Université ABBES LAGHROUR Khenchela
Faculté des Sciences et de la Technologie
Département de Génie Industriel
جامـــعة عبـــاس لـــغرور خـنـشـلة
كليـــة العلـــوم والتكنـــولـــوجيـا
قسم الهنـدسة الصنـاعية

N° Série :.....

Mémoire de fin d'étude

Pour l'obtention du diplôme de Master

Filière : Télécommunications

Spécialité : Systèmes des Télécommunications

THEME

COMMUNICATION SECURISEE PAR SYNCHRONISATION CHAOTIQUE

Réalisé par : - BOUBRIMA SABAH
- KHELIFI RADHIA

Soutenu le 15/ 09 /2020 Devant le jury composé de :

M me. Medjaldi Malika	*Président*	*Université Abbes Laghrour-Khenchela*
M me. Maamri Fouzia	*Encadreur*	*Université Abbes Laghrour-Khenchela*
Mr . Boumahrez Farouk	*Examinateur*	*Université Abbes Laghrour-Khenchela*

Promotion 2019/2020

الملخص

تعتبر أنظمة الفوضى أنظمة معلومة، غير خطية وتتأثر بصورة ملحوظة بالشروط الابتدائية. الاشارات الناتجة في هذه الانظمة تكون في أغلب الاحيان ذات مجال واسع من الموجات ،لهذا فهي تشبه الضوضاء الشبه عشوائية. منذ أن اكتشف العالمان "باكورا " و كارول " امكانية تزامن نظامين فوضويين ، بدأ توجه المجتمع العلمي نحو البحث عن إمكانية استغلال هذه الانظمة وخاصة في مجال تأمين الاتصالات و هذا الاهتمام راجع كون هذه الانظمة أكثر تطورا من أنظمة التأمين الكلاسيكية و أيضا سهولة انجازها مقارنة بالأنظمة السابقة تحت هذا المضمون يندرج عملنا المتواضع هذا .

إذا بعد إعطاء نظرة وجيزة عن أنظمة تأمين الاتصالات الكلاسيكية سوف نقدم دراسة نظرية حول أنظمة الفوضى وتزامنها وذلك باستعمال الحاسوب لنصل في الاخير إلى محاكات تطبيق نظرية الفوضى في تأمين الاتصالات .

الكلمات المفتاحية : النظام الفوضوي , تأمين الاتصال , التزامن الفوضوي , كريبتوغرافيا.

Abstract

We have presented in this paper the chaotic systems which are aperiodic nonlinear deterministic systems and very sensitive to the initial conditions. Since the discovery of Pecorra and Carroll, that two chaotic systems can synchronize significant interest has been given to the use of these systems to secure transmissions. This interests due to their unpredictability and could be used to create keys for cryptography, which exceeds of the conventional transmission systems.

Our work is a contribution that falls within this context. After having given a state of the art on conventional systems for securing communication, a computer-simulated on Matlab . Theoretical study on the chaotic phenomenon and its synchronization will be presented to finally lead to an application of securing communication chaos which is the goal of our work.

Keywords: Chaotic System, Secure communication, haotic Synchronization, Cryptography.

Résumé

Nous avons présenté dans ce mémoire les systèmes chaotiques qui sont des systèmes déterministes, non linéaires, non périodiques et très sensible aux conditions initials. Depuis la découverte de Pecorra et Carroll que deux systèmes chaotiques peuvent se synchroniser, un intérêt significatif a été accordé à l'usage de ces systèmes pour sécuriser les transmissions et pu être utilisé pour créer des clés pour la cryptographie. Cet intérêt est dû à leur imprévisibilité qui dépasse celle des systèmes de transmission conventionnels.

Notre travail est une contribution qui se situe dans le cadre de ce contexte. Ainsi dans ce mémoire après avoir donné un état de l'art sur les systèmes conventionnels de sécurisation de la communication, une étude théorique simulée par programmation Matlab, sur le phénomène chaotique et sa synchronisation sera présenté pour aboutir enfin à une application de la sécurisation de la communication par chaos qui est l'objectif de notre travail.

Mots clefs: Système Chaotique. Sécurisation de la communication. Synchronisation chaotique . Cryptographie.

DEDICACE

Je dédie ce modeste travail à mon

Très ***chère père Derradji***

Qui m'a toujours soutenu, et qu'a été

Toujours présent pour

Moi

A la plus chère au monde,

Ma mère Djamila *qui a*

Toujours m'encouragé durant

Mes études

A ***mes sœurs houda et Isra***

A ***mon frère Zakaria,***

A ma famille Boubrima et Ben Chabou

A ***toutes mes amies*** *et surtout* ***wafa*** *et* ***radhia***

A toute personne qui me connait

B.SABAH

DEDICACE

A la personne devant laquelle tous les mots de l'univers sont incapables d'exprimer mon amour et mon affection pour lui, à la source de ma persévérance et qu'il n'a rien épargné pour me voir heureuse, à celui qui a sacrifié jour et nuit pour ma réussite et mon bien être. ***A vous mon formidable père.***

C'est à vous que je dois cette réussite et je suis fière de vous l'offrir.

A la source de tendresse et l'exemple de dévouement qui n'a pas cessé de m'encourager et de prier pour moi.....

A toi chère maman.

A mes chers sœurs et frères avec j'ai grandi et partagé tant de moments et je tiens le plus que tout au monde qui me donnent de la joie à chaque instant et qui ont toujours été présents pour m'encourager et me pousser pour aller de l'avant. ***A vous mes chers sœurs et frères***

A tous les membres de la famille, petits et grands, et ***mes chers amis,*** *veillez trouver dans ce modeste travail l'expression de mon affection.*

KH . RADHIA

REMERCIMENT

*Nous remercions avant tout **Dieu Allah** tout puissant pour la volonté, la santé et la patience qu'il nous a donnée afin de réaliser ce modeste travail. Nous remercions également nos f**amilles** pour les sacrifices qu'elles ont faits pour que nous terminions nos études ainsi que nos **amis**. Nous exprimons notre plus grande reconnaissance et notre respect à notre encadreur **Mme .Maamri Fouzia**, Pour nous inspirer sur ce sujet et de nous guider tout au long de son développement, nous lui sommes très reconnaissants, pour ses conseils, sa disponibilité et surtout sa patience. On ne manquera pas de remercier tous **les membres du jury** pour notre avoir honorée par leur présence et pour avoir accepté d'évaluer ce travail de mémoire.*

Enfin, nous remercions tous les enseignants et toutes les personnes qui ont contribué directement ou indirectement à la réalisation de ce travail.

Sommaire

Table des matières

Liste des Tableaux

Liste Des Tableaux

Liste des Figures

Liste Des Figures

Liste des Symboles

Symboles mathématique

x_0, y_0, z_0	**C**onditions **I**nitiales **D**'un **S**ystème d'équations différentielles
x, y, z	Les variables d'états d'un système d'équations différentielles
a,b,c	Paramètres du système de Hénon ,lorenz ,Rössler
$\|.\|$	Valeur absolue
$\sum$	Somme algébrique
a	facteur d'échelle.
τ	Retard positif.
$\dot{X}$	Dérivée du vecteur d'état X
u	l'entrée de système
$v1, v2 i_l$	sont respectivement la tension
Lim	Limite
Ln	Logarithme népérien
L	La bobine
R	L'ensemble des nombres réels
$\mathbf{R^P}$	Espace vectorielles de dimension **P**
$\mathbf{R^n}$	Espace vectorielles de dimension **n**
R	résistance
r	paramètre de bifurcation

C1,C2	les bornes
G	la tension de la résistance additionnelle au niveau de la bobine L
H	désignant le champ de vecteur
k	Clé de cryptage

Liste des abréviations

A

AES	**A**dvanced **E**ncryptions **S**tandard

D

DES	**D**ata **E**ncryptions **S**tandard

R

RSA	**S**ystème **D**e **C**ryptage **A**symétrique (**R**ivest **S**hamir **A**dleman)

Communications Numériques

m(t)	message informatif
x(t)	signal chaotique
s(t)	signal crypté

Introduction générale

Introduction générale

Depuis longtemps, l'homme a cherché les différents moyens pour transmettre un message à son correspondant et pouvoir ainsi communiquer avec lui en toute sécurité, tout système de communication performant nécessite un système de sécurisation afin de le protéger vis à vis des attaques possibles, en 1990, Picora et Carroll présentent une démonstration théorique et expérimentale de la possibilité de synchroniser deux systèmes chaotiques. Ici, la synchronisation signifie que deux systèmes chaotiques ayant la même structure avec des conditions initiales différentes sont amenés à reproduire le même signal chaotique, 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 les propriétés du chaos, Un signal chaotique est un signal à large spectre d'une part, il permet de transmettre des signaux très variés, d'autre part, un signal chaotique est obtenu à partir d'un système déterministe.

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 **[31].**

La cryptographie chaotique, basée sur l'utilisation de systèmes chaotiques. L'utilisation du chaos pour sécuriser les données est un sujet d'étude depuis plusieurs années. Le chaos trouve ses fondements dans l'article de Lorenz, il est obtenu à partir de systèmes non linéaires. Il correspond à un comportement borné de ces systèmes ayant l'apparence d'un bruit pseudo aléatoire. Il peut donc être utilisé pour masquer ou mélanger les informations dans une transmission sécurisée.

Dans ce mémoire consiste à réaliser un système de transmission sécurisée à base du chaos. Il repose d'une part sur la synchronisation chaotique et d'autre part sur le masquage de l'information secrète. notre travail entre dans cette thématique. Il consiste à la conception d'un système de transmission sécurisée de données à base d'oscillateur chaotiques choisies dits de Chua.

Ce mémoire est organisé comme suit :

Le premier chapitre donne**,** après quelques généralités sur les systèmes dynamiques non linéaires des notions primordiales pour l'étude des systèmes chaotiques, pour lesquels nous permettront de mieux comprendre le comportement de systèmes chaotique.

Le second chapitre, sera consacré à la synchronisation des systèmes chaotiques et aux différentes méthodes de cryptage. Nous parlerons ainsi du principe de la synchronisation de ces systèmes et les différentes méthodes utilisées. Nous citerons aussi des éléments sur la cryptographie et les différentes méthodes de cryptages décryptage des systèmes chaotiques, ainsi que la cryptanalyse.

Le troisième chapitre, est dédié à la simulation sous MATLAB d'un système chaotique choisi, le circuit de Chua en l'occurrence ainsi que la méthode choisie pour sa synchronisation.

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

Chapitre I

Etude de comportement chaotique

I.1. Introduction

Le chaos était synonyme de désordre et de confusion. Il s'opposait à l'ordre et devait être évité. 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.

Le terme "chaos'' définit un état particulier d'un système dont le comportement ne se prédit pas. Il est dû au fait qu'ils sont très sensibles aux conditions initiales, entraînant des résultats totalement différents pour de tels système, rendant en générale toute prédiction impossible à long terme.

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.

I.2.Système dynamique

I.2.1.Définition des systèmes dynamiques

Un système dynamique est une structure qui évolue au cours du temps de façon à la fois :

– Causale, où son avenir ne dépend que de phénomènes du passé ou du présent

– Déterministe, c'est-à-dire qu'à partir d'une « condition initiale » donnée à l'instant« Présent» va correspondre à chaque instant ultérieur un et un seul état « futur» possible.

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

- Une évolution continue dans le temps, représentée par une équation différentielle ordinaire.
- Une évolution discrète dans le temps, l'étude théorique de ces modèles discrets est fondamentale, car elle permet de mettre en évidence des résultats importants, qui se généralisent souvent aux évolutions dynamiques continues. Elle est représentée par le modèle général des équations aux différences finies.

Les systèmes dynamiques sont classés en deux catégories :

- **En temps continu**

$$\begin{cases} X(t) = f(x(t), u(t), t) \\ Y(t) = h(x(t), u(t), t) \end{cases} \quad \textbf{(I.1)}$$

Où : $x \in \cup \subseteq \mathbb{R}^n$ est un vecteur de dimension n, $f : \mathbb{R}^n \rightarrow \mathbb{R}^n$ est une fonction non linéairedésignant le champ de vecteur $h : \mathbb{R}^n \rightarrow \mathbb{R}^n$ une fonction éventuellement qui désigne le vecteur de sortie de sortie et $u \in V \subseteq \mathbb{R}^p$ représentent l'entrée du système.

- **En temps discret**

Comme il a été déjà précisé le système dynamique est dans ce cas représenté par des équations aux différences finies, avec le modèle général suivant :

$$\begin{cases} x(k+1) = G(k, x(k), u(k)) \\ y(k) = h(k, x(k), u(k)) \end{cases} \quad \textbf{(I.2)}$$

Où : $\mathbb{R}^n \rightarrow \mathbb{R}^n \times Z^+ \rightarrow \mathbb{R}^n$ désigne la dynamique du système en temps discret **[1].**

I.2.2. Notions des systèmes dynamiques

Le chaos est défini généralement comme un comportement particulier d'un système dynamique déterministe non-linéaire. Du point de vue mathématique la notion générale de système dynamique est défini à partir d'un ensemble de variables qui forment le vecteur d'état. Ces variables ont la propriété de caractériser complètement l'état instantané du système dynamique. En associant en plus un système de coordonnées on obtient l'espace d'état qui est appelé également l'espace des phases. Conjointement avec l'espace d'état un système dynamique est défini aussi par une loi d'évolution, généralement désignée par dynamique, qui caractérise l'évolution de l'état du système en temps. La notion de déterminisme provient du fait que le système considéré est complètement caractérisé par son état initial et sa dynamique **[2][3].**

I.2.2.1 Systèmes dynamiques linéaires

Un système physique est dit linéaire si la relation entre les grandeurs d'entrée et de sortie peut être définie par des équations différentielles linéaires (à coefficients constants).Ces deniers vérifient alors les principes de proportionnalité des effets aux causes, et de superposition **[2].**

I.2.2.2 Systèmes dynamiques non linéaire

Un système non linéaire est un système qui n'est pas linéaire, c'est-à-dire (au sens physique) qui ne peut pas être décrit par des équations différentielles linéaires à coefficients constants. Cette définition, ou plutôt cette non-définition explique la complexité et la diversité des systèmes non linéaires et des méthodes qui ne sont pas une théorie générale pour ces systèmes, mais plusieurs méthodes adaptées à certaines classes de systèmes non linéaires **[3].**

I.3 Etudes de systèmes chaos

I.3.1.Historique de la théorie du chaos

Le tableau suivant retrace les moments forts de l'évolution de la théorie du chaos **[4].**

1890	Henri Poincaré gagne le premier prix du roi Oscar II, étant le plus proche à résoudre le problème de n-corps des orbites des corps célestes. Il a découvert que l'orbite de trois corps célestes agissant l'un sur l'autre peut engendrer un comportement instable et imprévisible. c'est ici que le chaos est né
1963	Edward Lorenz découvre qu'un simple ensemble de trois équations non linéaires peut donner lieu à des trajectoires complètement chaotiques. Ainsi, il a mis en évidence un des premiers exemples du chaos déterministe.
1975	Le terme « chaos » a été introduit pour la première fois par tien-Yien Li et James A.Yorke
1978	-Mitchell Feigenbaum introduit un nombre universel associé au chaos -Edward Ott, James A.Yorke et Celso
1990	-Edward Ott, James A.Yorke et CelsoGrebogi, introduisent la notion du contrôle de chaos. -Picora et Carroll : synchronisation des systèmes chaotiques

Tableau I.1 Historique du chaos

I.3.2 Quelques Définition sur le chaos

Selon la littérature que nous avons consultée, la notion du chaos répond aux définitions ci-Dessous **[5], [6], [7] :**

Définition 1

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

Définition 2

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

Définition 3

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

I.3.3.Classes des systèmes chaotiques

Il existe plusieurs systèmes chaotiques qui sont utilisés pour générer les signaux chaotiques. Dans ce paragraphe, nous présenterons deux classes : Les systèmes chaotiques continus et les systèmes chaotiques à temps discret.

I.3.3.1.Systèmes chaotiques continus

Un système chaotique à temps continu est décrit par un système d'équation différentielle de forme **[2]** :

$$X = f(t, x, u)\ ,\ Y = (t\ ,\ x\ ,\ u) \qquad \textbf{(I.3)}$$

Où : x le vecteur d'état de dimension n, f : R^n ; R^n est une fonction non linéaire désignant le champ de vecteur, h : $R^n \rightarrow R$ une fonction éventuellement non linéaire qui désigne le vecteur de sortie et $u \in V \subseteq R^p$ représente l'entrée du système. Si ce système ne dépend pas de l'entrée, on aura alors.

$$X = f(t\ ,x) \qquad \textbf{(I.4)}$$

Il existe plusieurs systèmes chaotiques continus. Parmi eux, on peut citer les systèmes de Lorenz, Rössler, Bogdanov, le circuit de Chua,…etc.

