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 EN FONCTION LOGISTIQUE

Réalisé par : - Khalihenna Moulay Idriss
- KHil Lekhdar

Devant le jury :

Dr.Djamai Djemouai	***Président***	***Université Abbes Laghrour-Khenchela***
Dr. Maamri Fouzia	***Encadreur***	***Université Abbes Laghrour-Khenchela***
Dr.Sahour Abd elhakim	***Examinateur***	***Université Abbes Laghrour-Khenchela***

Promotion 2020/2021

الملخص:

تعتبر أنظمة الفوضى أنظمة معلومة، غير خطية وتتأثر بصورة ملحوظة بالشروط ابتدائية. في أغلب الأحيان الإشارات الناتجة في هذه الأنظمة تكون ذات مجال واسع من الموجات، لهذا فهي تشبه الضوضاء الشبه عشوائية. منذ أن اكتشف العالمان "بكورا " و كارول "إمكانية تزامن نظامين فوضويين ، بدأ توجه المجتمع العلمي نحو البحث عن إمكانية استغلال هذه الأنظمة وخاصة في مجال تأمين الاتصالات و هذا الاهتمام راجع كون هذه الأنظمة 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 الأخير إلى محاكاة تطبيق نظرية الفوضى في تأمين الاتصالات .

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

Abstract

We have presented in this paper the chaotic systems which are periodic 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 study 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, chaotic 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 initiaux. 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 étude 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

On dédie ce modeste travail à nos parents qui ont eu foi en nous et qui ont su être là pour nous soutenir et nous encourager durant le long de nos études.

A tout les membres de nos familles ainsi qu'à tout nos amis(e).

Merci à vous.

K.LEKHDAR&K .MOULAY IDRISS

DEDICACE

Je dédie mon travail à mon cher père, que Dieu le préserve, et à qui Dieu a fait le paradis sous ses pieds, à celui qui m'a inondé de sa tendresse débordante, à celui qui a été brûlé, pour éclairer mon chemin vers celui qui avait faim d'être rassasié et resté endormi et fatigué pour se reposer et pleuré de rire et m'a conduit de la source de sa tendresse et de son honnêteté à celle qui m'a élevé petit et m'a beaucoup conseillé Ma chère mère, que Dieu prolonge sa vie et faire d'elle une tente au-dessus de nos têtes, à mes frères et sœurs et ses familles, à ceux qui ont partagé mes joies et ma peine pour mes frères à ceux avec qui le forum de la connaissance et de l'amitié a été réuni par mes collègues, pour qui j'ai utilisé les plus hautes expressions d'amour à tous mes professeurs qui m'ont accompagné tout au long de mon parcours académique.

Khalihenna Moulay Idriss

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.

Symboles mathématique

x_0, $y0$, 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
$\lvert . \rvert$	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
Lim	Limite
Ln	Logarithme népérien
R	L'ensemble des nombres réels
R^P	Espace vectorielles de dimension **P**
R^n	Espace vectorielles de dimension **n**
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

TABLE DES MATIERES

LISTE DES FIGURES

LISTE DES TABLEAUX

INTRODUCTION GENERALE

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 **[36].**

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.

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 simulation d'un système de transmission sécurisée de données à base de la fonction logistique.

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, la fonction logistique 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 LES SYTEMES DYNAMIQUES ET CHAOTIQUES

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 répète jamais qui est très sensible aux conditions initiales, et imprédictible 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**

$X(t)= f(x(t), u(t), t)$
$Y(t) = h(x(t), u(t), t)$ **(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 :

$x(k + 1)= G(k, x(k), u(k))$
$y(k) = h(k, x(k), u(k))$ **(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 .Le chaos :

I. 3.1. Définition du chaos :

Le chaos tel que le scientifique le comprend ne signifie pas l'absence d'ordre; il se rattache plutôt à une notion d'imprévisibilité, d'impossibilité de prévoir une évolution à long terme du fait que l'état final dépend de manière si sensible de l'état initial. On appelle donc un système dynamique chaotique, un système qui dépend de plusieurs paramètres et caractérisé par une extrême sensibilité aux conditions initiales. Ils ne sont pas déterminés ou modélisés par des systèmes d'équations linéaires ni par les lois de la mécanique classique; pourtant, ils ne sont pas nécessairement aléatoires, relevant du seul calcul des probabilités.

Les définitions et propriétés suivantes permettent de comprendre qualitativement les points marquants des systèmes chaotiques ***[4].***

I.3.1.1. La non-linéarité :

Un système chaotique est un système dynamique non linéaire. Un système linéaire ne peut pas être chaotique.

I.3.1.2. Le déterminisme :

La notion de déterminisme signifie la capacité de « prédire » le futur d'un phénomène à partir d'un évènement passé ou présent. L'évolution irrégulière du comportement d'un système chaotique est due aux non linéarités Dans les phénomènes aléatoires, il est

absolument impossible de prévoir la trajectoire d'une quelconque particule. À l'opposé, un système chaotique a des règles fondamentales déterministes et non probabilistes.

I.3.1.3. L'aspect aléatoire :

Tous les états d'un système chaotique présentent des aspects aléatoires **.La figure (I.1)** représente l'état chaotique x_1 du système de Rössler :

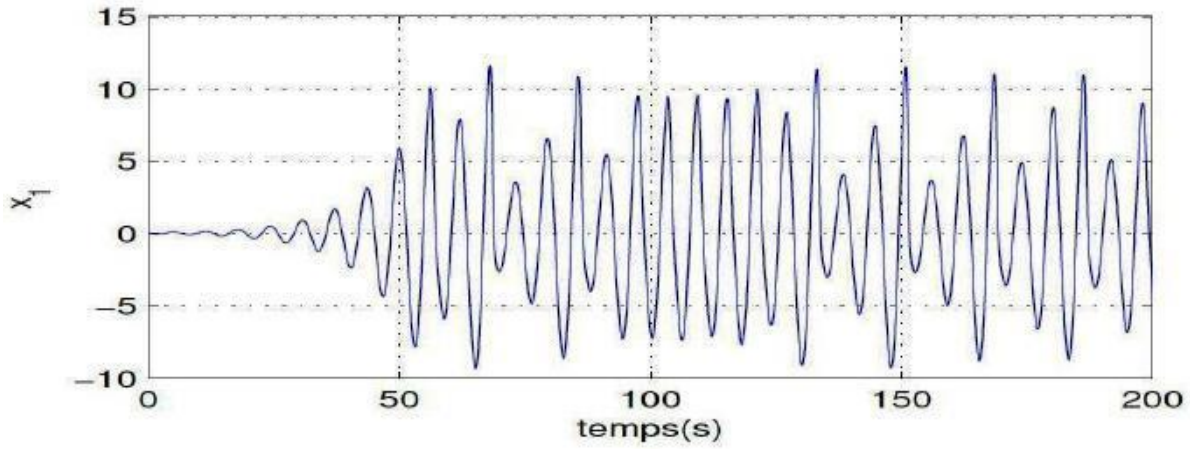


Figure I.1 : Etat chaotique du système de Rössler [4].

I.3.1.4. Sensibilité aux conditions initiales :

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

Il est clair que la moindre erreur ou imprécision sur la condition initiale interdit de décider à tout temps quelle sera la trajectoire effectivement suivie et de faire une prédiction sur l'évolution à long terme du système.

Une des propriétés essentielles du chaos est donc bien cette sensibilité aux conditions initiales que l'on peut caractériser en mesurant des taux de divergence des trajectoires. Ceci est illustré par **la figure (I.2).**

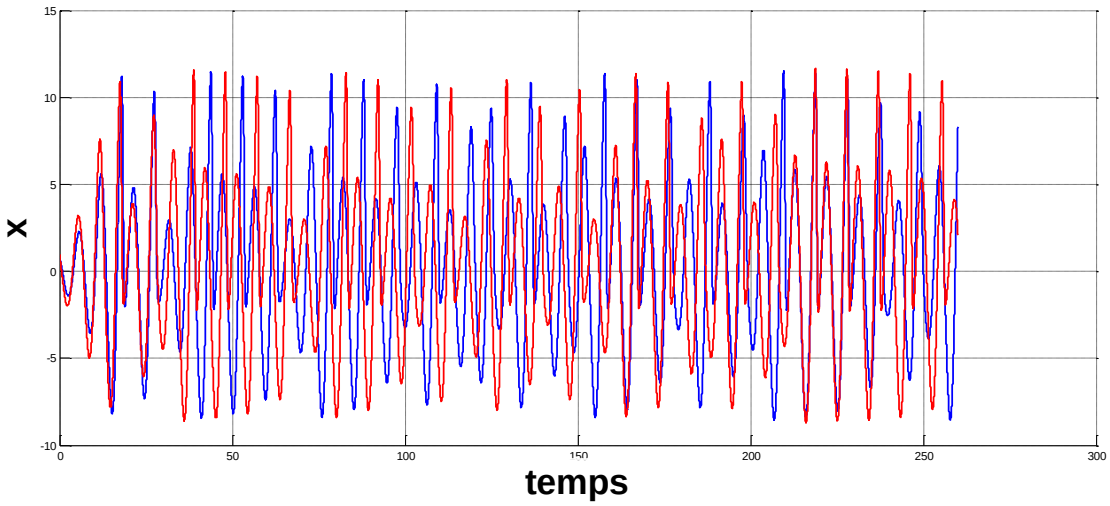


Figure I.2 : Illustration de la propriété de sensibilité

Aux conditions initiales sur l'état du système.

