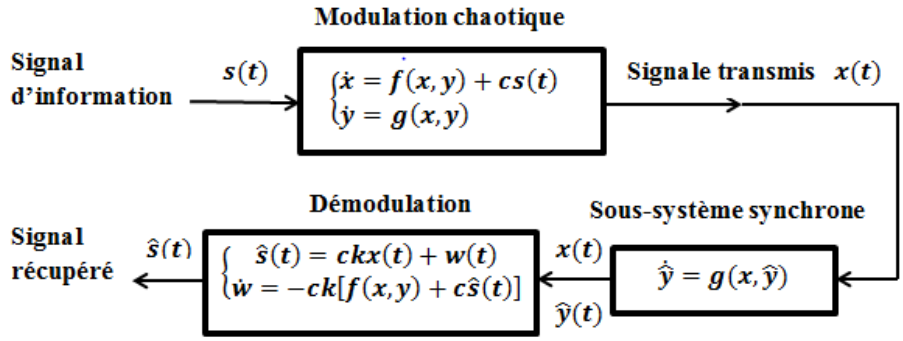


Figure (4.1) :L'architecture de communication.

4.3. Résultats de simulation :

4.3.1. Système émetteur (maitre):

Le système proposé pour générer le signal chaotique est l'oscillateur Memristor défini par les équations d'état suivantes [53] :

$$\begin{cases} \dot{x}_1 = x_2 \\ \dot{x}_2 = \alpha[x_3 - W(x_1)x_2] \\ \dot{x}_3 = x_2 - \gamma x_3 + x_4 \\ \dot{x}_4 = -\beta x_3 \end{cases} \tag{4.7}$$

Nous injectons un signal d'information s (t) dans l'oscillateur Memristor comme suit:

$$\begin{cases} \dot{x}_1 = x_2 + cs(t) \\ \dot{x}_2 = \alpha[x_3 - W(x_1)x_2] \\ \dot{x}_3 = x_2 - \gamma x_3 + x_4 \\ \dot{x}_4 = -\beta x_3 \end{cases} \quad (4.8)$$

Où $\boldsymbol{c}$ est une constante d'échelle, α, β et γ, a et b sont des paramètres où: $\alpha = 21,\ \beta = 48,$ $\gamma = 0.6,\ a = 1/7\ et\ b = 2/7, W(x_1) = -a + 3b{x_1}^2$ [60].

Sous Matlab (Simulink), nous réalisons la conception de l'émetteur chaotique Memristor à partir de l'équation d'états (4.7), avec le signal d'information injecté dans la dynamique de système Memristor.

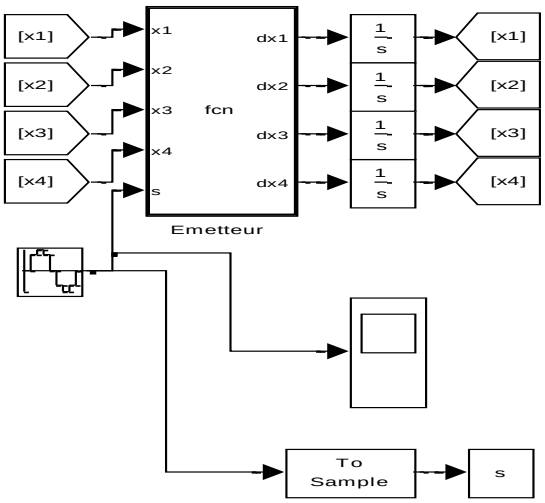


Figure (4.2) : Conception de l'émetteur chaotique Memristor avec le signal d'information injecté.

Le signal à transmettre est montré sous la figure ci-dessous :

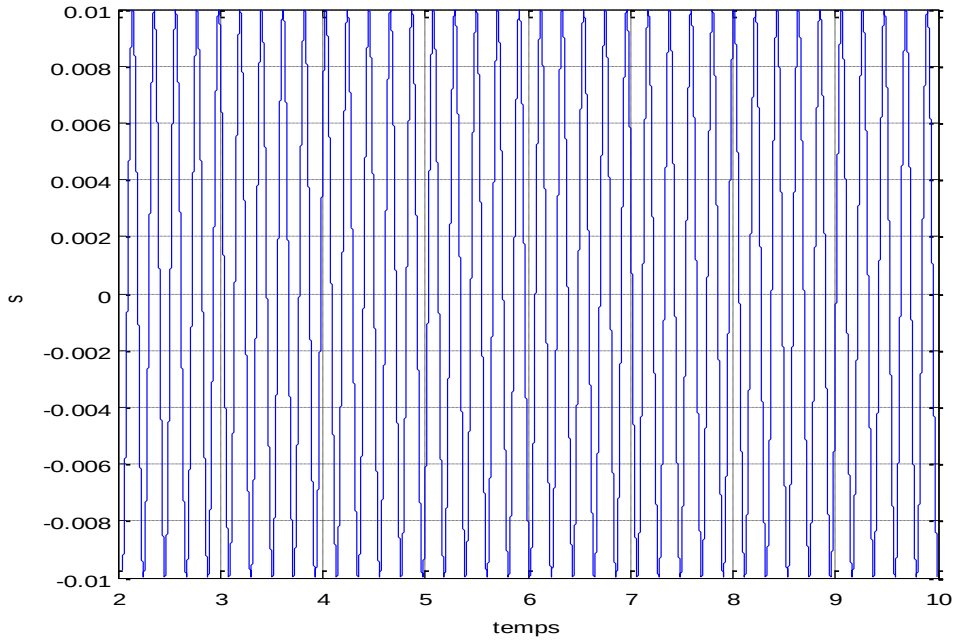


Figure (4.3): Le signal informatif s(t)

4.3.2. Système récepteur (esclave)

Concernant le récepteur, c'est un circuit Memristor identique à l'émetteur et a les mêmes paramètres α, β et γ, a et b, et $W(y_1) = -a + 3by_1{}^2$.