❖ **Système de Lorenz**

Le système de Lorenz est généré par le système d'équations suivant **[8]** :

$$\begin{cases} X = a\,(y - x) \\ Y = x\,(b - z) - y \\ Z = xy - cz \end{cases} \qquad \textbf{(I.5)}$$

Cet exemple a été publié en 1963 dans un journal météorologique.

Les variables x, y et z représentent les états du système à chaque instant. a, b, c sont les paramètres du systèmes. Le système présente un comportement chaotique pour a=12, b=26, c=9 et présente un attracteur étrange en forme d'ailes de papillon [**3].**

❖ **Système de Rössler**

Le système de Rössler est donné par les équations suivantes :

$$\begin{cases} X = -\,(y - z) \\ Y = x + ay \\ Z = b + z\,(x-c) \end{cases} \qquad \textbf{(I.6)}$$

x, y, et z sont les variables d'états du système .a, b, c sont les paramètres réels .Les paramètres et les conditions initiales de cette équation ont été choisis de la manière suivants :

a=b=0.1, c=12, (x_0, y_0,z_0) = (0.01, 0.01,0.01)

L'ensemble des trajectoires de ce système définissent un attracteur étrange aux propriétés fractales sur le long terme **[3].**

I.3.3.2 Systèmes Chaotiques discrets

Un système chaotique à temps discret est décrit par un système d'équations aux différences finies, dont le modèle général est le suivant :

$$X(k+1) = G(x(k), u(k)), \quad y(k) = h(x(k), u(k)) \qquad \textbf{(I.7)}$$

La dynamique du système en temps discret. Parmi les systèmes chaotiques discrets, nous pouvons citer les systèmes de Hénon, Hénon modifié, Lozi, la fonction logistique, etc.… **[3]**

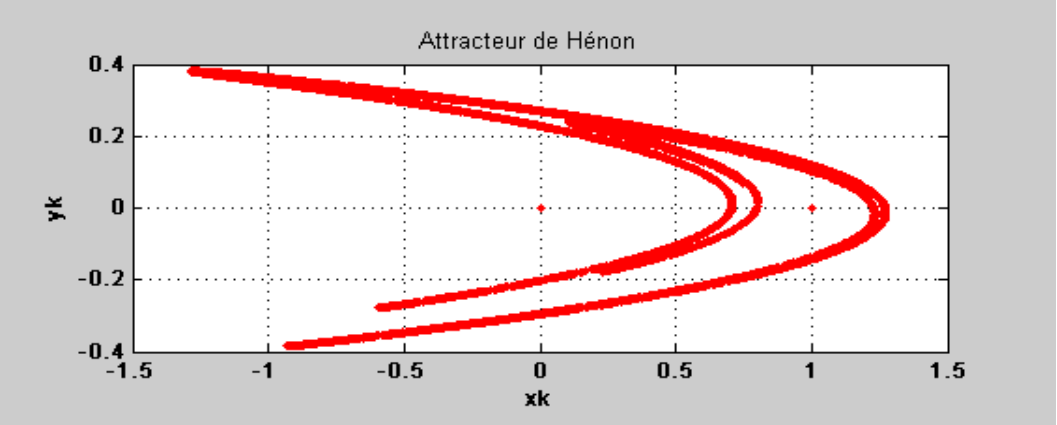
- **Système de Hénon**

Introduit par l'astronome Michel Hénon en 1976, il est présenté par des équations le suivant **[3]** :

$$\begin{cases} X(K+1) = y(K) + 1 - a * X(K) \\ Y(K+1) = b * X(K) \end{cases} \qquad \textbf{(I.8)}$$

Tel que (x(k) , y(k)) ϵ R2 Représente le vecteur d'état.

Pour les valeurs a=1.4 et b = 0.3 le système présente un comportement chaotique Les conditions initiales prises sont x0=0.1, y0=0. Pour d'autres valeurs de a et b, il peut être chaotique, intermittent ou converger vers une orbite périodique. Ainsi la **figure (I.1)** représente l'attracteur de Hénon.



FigureI.1 Attracteur chaotique de Hénon

❖ **Système Hénon-Heiles ou Hénon modifié**

Il est donné par les équations suivantes :

$$\begin{cases} X(K+1) = a - Y_2(K) - bZ(K) \\ Y(K+1) = X(K) \\ Z(K+1) = Y(K) \end{cases} \quad \textbf{(I.9)}$$

Pour avoir un comportement chaotique, les paramètres du système sont donnés comme suit : a =1.76 et b=0.1 et les conditions initiales du système : x0= 0.1, y0= 0.1, z0 =0.1**[3].**

I.3.4 Propriétés de systèmes chaotiques

Bien qu'il n'y ait pas de définition mathématique du chaos universellement acceptée, une définition couramment utilisée pour qu'un système dynamique soit classifié en tant que chaotique, il doit comporter les propriétés suivantes **[3] :**

- Aspect aléatoire
- Sensibilité aux conditions initiales
- Notion d'attracteur
- Fonction d'auto corrélation et spectre de puissance
- Bifurcation.

I.4. Caractéristiques essentielles du chaos [9]

I.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.

I.4.2.Le déterminisme

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

I.4.3. Sensibilité aux conditions initiales

Certains phénomènes dynamiques non linéaires sont si sensibles aux conditions initiales que, même s'ils sont régis par des lois rigoureuses et parfaitement déterministes, les prédictions

exactes sont impossibles. Comme la plupart des phénomènes sont non linéaires, on comprend alors l'importance de la découverte de Lorenz.

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.

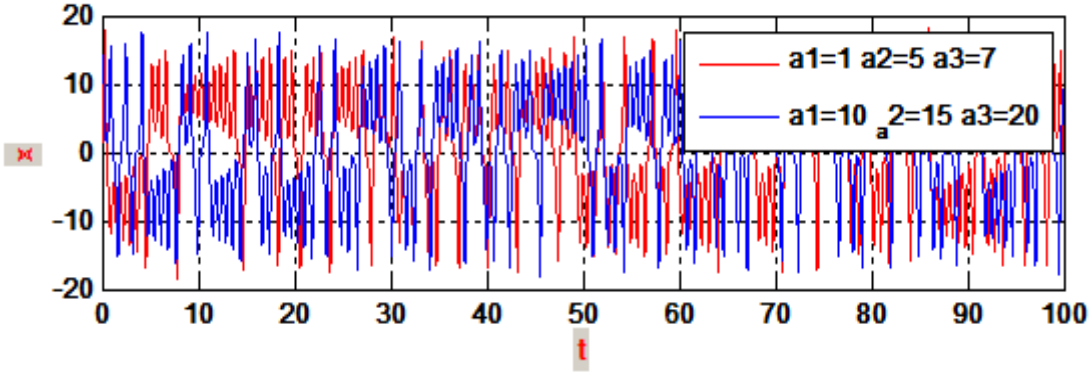


Figure. I.2. Sensibilité aux conditions initiales

La **figure (I.2)** représente deux signaux chaotiques, illustré par le système de lorenz .Cette figure montre la sensibilité aux conditions initiales : alpha1=10;alpha2=19;alpha3=12;(en Bleu) ; alpha1=4;alpha2=7;alpha3=9; (en rouge).

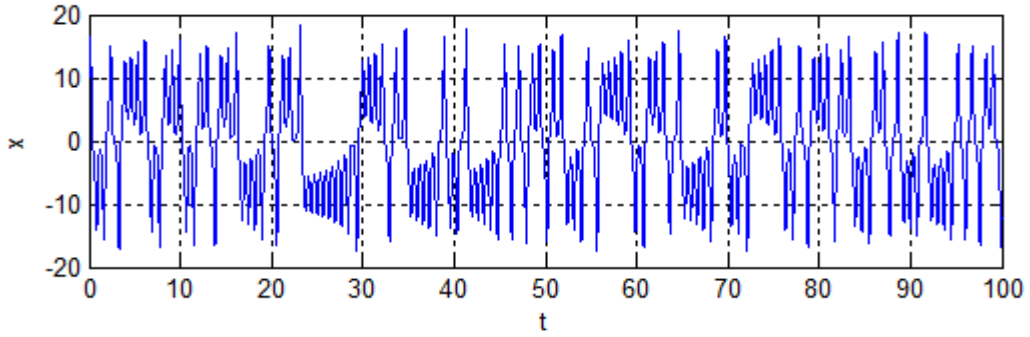
I.4.4. Espace des phases

Il est possible de suivre l'évolution de l'état d'un système physique dans le temps. Pour cela, on construit d'abord un modèle avec les lois physiques et les paramètres nécessaires et suffisants pour caractériser le système. Ce modèle est bien souvent constitué par des équations différentielles. On définira, à un instant donné, un point dans un "repère". Ce point caractérisera l'état du système dans l'espace à cet instant. Cet espace est appelé "l'espace des phases". Lorsque la variable d'évolution change de valeur (quand le temps s'écoule, par exemple), le point figurant l'état du système décrit en général une courbe dans cette espace. Il faut bien comprendre qu'il n'existe aucune relation entre un cas d'image à trois dimensions et notre espace de phases tridimensionnel. Il s'agit là d'un espace purement mathématique qui comporte autant de dimensions qu'il y a de paramètres dans le système dynamique étudié. On va pouvoir tracer 3 graphiques dans l'espace des phases à 2 dimensions **[1] :**

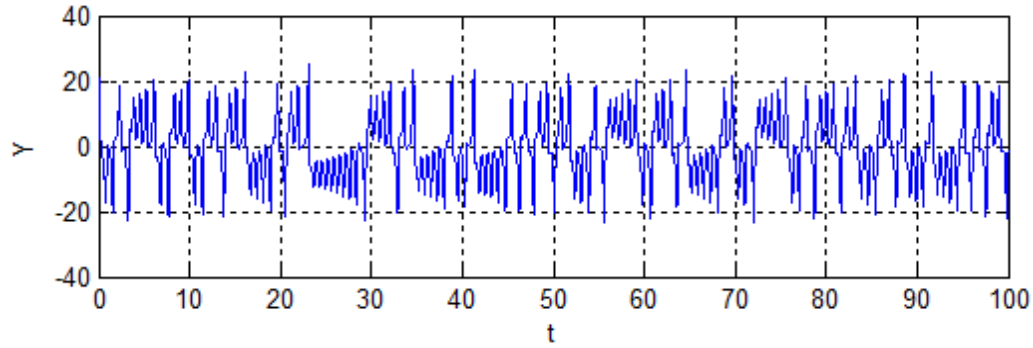
- en fonction de x et de y.
- en fonction de x et de t.
- en fonction de y et de t.

I.4.5. Le caractère pseudo aléatoire

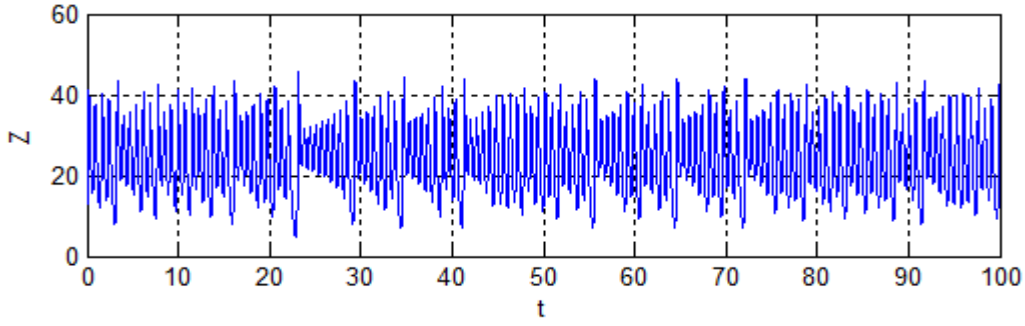
Tous les états d'un système chaotique présentent des aspects aléatoires La **figure (I.3)** illustre l'aspect aléatoire des états du système Lorenz.



a. Système de Lorenz : Evolution de X par rapport à t



b. Système de Lorenz : Evolution de Y par rapport à t



c. Système de Lorenz : Evolution de x par rapport à t

Figure I.3. Aspects aléatoires des états du système de Lorenz.

I.4.6.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 :

- Un volume nul.
- Une séparation exponentiellement rapide de trajectoire initialement proche.
- 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.

La **Figure (I.4)** suivante illustre L'évolution de l'attracteur de Lorenz en 2 et 3 dimensions.

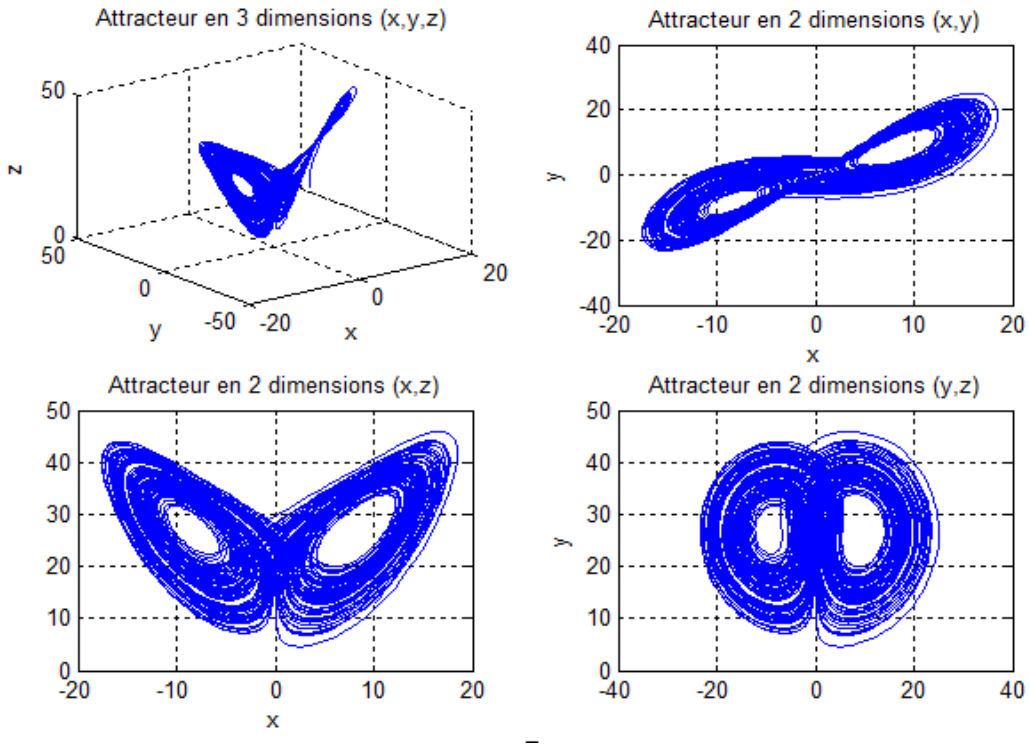


Figure. I.4. Evolution de l'attracteur de Lorenz en 2 et 3 dimensions.

❖ **Exemple de Rossler**

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

$$\begin{cases} X = -(y+z) \\ Y = x + ay + 0.01\, x\ln(z) \\ Z = c + z(x-b) \end{cases} \qquad \textbf{(I.10)}$$

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 (I.5)** suivante illustre attracteur étrange de Rössler.

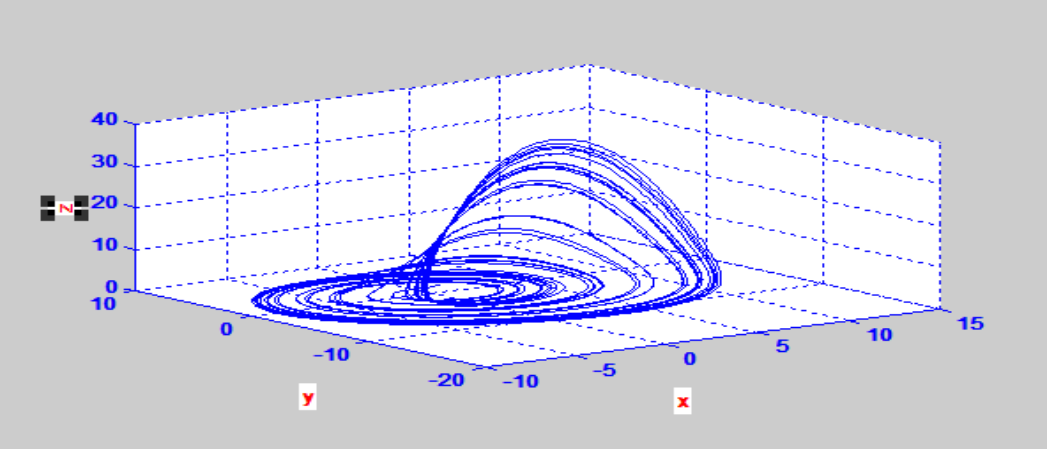


Figure .I.5. Attracteur de Rossler

I.4.7.Exposants de Lyapunov

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. 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. Le nombre d'exposants de Lyapunov est égal à la dimension de l'espace des phases et ils sont généralement indexés du plus grand au plus petit λ1, λ2, λ3, ...