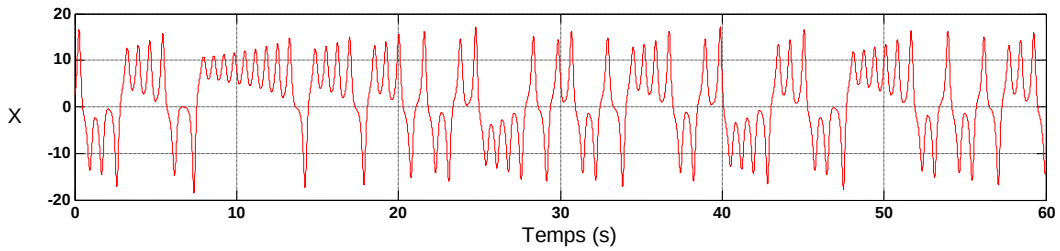
I.3.1. 5.Espace des phases :

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] :**

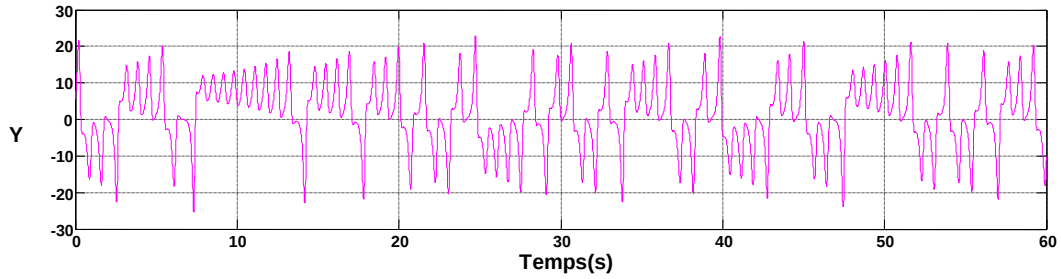
- en fonction de x et de y.
- en fonction de x et de t.
- en fonction de y et de t.

I.3.1.6. Le caractère pseudo aléatoire :

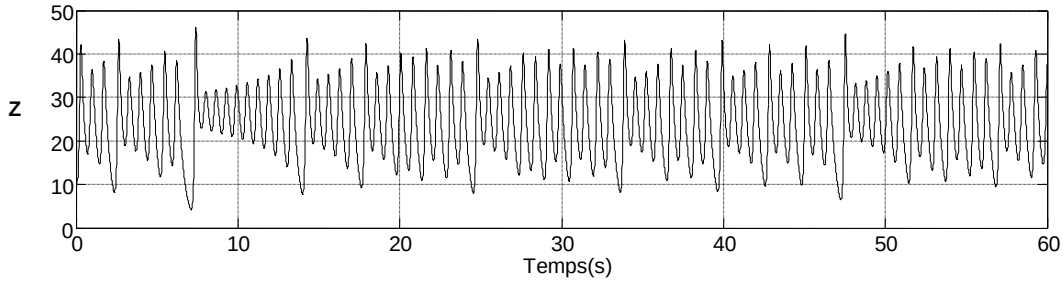
Tous les états d'un système chaotique présentent des aspects aléatoires La **figure (I.3)** illustre l'aspect aléatoire des états du système Lorenz.



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



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



c. Système de Lorenz : Évolution de Z par rapport à t

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

I.3.1.7. 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) illustre L'évolution de l'attracteur de Lorenz en 2 et 3 dimensions.

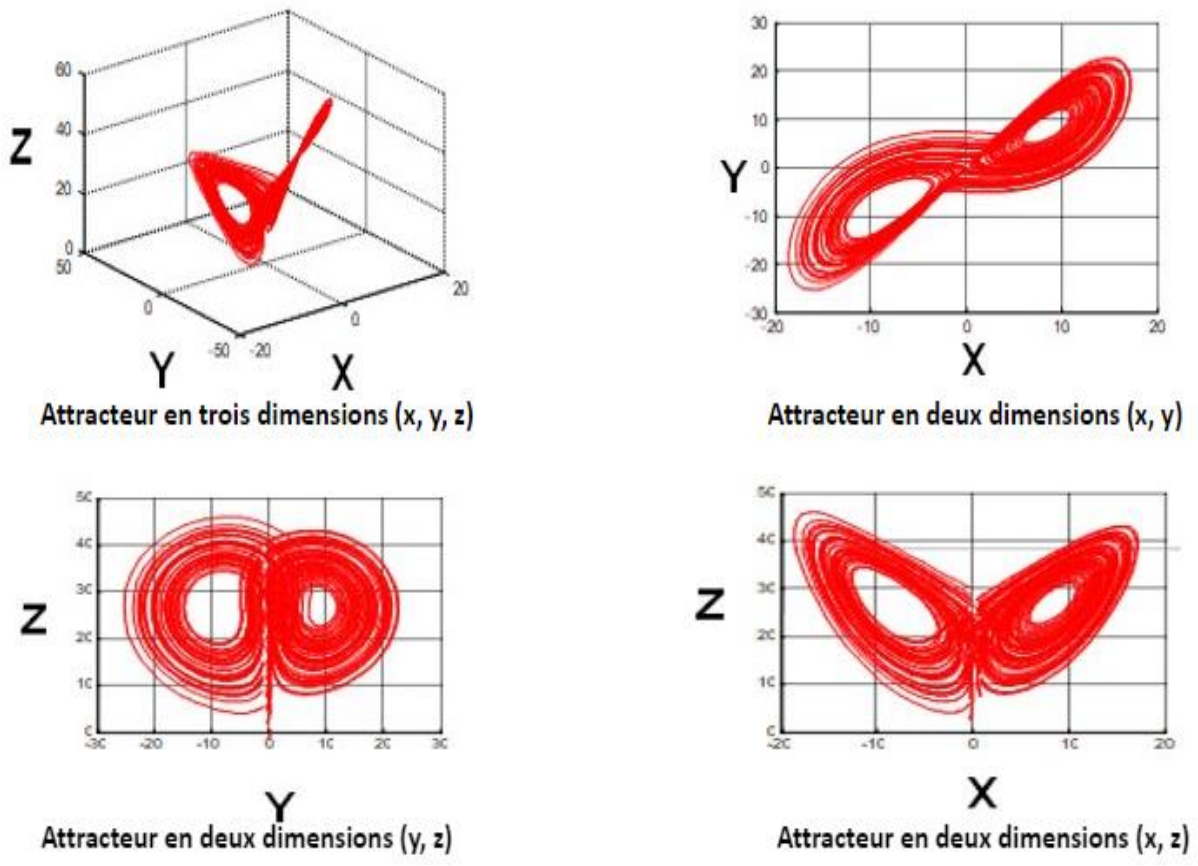


Figure I.4. Evolution de l'attracteur de Lorenz en 2 et 3 dimensions.

❖ **Exemple de Rössler**

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

$$X = -(y + z)$$

$$Y = x + ay \qquad \textbf{(I.3)}$$

$$Z = b + z(x - c)$$

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=0.3, b=-0.3, c=5 avec les conditions initiales x(0) =0.8; y (0) =0.5 ; z(0) =0.3. **La figure (I.5)** suivante illustre attracteur étrange de Rössler.

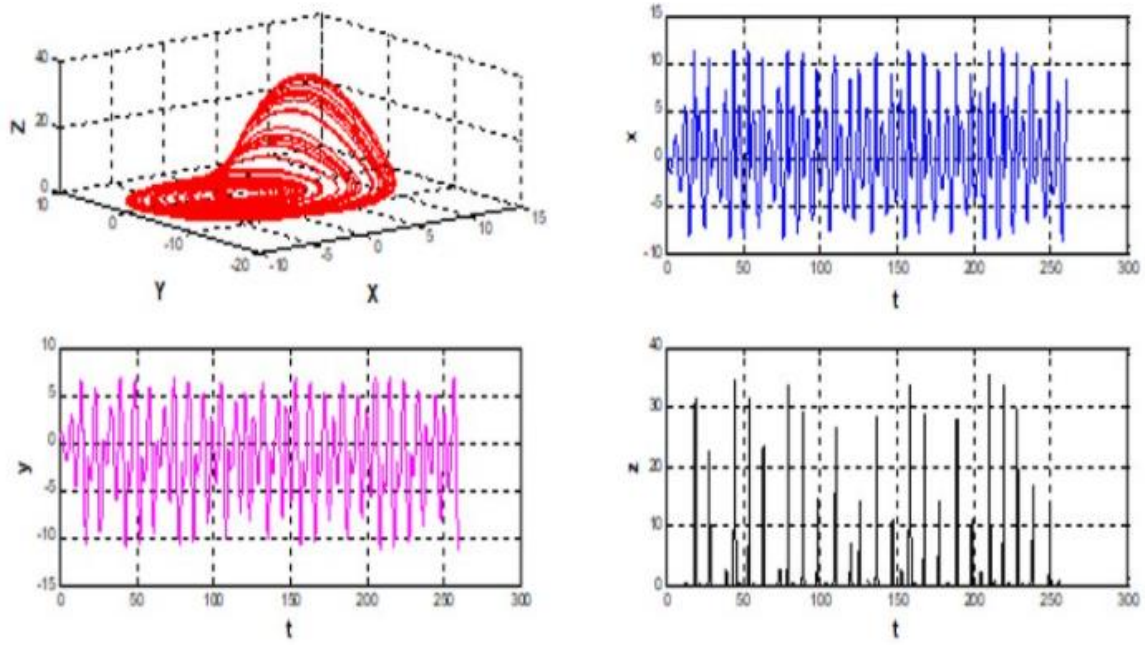


Figure I.5. Attracteur de Rössler

I.3.1.8. Exposants de Lyapunov :

Les exposants de Lyapunov, présentés par Oseledec pour la première fois en1968, jouent un rôle important dans l'étude des systèmes dynamiques non linéaires notamment les systèmes chaotiques. Ils qualifient le degré de divergence des trajectoires d'un système dynamique non linéaire soumis à des conditions initiales différentes. Cette divergence est exprimée par les exposants de Lyapunov [9].Ainsi le nombre d'exposants de Lyapunov est égal à la dimension de l'espace de phase et ils sont généralement indexés du plus grand au plus petit$\lambda 1, \lambda 2, \lambda 3, \ldots$ [10].