L'équation d'état est définit par :

$$\begin{cases} \dot{y}_1 = y_2 + u_1 \\ \dot{y}_2 = \alpha[y_3 - W(y_1)y_2] + u_2 \\ \dot{y}_3 = y_2 - \gamma y_3 + y_4 + u_3 \\ \dot{y}_4 = -\beta y_3 + u_4 \end{cases} \quad (4.9)$$

La conception de récepteur chaotique Memristor sous Matlab (Simulink) est réalisée par le montage suivant :

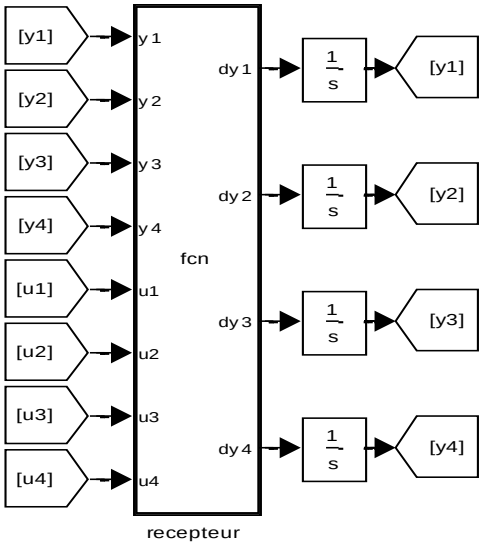


Figure (4.4) : Récepteur chaotique Memristor sous Matlab (simulink).

Pour récupérer le signal d'information transmite de l'émetteur vers le récepteur, il faut établir la synchronisation entre les deux systèmes chaotique et appliquer la démodulation chaotique pour récupérer ce dernier.

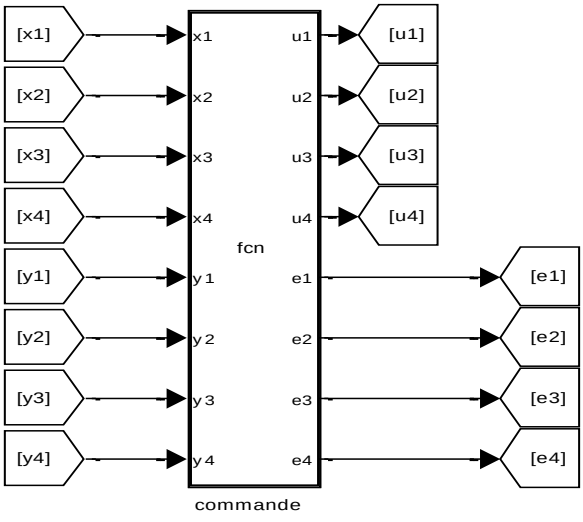


Figure (4.5) : La commande sous Matlab (Simulink)

Les figure suivant représentent les résultats de synchronisation prédictive entre l'émetteur x(t) et le récepteur y(t) sur les quatre états :

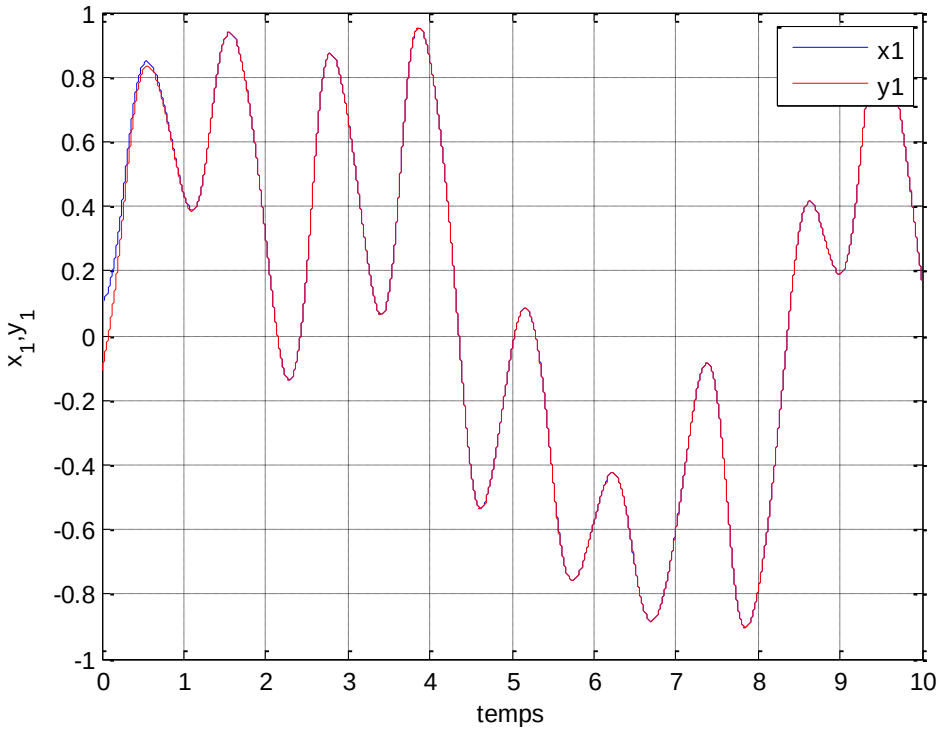


Figure (4.6) : Etats x_1 /y_1.