L'apparition du chaos exige que les exposants de Lyapunov doivent remplir trois conditions :

- Au moins l'un d'eux est positif pour expliquer la divergence des trajectoires.
- Au moins l'un d'eux est négatif pour justifier le repliement des trajectoires.
- Aa somme de tous les exposants est négative pour expliquer qu'un système chaotique est dissipatif, c'est-à-dire qu'il perd de l'énergie. La valeur du plus grand exposant de Lyapunov quantifie le degré de chaos du système, mais le fait que les trois conditions énoncées ci- dessus soient réunies ne suffit pas à conclure qu'un système est chaotique **[11].**

Le tableau suivant résume les différentes configurations d'exposants de Lyapunov évoquées précédemment **[12]** :

Régime permanent	Attracteur	Spectre	Exposants de Lyapunov
point d'équilibre	Point	composante continue	$\lambda_n \leq \lambda_{n-1} \leq \ldots\ldots \leq \lambda_1 < 0$ 0
Périodique	courbe fermée	Fréquence fondamentale+ harmoniques entières	$\lambda_n \leq \lambda_{n-1} \leq \ldots\ldots \lambda_2 < \lambda_1 = 0$
quasi-périodique	Tore	composantes fréquentielles en rapport irrationnel	$\lambda_1 = \ldots = \lambda_i = 0$ $\lambda n \leq \lambda n-1 \leq . \leq \lambda_{i+1} < 0$
Chaotique	Fractale	spectre large	$\lambda_1 > 0$ $\lambda_n \leq \lambda_{n-1} \leq \ldots\ldots \leq \lambda_2 < 0$

Tableau 1.2 Attracteurs et exposants de Lyapunov

I.5.application du chaos [13]

Contrôle	Première application du chaos est le contrôle du comportement irrégulier dans les circuits et les systèmes.
Synchronisation	Communication sécurisée, cryptage, radio.
Traitement d'information	Codage, décodage et stockage d'information dans des systèmes chaotiques, tel que les éléments de mémoires et les circuits. Reconnaissance de forme.
Prédiction à court terme	Les maladies contagieuses, température, économie.

Tableau I.3 Application du chaos

I.6. Domaines d'application du comportement chaotique

En télécommunication : L'utilisation du chaos pour masquer ou mélanger les informations dans une transmission sécurisée. L'originalité repose sur la prise en compte des

propriétés de signaux chaotiques issus soit d'équations différentielles soit de récurrences discrètes non linéaires **[14].**

En informatique : Des procédés de compression d'images ont été mis au point à partir des fractales. Des images de synthèse, au cinéma ou dans le domaine des jeux vidéo, sont rendues de plus en plus réalistes, toujours grâce aux fractales. En effet, les objets fournis par la géométrie euclidienne sont assez peu aptes à représenter fidèlement le monde : les formes de la nature répondent bien plus aisément aux formes fractales **[14].**

En biologie : La théorie du chaos permet d'expliquer les variations des populations animales, les oscillations du cerveau. (C'est-à-dire un enregistrement graphique de l'activité électrique du cerveau au moyen d'électrodes placées sur le cuir chevelu, est un attracteur étrange). Ce pourrait donc être en vertu de la théorie du chaos que l'homme est libre et unique.

Les arythmies cardiaques typiques de nombreuses maladies du cœur se trouvent aussi expliquées par la théorie du chaos. Dans un cœur normal, des impulsions électriques se répandent de manière régulière dans les fibres musculaires, qui forcent le ventricule du cœur à se contracter et à pomper le sang. Une fois contractées, les fibres sont insensibles aux signaux électriques ; on parle de période réfractaire. Ce sont ainsi les variations de la durée de la période réfractaire d'une zone du ventricule à un autre qui seraient la cause de la contraction spasmodique à l'origine d'une crise cardiaque **[14].**

En économie : Les mouvements commerciaux et les marchés financiers, ainsi que les cycles économiques, peuvent être expliqués en partie par la théorie du chaos, où les fractales ont un lien très étroit avec le hasard, et permettent donc de modéliser des expériences aléatoires complexes, d'où l'utilisation en finance, pour modéliser les variations des cours de la Bourse **[14].**

En art : Dans le domaine de l'*art*, depuis les années 1980, la beauté des fractales est exploitée et appréciée, et on voit des expositions se multiplier avec pour thème ces images fascinantes. Les images fractales ont un intérêt esthétique certain, mais on peut **[14].**

I.7.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 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 saut moment du changement sont appelées valeurs de bifurcation **[26]**.

- **La fonction logistique**

La fonction logistique très connue dans la théorie des systèmes dynamiques sert de modèle universellement utilisé pour l'étude des systèmes discrets. Ce système à une dimension définie par la suite suivante **[26]** :

$$x_{k+1} = f(x_k) = rx_k(1\text{-}x_k) \qquad \textbf{(I. 11)}$$

La fonction logistique correspond à un comportement intéressant selon la valeur du paramètre r. on trouve un *cascade de doublements de période* pour décrire la transition entre un comportement périodique et un attracteur chaotique. Une plus grande variété de régimes permanents se présente, parmi lesquelles on trouve :

Pour r < 3, le système possède un point fixe attractif, qui devient instable lorsque r = 3.

Pour r > 3, le système évolue périodiquement de période 2n, (n entier qui tend vers l'infini lorsque r tend vers 4). On obtient donc une succession de bifurcations lorsque r augmente.

Cette courbe présente un diagramme de bifurcation parce que le comportement asymptotique subit, pour des valeurs du paramètre *r* bien déterminées, une bifurcation de l'ensemble des états limites.

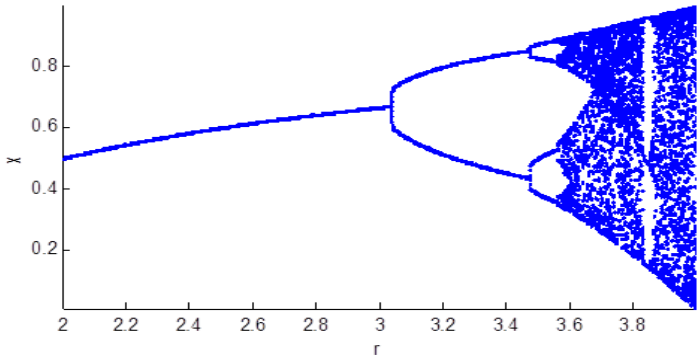


Figure. I.6. Diagramme de bifurcation pour la fonction logistique

I.7.1 Types de bifurcations

- **Bifurcation de type nœud-col (ou tangente, ou pli)**

Sur le diagramme des bifurcations on observe, dans ce cas, une courbe de points fixes continue tangente à la ligne droite verticale. Deux points d'équilibres existent (un stable et un instable) avant la bifurcation. Après la bifurcation, plus aucun équilibre n'existe **[10].**

- **Bifurcation transcrit que**

Sur le diagramme de bifurcations cela se traduit par deux branches différentes de points fixes qui se croisent en un point et par le changement de stabilité des deux branches au passage par le point d'intersection **[10].**

- **Bifurcation de doublement de période (ou flip)**

Un cycle d'ordre k qui subie cette bifurcation va changer de nature et crée un cycle d'ordre 2k. Un point fixe stable d'ordre1, devient instable en même temps que l'apparition d'un cycle d'ordre 2 stable **[10].**

I.8. Route vers le chaos

On ne sait pas à l'heure actuelle sous quelles conditions un système devient chaotique. Cependant il existe plusieurs types d'évolution possibles d'un système dynamique régulier vers le chaos. Supposons que la dynamique étudiée dépende d'un paramètre de Contrôle. Lorsqu'on varie ce paramètre, le système peut passer d'un état stationnaire à un état périodique, puis au-delà d'un certain seuil, suivre un scénario de transition et devenir chaotique **[15].** Nous allons en exposer brièvement trois types d'évolution possibles.

I.8.1 Le doublement de période

Ce scénario de transition vers le chaos est sans doute le plus connu. Par augmentation d'un paramètre, la fréquence double, puis est multipliée par 4, par 8, par 16..etc. Le doublement étant de plus en plus rapproché. On tend vers un point d'accumulation auquel on obtiendrait hypothétiquement une fréquence infinie, c'est à ce moment que le système devient chaotique **[15]**.

I.8.2 Intermittence

Ce deuxième scénario est caractérisé par un mouvement périodique stable entrecoupé par des mouvements chaotiques qui apparaissent de manière irrégulière. Le système conserve pendant ce mouvement un régime pratiquement quasi-périodique et il se stabilise brutalement pour donner lieu à un comportement chaotique **[15]**.

I.8.3 Quasi-périodique

Le scénario via la quasi-périodicité a été mis en évidence par les travaux théoriques de Ruelle et Takens (1971) illustré par exemple sur le modèle de Lorenz (1963). Ce scénario a été confirmé par de nombreuses expériences dont les plus célèbres se trouvent en thermo-hydrodynamique - convection de Rayleigh-Bénard dans une petite boîte - et en chimie - réaction de Bélousov - Zabotinsky - entre autres. Cette route vers le chaos résulte de la "concurrence" de différentes fréquences dans le système dynamique. Dans un système à comportement périodique à une seule fréquence, si nous changeons un paramètre alors il apparaît une deuxième fréquence. Si le rapport entre les deux fréquences est rationnelle comportement est périodique. Mais, si le rapport est irrationnel, le comportement est quasi périodique Dans ce cas, les trajectoires couvrent la superficie d'un tore. Alors, on change de nouveau le paramètre et il apparaît une troisième fréquence, et ainsi de suite jusqu'au chaos. n existe aussi des systèmes qui passent directement de deux fréquences au chaos **[11].**

I.9 .Conclusion

Dans ce chapitre, nous avons présenté les propriétés permettent de caractériser le dynamique chaotique, puis nous avons défini le chaos en général, en suite nous avons ainsi introduit quelques exemples des systèmes chaotique très connus, comme le système de Lorenz et Rossler, aussi nous avons présenté la Bifurcation et cité les déférents types de la Bifurcation, et les domaines d'application du comportement chaotique.

Dans le prochain chapitre nous allons présenter la synchronisation d'une communication sécurisée par chaos.

Chapitre II

Etude de la synchronisation d'une communication sécurisée par chaos

II.1. Introduction

Il y'a des années, l'usage de la cryptographie était monopolisé par des particuliers comme les militaires ou les gens du secret d'état. Mais l'explosion des techniques de communication personnelles et la miniaturisation des objets communicants, tels que les téléphones portables, l'usage d'Internet ainsi que l'utilisation des réseaux publics pour les transactions économiques ont engendré un très grand besoin de la sécurité, donc de l'utilisation de la cryptographie **[16].**

Dans les systèmes de communication, la synchronisation est une clé très importante pour une transmission réussie. La synchronisation classique employée dans les systèmes de télécommunication cherche à reproduire juste le signal périodique de la porteuse. Par contre, la synchronisation chaotique au niveau du récepteur cherche à dupliquer le signal chaotique envoyé de l'émetteur. Cela veut dire que deux signaux chaotiques seront dit synchronisés s'ils sont asymptotiquement identiques lorsque le temps «t» tend vers l'infini.

Dans ce chapitre, nous allons présenter le cryptage en général, puis nous parlons de la cryptographie par un signal chaotique et les méthodes de cryptage par chaos, à la fin nous expliquons la synchronisation chaotique.

II. 2.Terminologies

- **Texte en clair :** est le message à protéger.
- **Texte chiffré :** est le résultat du chiffrement du texte en clair.
- **Chiffrement :** est la méthode ou l'algorithme utilisé pour transformer un texte en clair en texte chiffré.
- **Déchiffrement :** est la méthode ou l'algorithme utilisé pour transformer un texte chiffré en texte en clair.
- **Clé :** est le secret partagé utilisé pour chiffrer le texte en clair en texte chiffré et pour déchiffrer le texte chiffré en texte en clair. On peut parfaitement concevoir un algorithme qui n'utilise pas de clé, dans ce cas c'est l'algorithme lui-même qui constitue la clé, et son principe ne doit donc en aucun cas être dévoilé.
- **Cryptographie :** cette branche regroupe l'ensemble des méthodes qui permettent de chiffrer et de déchiffrer un texte en clair afin de le rendre incompréhensible pour qui conque n'est pas en possession de la clé à utiliser pour le déchiffrer.

- **Cryptanalyse :** c'est l'art de révéler les textes en clair qui ont fait l'objet d'un chiffrement sans connaître la clé utilisée pour chiffrer le texte en clair.
- **Cryptologie :** il s'agit de la science qui étudie les communications secrètes. Elle est composée de deux domaines d'étude complémentaires, la cryptographie et la cryptanalyse.
- **Décrypter :** c'est l'action de retrouver le texte en clair correspondant à un texte chiffré sans posséder la clé qui a servi au chiffrement. Ce mot ne devrait donc être employé que dans le contexte de la cryptanalyse.
- **Crypter :** en relisant la définition du mot décrypter, on peut se rendre compte que le mot crypter n'a pas de sens et que son usage devrait être oublié. Le mot cryptage n'a pas plus de sens non plus.
- **Coder, décoder :** c'est une méthode ou un algorithme permettant de modifier la mise en forme d'un message sans introduire d'élément secret. Le Morse est donc un code puisqu'il transforme des lettres en trait et points sans notion de secret. L'ASCII est lui aussi un code puisqu'il permet de transformer une lettre en valeur binaire **[17].**

II.3. Technique de cryptage

Dans les différentes applications actuellement envisagées, les signaux chaotiques servent soit à véhiculer l'information soit à réaliser le cryptage de données. Nous intéressons au cryptage de données à transmettre et plus particulièrement dans un contexte de transmission sécurisée. En effet, un signal chaotique apparaît comme un « bruit » pseudo-aléatoire. Il peut donc être utilisé lors de cryptage de données, pour masquer les informations dans une transmission sécurisée : il suffit de le « mélanger » de manière appropriée au message à envoyer confidentiellement **[18].**

II.3.1.Les types de cryptage

Lorsqu'on communique sur un support non sécurisé comme Internet, vous devez faire attention à la confidentialité des informations que vous partagez avec d'autres. Cryptage symétrique et asymétrique sont les deux techniques utilisées pour préserver la confidentialité message **[19].**

II .3.1.1 Cryptage symétrique

Ce type de cryptage se base sur l'utilisation d'une clé pour crypter et décrypter les messages. La sécurité de cette solution repose sur le fait que la clé est connue uniquement par l'émetteur et le récepteur du message.

L'exemple historique de l'utilisation du cryptage symétrique est le fameux téléphone rouge qui reliait le Kremlin à la Maison Blanche. La clé privée était alors transmise dans une valise diplomatique. Pour une meilleure sécurité, elle était détruite et réinitialisée après chaque conversation.

Le cryptage symétrique fonctionne selon deux procédés différents :

- **le cryptage par flot :** le cryptage s'effectue en continu, bit par bit
- **le cryptage par bloc :** le cryptage s'effectue sur des blocs de bits **[20].**

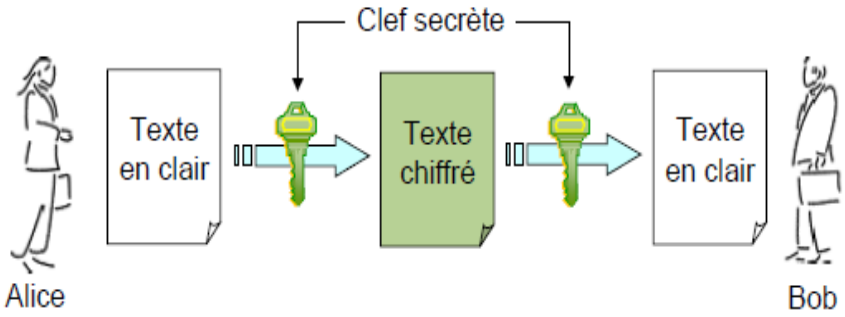


Figure II.1. Principe de cryptage symétrique.

II.3.1.2 Cryptage asymétrique

Ce cryptage, contrairement au symétrique, se base sur l'utilisation de deux clés, l'une publique (Pour crypter, elle est accessible publiquement) et l'autre privée (pour décrypter le message, elle est gardée secrète). Ce type de cryptage élimine la problématique de la transmission de la clé. Ce mode de cryptage est également nommé le cryptage à clé publique. Il est essentiel Que l'on ne puisse pas déduire la clé privée de la clé publique.