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.

- Au 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	$\lambda_n \leq \lambda_{n-1} \leq \ldots\ldots \leq \lambda_1 < 0$
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 I.1 Attracteurs et exposants de Lyapunov

I.3.2.Historique de la théorie du chaos :

Le tableau suivant retrace les moments forts de l'évolution de la théorie du chaos **[5].**

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.2 Historique du chaos

I.3.3 .Quelques Définition sur le chaos :

Selon la littérature que nous avons consultée, la notion du chaos répond aux définitions ci-dessous **[6], [7], [8] :**

Définition 1

Le chaos tel que le scientifique le comprend ne signifie pas l'absence d'ordre; il se rattache plutôt à une notion d'imprévisibilité, d'impossibilité de prévoir une évolution à long terme du fait que l'état final dépend de manière si sensible de l'état initial.

Définition 2

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 3

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 4

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 aussi prédictible.

I.3. 4.Domaine d'application du chaos:

Les domaines d'applications du chaos sont très nombreux, on peut citer principalement les domaines suivants :

I.3.4.1. Ingénierie :

Contrôle de vibrations, stabilisation des circuits, réactions chimiques, turbines, étages de puissance, lasers, combustion, et beaucoup plus.

I.3.4.2. Ordinateurs :

Commutation des paquets dans des réseaux informatiques. Cryptage. Contrôle du chaos dans les systèmes robotiques.

I.3.4.3. Communications :

Compression et stockage d'images. Conception et management des réseaux d'ordinateurs.

I.3.4.4. Médecine et biologie :

Cardiologie, analyse du rythme du cœur (EEG), prédiction et contrôle d'activité irrégulière du cœur.

I.3.4.5. Management et finance :

Prévisions économiques, analyse financière, et prévision du marché.

I.3.4.6. Télécommunication :

L'utilisation du chaos pour sécuriser les télécommunications est un sujet d'études depuis plusieurs années. Le chaos est obtenu à partir de systèmes non linéaires ; il correspond à un comportement stable, apériodique et éventuellement borné, de ces systèmes, ce qui le fait apparaître comme du « bruit » pseudo aléatoire. Il peut donc être utilisé pour masquer ou mélanger les informations dans une transmission sécurisée.

I.3.5.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.3.5.1.Systèmes chaotiques continus :

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

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

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 :

$$X = f(t, x) \qquad \textbf{(I.5)}$$

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]** :

$$\begin{aligned} X &= 10\,(-x+y) \\ Y &= x\,(28-z)-y \\ Z &= xy-2.67*z \end{aligned} \qquad \textbf{(I.6)}$$

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=10, b=28, c=8/3 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 :

$$\begin{aligned} X &= -\,(y - z) \\ Y &= x + ay \\ Z &= b + z\,(x-c) \end{aligned} \qquad \textbf{(I.7)}$$

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 choisies de la manière suivante :

$a=b=0.3$, $c=5$, $(x_0, y_0, z_0) = (1, 1, 1)$

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

I.3.5.2 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 :

$$X(k+1) = G(x(k), u(k)), \quad y(k) = h(x(k), u(k)) \qquad \textbf{(I.8)}$$

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]** :

$$X(I) = y(I-1) + 1 - a * X(I-1)$$

$$Y(I) = b * X(I-1) \qquad \textbf{(I.9)}$$

Tel que $(x(k), y(k)) \in R2$ 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.6)** représente l'attracteur de Hénon.

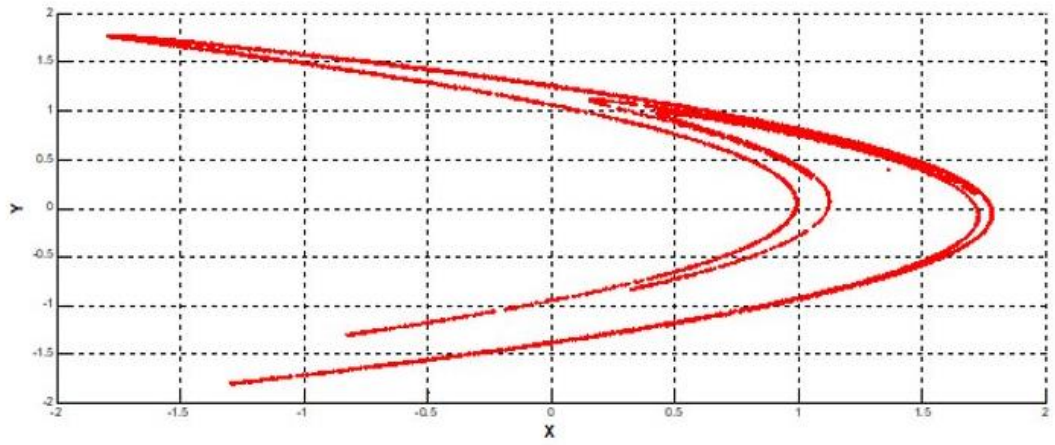


Figure I.6. Attracteur chaotique de Hénon

I.3.6 Propriétés de systèmes chaotiques :

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.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.5.Bifurcation :

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

Une bifurcation survient lorsqu'une variation quantitative d'un paramètre du 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 **[30]**.

- **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 **[30]** :

$$x_{k+1} = f(x_k) = rx_k(1\text{-}x_k) \qquad \textbf{(I.10)}$$

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 limitent.

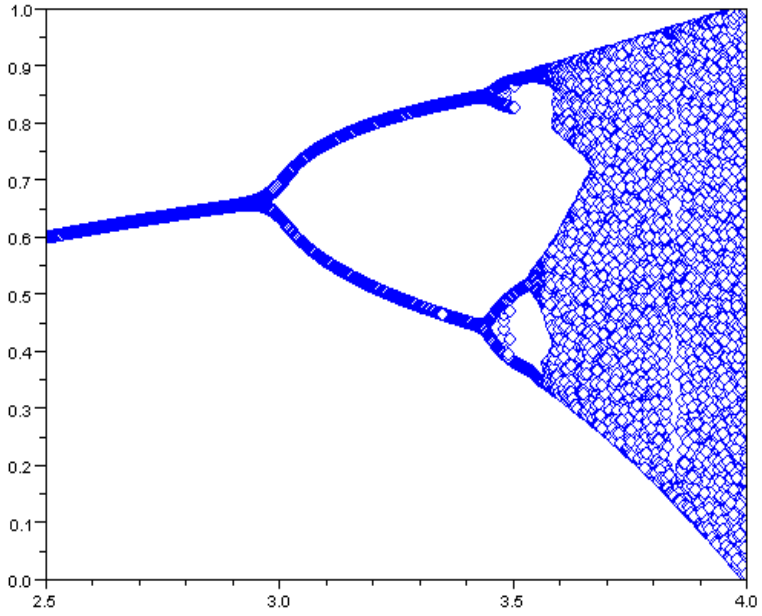


Figure I.7. Diagramme de bifurcation pour la fonction logistique

I.5.1 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 **[13].**

- **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 **[13].**

- **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 **[13].**

I.6. 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 **[14].** Nous allons en exposer brièvement trois types d'évolution possibles.

I.6.1 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 **[14]**.

I.6.2 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 **[14]**.

I.6.3 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.7.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 Rössler, nous avons cité les domaines d'application du comportement chaotique, et présenté la Bifurcation aussi bien cité les déférents types de la Bifurcation et les conductions d'un système devient 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 CHAOTIQUES

II.1. Introduction :

L'utilisation du chaos dans les systèmes de télécommunication a été rendue possible depuis la maîtrise de la synchronisation des systèmes chaotiques **[15] [16]**. En effet la synchronisation de ces systèmes présente plus de contraintes contrairement au cas d'oscillations périodiques où il n'y a pas d'instabilité intrinsèque. Dans la littérature plusieurs concepts de synchronisation chaotique ont été proposés tout d'abord avec les travaux de Yamada et Fujisaka **[17]** qui ont utilisé une approche locale de la synchronisation chaotique.

Dans ce chapitre, nous citerons les différentes approches de synchronisation des systèmes chaotiques. Ensuite, on introduit le concept de synchronisation impulsive de deux systèmes chaotiques identiques.

II.2.Communication sécurisée a base du chaos :

En 1990, L.M.Pecora et T.L.Caroll **[16]** ont introduit la notion de synchronisation de deux systèmes chaotiques identiques. Trois ans plus tard, Cuomo et Oppenheim **[18]** présentèrent le premier dispositif de communication entre deux systèmes chaotiques de Lorenz identiques. En 1997 Kolumban, Kennedy et Chua **[19] [20]** réalisèrent des communications numériques à base de deux circuits de Chua identiques. Plus tard, le domaine du chaos attira l'attention de la communauté scientifique et plusieurs systèmes de communications symétriques furent présentés.