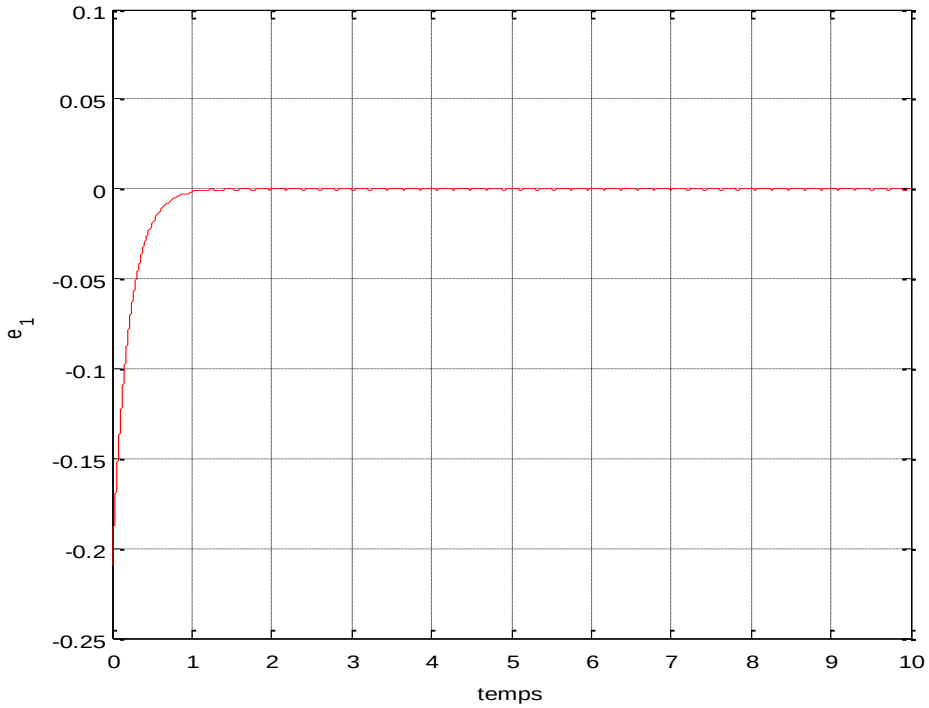


Figure (4.7) : Erreur de synchronisation $e_1 = y_1 - x_1$

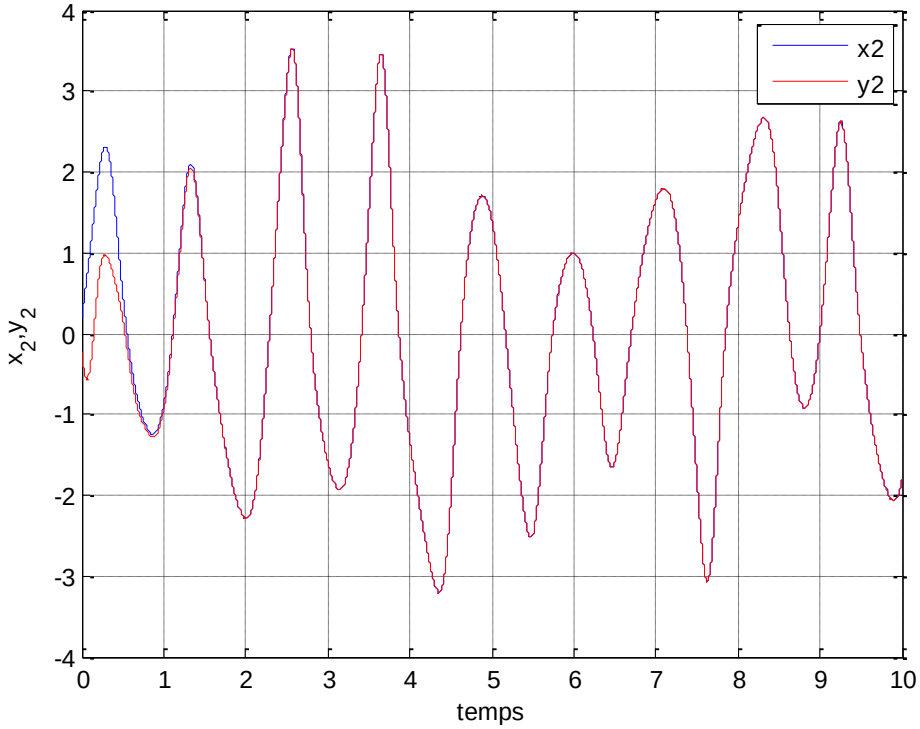


Figure (4.8) : Etats x_2 /y_2.