Pour bien comprendre le principe, on peut l'illustrer avec l'échange d'une lettre entre un émetteur et un destinataire**.**

- l'émetteur possède deux clés : privé et publique. Il envoie sa lettre contenant la clé publique au destinataire.
- le destinataire utilise la clé publique pour crypter son message ; il envoie tout à l'émetteur initial
- l'émetteur utilise sa clé privée pour décrypter le message **[20].**

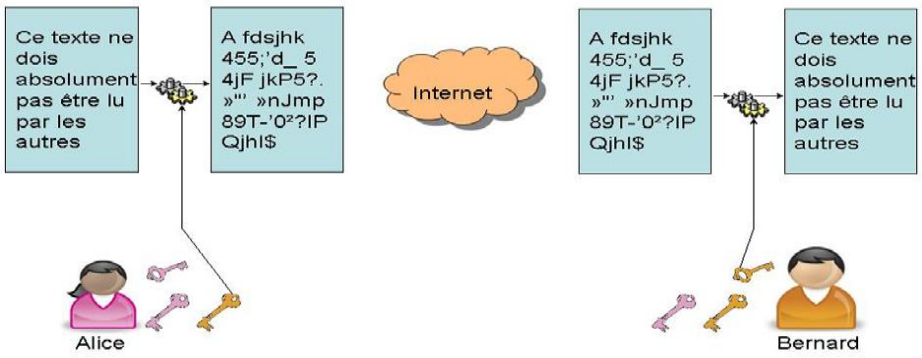


Figure II.2.Principe de cryptage Asymétrique.

II.3.2. Différences clés entre le chiffrement symétrique et asymétrique [19].

- Le **cryptage symétrique** utilise toujours une seule clé pour le cryptage et le décryptage du message. Cependant, dans le cryptage asymétrique, l'expéditeur utilise la clé publique pour le cryptage et la clé privée pour le déchiffrement.
- L'exécution d'algorithmes de **cryptage asymétrique** est plus lente par rapport à l'algorithme de **cryptage symétrique**. C'est parce que les algorithmes de **cryptage asymétrique** sont plus complexes et ont la charge de calcul élevée.
- Les algorithmes de **cryptage symétrique** les plus couramment utilisés sont DES, 3DES, AES et RC4. Tandis que, Diffie-Hellman et RSA représentent l'algorithme le plus commun utilisé pour le **cryptage asymétrique**.
- Le **cryptage asymétrique** est généralement utilisé pour l'échange de clés secrètes alors que le **cryptage symétrique** est utilisé pour échanger une masse de données.

II.4. Cryptographie

La cryptographie est une discipline qui traite et étudie les algorithmes et protocoles de transformations de données, servant à cacher des informations sensibles à des fins de sécurité et dans le but de les protéger des éventuelles attaques ou utilisations illégales lors d'une transmission à travers un canal publique.

II.4.1. Principe

Afin d'obtenir une donnée cryptée et protégée, on applique une des fonctions de chiffrement sur la donnée qu'on désignera par « message », une fois que le message a été crypté on obtient un message chiffré **[21].**

II.5. Objectifs de la cryptographie

La cryptographie garantit entre autre l'intégrité, le non reniement et l'authenticité des données en plus de leurs confidentialité **[22].**

II.5.1 Confidentialité

Des Données Concept permettant de garantir que seul le destinataire ou le détenant de la clé puisse découvrir le message en clair.

II.5.2 Authentification

Concept permettant de s'assurer que l'identité de l'interlocuteur et bien celle qu'il prétend.

II.5.3 Non-Reniement

Ensemble de moyens et techniques permettant de prouver la participation d'une entité dans un T'échange de données.

II.5.4 Intégrité des données

Ensemble de moyens et techniques permettant la non modification ou non altération des données échangées.

II.6. Principe du cryptage par 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 **[18].**

II.7.Méthodes de cryptage chaotique

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.

II.7.1 Cryptage par addition

Avec cette méthode, le message confidentiel est additionné à un signal chaotique (laSortie 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 **[23]**.

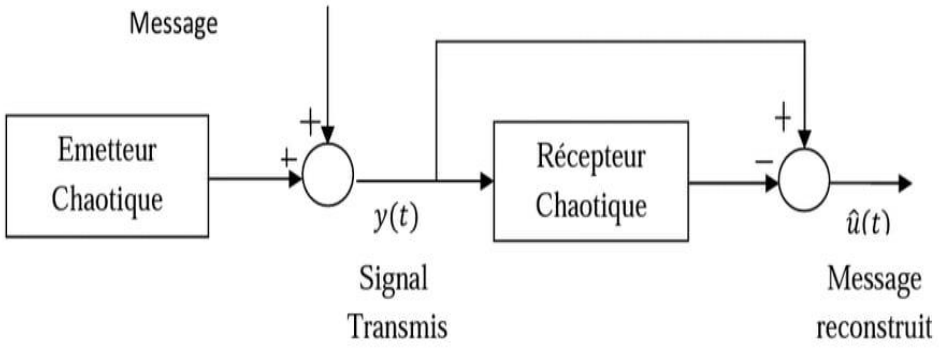


Figure II.3. Principe de cryptage par addition.

II.7.2 Cryptage par inclusion

Dans le cryptage par inclusion, le message source est inclus dans la structure du Système chaotique du côté de l'émetteur. Dans ce cas, 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 **[24].**

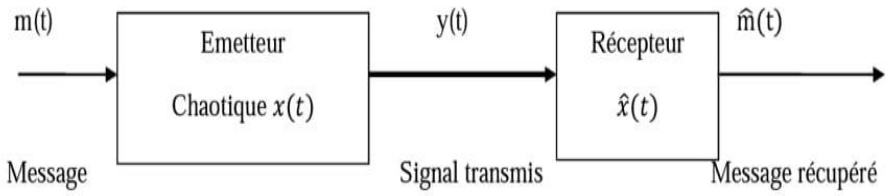


Figure II.4.Principe de cryptage par inclusion.

II.7.3 Cryptage par commutation

Cette méthode exige que le message à transmettre soit en binaire. Le diagramme de cette approche est illustré dans la **figure(II.5)** ou une opération de commutation est employée Selon la valeur du message binaire :

Si sa valeur est 0 alors le système chaotique 1 est choisi et le signal de sortie est transmis, si non la sortie du système chaotique 2 est transmise. Dans ce sens, le message binaire commute avec l'émetteur entre deux attracteurs étranges correspondants aux deux systèmes chaotiques.

Du coté récepteur, il y'a deux sous-systèmes chaotiques 3 et 4 qui correspondent Respectivement à 1 et 2. Supposons que le canal soit parfait, et que le signale transmis est 0, Alors le sous-système 3 se synchronisera avec le système chaotique 1, mais le sous-système 4 ne pourra pas être synchronisé, selon les erreurs de synchronisation (1,3) et (2, 4), le signal ne pourra pas être synchronisé**[24].**

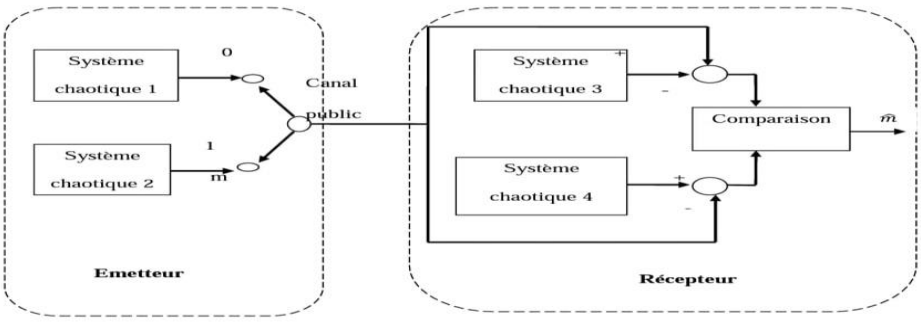


Figure II .5. Principe de cryptage par communication.

II.7.4 Cryptage par modulation

Cette technique utilise le message contenant l'information pour moduler un paramètre de l'émetteur chaotique. Un contrôleur adaptatif est chargé de maintenir la synchronisation au niveau du récepteur, tout en suivant les changements du paramètre modulé. Le schéma correspondant est présenté à la **Figure (II.6)** Au niveau de l'émetteur, le fait de moduler un (ou plusieurs) paramètre(s) impose à la trajectoire de changer continûment d'attracteur, et de ce fait, le signal transmis est plus complexe qu'un signal chaotique "normal". Cependant, la façon d'injecter le message et donc la fonction de modulation des paramètres ne doivent pas supprimer le caractère chaotique du signal envoyé au récepteur. Il est important de souligner que cette technique exploite pleinement les qualités des systèmes chaotiques. Elle n'a pas d'équivalent parmi les systèmes de communication "classique"**[25].**

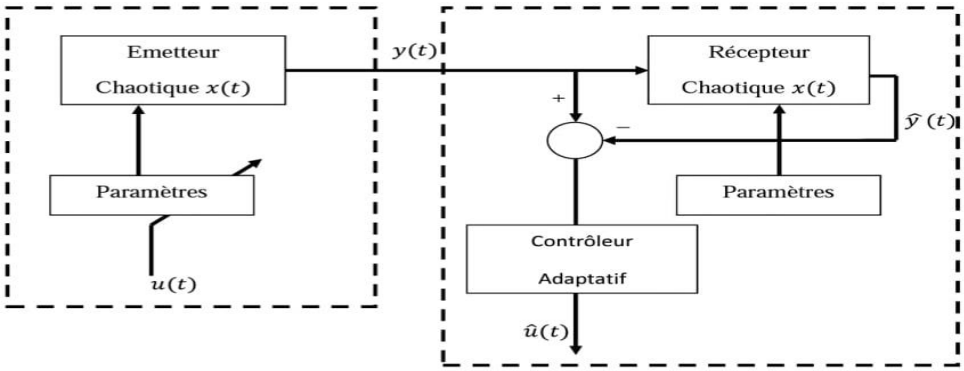


Figure II.6. Principe de cryptage par modulation

II.7.5 Cryptage mixte

Cette méthode combine les principes de la cryptographie standard et la synchronisation chaotique. Le message contenant l''information est crypté grâce à une clé C(t), générée par l'émetteur chaotique. Le message crypté est alors injecté dans la dynamique du système chaotique pour la rendre plus complexe. Ensuite, un signal fonction des variables d'état de l'émetteur est transmis au récepteur, qui établit une synchronisation avec l'émetteur. La clé est alors reconstruite par le récepteur, qui peut finalement décoder le message. Le principe général de la méthode est illustré dans la **Figure (II.7) [25].**

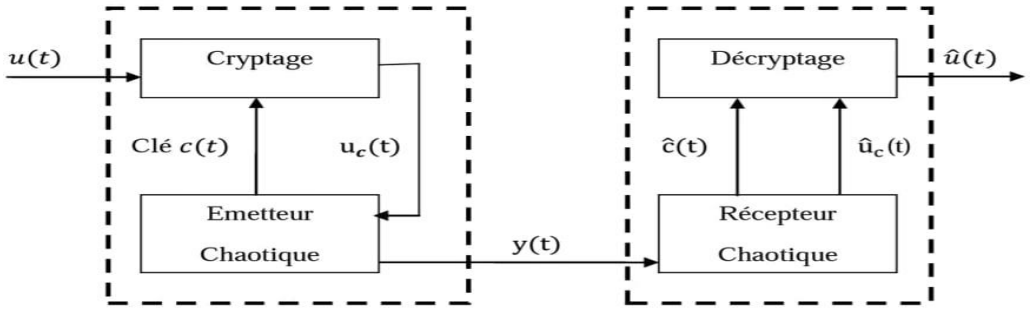


Figure II.7. Principe de cryptage par mixte.

II.7.6 Transmission par deux voix

Dans ce schéma de communication, l'émetteur envoie deux signaux au récepteur :

- Le premier signal y, est une fonction à valeurs réelles de l'état x du système chaotique Émetteur, dont l'unique but est de permettre la synchronisation du récepteur.

- Le second signal*y*2, envoyé sur un autre canal, est un signal chaotique contenant L'information, Cette méthode présente plusieurs avantages :

- Le signal *y* ne contient aucune information, par conséquent la synchronisation peut
- S'établir de façon optimale.
- Le second signal *y*2 contient l'information qui peut être soit cryptée par un fonction
- Non linéaire de l'état x, soit simplement masqué par un signal chaotique généré
- Par l'émetteur, qui sert de porteuse.
- Les deux étapes de synchronisation et de cryptage étant totalement indépendantes, le décryptage n'est pas nécessairement effectué, au niveau du récepteur, en même temps que la synchronisation **[26].**

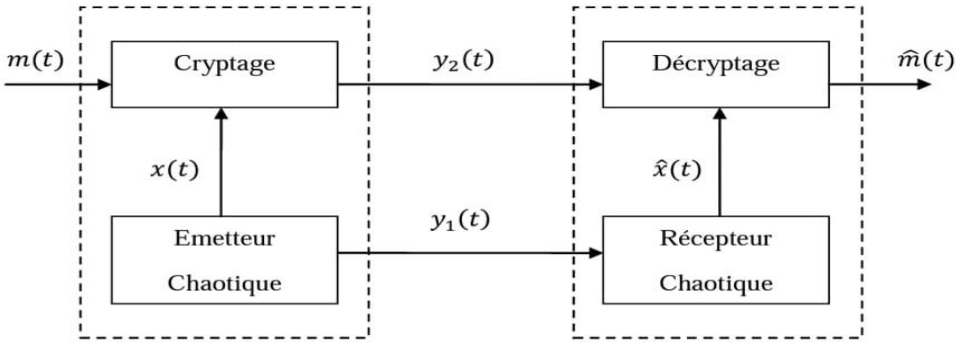


Figure II.8.Principe de cryptage par deux voix

II.8 Cryptanalyse

La cryptanalyse est la science qui consiste à tenter de déchiffrer un message ayant été Chiffré sans posséder la clé de chiffrement, c'est aussi l'étude de la sécurité d'un crypto Système en « cassant» les fonctions cryptographiques qui le composent.

La cryptographie et la cryptanalyse sont deux domaines d'étude évoluant constamment et en parallèle. En effet, de nouveaux crypto-systèmes, plus complexes les uns que les autres sont développés afin de remplacer ceux qui ont déjà été "cassés" par la cryptanalyse puis encore de nouvelles techniques de cryptanalyse sont inventées pour tester ces nouveaux Crypto systèmes. Le problème de la cryptographie est de concevoir des systèmes sûrs et de faire en sorte que la durée nécessaire pour "casser" un crypto- système soit supérieure à sa durée de validité. La tendance actuelle est de chercher à prouver la sécurité d'un système surla base d'hypothèses sur la puissance de calcul requise ou sur la quantité de texte clair. La réussite pratique d'une attaque dépend d'un certain nombre d'éléments, comme les Connaissances nécessaires a priori, l'effort demandé (complexité, temps de calcul), la quantité et la qualité des informations pouvant être déduites de l'attaque (déchiffrement de la clé secrète, algorithme de chiffrement découvert sans connaître la clé secrète, information sur le texte clair, etc.). La complexité de l'attaque se caractérise par le temps en nombre d'opérations effectuées (addition, ou exclusif, etc.), par la mémoire nécessaire et par la quantité de données (texte clair et texte chiffré) requises.

A travers les années, de nombreuses attaques possibles contre les crypto- systèmes ont été identifiées, de telle sorte qu'il est difficile d'en établir une liste exhaustive. En revanche, on distingue deux classes d'attaques : les attaques actives et les attaques passives.

Dans l'attaque active, l'adversaire agit sur l'information. Il altère l'intégrité des données, l'authentification et la confidentialité. Il peut chercher à altérer la transmission du message sur le canal, par exemple, en modifiant le message (suppression, ajout, modification des séquences du message), en retardant (ou empêchant) sa transmission, en répétant son envoi, etc.…

Dans les attaques passives, l'adversaire observe l'information qui transite sur le canal sans les modifier. Il cherche à récupérer des informations sur le crypto-système sans l'altérer, telles que le message, la clé secrète, etc. Dans ce cas, l'adversaire touche à la confidentialité des données **[27].**

II.9.Communications Sécurisées par chaos

Dans les différentes applications actuellement envisagées, les signaux chaotiques servent soit à véhiculer l'information soit à réaliser le cryptage de données.

Nous intéressons au cryptage de données à transmettre et plus particulièrement dans un contexte de transmission sécurisée.

Comme il a été déjà mentionné, le chaos déterministe peut générer des comportements dynamiques d'apparences aléatoires. Il serait donc intéressant d'utiliser ces derniers comme porteuses d'informations en télécommunication.

Le diagramme principal de la communication sécurisée par le chaos est montré sur la **Figure II.9**.Le principe est de masquer une information par des signaux chaotiques et de l'envoyer vers le récepteur sur un canal public. L'information cryptée est récupérée au niveau du récepteur.

La clé du système de transmission est l'ensemble des paramètres des deux générateurs chaotiques à l'émission et à la réception qui doivent être synchronisés.