Le diagramme principal de la communication sécurisée par le chaos est montré sur **la figure (II.1)**. 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.

Laclédusystèmedetransmissionestl'ensembledesparamètresdesdeuxgénérateurs chaotiques à l'émission et à la réception qui doivent être synchronisés, c'est-à-dire x=y

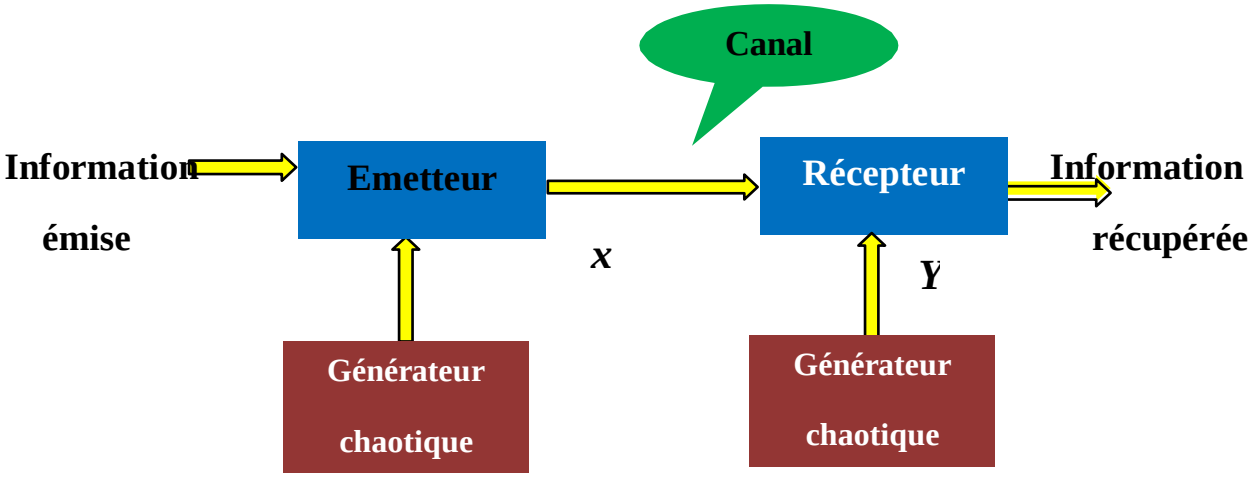


Figure II.1.Principe de la communication sécurisée à base du chaos

II.3.Concept et méthodes 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 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 ; on distingue la synchronisation unidirectionnelle et la synchronisation bidirectionnelle.

II.3.1.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 fonctionnant dans un seul sens, par exemple l'utilisation d'un circuit électrique suiveur **[21]**.

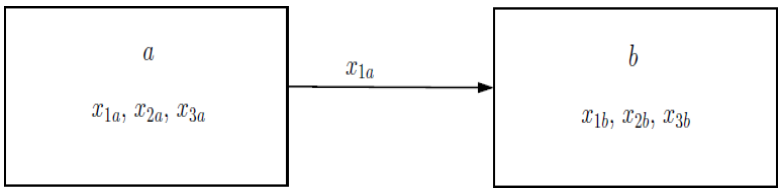


Figure II.2.Couplage unidirectionnel

II.3.2.Synchronisation bidirectionnelle :

Dans le cas d'une synchronisation bidirectionnelle, le couplage entre deux systèmes identiques a et b est réalisé à l'aide d'un élément permettant l'échange d'énergie dans les deux sens, par exemple l'utilisation d'une simple résistance **[21].**

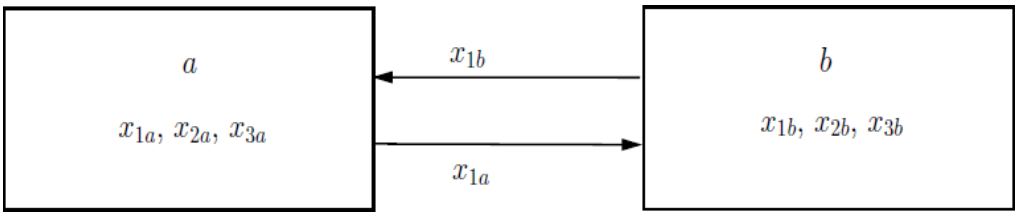


Figure II.3.Couplage bidirectionnel

II.4. 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 et avantages **[21]**.

II.4.1.Synchronisation par boucle fermé :

La synchronisation des systèmes chaotiques par les méthodes en boucle ouverte implique une sensibilité aux variations paramétriques. Cette technique permet également la synchronisation entre des paires différentes de systèmes chaotiques. La **figure (II.4)** indique un schéma simplifié de la synchronisation par boucle fermée **[22].**

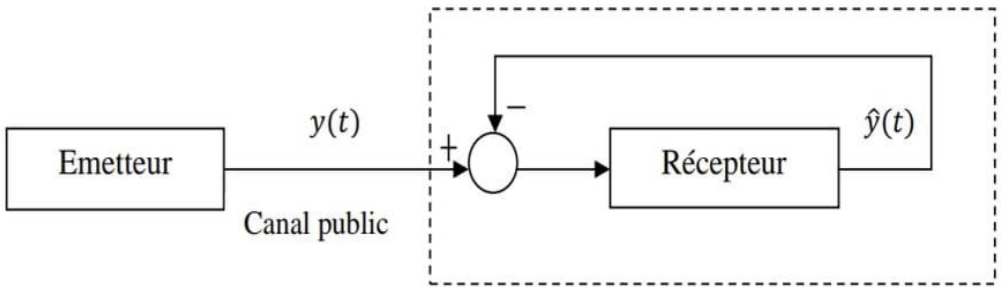


Figure II.4. Synchronisation par boucle fermée

II.4.2. 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.

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 :

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

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 **[23].**

II.4.3. 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.5),** 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 **[23].**

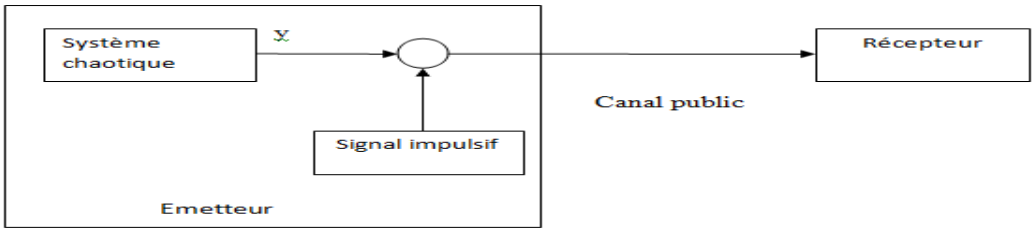


Figure II.5. Principe de la synchronisation impulsive

Cette méthode sera mieux développée et discutée par la suite pour être appliquée pour la réalisation d'un système de transmission sécurisée.

II.4.4. 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 :

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

Où α est le facteur d'échelle, $x(t)$ est l'état du système émetteur,$x'(t)$ est l'état du système récepteur et τest 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 **[22].**

II.4.5.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 **[23].**

II.4.6.Synchronisation de phases :

Pour deux systèmes périodiques de phases Φ_1 et Φ_2, la synchronisation est exprimée par la relation [6] :

$$n\Phi_1 - m\Phi_2 < c \qquad \textbf{(II. 4)}$$

Avec m, n des entiers naturels et c est une constante positive.

Cette notion de synchronisation a été étendue aux systèmes chaotiques, l'approche analytique est l'une des solutions permettant de définir la phase d'un système chaotiques.

Un signal analytique Ψtest une fonction complexe définie comme suit :

$$\Psi t = st + jst = Ate^{j\Phi t} \quad \textbf{(II. 5)}$$

Où $s(t)$ est la transformée de Hilbert de la série temporelle (t), $A(t)$ est l'amplitude de $\Psi(t)$ et $\Phi(t)$ sa phase.

La synchronisation de phase entre deux systèmes chaotiques couplés se produit si

$$n\Phi_1\ (t) - m\Phi_2\ (t) < c \quad \textbf{(II. 6)}$$

Il est à noter que dans ce cas, les amplitudes restent non corrélées.

II.4.7. Synchronisation par observateur :

Dans cette approche, Le système maître est un système chaotique quelconque et le système esclave est un observateur d'état. Théoriquement, le problème de la conception d'un observateur pour un système (non linéaire) est défini comme suit :

$$Lim_{t\to\infty}\ \| x(t) - \hat{x}\ (t)\| = 0 \quad \textbf{(II.7)}$$

Où x(t) est l'état du système et$\hat{x}(t)$ est l'état estimé .Ce principe est illustré par la **figure (II.6)** suivante :

Le signal chaotique transmis

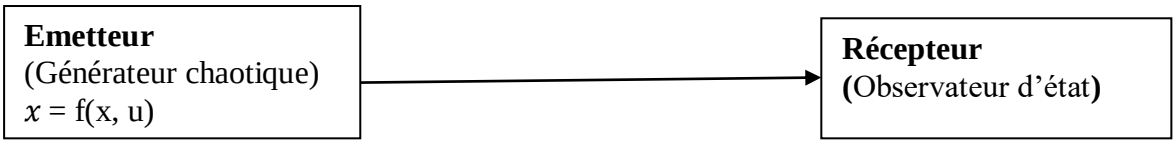


Figure II.6. Principe de la synchronisation à base d'observateur

La synchronisation peut également être réalisée en employant un observateur .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 **[23].**

II.5.Propriétés des systèmes de communication a base du chaos :

Dans cette partie, des propriétés des systèmes de communication chaotiques seront étudiées et comparées aux propriétés des systèmes classiques.