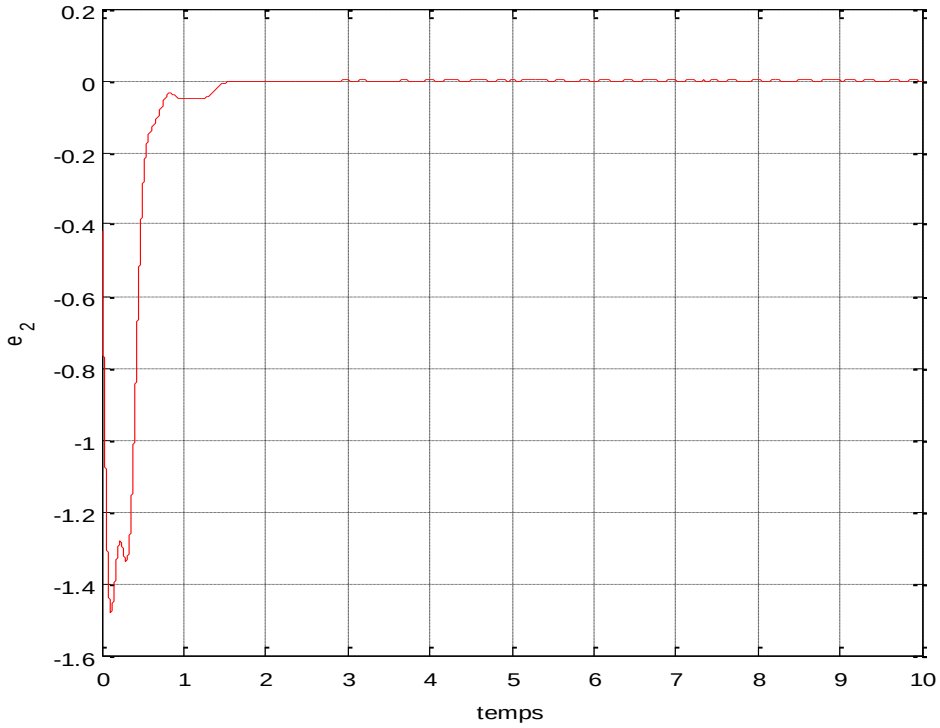


Figure (4.9): Erreur de synchronisation $e_2 = y_2 - x_2$.

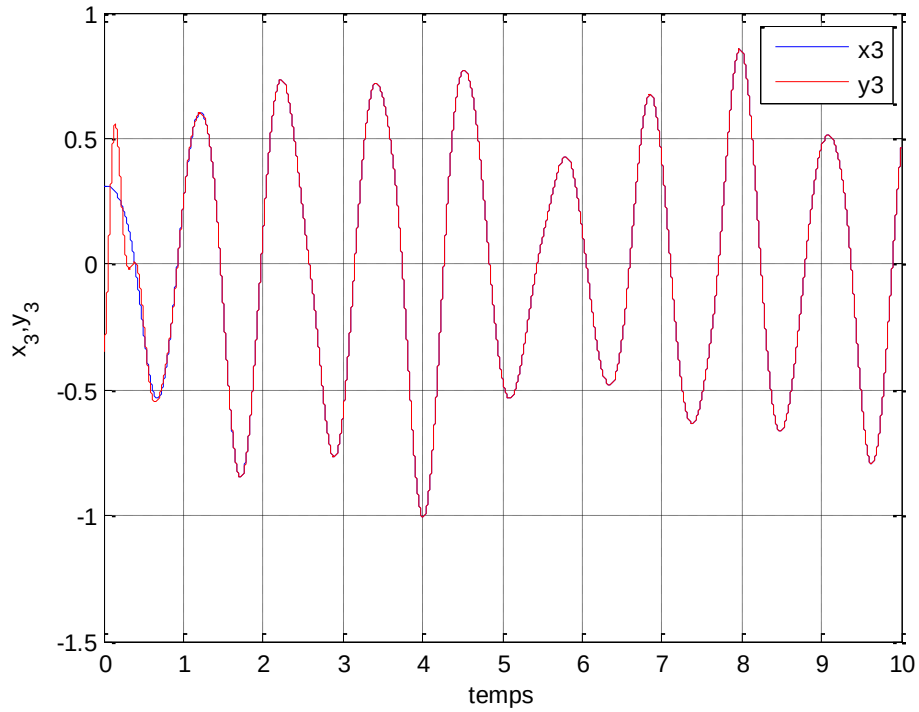


Figure (4.10) : Etats x_3 /y_3.

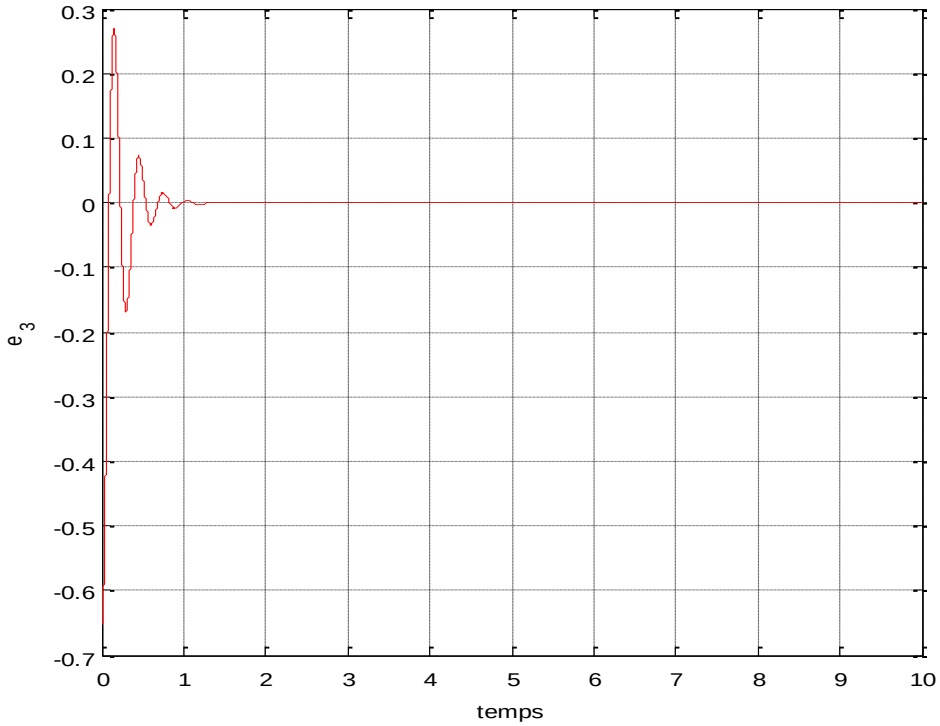


Figure (4.11): Erreur de synchronisation e_3= $y_3 - x_3$.