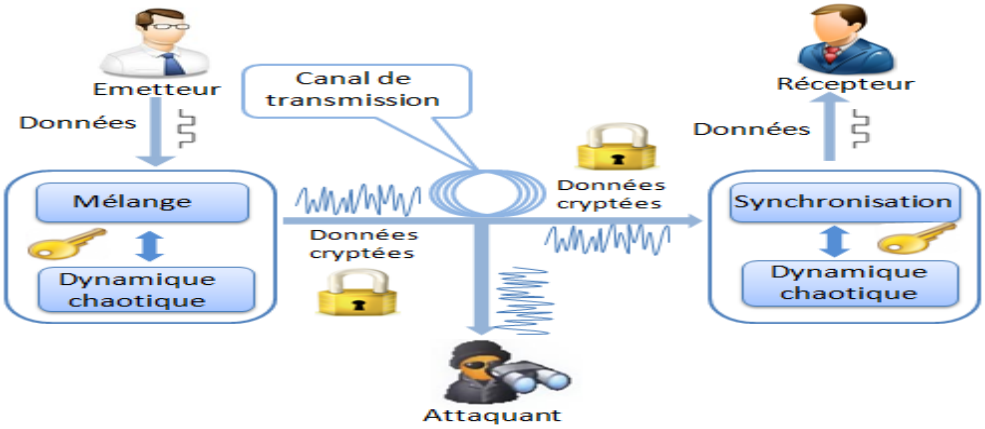


Figure II.9. Principe de Chiffrement par Chaos.

Le chiffrement d'un message par le chaos s'effectue donc en superposant à l'information initiale un signal chaotique. On envoie par la suite le message noyé dans le chaos à un récepteur qui lui 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 **[28][29].**

II.10 Comparaison entre chaos et cryptographie [20]

Théorie du chaos	Cryptographie
Système chaotique	Transformation non linéaire
Transformation non linéaire	Transformation non linéaire
Nombre infini d'états	Nombre fini d'états
Nombre infini d'itérations	Nombre fini d'itérations
État initial	Texte brut
État final	Texte chiffré
Condition initiale (s) et/ou paramètre (s)	Clé (s)
Indépendance asymptotique des états initiaux et finaux	Confusion
Sensibilité aux conditions initiales (s) et paramètre (s)	Diffusion

Tableau II.2 Synchronisation des systèmes chaotique

II.11.Synchronisation des systèmes chaotique

Dans les systèmes de transmission, la synchronisation est une clé très importante pour une transmission réussie. La synchronisation classique employée dans les systèmes de transmission cherche à reproduire juste le signal périodique de la porteuse. Par contre, la synchronisation chaotique au niveau du récepteur cherche à dupliquer le signal chaotique généré par l'émetteur selon les travaux de Pecora et Carollen Les deux chercheurs ont défini la synchronisation chaotique ou synchronisation identique qui 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, dans chacun des sous-systèmes. 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 maitre) sert à synchroniser le premier des sous-systèmes dupliqués mis en cascade qui lui-même permet de synchroniser le second sous-système dupliqué. La synchronisation des systèmes chaotiques est devenue un thème de recherche très actif depuis 1990. Plusieurs techniques de synchronisation des systèmes chaotiques ont été proposées et exploitées dans les transmissions sécurisées. Leur fonctionnement consiste à appliquer un couplage aux systèmes chaotiques (émetteur /récepteur), par la transmission de quelques composantes du vecteur d'états du système maître, en vue d'unifier leurs comportements. Ainsi selon la nature de liens on distingue : le couplage mutuel ou le couplage unidirectionnel (maître-esclave). Ce dernier est le plus convenable aux transmissions sécurisées, car il est plus simple à mettre en œuvre, comme il peut être traité comme un problème de conception d'observateur non linéaire, qui supporte plusieurs configurations adaptées aux différentes classes de systèmes chaotiques **[30].**

II.12 Les classes de synchronisation

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 le synchroniser de façon que les deux signaux chaotiques issus des deux exemplaires soient identiques. Il existe deux classes de synchronisation suivant la manière avec laquelle les deux systèmes chaotiques sont couplés : unidirectionnelle et bidirectionnelle **[31].**

II.12.1. Synchronisation unidirectionnelle

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

La **figure(II.10)** représente le couplage unidirectionnel **[31].**

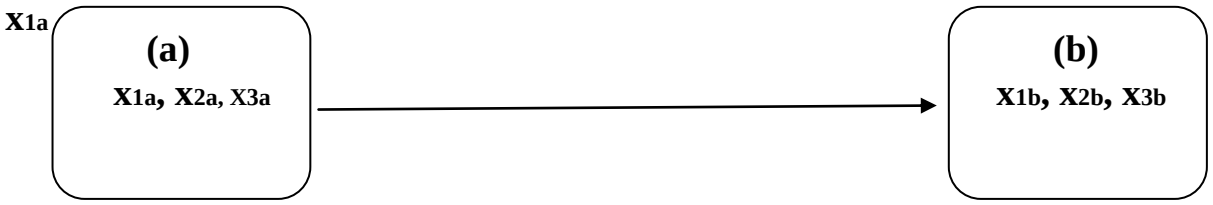


Figure II .10. Couplage unidirectionnel

II.12.2. Synchronisation bidirectionnelle

Dans le cas d'une synchronisation bidirectionnelle, le couplage entre deux systèmes identiques a et b **(figure II.11)** 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].**

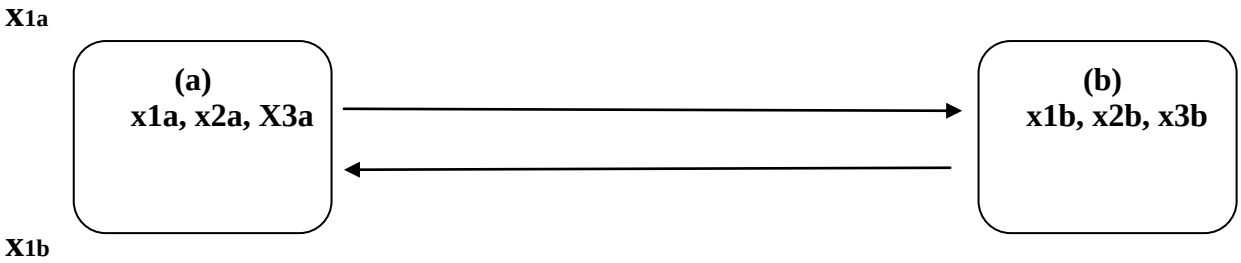


Figure II.11. Couplage bidirectionnel

II.13. Les méthodes de synchronisation

Plusieurs méthodes de synchronisation ont été proposées dans la littérature. Dans ce qui suit nous citerons quelques approches en expliquant leurs principes.

II.13.1Synchronisation par boucle fermé

La synchronisation des systèmes chaotiques par les méthodes en boucle ouverte implique une sensibilité aux variations paramétriques. Pour y remédier, de nouvelles techniques basées sur un bouclage par contre-réaction ont été proposées. L'idée est d'appliquer une correction au système me en fonction de l'erreur entre le signal transmis par le premier système et le signal régénéré par l'autre. Cette erreur est ainsi injectée en contre-réaction d'où l'appellation de l'approche. Cette technique permet également la synchronisation entre des paires différentes de systèmes chaotiques. La **figure (II.12)** indique un schéma simplifié de la synchronisation par boucle fermée **[32].**

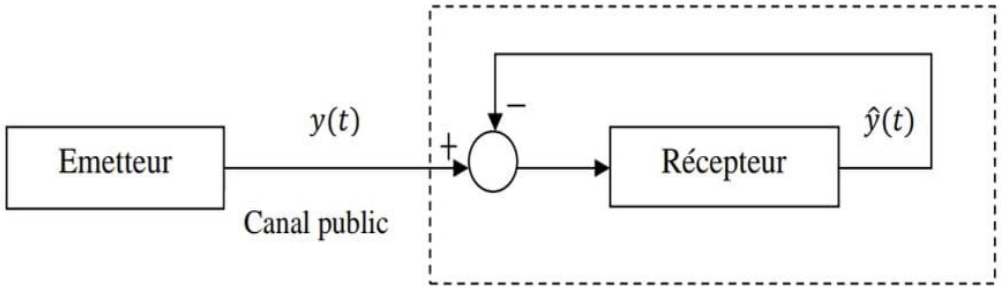


Figure II.12. Synchronisation par boucle fermée

II.13.2. Synchronisation généralisée

En générale**,** c'est quand il existe une différence entre les systèmes couplés c'est-à-dire quand on trouve un obstacle pour une réalisation pratique d'un sous-système esclave purement identique à un autre sous-système issu d'une décomposition d'un système maître.

La méthode généralisée est proposée afin de s'affranchir de cet obstacle, qui est une généralisation du concept de la synchronisation identique.

En conséquence les possibilités d'appliquer la synchronisation généralisée, peuvent être plus larges que la synchronisation identique, on dit que deux systèmes se synchronisent, au sens généralisé s'il existe une matrice M telle que :

$$\text{Lim } t\to\infty \ \| \hat{x} \ (t) - Mx \ (t) \ \| = 0 \qquad \textbf{(II.1)}$$

Avec :

$\hat{x}(t)$ **:** l'état du système émetteur

$x\ (t)$**:** l'état du système récepteur

Séparément des conditions initiales, si M est inversible, alors $M^{-1}(\hat{x})$ fournit une estimation de l'état de x du système émetteur. Dans le cas contraire, il serait impossible de fournir une estimation de l'état x du système récepteur, ceci présente alors un inconvénient majeur pour les techniques de communications utilisant l'état pour décrypter le message transmis **[33].**

II.13.3. Synchronisation impulsive

Lorsque deux systèmes communiquent usuellement, le premier système dynamique (émetteur) transmis un état afin de pouvoir réaliser une synchronisation avec le second (récepteur). La synchronisation impulsive à été proposée, **Figure (II.13),** Afin de réduire la redondance du signal transmis (rapport signal/bruit). Le contrôle impulsif d'un système signifie qu'à des moments choisis, les états du système subit des changements soudains.

On considère le signal maitre défini par x = f(x(t)), et on définit un signal impulsif qui consiste en une suite d'instants discrets auxquelles un signal y(t) est envoyé par le système maitre au système esclave, un changement dont les variables d'état subissent un saut et un changement d'état **[33].**

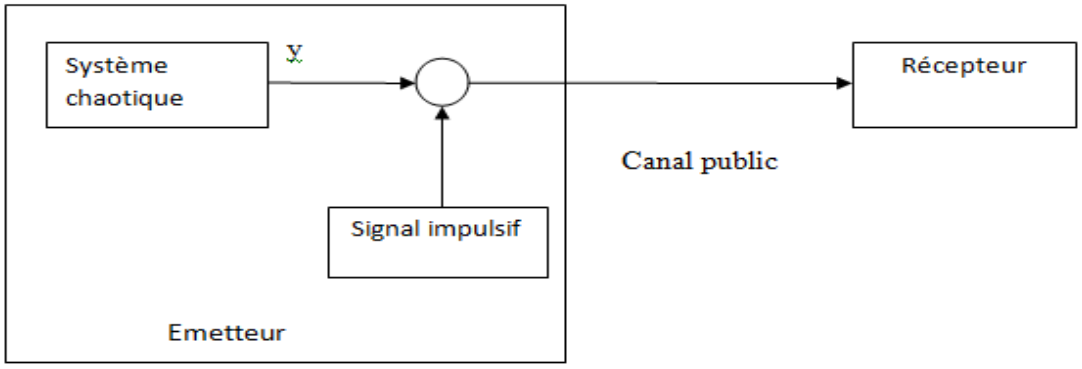


Figure II.13. Principe de la synchronisation impulsive

II.13.4. 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 :

$$Lim_{t\to\infty} \ \|x'(t) - \alpha x(t-\tau)\| = 0 \qquad \text{(II.2)}$$

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 **[32].**

II.13.5.Synchronisation retardée

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

$$Lim_{t\to\infty} \| x\,(t) - (t-\tau)\| = 0 \qquad \textbf{(II. 3)}$$

Où x(t) est l'état du système maître, $\hat{x}$(t) est l'état du système récepteur et τ est un retard positif. Cette approche est utilisée pour les systèmes linéaires **[33].**

II.13.6. 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 :

$$Lim_{t\to\infty} \quad \| x(t) - \hat{x}\,(t) \| = 0 \qquad \textbf{(II.4)}$$

Où x(t) est l'état du système et$\hat{x}(t)$ est l'état estimé .Ce principe est illustré par la **figure (II.14)** suivante :

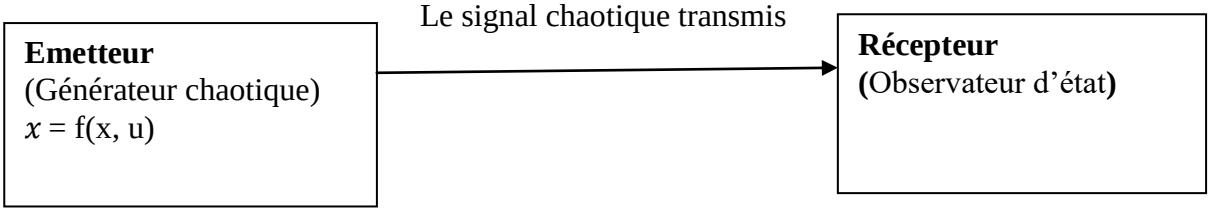


Figure II.14. Principe de la synchronisation à base d'observateur

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 **[33].**

II.14. Propriétés des systèmes chaotiques appliqués au cryptage d'une transmission de données.

II.14.1 Spectre à large bande

Les systèmes chaotiques ont spécifiquement un spectre à large bande. Cette propriété est bénéfique pour les applications qui nécessitent une importante robustesse face aux interférences et une faible probabilité de détection. Ces problèmes ont été pris en compte par les premiers systèmes de transmission en utilisant des spectres larges et des modulations par saut de fréquences. Cependant malgré le recours à ces moyens, la synchronisation entre l'émetteur et le récepteur reste une tâche qui n'est pas toujours triviale. En effet les schémas de transmission qui utilisent un saut de fréquence requièrent une nouvelle synchronisation à chaque changement de fréquence de la porteuse. Donc l'utilisation des systèmes chaotiques permet la transmission des signaux à large bandes, ainsi la synchronisation entre l'émetteur et le récepteur est plus simple [31].

II.14.2 Signal non périodique

La périodicité, dans la communication sécurisée engendre des pics spectraux indésirables. Par contre, un signal chaotique est non périodique et son évolution ne peut être prédite sur un long intervalle de temps. Par conséquent, il y a absence des pics spectraux. De plus il est plus difficile de développer un modèle de prévisions pour les dynamiques non périodiques [31].

II.15. Conclusion

L'objectif principal de ce chapitre était de présenter, la cryptologie en générale et la cryptographie par chaos avec son principe et son objectif.

La synchronisation des systèmes chaotiques nous donne accès à la réalisation des différents systèmes permettant d'effectuer une transmission sécurisée d'information. Cette dernière est assurée par diverses méthodes de cryptages exploitant le chaos, à savoir le cryptage par addition, par inclusion, par commutation, par modulation, par mixte et nous avons fini par les techniques de transmission à deux voies. En suite nous avons indiqué les classes de synchronisation et ses méthodes .En fin nous avons présenté les propriétés des systèmes chaotiques appliqués au cryptage d'une transmission de données.

Chapitre III

Cryptage par chaos et synchronisation

III.1.Introduction

Le chaos est l'une des dynamiques les plus complexes que peut présenter les systèmes non linéaires. De ce fait, les systèmes chaotiques ont été utilisés pour sécuriser les communications. Dans les systèmes de communication, la synchronisation est une étape fondamentale et importante pour la transmission et le chiffrement chaotique. La synchronisation classique dans les systèmes de télécommunication cherche à reproduire la porteuse. Dans la synchronisation dans la transmission par un signal chaotique au niveau du récepteur cherche à dupliquer le signal chaotique transmis de l'émetteur.

L'utilisation d'oscillateurs est requise pour générer un signal chaotique. Plusieurs types d'oscillateurs existent. Ces derniers diffèrent par leurs structures, la technologie impliquée ainsi que les composants utilisés dans leur création. Les oscillateurs les plus répandus sont le circuit de Chua. Pour étudier le comportement du système, on a recourt aux méthodes d'intégration numérique. Les simulations numériques sont effectuées en utilisant l'algorithme d'intégration numérique de Runge-Kutta d'ordre *4* sous simulateur Matlab.

III.2. Synchronisation et application à la transmission sécurisée

Pendant les deux dernières décennies, la configuration maitre-esclave a été appliquée avec succès, dans les systèmes de communication sécurisée basés sur la synchronisation des systèmes chaotiques ou un émetteur chaotique (le système maitre)génère un signal d'informatique chiffré transmis dans le canal de communication vers un système récepteur (le système esclave)qui a pour objectif de synchroniser avec l'émetteur et de restaurer le signal d'informatique .