II.5.1.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 **[24].**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.

II.5.2.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 **[24].**

II.6. Implémentation analogique simple :

Les systèmes de communication à base du chaos peuvent être implémentés en utilisant des dispositifs électriques ou optiques. Dans les schémas traditionnels par exemple, la transmission par saut de fréquences nécessite la numérisation des données, ceci impliques des circuits indépendants plus complexes **[24].**

II.7.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 **[25].**

II.8. 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 **[26].**

II.9.Méthodes de cryptage chaotique :

Les systèmes chaotiques constituent une classe particulière de systèmes non linéaires, il est donc possible de leur appliquer toutes les méthodes relatives aux systèmes non linéaires. 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.

II.9.1 Cryptage par addition :

Avec cette méthode, le message confidentiel est additionné à un signal chaotique (la Sortie d'un système chaotique), et le signal résultant est envoyé au récepteur, et par exemple le système de Pecora et Carroll. Dans cette classe deux canaux de transmission sont nécessaires, l'un pour la synchronisation et l'autre pour le signal de transmission. En conséquence, après la synchronisation le message confidentiel peut être récupéré par une simple opération de soustraction entre la sortie du récepteur et le signal émis sur le canal public **[27]**.

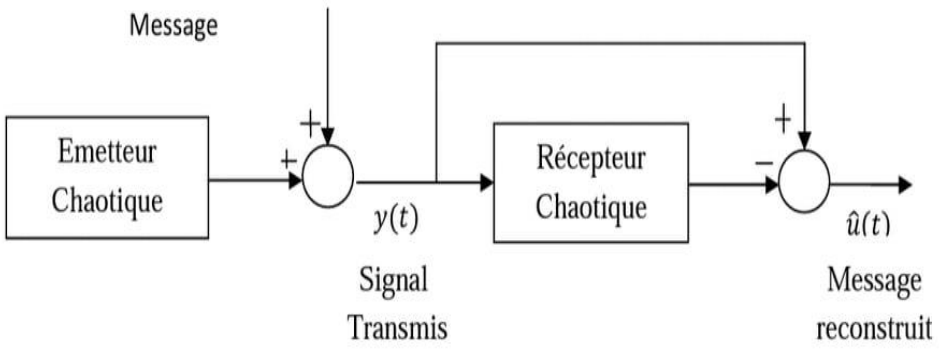


Figure II.7. Principe de cryptage par addition

II.9.2 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].**

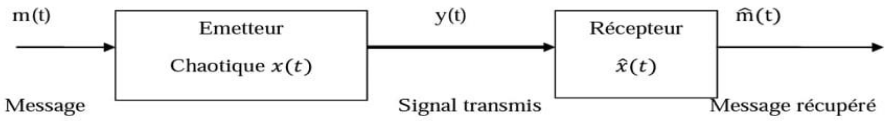


Figure II.8.Principe de cryptage par inclusion.

II.9.3 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.9)** 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

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 **[28].**

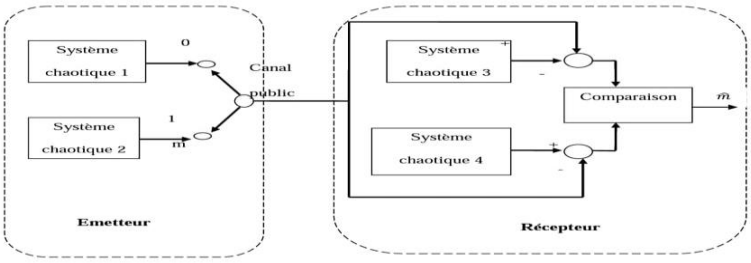


Figure II .9. Principe de cryptage par communication.

II.9.4 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.10)** 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"**[29].**

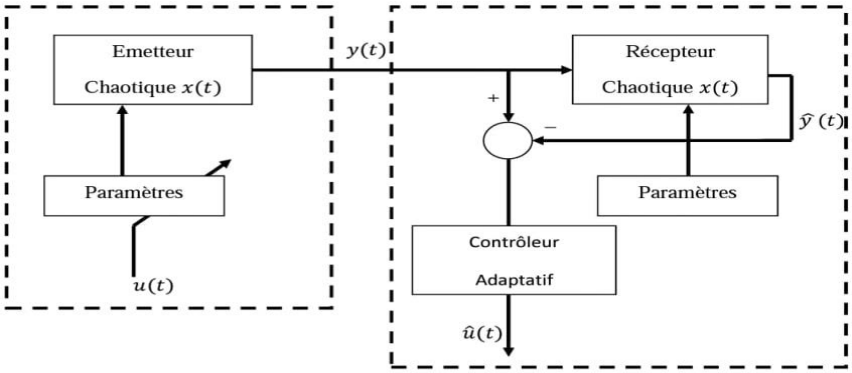


Figure II.10. Principe de cryptage par modulation

II.9.5 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.11) [29].**

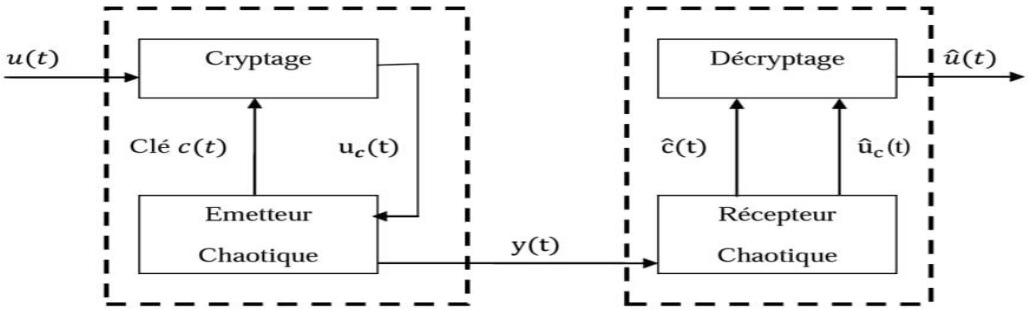


Figure II.11. Principe de cryptage par mixte

II.9.6 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 $y2$, 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 $y2$ 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 **[30].**

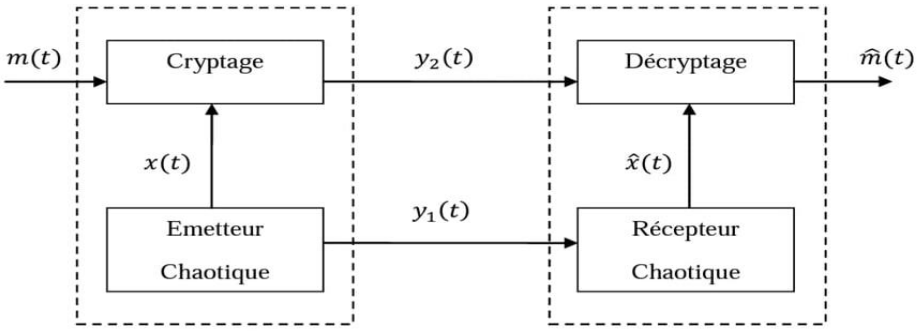


Figure II.12.Principe de cryptage par deux voix

II.10. 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 **[26].**

II.11. Définition Cryptographie :

Le mot cryptographie est un terme générique désignant l'ensemble des techniques permettant de chiffrer des messages, c'est-à-dire permettant de les rendre inintelligibles sans une action spécifique. Le verbe crypter est parfois utilisé mais on lui préfèrera le verbe chiffré. Le fait de coder un message de telle façon à le rendre secret s'appelle chiffrement. La méthode inverse, consistant à retrouver le message original, est appelée déchiffrement

Le chiffrement se fait généralement à l'aide d'une clef de chiffrement, le déchiffrement nécessite quant à lui une clef de déchiffrement. On appelle clé une valeur utilisée dans un algorithme de cryptographie, afin de chiffrer une donnée.
On distingue généralement deux types de clefs :
Les clés symétriques: il s'agit de clés utilisées pour le chiffrement ainsi que pour le déchiffrement. On parle alors de chiffrement symétrique ou de chiffrement à clé secrète.
Les clés asymétriques: il s'agit de clés utilisées dans le cas du chiffrement asymétrique (aussi appelé chiffrement à clé publique). Dans ce cas, une clé différente est utilisée pour le chiffrement et pour le déchiffrement.

Les clés doivent être stockées de manière sécurisée et de manière à ce que seul leur propriétaire soit en mesure de les atteindre et de les utiliser.

II.11. 1.Buts de la cryptographie :

La cryptographie permet de résoudre quatre problèmes différents :

- **La confidentialité**. Le texte chiffré ne doit être lisible que par les destinataires légitimes. Il ne doit pas pouvoir être lu par un intrus.
- **L'authentification**. Le destinataire d'un message doit pouvoir s'assurer de son origine. Un intrus ne doit pas être capable de se faire passer pour quel qu'un d'autre.
- **L'intégrité.** Le destinataire d'un message doit pouvoir vérifier que celui-ci n'a pas été modifié en chemin. Un intrus ne doit pas être capable de faire passer un faux message pour légitime.
- **Le non répudiation**. Un expéditeur ne doit pas pouvoir, par la suite, nier à tort avoir envoyé un message.