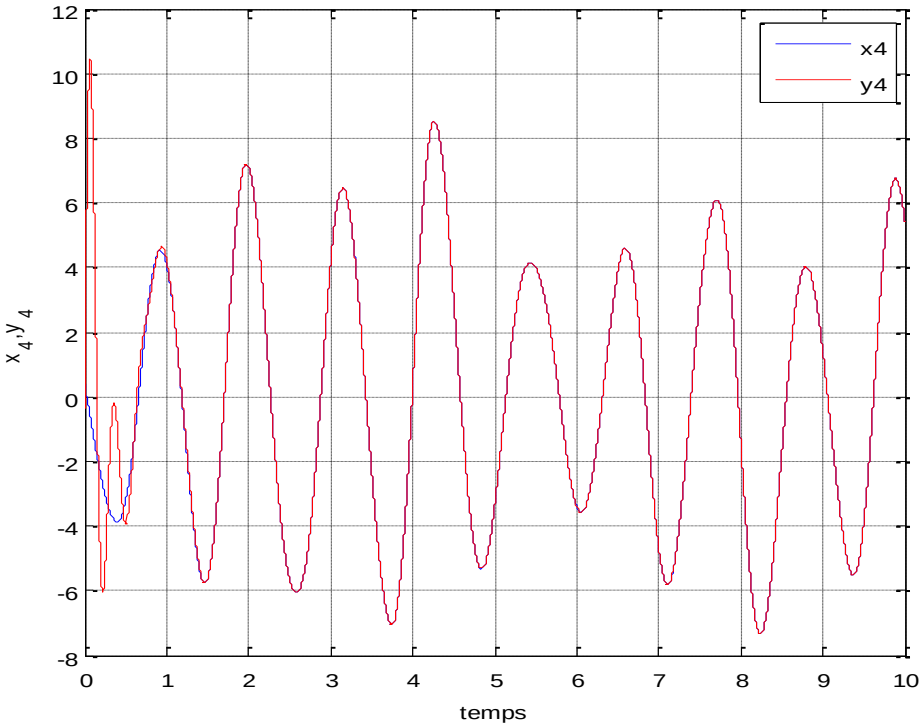


Figure (4.12) : Etats x_4 /y_4.

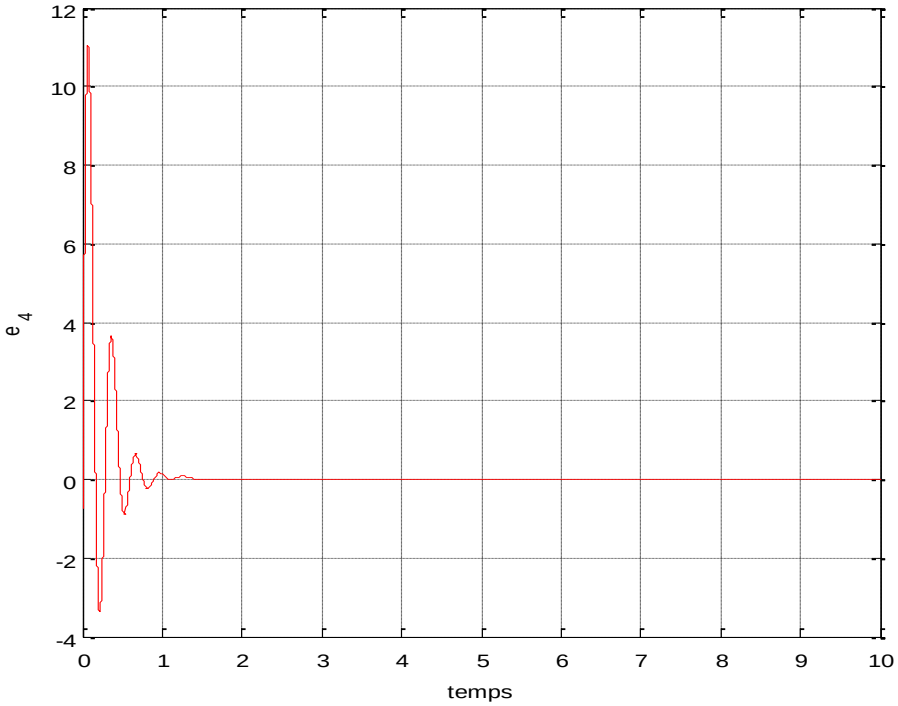


Figure (4.13): Erreur de synchronisation e_4=$y_4 - x_4$.

Les signaux transmit (s(t)) et récupéré (m(t)) sont illustrés sur la figure suivante :