Plusieurs méthodes ont été proposées pour la synchronisation et la communication sécurisée. Le masquage chaotique est la technique la plus élémentaire pour sécuriser l'information. La **Figure(III.1)** illustre le principe de base de cette technique **[33].**

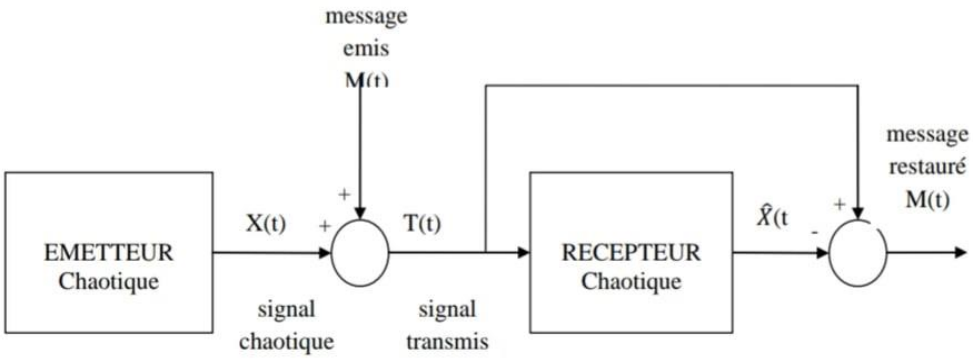


Figure III.1. Schéma présentatif de la technique de masquage chaotique

Le système de transmission proposé est constitué de deux bloques :

III.2.1. Bloc émetteur

Ce bloc contient un oscillateur chaotique, un signal en temps discret et un module de cryptage en utilisant la méthode de cryptage par addition pour masquer le signal choisi.

III.2.2 .Bloc récepteur

Ce bloc contient un observateur pour estimer les états du système et un bloc de décryptage qui consiste en un soustracteur.

III.3.Circuit de Chua

III.3.1. Oscillateur chaotique de Chua

Le circuit de Chua est le circuit électronique le plus simple montrant le chaos et beaucoup de phénomènes bien connus de bifurcation, comme il a été vérifié par de nombreuses expériences de laboratoire, de simulation par ordinateur et d'analyse mathématique.

Ainsi ce circuit a été proposé par Leon Chua en 1983 en réponse à deux questions non résolues par beaucoup de chercheurs au sujet du système chaotique de Lorenz. La première est la conception d'un système de laboratoire qui peut être normalement modélisé par les équations de Lorenz, afin de démontrer que le chaos est un phénomène physique robuste, et pas simplement une simulation réalisée à l'aide d'ordinateurs. La deuxième est le besoin de montrer que l'attracteur de Lorenz simulé par ordinateur, est en effet chaotique dans un sens mathématique rigoureux. L'existence des attracteurs chaotiques du circuit de Chua avait été confirmée numériquement par Matsumoto et expérimentalement observée par Zhong et Ayrom **[34].**

III.3.2.Présentation du circuit de Chua

Un circuit électronique doit respecter certaines conditions pour montrer un comportement chaotique, appelés critères chaotiques. Il doit contenir :

- Au moins 1 élément non linéaire
- Au moins une résistance active
- Au moins 3 éléments capables de stocker de l'énergie (capacité, inductance) On obtient alors un système d'équations différentielles d'ordre 3.

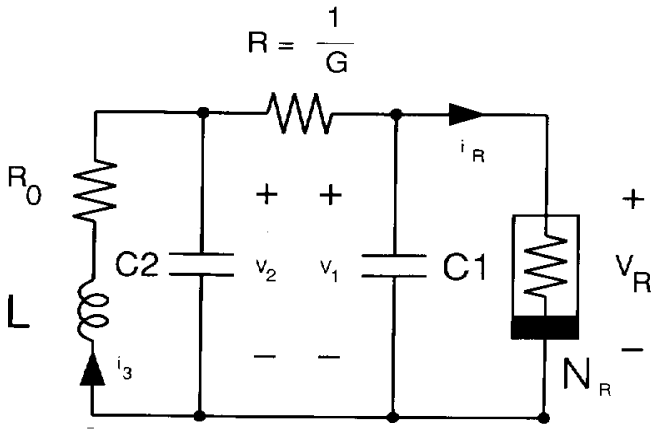


Figure III.2. Le circuit électrique de l'oscillateur de Chua.

Où :

V_1: la tension aux bornes de C1 et la résistance non linéaire.

V_2: la tension au bornes de C_2 et l'inductance L (R_0 la résistance interne de L)

I_3: le courant traversant L.

N_R: la résistance non linéaire.

La caractéristique de la résistance non linéaire N_R est donnée par la figure suivante :

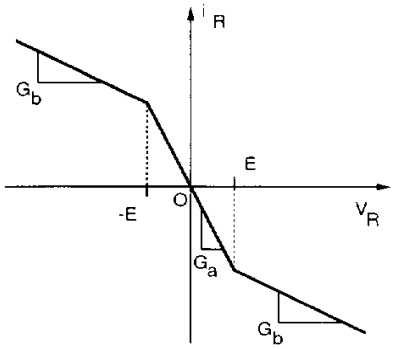


Figure III.3. La caractéristique de la résistance non linéaire N_R.

Le circuit de Chua est décrit par le système d'équations suivant :

$$\begin{aligned}\frac{dV_1}{dt} &= \frac{G}{C_1}(V_2 - V_1) - \frac{1}{C_1}g(V_1)\\ \frac{dV_2}{dt} &= \frac{G}{C_2}(V_1 - V_2) + \frac{1}{C_2}i_3\\ \frac{di_3}{dt} &= -\frac{1}{L}(V_2 - R_0 i_3)\end{aligned} \qquad \textbf{(III.1)}$$

Où: $G = 1/R$ est la conductance de la la résistance R et R_o est la résistance interne de l'inductance L.

Les variables d'état de ce circuit sont données par :

$$\begin{cases} x_1 = \alpha\big(x_2 - x_1 - g(x_1)\big)\\ x_2 = x_1 - x_2 + x_3\\ x_3 = -\beta x_2 - \gamma x_3 \end{cases} \qquad \textbf{(III.2)}$$

Avec:

$\alpha = C_2/C_1, \quad \beta = C_2R^2/L, \quad \gamma = r/R$

L'élément non linéaire est caractérisé par la fonction $g(x_1)$

$$g(x_1) = G_b x_1 + 0{,}5(G_a - G_b)\big(|x_1 + E| - |x_1 - E|\big) \qquad \textbf{(III.3)}$$

Où: x_1, x_2 et x_3 sont les variables d'états.

α, β, γ, G_a, G_b les paramètres du système.

Le circuit complet de l'oscillateur de Chua est représenté sur la **figure (III.4)**. La résistance de Chua est réalisée en utilisant des amplificateurs opérationnels.

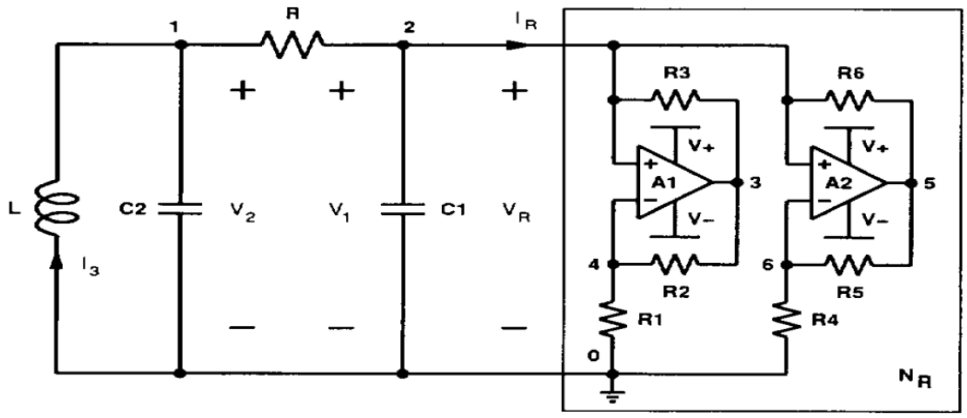


Figure.III.4. Circuit complet de l'oscillateur de Chua.

❖ **Exemple**

Pour clarifier ce concept et illustrer la technique de Pécorra-Carroll on reprend un exemple sur la synchronisation identique du système de Chua donné dans la référence. Le modèle mathématique de ce système est :

$$\begin{cases} \dot{x}_1 = \alpha\left(x_2 - x_1 - g(x_1)\right) \\ \dot{x_2} = x_1 - x_2 + x_3 \\ \dot{x}_3 = -\beta x_2 - \gamma x_3 \end{cases} \qquad \textbf{(III.4)}$$

Avec:

$\alpha = C_2/C_1, \quad \beta = C_2R^2/L, \quad \gamma = r/R$

Pour le choix du sous-système esclave trois configurations de deux variables sont possibles

$$\begin{cases} \acute{x_2} = x_1 - \acute{x_2} + \acute{x_3} \\ \acute{x_3} = -\beta\acute{x_2} - \gamma\acute{x_3} \end{cases}$$

Configuration (x_2, x_3) avec x_1 entrée d'accouplement

$$\begin{cases} \acute{x_1} = \alpha\left(x_2 - \acute{x_1} - g(\acute{x_1})\right) \\ \acute{x_3} = -\beta x_2 - \gamma\acute{x_3} \end{cases}$$

Configuration (x_1, x_3) avec x_2 entrée d'accouplement

$$\begin{cases} \dot{x_1} = \alpha(\dot{x_2} - \dot{x_1} - g(\dot{x_1})) \\ \dot{x_2} = \dot{x_1} - \dot{x_2} + x_3 \end{cases}$$

Configuration (x_1, x_2) avec x_3 entrée d'accouplement

III.4.Simulation sous Matlab

III.4.1.présentation de méthode de Runge-Kutta d'ordre 4

Les méthodes de Runge-Kutta constituent une famille de procédure d'intégration numérique d'ordre croissant, dont la méthode d'Euler est le premier ordre. Toutes les méthodes d'intégration consistent, en connaissant une valeur y(tn) à l'instant tn de la fonction à déterminer, à calculer sa valeur voisine a l'instant ultérieur tn +h. L'expression de la dérivée est approchée à l'aide de 4 valeurs pondérées entre deux points voisins en utilisant l'algorithme suivant **[35] :**

$$\begin{cases} k1 = h.\ f\ (tn, yn\ ) \\ k2 = h.\ f\ (tn + h\ 2\ , yn + k1\ 2\ ) \\ k3 = h.\ f\ (tn + h\ 2, yn + k2\ 2\ ) \\ k4 = h.\ f(tn + h,\ yn + k3\ ) \end{cases} \qquad \textbf{(III.5)}$$

III.5. Résultats des simulations

Pour simuler le comportement du circuit de Chua, nous avons utilisé le logiciel de calcul numérique Matlab. Cette simulation permettra de comprendre le comportement dynamique de ce circuit, et ainsi la façon de choisir les paramètres expérimentaux par la suite.

III.5.1. Signal chaotique du circuit de Chua

Le système non linéaire du chua présent un comportement chaotique .Le système non linéaire de Chua présente un comportement chaotique. Les **figures (III.5, III.6, III.7 et III.8**) présentent un exemple d'une trajectoire chaotique de ce circuit.

Nous avons obtenue les figures suivantes par l'utilisation de l'algorithme de Runge –kutta sous MATLAB.

La **figure (III.5)** et la **figure (III.6)** montres deux trajectoires du circuit électriques de Chua pour les valeurs des paramètres du circuit (a=-1.20, b=-0.65, α =10, β =0, γ=16,alpha1=-0.2, alpha2=-0.2 ,alpha3=-0.2).

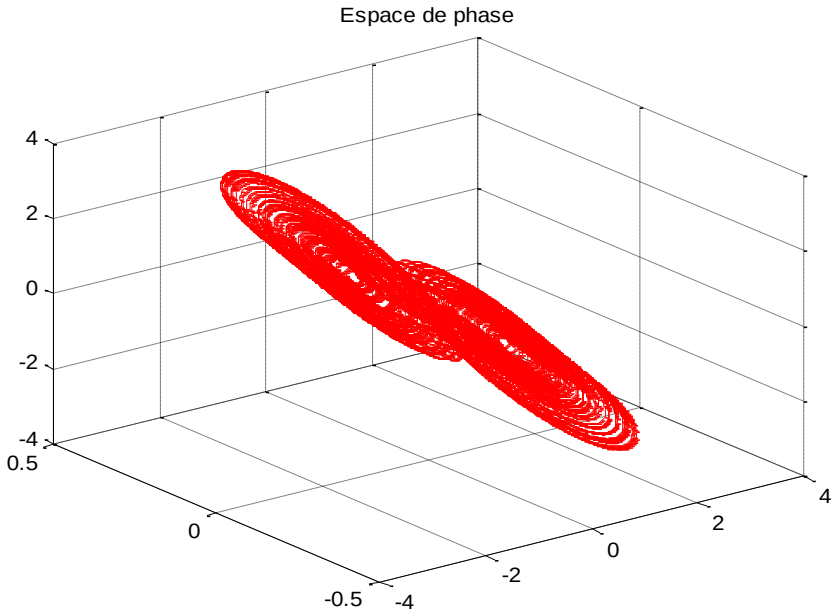


Figure.III.5. L'espace de phase.

La **figure (III.5)** montre le comportement chaotique du circuit de Chua et présente l'évolution dans l'espace de phase et la **figure(III.6)** présente l'évolution des trois variables du système en fonction de temps.

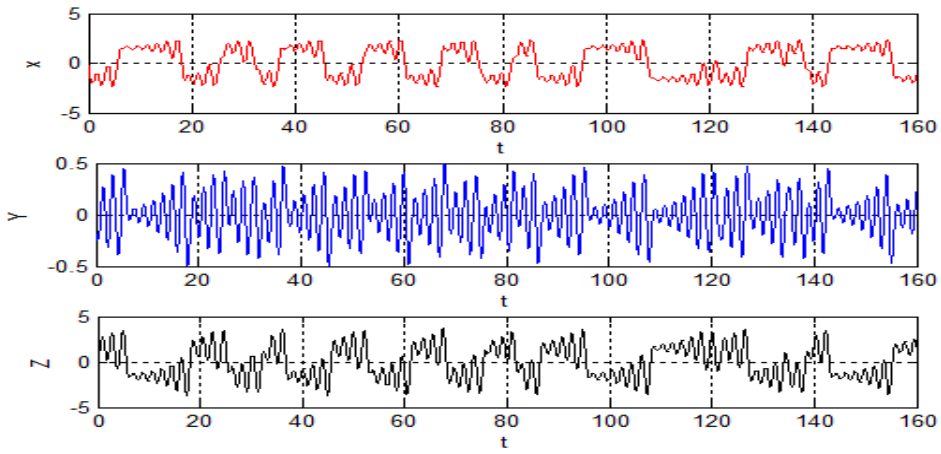


Figure.III.6. Trajectoire chaotique du circuit de Chua.

La **figure (III.7)** et la **figure (III.8)** montres deux trajectoires du circuit électriques deChua pour les valeurs des paramètres du circuit (a=-1.20, b=-0.65,α =10, β=0,γ =16 ,alpha1=0.48, alpha2= 0.488 ,alpha3=-0.49).

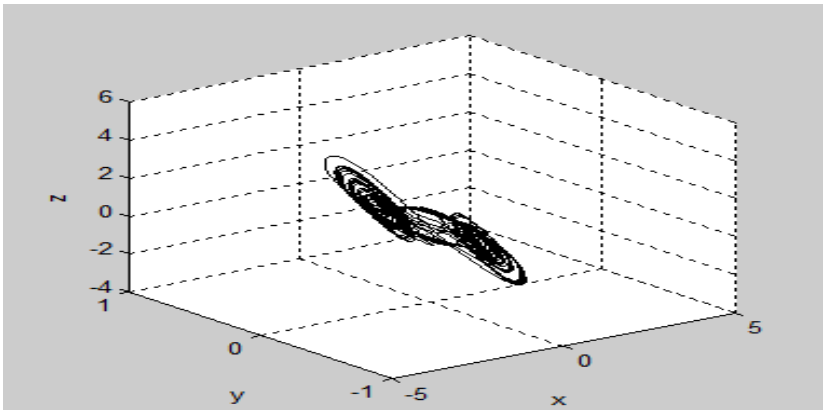


Figure. III.7. L'espace de phase.