II.11. 2.Mécanismes de la cryptographie :

Un algorithme de cryptographie ou un chiffrement est une fonction mathématique utilisée lors du processus de cryptage et de décryptage. Cet algorithme est associé à une clef (un mot, un nombre, ou une phrase). Afin de crypter une donnée avec des clés différentes le résultat du cryptage variera également. La sécurité des données cryptées repose entièrement sur deux éléments : l'invulnérabilité de l'algorithme de cryptographie et la confidentialité de la clef.

Un système de cryptographie est constitué d'un algorithme de cryptographie, ainsi que de toutes les clefs et tous les protocoles nécessaires à son fonctionnement.

II.11. 3.La cryptographie classique :

II.11. 3.1. La cryptographie par substitution mono alphabétique :

Le codage par substitution mono-alphabétique (on dit aussi les alphabets désordonnés) est le plus simple à imaginer. Dans le message clair, on remplace chaque lettre par une lettre différente.

II.11. 3.2. La cryptographie par substitution poly alphabétique :

Cet algorithme de cryptographie comporte beaucoup de points forts. Il est très facile d'utilisation, et le décryptage est tout aussi facile si on connait la clé. Il suffit, sur la colonne de la lettre de la clé, de rechercher la lettre du message codé. A l'extrémité gauche de la ligne, on trouve la lettre du texte clair.

II.12. Algorithmes de la cryptographie :

II.12. 1.Algorithmes symétriques (clef secrète) :

Un algorithme symétrique est un algorithme qui permet de transformer un texte en clair en texte chiffré en utilisant une clé et de retransformer le texte chiffré en texte en clair en utilisant la même clé.

Le secret de la communication est uniquement assuré par la clé qui est utilisée lors de la phase de chiffrement et de déchiffrement. L'algorithme utilisé ne fait pas partie du secret.

On parle d'algorithmes symétriques car c'est la même clé qui sert à la fois au chiffrement et au déchiffrement du message.

Figure II.13.Principe de l'algorithme symétrique

II.12. 2.Algorithmes asymétriques (clef publique) :

Les algorithmes symétriques vus sont tous fiables mais ils posent un problème, c'est celui de l'échange de la Clé :

Comment transmettre de manière fiable à mon interlocuteur la clé de chiffrement utilisée pour chiffrer le message que je lui envoie? Il y a bien sûr le téléphone, mais il y a aussi les écoutes téléphoniques Les algorithmes asymétriques ont été inventés pour pallier précisément le problème de transmission sécurisée de la clé.

On parle d'algorithmes asymétriques car ce n'est pas la même clé qui sert au chiffrement et au déchiffrement. Dans le cas de ces algorithmes, on parlera alors de clé privée et de clé publique. Ces deux clés, clé privée et clé publique, sont intimement liées par une fonction mathématique complexe.

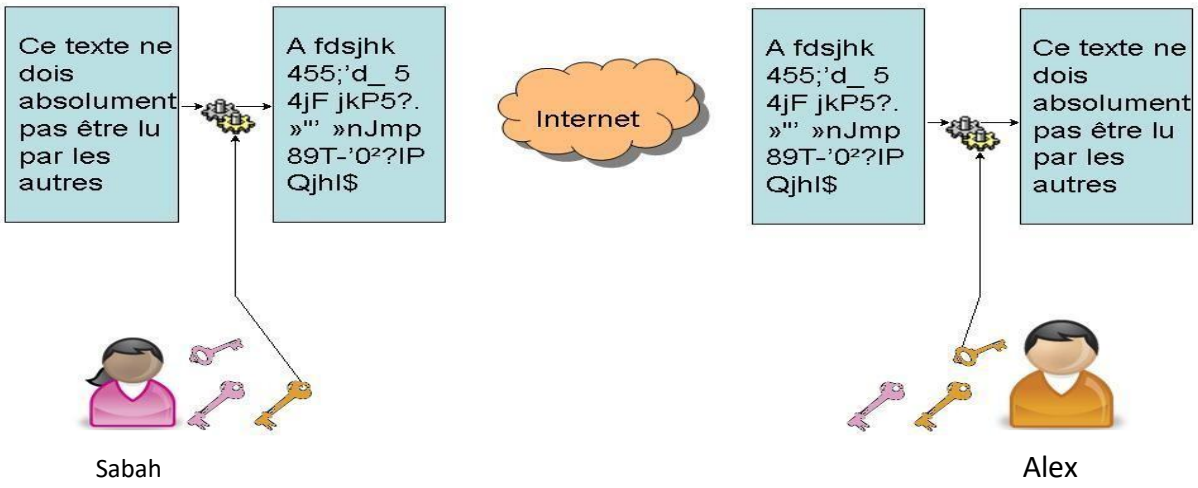


Figure II.14.Chiffrement avec l'algorithme asymétrique

Donc pour résumer :

- L'émetteur chiffre avec la clé publique du destinataire, le destinataire déchiffre avec sa clé privée.
- L'émetteur signe avec sa clé privée, le destinataire vérifie la signature avec la clé publique de l'émetteur.

II.13.Cryptage symétrique vs cryptage asymétrique :

Cryptage symétrique :	***Cryptage asymétrique :***
-Chiffrement à clé privé (utilisation une clé pour crypter qui fonctionne aussi pour décrypter -Très facile -Très rapide -les clés de chiffrement symétrique doivent être conservées en toute sécurité - vous devez vous assurer que chaque personne qui a besoin de la clé, il obtient sans aucun risque de le sortir.	-Chiffrement à clé publique (utilisation deux clés un pour crypter **clé publique** et autre pour décrypter **clé privé** -Difficile par rapport au cryptage symétrique -Plus lent -les clés publiques qu'ils utilisent sont sans danger pour être publié n'importe où parce que pour obtenir la clé privée à partir d'une clé publique peut prendre des centaines d'années de travail.

Tableau II.1. Correspondance entre cryptage symétrique et cryptage asymétrique.

II.14. Comparaison entre chaos et cryptographie :

Les techniques de chiffrage basées sur le chaos, fournissent une bonne combinaison de vitesse, de haute sécurité, de complexité, de frais généraux raisonnables de calcul et de puissance de calcul, etc. Plusieurs propriétés font des systèmes chaotiques, des candidats attrayants pour la sécurité des communications. Nous pouvons citer entre autres un spectre à large bande, des trajectoires qui ne repassent jamais par le même état, un aspect pseudo-aléatoire (comme du bruit par exemple), une implémentation relativement simple des systèmes chaotiques. De plus, depuis les années 90, plusieurs chercheurs ont noté qu'il existe un rapport intéressant entre le chaos et la cryptographie. En effet, plusieurs propriétés des systèmes chaotiques présentent des correspondances similaires ou presque, avec des systèmes cryptographiques traditionnels. Le tableau suivant illustre parfaitement cette correspondance.

Théories du chaos	**Cryptographie**
Système chaotique	Système pseudo-aléatoire
Transformation non linéaire	Transformation non linéaire
Nombre infini d'états	Nombre fini d'états
Nombre infini d'itérations	Nombre fini d'itérations
État initial	Plaintext
État final	Cipher text
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 : Correspondance entre la théorie du chaos et la cryptographie.

II.15. Cryptanalyse :

La cryptanalyse est l'étude des probabilités de succès des attaques possibles sur les systèmes cryptographiques afin de déterminer leurs éventuelles faiblesses **[33].** L'un des principaux objectifs de la cryptanalyse est de tester si un adversaire peut déchiffrer le texte clair ou récupérer la clé secrète. Pour cela, il est nécessaire de se mettre à la place de l'adversaire ou pirate.

La cryptographie et la cryptanalyse sont deux domaines d'études évoluant en parallèle. En effet, de nouveaux systèmes de chiffrement, toujours plus complexes, sont conçus pour remplacer ceux qui ont été éliminés par la cryptanalyse et de nouvelles techniques de cryptanalyse sont inventées pour tester ces nouveaux systèmes. Le problème de la

cryptographie est de concevoir des systèmes sûrs et de faire en sorte que la durée nécessaire à un intrus pour déchiffrer l'information soit supérieure à sa durée de validité.

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.il existe différentes attaques qui peuvent avoir lieu sur les systèmes cryptographiques. Dans ce qui suit nous citerons les attaques les plus fréquentes **[24].**

II.16.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.15**.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.

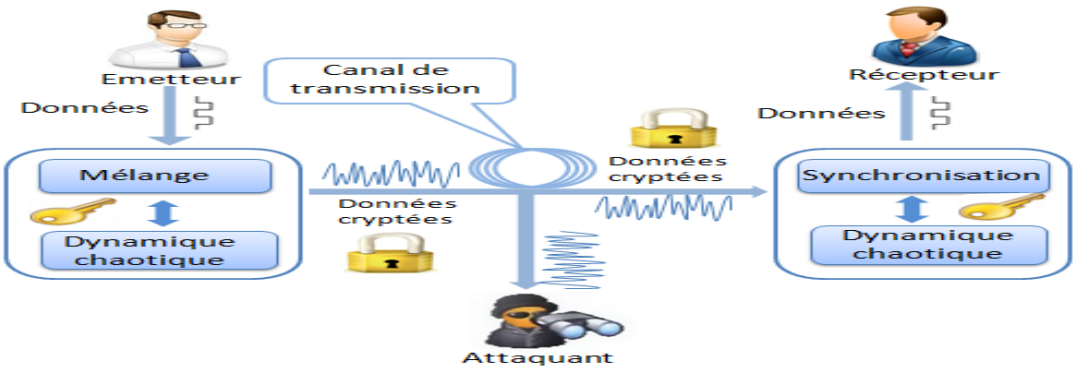


Figure II.15. Principe de Chiffrement par Chaos.