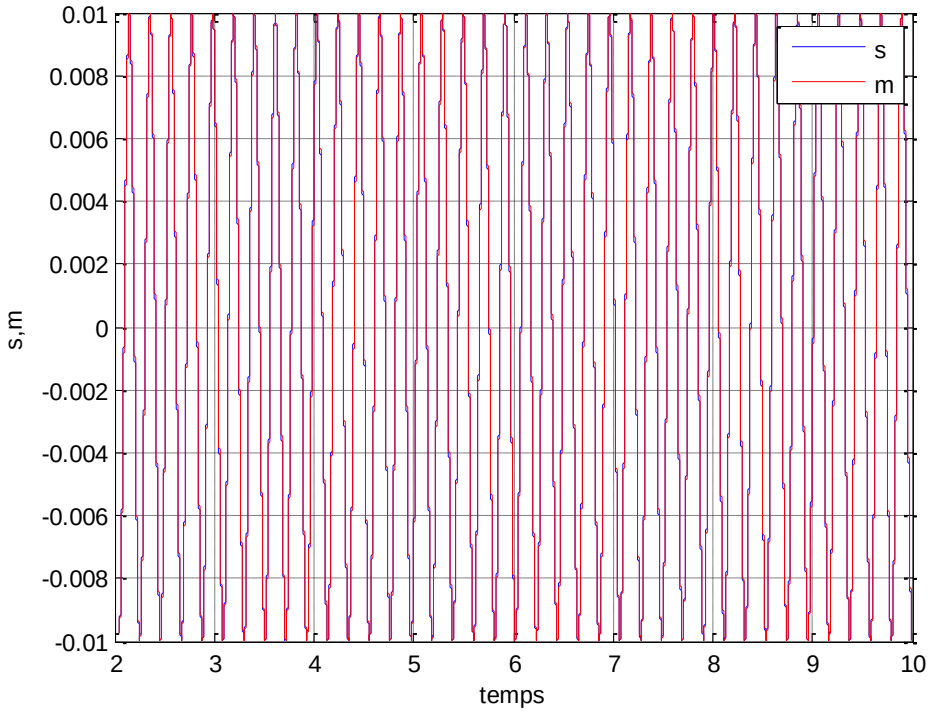


Figure (4.14) : Signal récupéré m(t) et le signal transmit s(t).

D'après la figure (4.14) on peut constater que le message est bien récupéré.

4.4. Conclusion

Dans ce chapitre, nous avons présenté une approche pour le chiffrement d'information à base la commande prédictive et la Modulation/démodulateur chaotique. Le principe de base de cette approche consiste en premier lieu d'établir une synchronisation entre l'émetteur et le récepteur à l'aide de la commande prédictive puis resituer le message injecté dans dynamique de l'émetteur, par la technique de démodulation chaotique. Les résultats obtenus montrent l'efficacité de cette approche.

Conclusion générale

Dans ce mémoire, nous avons étudié et testé par simulation un système de transmission sécurisé de données basé sur les systèmes chaotiques.

Notre travail a été entamé par évoquer d'abord quelques notions sur les systèmes dynamiques qu'ils soient en temps continu ou en temps discret. Par la suite, nous nous sommes intéressés à une classe particulière de systèmes non linéaires qui sont dits chaotiques.

Ces systèmes chaotiques présentent plusieurs caractéristiques dont l'exploitation serait intéressante pour la transmission de données. Parmi ces caractéristiques que nous avons défini le déterminisme qui signifie que ces systèmes sont régis par des règles fondamentales non probabilistes, ainsi que leurs sensibilité mêmes aux faibles variations des conditions initiales. Ceci implique l'impossibilité de prédiction à long terme le comportement du système chaotique. Une troisième propriété est les attracteurs étranges qui sont des formes géométriques complexes et qui caractérisent l'évolution des systèmes chaotiques. Par la suite, nous avons défini les exposants de Lyapunov servi à mesurer le degré de stabilité d'un système chaotique.

Dans le deuxième chapitre, nous avons fait un tour d'horizon sur les différentes approches de synchronisation, puis nous avons mis en relief les différentes techniques de transmission sécurisée à base du chaos.

Le troisième chapitre à portée sur la synchronisation de deux systèmes Memristor chaotiques à l'aide de la commande prédictive avec présentation détaillée du Memristor et les résultats de simulations obtenus.

Dans le dernier chapitre, nous avons détaillé une proche de chiffrement d'infirmations à base de la démodulation chaotique. Les résultats de simulation montrent les performances du système de transmission proposé.

Comme suite à ce travail, on propos l'implémentation de l'approche proposée sous FPGA pour une application temps réel.

Bibliographie

[1] O.Megherbi, “Etude et réalisation d’un système sécurisé à base de systèmes chaotiques,” Mémoire de Magister en Automatique, Université Mouloud Mammeri de Tizi-Ouzou, Algérie, 2013.

[2] F. Anstett.Les systèmes dynamiques chaotiques pour le chiffrement synthèse et cryptanalyse.2006.

[3] N, Lorenz. E. The Essence of Chaos. University of Washington Press, 1993.

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

[5] L.M. Pecora, T.L.Caroll. "Synchronization in chaotic systems." *PHYSICAL REVIEW LETTERS*, February 19, 1990: 821-825.

[6] L.M. Pecora, T.L.Caroll. "Synchronizing nonautonomous chaotic circuits." IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing, Oct 1993: 646-650

[7] C. Li, X. Liao K.W. Wong. "Chaotic lag synchronization of coupled time-delayed Systems and its application in secure communication." Systems & Control Letters, 1986: 133-142.

[8] R. Mainieri, J. Rehacek. "Projective synchronization in three-dimensional chaotic, "Physical Review Letters, 1999: 3042–3045.

[9] T. Yang, L.O. Chua. "Impulsive stabilization for control and synchronization of chaotic systems: theory and application to secure communication." IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, Oct 1997: 976-988.

[10] K. Hannoun, “ Etude, Simulation et implémentation d’un émetteur hyper chaotique sur carte Arduino Uno, ” Mémoire de Fin d’Etudes de Master Academique en Electronique, Université Mouloud Mammeri de Tizi-Ouzou, 2014.

[11] C. Benhabib, “ Etude d’un système chaotique pour la sécurisation des communications optiques, ”Mémoire de master, Université Abou Bakr Belkaid Tlemcen, 2014.

[12] M. B. Luca, “Apports du chaos et des estimateurs d’états pour la transmission sécurisée de l’information, ”Thèse de doctorat en électronique, université de Bretagne Occidentale, 2006.

[13] A. Sabour, “ Conception et validation d’un régénérateur de suites binaires crypto graphiquement sures basé sur les algorithmes évolutionnistes, ”Thèse de doctorat en informatique, Université Mohamed V – Agdal faculté des sciences Rabat, 2007.