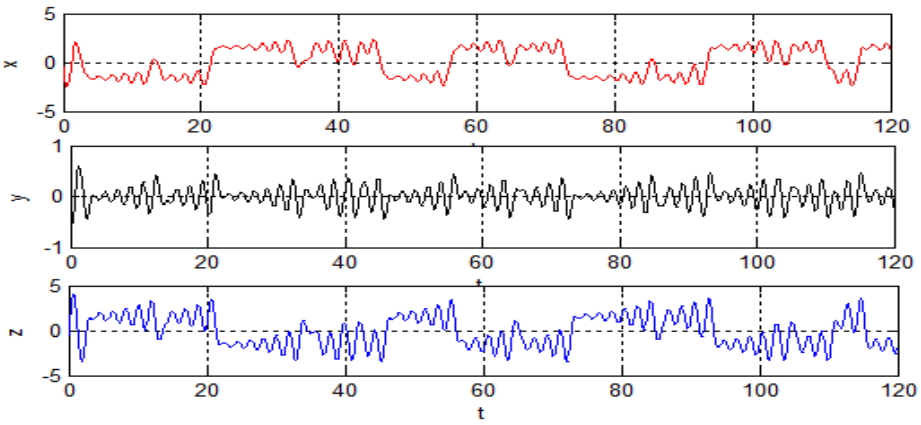


Figure.III.8. Trajectoire chaotique du circuit de Chua

Ces figures présentent deux solutions "chaotiques" au système Chua. On observe que la trajectoire dans l'espace des phases reste confinée dans une région bien définie, après une période transitoire de durée variable.

III.5.2.Cryptage par chaos

Après la simulation du système « Emetteur _ Récepteur » sous MATLAB, on visualise les signaux suivants :

- Le signal émis m(t).
- Le signal chaotique x(t).
- Le signal crypté s(t) = m(t) +x(t).

Le principe de synchronisation

Considérons les deux systèmes suivants :

$$\dot{x} = f1(x, u)$$

$$\widehat{\dot{x}} = f2(\hat{x}, u) \qquad \textbf{(III.6)}$$

La récupération de l'information est généralement basée sur la synchronisation des états $x$del'émetteur et des états $\hat{x}$ du récepteur.

A cause de la sensibilité aux conditions initiales des signaux chaotiques, les deux oscillateurs de l'émetteur et du récepteur n'auront jamais leurs états identiques dans n'importe quelle valeur de temps.

Les deux systèmes sont dits synchronisés si l'erreur de synchronisation e:

$$e = |\hat{x}(t) - x(t)| \rightarrow 0 \; quand \; t \rightarrow \infty \qquad \textbf{(III .7)}$$

III.5.2.1.Présentation de la technique utilisée

- **Test de la synchronisation**

Pour tester la synchronisation d'une communication sécurisée par chaos, nous avons utilisés un signal carré présenté dans la figure suivante.

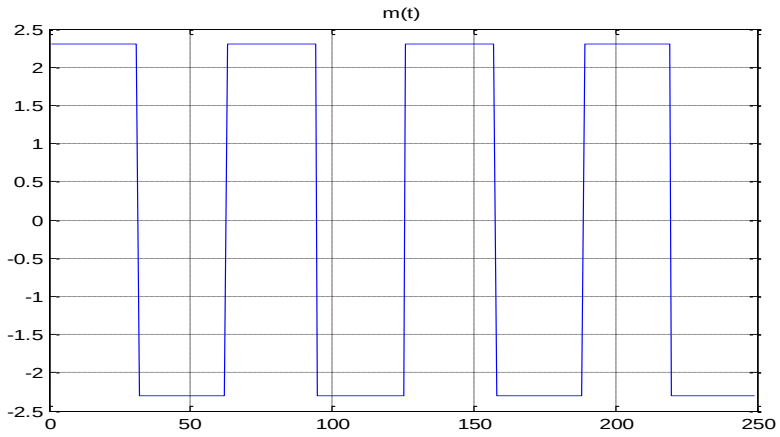


Figure.III.9. Figure Signal m(t) original

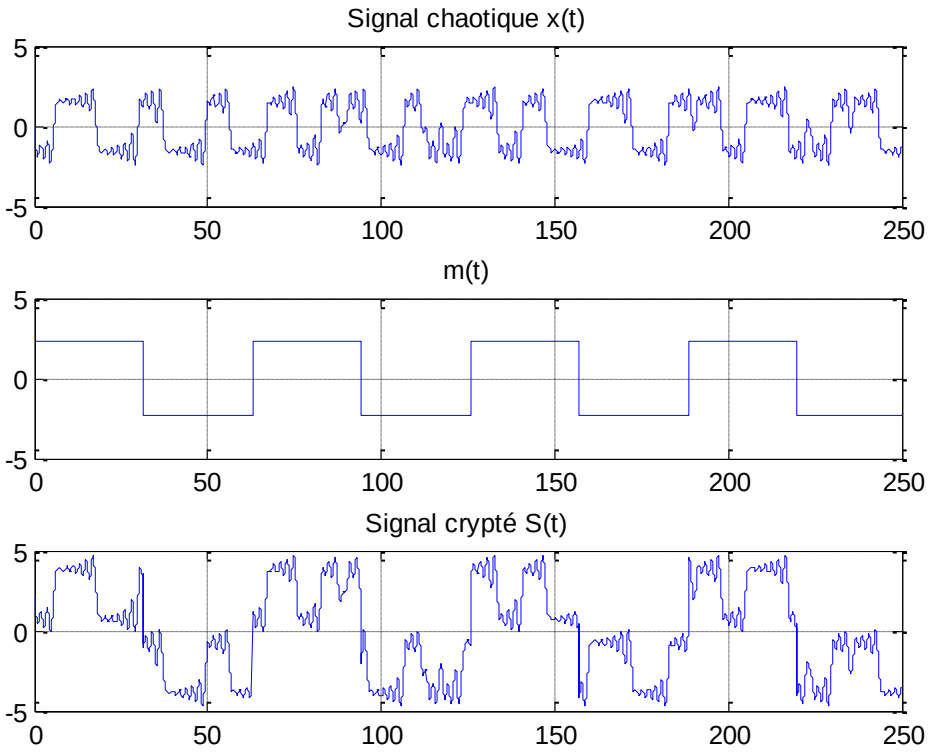


Figure.III.10. L'allure du signal chaotique x(t), le signal original m(t) et le signal après cryptage S(t).

Au niveau de la réception, l'erreur entre le signal original et le signal reçu est donné par la figure suivante. La première figure dans le cas où il n'ya pas une synchronisation et dans la deuxième figure les deux signaux sont synchronisés.

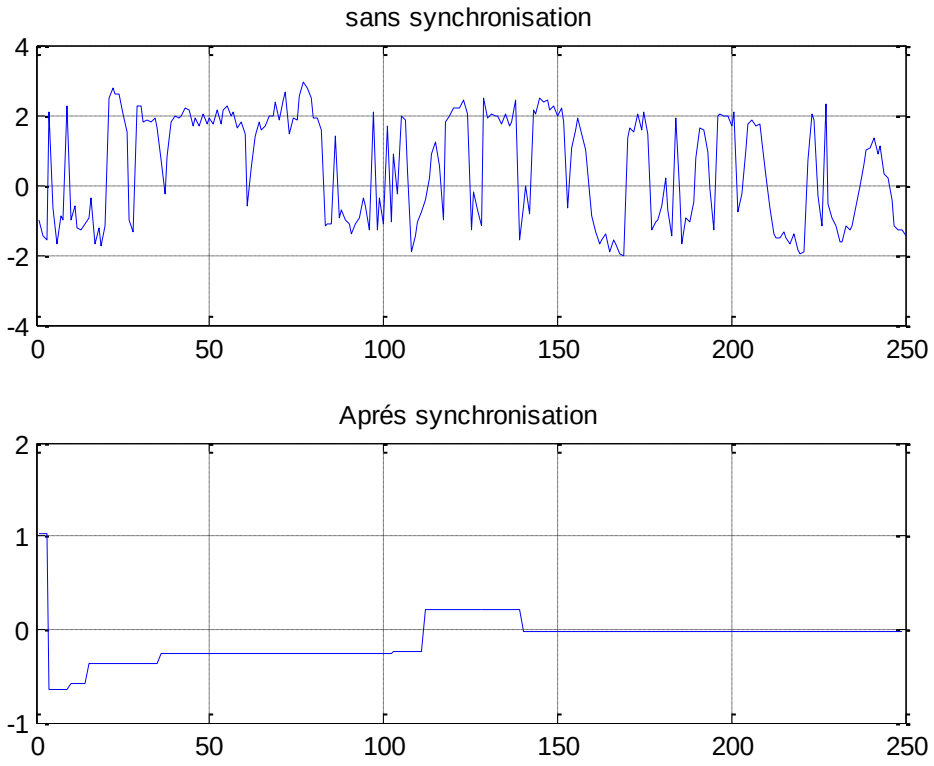


Figure III.11. L'erreur de synchronisation

L'erreur de la synchronisation entre les deux signaux chaotiques, La bonne décision c'est d'avoir l'erreur nulle c'est-à-dire la synchronisation est réussie.

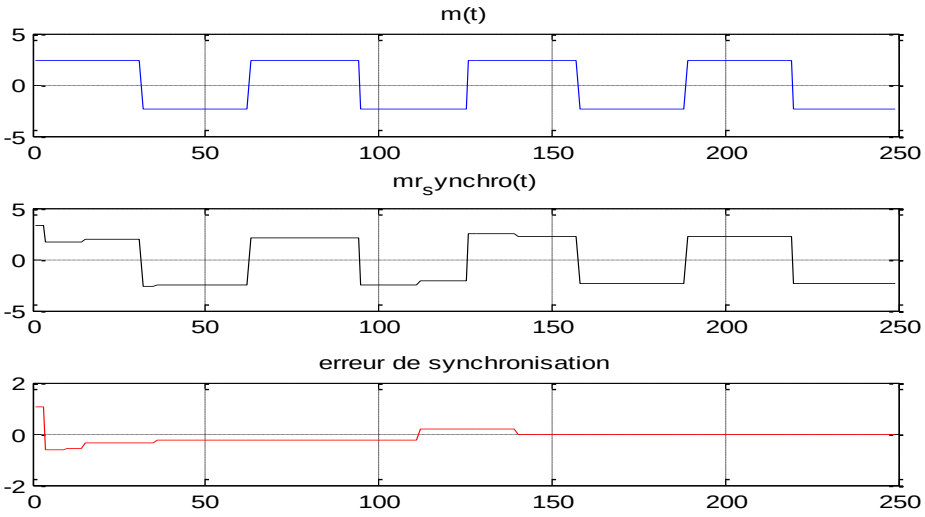


Figure .III.12. L'allure du signal original m(t) ,le signal récupéré mr (t) et l'erreur de synchronisation.

Une fois la synchronisation des états sont assurées, en observant les résultats obtenus, nous déduisons que le message est bien noyé dans le signal chaotique et que le message envoyé a été récupéré. Ce qui montre l'efficacité de la méthode de synchronisation.

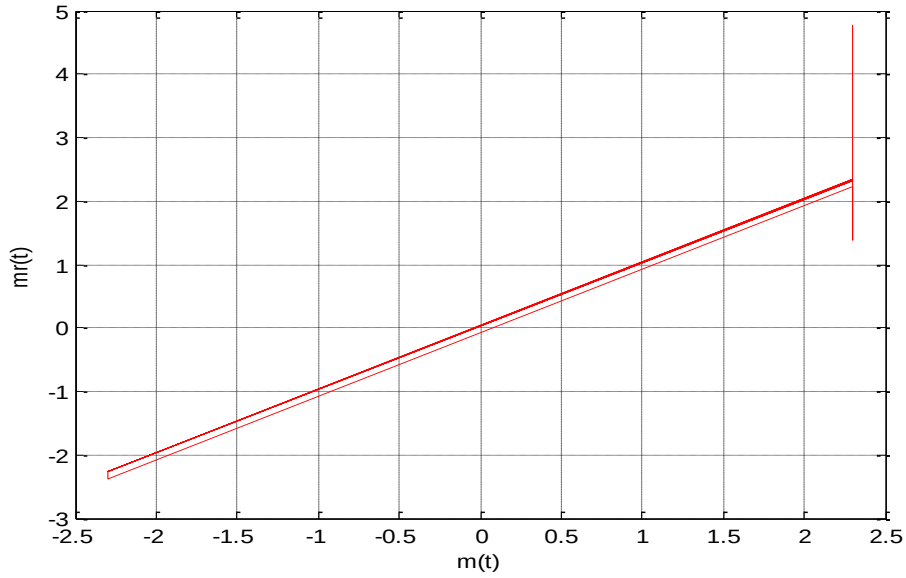


Figure III.13. Synchronisation des deux circuits.

Cette figure montre la synchronisation des deux circuits après un temps transitoire.

❖ **Le deuxième exemple**

La **figure (III.14)** représente les signaux résultants des erreurs.

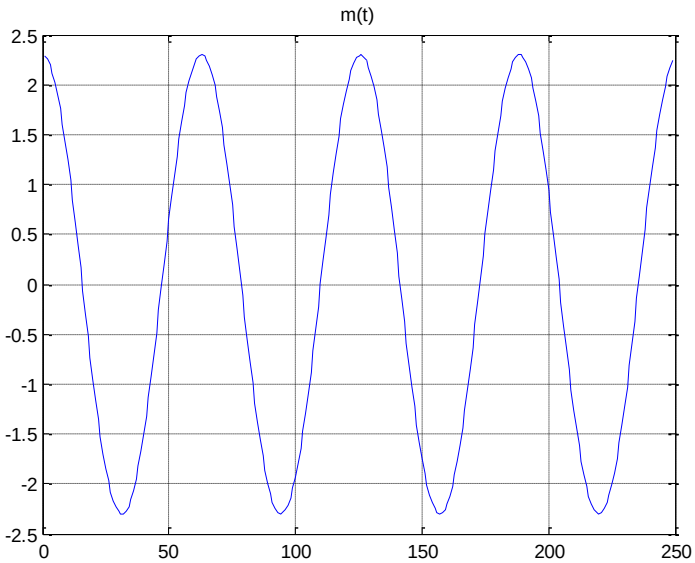


Figure .III.14. Message original m(t).

La **figure (III.15)** présente un signal chaotique x(t) issu du système de Chua.

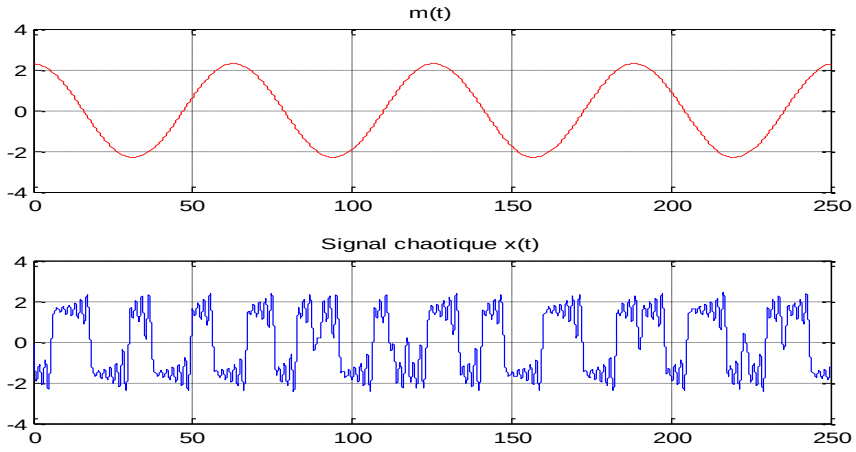


Figure .III.15. Résultat de simulation de l'état x(t) du système de Chua .

Le chiffrement d'un message par le chaos s'effectue donc en superposant à l'information initiale un signal chaotique. On envoie par la suite le message noyé dans le chaos à un récepteur.

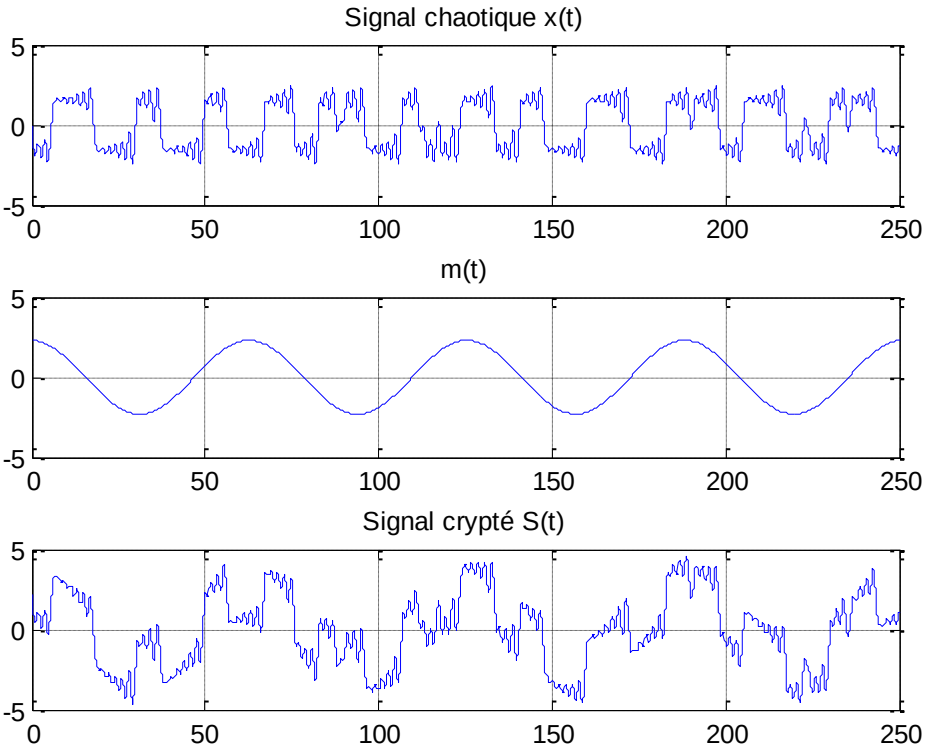


Figure III.16. Signal crypté avec chaos.