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 **[31][32].**

II.17. Conclusion :

L'objectif principal de ce chapitre était de définir La synchronisation des systèmes chaotiques, nous donne accès à la réalisation des différents systèmes permettant d'effectuer une transmission sécurisée d'information. Pour 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.

On présente la cryptologie en générale et la cryptographie par chaos avec son principe et son objectif.

CHAPITRE III APPLICATION DE LA FONCTION LOGISTIQUE POUR LA SECURISATION DES DONNEES

III.1.Introduction :

Le chaos apparue au début des années soixante en météorologie, elle s'est rapidement étendue à peu près toutes les sciences. C'est en 1963, qu'Edward Lorenz, météorologiste au M.I.T, découvrit un exemple concret d'un système dynamique simple présentant un comportement complexe **[34].** Les chercheurs essayent d'apporter de nouvelles idées et techniques qui utilisent la nature elle même du chaos afin de le contrôler **[35].** Les phénomènes chaotiques que l'on observe sont souvent dus aux non linéarités que présentent les systèmes, dans des domaines très variés : mécanique, circuits électroniques, réactions chimiques, dynamique des fluides, processus biologiques et systèmes de sécurité de l'information.

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.

La fonction logistique peut être utilisée pour illustrer l'état d'avancement de la diffusion d'une innovation durant son cycle de vie. Historiquement, lorsque de nouveaux produits sont introduits, une intense phase de recherche et de développement permet une amélioration spectaculaire de la qualité et une réduction des coûts créées par Pierre François Verhulst. Chargé par son professeur. 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 *3* 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

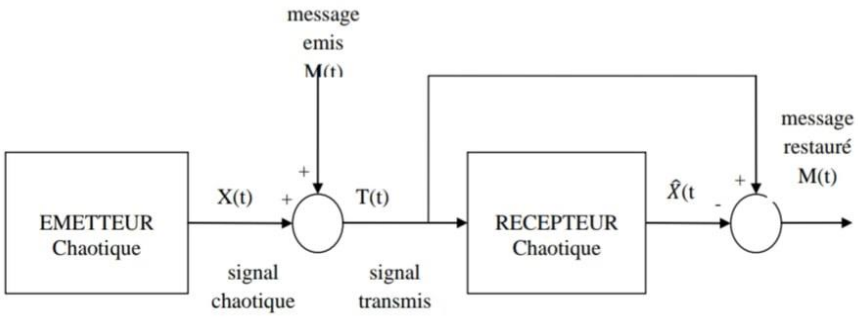


Figure III.1.Schéma présentatif de la technique de masquage chaotique

Le système de transmission proposé est constitué de deux bloques :

- **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.

- **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. La fonction logistique :

En mathématiques, la fonction logistique est une fonction polynômiale, souvent citée comme exemple de la complexité pouvant surgir de simples équations non-linéaires. Cette fonction fut popularisée par le biologiste Robert May en 1976.
Le modèle logistique fut introduit initialement en tant que modèle démographique par Pierre François Verhulst. Il écrit en 1845 dans son ouvrage consacré à ce phénomène : *nous donnerons le terme de logistique à cette courbe*. L'auteur n'explique pas ce choix mais "logistique" a un lien avec les logarithmes : les deux termes étaient synonymes au XVIIIe siècle et *logistikos* signifie "calcul" en grec.

III.4.Système de chiffrement à base d'une carte logistique :

Dans ce mémoire, on va utiliser une carte logistique discrète pour chiffrer le signal informationnel, la méthode de cryptage par addition est utilisée. Le schéma synoptique du système est représenté dans **Figure (III.2).**

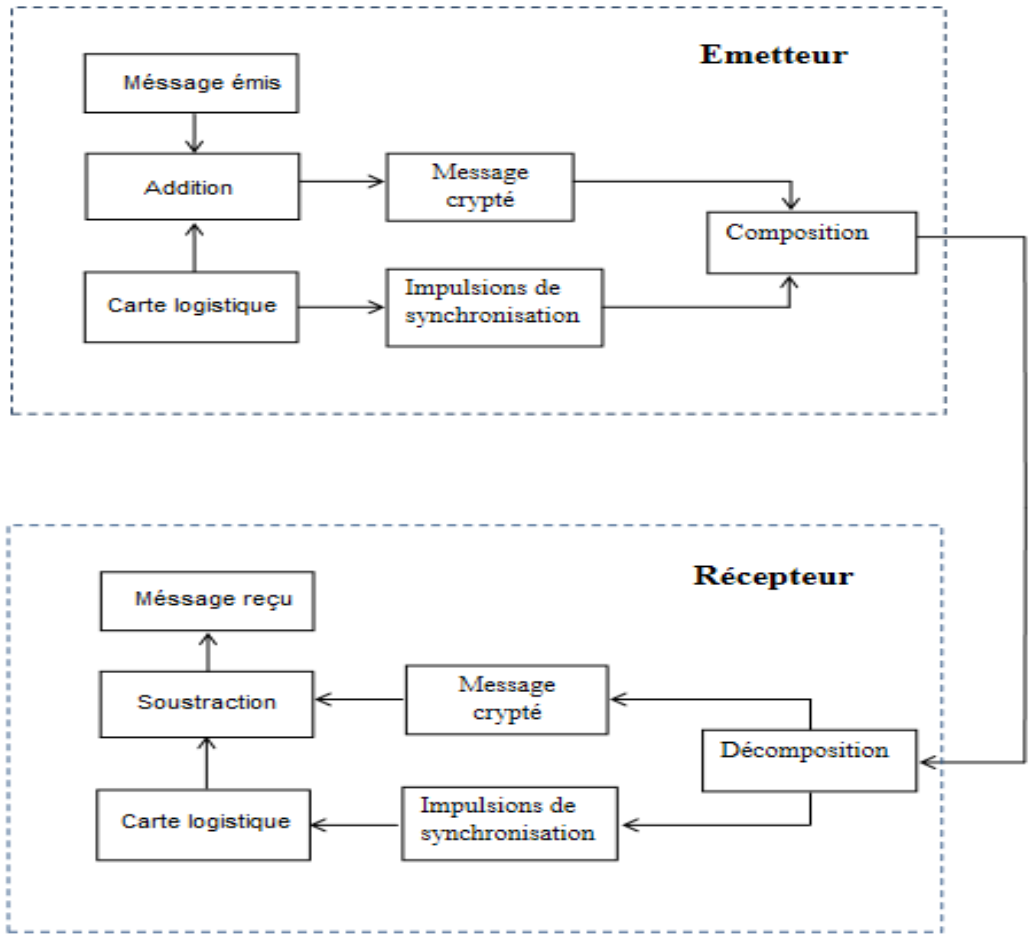


Figure III.2. Schéma synoptique du système de cryptage par carte logistique

Une carte logistique est utilisée pour générer un signal chaotique, le message informationnel est additionné au signal chaotique pour obtenir le signal crypté qui sera transmis avec les impulsions de synchronisation au récepteur via un canal de transmission non sécurisé.

L'opération inverse est effectuée au niveau du récepteur, après récupération des impulsions de synchronisation, le signal chaotique est régénéré, le message crypté est soustrait du signal chaotique afin de récupérer le message informationnel.

III.4.1. Modélisation d'une suite logistique par un circuit électronique :

Un circuit de modélisation d'une suite logistique a été proposé par MADHEKAR SUNEEL, le schéma synoptique du circuit est donné à la **Figure(III.3).**

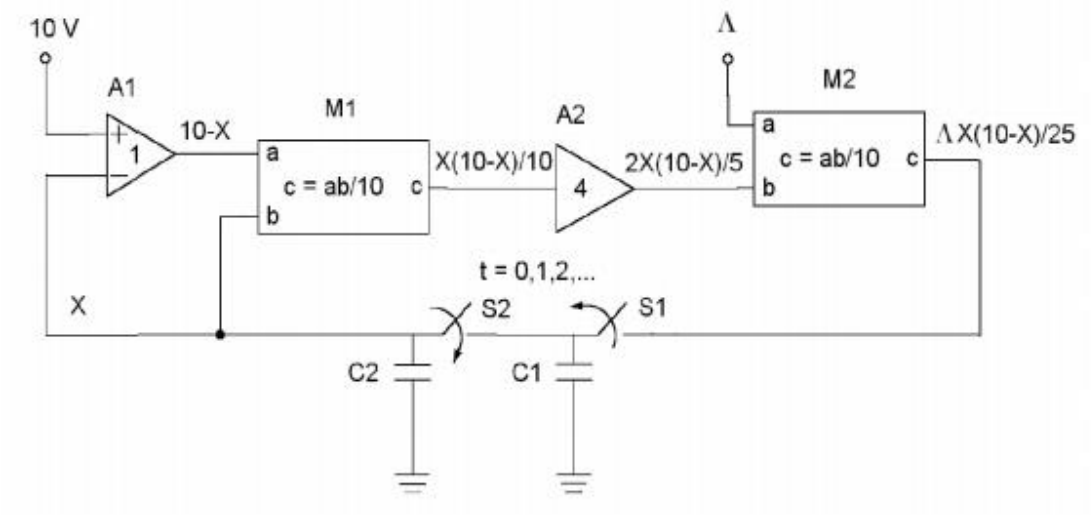


Figure III.3. Schéma synoptique du circuit électronique d'une suite logistique [37]