[14] J. Aguilar Angulo, "Conception d'un Générateur de Valeurs aléatoires en Technologie CMOS AMS 0.35 µm, "pour obtenir le grade de Docteur en sciences, Spécialité : Microélectronique, Université du Sud Toulon Var, 15 juin 2015.

[15] G.Kaddoum, " Contributions à l'amélioration des systèmes de communication multiutilisateurs par chaos : synchronisation et analyse des performances, " Thèse de Doctorat de l'Université de Toulouse, 2008.

[16] A. Zemouche, "Sur l'observation de l'état des systèmes dynamiques non linéaires. " Thèse de doctorat en électronique, université Louis Pasteur Strasbourg I, 2007.

[17] DJ. GOUMIDI, " Fonction logistique et standard chaotique pour le chiffrement des images satellitaires, "thèse magister, Université Mentouri de Constantine, 2010.

[18] S. Rezzag, "Etude et estimation des bornes de systèmes dynamiques chaotiques et hyper chaotiques, " thèse doctorat, Université Larbi Ben M'hidi.

[19] HONGRE, L. SAILHAC, P. ALEXANDRESCU, M. et DUBOIS, J, "Nonlinear and multifractals approaches of the geomagnetic field," Physics of the Earth and Planetary Interiors 1999, 110, 157-190.

[20] ROSENSTEIN, M. COLLINS, J. et DE LUCA, C, " A practical method for calculating Largest Lyapunov exponents for small data sets, " Physica 1993, D 65, 117-134.

[21] M.Maizi, " Etude et Contrôle du chao dans des systèmes physiques, " Mémoire de master, Université Larbi Tébessi- Tébessa, Algérie, 2016.

[22] A. AIT HAMMI, " étude et réalisation d'un système chaotique basé sur le circuit de Chua, "thèse de master professionel, Université Mouloud Maameri Tizi-Ouzou, 2014.

[23] A. R. Kihal, "Système chaotique pour la transmission sécurisée de donnée," Mémoire de magister, Université Mohammed Khider, Biskra, 2013.

[24] E.Cherrier, "Estimation de l'état et des entrées inconnues pour une classe de systèmes non linéaires, " Doctorat de l'Institut National Polytechnique de Lorraine,
Spécialité automatique et traitement du signal, école doctorale IAEM Lorraine, 26 octobre 2006.

[25] A. Khadra, "Impulsive Control and Synchronization of Chaos-Generating-Systems with Applications to Secure Communication," Thèse de Doctorat, Université de Waterloo, Ontario, Canada, 2004.

[26] L.M. Pecora, T.L.Caroll, "Synchronization in chaotic systems," PHYSICAL REVIEW LETTERS, February 19, 1990: 821-825.

[27] L.M. Pecora, T.L.Caroll, “Synchronization in chaotic systems,” Physical Review Letters, February, volume 64, (8), pp. 821-825, 1990.

[28] H.Dimassi, “Synchronisation des systèmes chaotiques par observateurs et applications à la transmission d’informations,” Thèse de Doctorat de l’Université de Paris Sud 11, 2012.

[29] A.Fradkov, A.Y. Pogromsky, “Introduction to control of oscillations and chaos World scientific,” Singapore, Series A, vol. 35, 1998.

[30] E. Ott, T. Sauer and J. A. Yorke, “Coping with chaos: Analysis of chaotic data and exploitation of chaotic systems,” Wiley-Interscience, NY, 1994.

[31] H.Hamiche, “Inversion à Gauche des Systèmes Dynamiques Hybrides Chaotiques, Applications à la Transmission Sécurisée de Données,” Thèse de Doctorat, Université Mouloud Mammeri de Tizi-Ouzou, (2011).

[32] S. Penaud, “Etude des Potentialités du Chaos pour les systèmes de Télécommunications, Évaluation des performances de systèmes à accès Multiples à répartition par les Codes (CDMA) Utilisant des séquences d’étalement Chaotique,” Thèse de Doctorat de l’Université de Limoges, 2001.

[33] A.Berkane, “Transmission sécurisée à base de la synchronisation impulsive de deux systèmes chaotique discrets,” Mémoire de Master Professionnel en électronique industriel, Université Mouloud Mammeri Tizi-Ouzou, 2016.

[34] L.M Pecora, T.L. Carroll, “Synchronization in Chaotic systems,” physical review letters, vol 64 N° 8, 1990.

[35] I. Ameur, “Synchronisation Chaotification et Hyperchaotification des systèmes non linéaires: Méthodes et applications,” thèse de Doctorat de l’Université Mentouri de Constantine, 2011.

[36] T. Hoet, B. Lorenz, S. Sahin, “ la cryptographie Chaotique, ”Mémoire de Licence IMACS INSA Toulouse, 2012.

[37] Rulkov, Nikolai F and Sushchik, Mikhail M and Tsimring, Lev S and Abarbanel, Henry DI, “Generalized synchronization of chaos in directionally coupled chaotic systems,” Physical review E, vol. 51, No. 2, PP. 980–994, 1995. 95, 110.

[38] T.Hoet, B.Lorenzi, S.Sahin, “ la cryptographie chaotique, ” Mémoire de Licence IMACS INSA Toulouse, 2012.

[39] A.Pacha, N. Hadj-Saidi, A. M'hamed, A. Bbelghoraf, "Chaos Crypto-Système basé sur l'Attracteur de Hénon-Lozi, " Université d'Oran, Algérie, 2008.