Cette figure montre bien que le signal sinusoïdal est devenu un signal crypté et il est difficile à le décrypter sans connaitre la clé de chiffrement.

Pour bien décrypter l'information initiale il faut connaitre les caractéristiques du signal chaotique. Il ne reste alors plus au destinataire qu'à soustraire le chaos de son message pour retrouver l'information.

La **figure (III.11)** représente l'allure du signal sans synchronisation et après synchronisation.

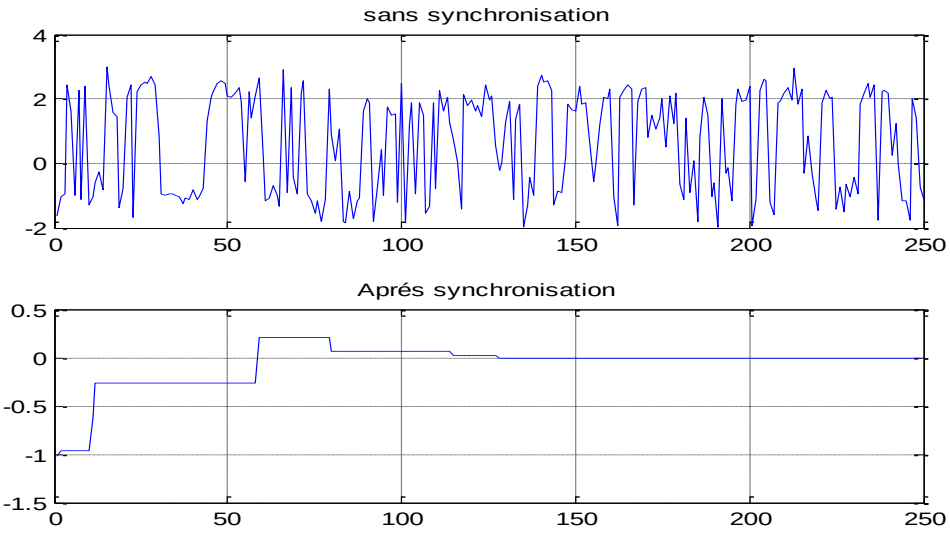


Figure .III.17. L'allure du signal sans synchronisation et après synchronisation.

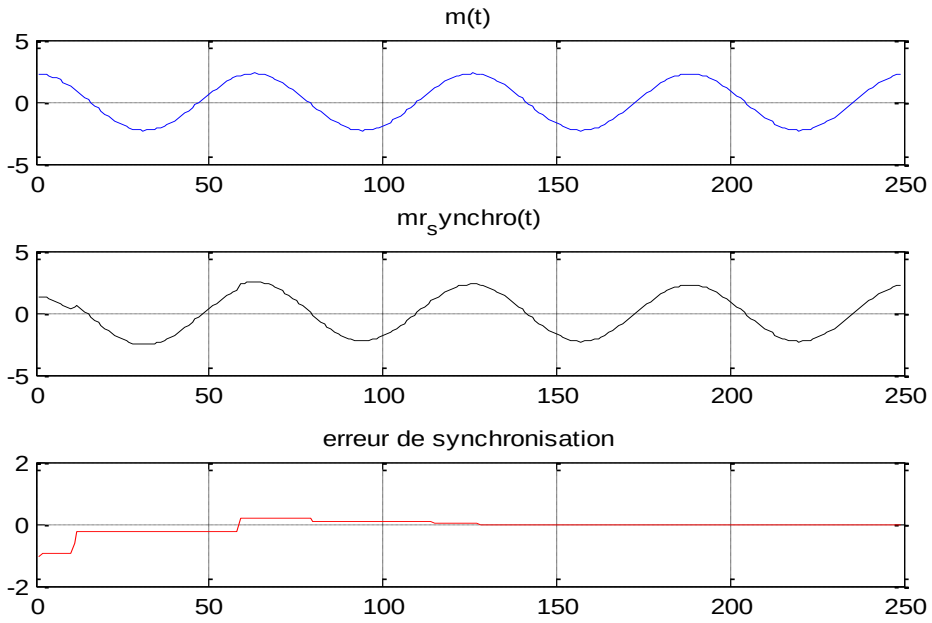


Figure.III.18. L'allure du signal original m(t), le signal récupéré mr(t) et l'erreur de synchronisation.

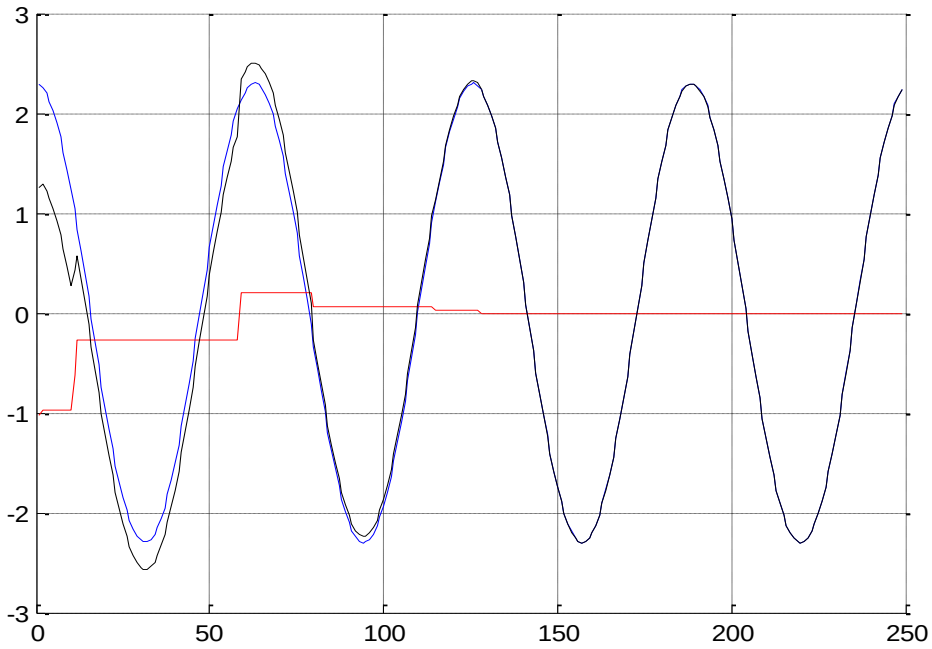


Figure. III.19. Le résultat de synchronisation.

A partir des résultats obtenus pour les deux exemples d'application (signal carrée et signal sinusoïdale) nous pouvons confirmer que le message est bien récupéré au niveau du récepteur pour les deux cas. Ceci implique l'efficacité de la méthode de synchronisation chaotique pour les deux exemples.

III.6. Conclusion

A travers cette étude nous avons défini le circuit de Chua qui permet de générer un signal chaotique déterministe à large spectre. Ce signal permet de crypter des informations avec une clé bien déterminée et nous avons intéressées par l'efficacité de la synchronisation. Nous avons également étudié la possibilité d'utiliser le chaos par ces différentes propriétés et de son comportement pour crypter l'information afin de sécuriser la transmission sécurisée. Dans le cas d'un cryptage chaotique l'émetteur et le récepteur ont les mêmes paramètres et les paramètres de système jouent le rôle de la clef de chiffrement.

Les résultats obtenus ont montré l'efficacité des signaux chaotiques pour crypter les informations.

Conclusion générale

Conclusion générale

Pour conclure nous pouvons mentionné que les systèmes chaotiques sont des systèmes dynamiques qui évoluent dans une région bornée, qui possèdent une infinité de trajectoires non périodiques denses. Ils sont caractérises par un comportement instable et non-linéaire, définit par une équation mathématique. Le comportement chaotique résulte de la grande sensibilité du système à l'état initial. Les formes d'onde chaotiques ont été largement utilisées dans divers domaines de recherche tels que la modulation de signaux et le cryptage chaotique de données de télécommunication.

Dans le premier chapitre de ce mémoire, nous avons présenté quelques généralités sur les systèmes chaotiques. , nous avons ainsi 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.

Par la suite nous avons ainsi introduit quelques exemples des systèmes chaotiques, comme le système de Lorenz , de Rössler et de Hénon. Nous avons aussi présenté la bifurcation par la fonction logistique et les domaines d'application d'un système chaotique.

Dans le deuxième chapitre, nous avons introduit les types de cryptage 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 à base du chaos. Nous avons aussi présenté les propriétés des systèmes chaotiques appliqués au cryptage d'une transmission des données.

Dans le dernier chapitre de ce mémoire, nous avons donné le circuit de l'oscillateur chaotique de Chua, ainsi nous avons étudié et tester par simulation sur Matlab un système de transmission sécurisé de données basé sur les systèmes chaotiques et la synchronisation Le phénomène de synchronisation se manifeste lorsque deux systèmes dynamiques évoluent d'une manière identique en fonction du temps.

Pour la synchronisation de deux systèmes (émetteur et récepteur), on injecte un signal généré par l'émetteur et l'envoyé au récepteur afin que ce dernier se synchronise avec l'émetteur.

Des résultats de simulation sont donnés pour illustrer l'efficacité de la méthode de synchronisation et a permis la récupération du message transmis.

Ce travail est un thème qui ouvre la recherche sur plusieurs axes. Les futurs travaux se concentreront sur l'avantage des oscillateurs chaotiques pour les problèmes de télécommunications, tels que le cryptage pour d'autres applications en télécommunication ainsi que l'application des algorithmes pour la synchronisation.

BIBLIEGRAPHIE

[1] H.Hamiche « Inversion à gauche des systèmes dynamiques hybrides chaotiques, application à la transmission sécurisée de données » Thèses de doctorat, Université Mouloud Mammeri Tizi Ouzou, Algérie, 2011.

[2] G. Kaddoum « Contributions à l'amélioration des systèmes de communication multi utilisateurs par Chaos : synchronisation et analyse des performances » thèses de Doctorat de l'Université de Toulouse, 2008.

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

[4] M.Aithammi ,abdelfatah « Etude et réalisation d'un système chaotique basé sur le circuit de chua » Mémoire de Master ,université Mouloud Mammri de Tizi – Ouzou ,2013 -2014.

[5] L. Kocarevet, S. Lian, « haos-Based Cryptography » : Theory, Algorithms and Applications, Springer, 2011.

[6] T.Kapitaniak,« Chaos for Engineers, Theory, Application and Control, Springer », 2000.

[7] G. Chen, X. Yu, Chaos Control: Theory and Applications, Springer, 2003.

[8] G.Zaibi « Sécurisation par dynamiques des réseaux locaux sans fil au niveau de la couche MAC », thèse de Doctorat de l'université de Toulouse, 2012.

[9] A .Benkhelifa , A Ghoul « Synchronisation des Systèmes Chaotiques .
Fractionnai » Mémoire de master , université de larbi Tébessi – Tébessa ,29/05/2016 .

[10] http://just.loic.free.fr/index.php?pas=hist

[11] T.Hamzia « Système dynamique et chaos 'application à l'optimisation à l'aide d'algorithme chaotique' », thèse de doctorat, université de Mentouri, Constantine, 2007.

[12] A. BERKANE « transmission sécurisée à base de la synchronisation impulsive de deux système chaotique discrets » Mémoire de master Professional. Université Mouloud Mammri de Tizi-Ouzo.

[13] 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 de doctorat Département d'électronique Université de Constantine Juin 2006.

[14] M . Boutobba,RNesraoui « UTILISATION DU COMPORTEMENTCHAOUTIQUE POUR LE CRYPTAGE DES SIGNAUX » Mémoire de master ,université abbes laghrour-khanchela,
30 /06/2019 .

[15] B.chauaib, « Photonique et réseaux optiques télécommunication » mémoire de master télécommunication, université de Tlemcen, 2014.

[16] A .HKihal « SYSTEMES CHAOTIQUES POUR LA TRANSMISSION SECURISEE DE DONNEES » Mémoire de magister, Electronique, 26/11/2013.

[17] http://ram-0000.developpez.com/tutoriels/cryptographie/?page=page_2#L2. » visité le :07/03/2017 .

[18] N. REBHI, M .BEN FARAH, A .KACHOURI, M .SAMET « Analyse De Sécurité d'une Nouvelle Méthode De Cryptage Chaotique » Laboratoire d'Electronique et des Technologies de l'Information (LETI) Ecole Nationale d'Ingénieurs de Sfax B.P.W. 3038 Sfax, Tunisie.

[19] Way To Learn X «Sécurité réseau »Différence entre le cryptage symétrique et asymétrique 23 .7.2018.

[20] N.Medjahdi « Cryptage Chaotique Basé Sur l'Attracteur Clifford » mémoire de fin d'étude de MASTER ,Université Abou BakrBelkaid– Tlemcen.2016-2017.

[21] D .ARBANE, K .ARAB « Conception de crypto-systèmes à base de systèmes chaotiques d'ordre fractionnaire : Application au cryptage de la parole » Mémoire de Fin d'Etudes de MASTER, Université Mouloud Mammeri De Tizi-Ouzou ,09 juillet 2018.

[22] I .YAGOUB, « Systèmes dynamiques discrets et chaos », université du havre, Année 2010/2011.

[23] F. DOUDJEDID ,K .BERROUCHE , « Transmison sécuriseé des données à base de systéme chaotique » Mémoire de Fin d'Etudes de MASTER, 2014.

[24] N .MEZAR, S .SEBTI, « Etude d'un système de transmission de données robuste à base de la synchronisation impulsive chaotique » Mémoire de Fin d'Etudes de MASTER , *24/09/ 2017.*

[*25*] A .ADANE, L .BOURAHMOUNE « Conception et étude d'un système de transmission sécurisée de données à base d'un système chaotique d'ordre fractionnaire » Mémoire de Fin d'Etudes de MASTER, *09 septembre 2015.*

[26] O.MEGHERBI « Etude et réalisation d'un système sécurisé à base de systèmes chaotiques » Mémoire de Fin d'Etudes de MASTER, 10/10/2013.

[27] A .Barkane « Transmission sécurisée à base de la synchronisation impulsive de deux systèmes chaotiques discrets » Mémoire de Fin d'Etudes de MASTER, université Mouloud Mammeri de Tizi-Ouzou, 2016.

[28] Y.GHEMBAZA Née BOUGUENAYA ,F . BAN BACHIR « cryptage des images et textes par système chaotique »Mémoire de fin d'étude pour de master , Université aboubakr bel kaid _ Tlemcen,2015-2016.

[29] M .Baba Ahmed , M . Anane , F . Benmansour, « Conception d'un crypto système pour les transmissions de données chiffrées » , université Abou Bekr belkaid , Tlemcen . 14 November 2014.

[30] N. BELLAHBIB, I .ABDELLI « L'EXPLOITATION DU CHAOS NUMERIQUE DANS LES TRANSMISSIONS SECURISEES » Mémoire de Fin d'Etudes de MASTER ,UNIVERSITE ABOU-BEKR BELKAID- TLEMCEN.2016/2017.

[31] M.Djenouri, M.Chikhi « communication sécurisée par chaos : Etude et implémentation sur carte FPGA ». Mémoire de Fin d'Etudes de MASTER, université saad dahlab de blida ,2013-2014.

[32] G.Zheng « Formes normales d'observabilité paramétriques par les sorties : Applications au cryptage par synchronisation de systèmes chaotiques » Thèse de doctorat, Université de Cergy-Pontoise, France, 2006.

[33] N. MEZAR, S. SEBTI, « Etude d'un système de transmission de données robuste à base de la synchronisation impulsive chaotique » Mémoire de Fin d'Etudes de MASTER, *24/09/ 2017*.

[34] T. Matsumoto « *A chaoti cattractor from Chua's* » *circuit IEEE Trans. Circuits Syst*, vol .31, pp .1055-1058, 1984 .