[40] A.Amirouche, L.Bourahmoune, "Conception et etude d'un système de transmission sécurisée de données à base d'un système chaotique d'ordre fractionnaire," Mémoire de Fin d'Etudes de Master Academique en Automatique, Université Mouloud Mammeri de Tizi-Ouzou, 2015.

[41] YAGOUB Imad Eddine, " Systèmes dynamiques discrets et chaos, " université du havre, Année 2010/2011.

[42] K. M. Cuomo, A. V. Oppenheim, and S. H. Strogatz, "Synchronization of lorenz-based chaotic circuits with applications to communications," IEEE *Trans. Circuits Syst. II*, 40(10):626–633, 1993.

[43] J.P. Barbot, I. Belmouhoub and L.Boutat-Baddas, "Observability Bifurcations: Application to Cryptography," In Chaos in Automatic Control, Taylor and Francis, 2005.

[44] L. Boutat-baddas, "Analyse des singularités d'observabilité et de détectabilité: Application à la synchronisation des circuits électroniques chaotiques," Thèse, Université de Cergy-Pontoise, 2002.

[45] A. Leuciuc, "Information transmission using chatic discrete-time lter," IEEE Transactions on Circuit and Systems, vol. 47, pp. 82_88, 2000.

[46] K.M. Short, "Unmasking a modulated chaotic communications scheme," International Journal of Bifurcations and Chaos, vol. 6, pp. 367–375, 1996.

[47] T. Yang, L.B. Yang and C.M. Yang, "Cryptanalysing chaotic secure communications using return maps," Physics letters A, vol. 245, pp. 495–510, 1998.

[48] H. Nijmeijer and I. Mareels, "An observer looks at synchronization." IEEE Trans. on Circ. Syst. I: Fundamental Theory and Applications, 44(10):882–890, 1997.

[49] M. Chen, D. Zhou, and Y. Shang, "A sliding mode observer based secure communication scheme," Chaos, Solitons and Fractals, 25:573–578, 2005.

[50] M. Boutayeb, M. Darouach and H. Raparalahy, "Generalized state-space observers for chaotic synchronization and secure communications,"IEEE Transactions on Circuits and Systems: Fundamantal Theory and Applications, vol. 49, No. 3, pp. 345–349, 2002.

[51] G. Millérioux and J. Daafouz, "Unknown input observers for message-embedded chaos synchronization of discrete-time systems," International Journal of Bifurcations and Chaos, vol. 14, No. 4 pp. 1357–1368, 2004.

[52] U. Feldmann, M. Hasler and W. Shwarz, "Communications par chaotic signals: the inverse system approach," International Journal of Circuit: Theory ans Applications, vol. 24, pp. 551–579, 1996.

[53] B.Bao et al., "A Simple Memristor Chaotique Circuit with complex dynamics, " Journal of Bifurcation and Chaos, Vol. 21, No. 9,pp 2629–2645,(2011).

[54] Chua, L. O. & Kang, S. M. [1976] "Memristive devices and systems," *Proc. IEEE* 64, 209–223.

[55] Itoh, M. & Chua, L. O. [2008] "Memristor oscillators," Int. J. Bifurcation and Chaos 18, 3183–3206.

[56] Bao, B. C., Liu, Z. & Xu, J. P. [2010a] "Steady periodic memristor oscillator with transient chaotic behaviors,"Electron. Lett. 46, 228–230.

[57] Bao, B. C., Liu, Z. & Xu, J. P. [2010b] "Transient chaos in smooth memristor oscillator," Chinese Phys. B 19, 030510.

[58] Muthuswamy, B. [2010] "Implementing memristor-based chaotic circuits," Int. J. Bifurcation and Chaos 20, 1335–1350.

[59] Muthuswamy, B. & Kokate, P. P. [2009] "Memristor based chaotic circuits," IETE Techn. Rev. 26, 415– 426.

[60] Barboza, R. & Chua, L. O. [2008] "The four-element Chua's circuit," Int. J. Bifurcation and Chaos **18**, 943–955.

[61] D. Sadaoui, A.Boukabou, N.Merabtine ET M.Benslama, "Predictive synchronization of chaotic satellites systems," Expert Systems with Applications, vol. 38, no 7, pp.9041-9045, 2011.

[62] BOUKABOU, Abdelkrim, CHEBBAH, Abdelhamid, et MANSOURI, Noura. Predictive control of continuous chaotic systems. *International Journal of Bifurcation and Chaos*, 2008, vol. 18, no 02, p. 587-592.

[63] A.Boukabou, "Méthodes de contrôle des systèmes chaotiques d'ordre élevé et leur application pour la synchronisation : Contribution à l'élaboration de nouvelles approches," Thèse Pour l'obtention du degré de Docteur es-Science en électronique, Université de Constantine, Juin 2006.

[64] EL GHAOUI, Laurent et NICULESCU, Silviu-lulian (ed.). *Advances in linear matrix inequality methods in control*. Society for Industrial and Applied Mathematics, 2000.

[65] Pecora, L. M. & Carroll, T. L. [1991] “Driving systems with chaotic signals,” Phys.Rev. A44 (4), 2374-2382.

[66] Kolumban, G., Kennedy, M. P. & Chua, L. O. [1998] “The role of synchronization in digital communication using chaos _ Part II: Chaotic modulation and chaotic synchronization,” IEEE Trans. Circuits Syst.45 (11), 1129-1140.

[67] Kennedy, M. P., Rovatti, R. & Setti, G. [2000] “Application of Chaotic Electronics to Telecommunications,” (CRC Press, FL).

[68] Xiao Fan Wang, Zhi Quan Wang, “A Robust Demodulation Approach to Communication using Chaotic Signals,” Bifurcation and Chaos, Vol. 13, No. 1 (2003), pp. 227-231.