Dans ce schéma, A1 est un amplificateur unitaire (de gain égal à 1), M1 et M2 sont deux multiplicateurs analogiques, A2 est un amplificateur linéaire de gain égal à 4. Une des entrées de M2 est la tension continue égal à A. S1 et S2 sont deux interrupteurs constituants un convertisseur analogique-digitales et qui fonctionnent de telle sorte que si l'un d'eux est ouvert, l'autre est fermé et vice-versa. La dernière valeur de X est obtenue en fermant S1. Ce circuit permet d'obtenir les équations suivantes :

$$\mathrm{X(k+1)} = \mathrm{X(k)(10 - X(k))/25} \qquad \textbf{(III.1)}$$

Cette équation se transforme facilement en une suite logistique :

$$x(k+1) = \lambda x(k)(1 - x(k)) \qquad \textbf{(III.2)}$$

$$X = 10x, A = 2.5\lambda \qquad \textbf{(III.3)}$$

L'implémentation de ce schéma synoptique est donnée à la **Figure (III.4)**, cette implémentation est réalisée en utilisant des composants analogiques tels que les ampli-op (LM1458), les multiplicateurs (MPY634). Le convertisseur analogique-digitale est implémenté en utilisant le circuit intégré LF398. Un générateur de signaux carrés basé sur le circuit NE555 est utilisé pour contrôler S1, ce signal carré est inversé afin de contrôler le deuxième interrupteur S2. L'inverseur utilisé est à base d'un transistor 2N3904.

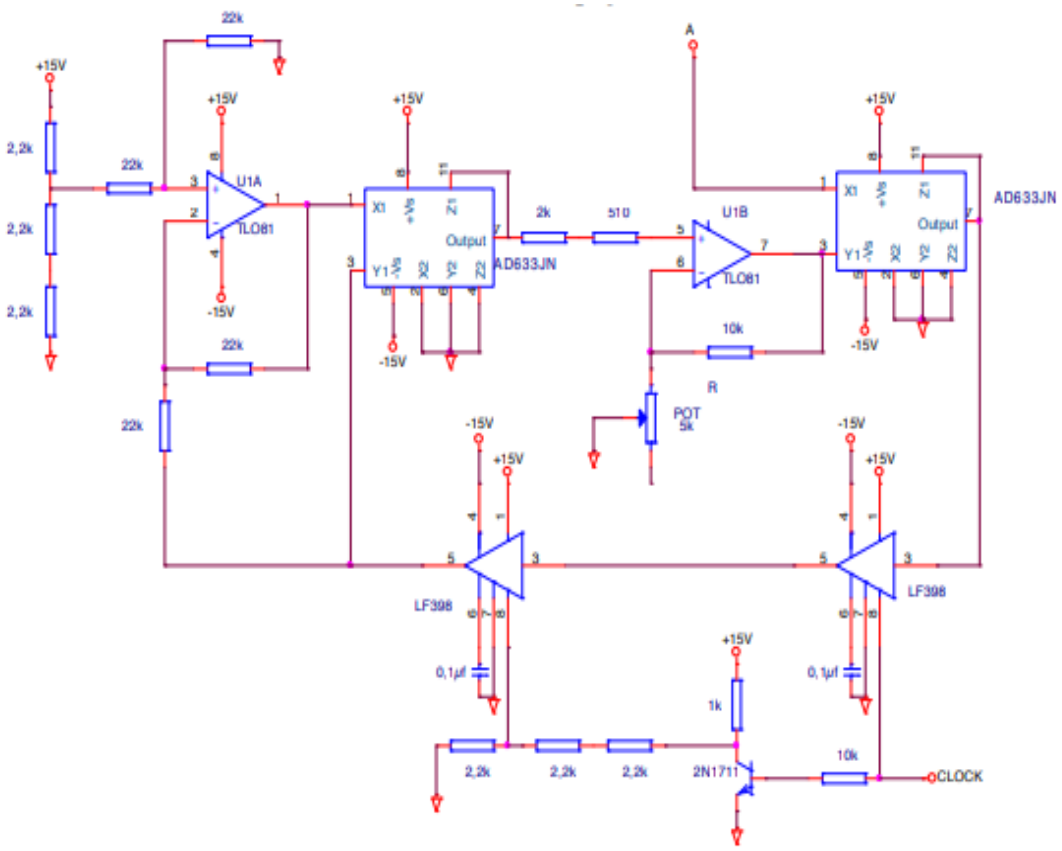


Figure III.4.Schéma du circuit électronique modélisant une suite logistique [37]

III.4.2 .Simulation de la fonction logistique :

Nous pouvons constater que pour (1 < r < 3), toutes les conditions initiales (0 <x_0 <1) convergent à la position p=a, (a est un point attracteur correspond à l'intersection de la parabole de la fonction logistique avec la droite y = x).

- Si r = 2, la trajectoire converge au point p=0.5, à partir de r = 3, après la disparition du comportement transitoire, un changement important est constaté, x prend maintenant deux positions d'équilibre qui se commutent alternativement, p1 = 0.6503 et p2 = 0. 6823 (x_0=0.3 et x_0=0.4).
- Pour r>3, un autre doublement de période est apparu x prend maintenant quatre positions d'équilibre. Et ainsi de suite jusqu'à l'apparition de chaos.

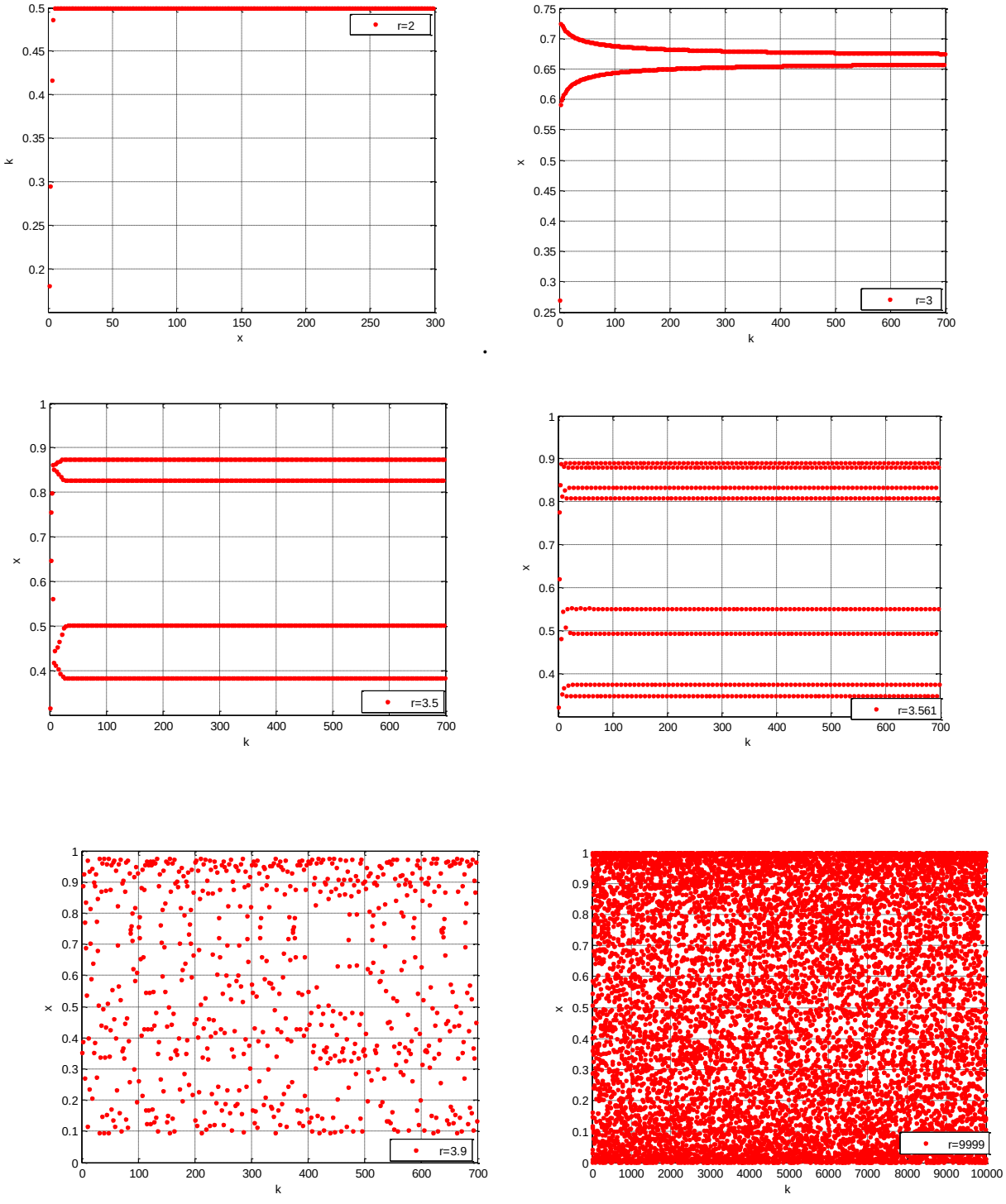


Figure III.5. Comportement dynamique de la fonction logistique pour différentes valeurs du paramètre r.

Cette variation du régime linéaire (un seul état d'équilibre) en régime non linéaire, passant par une valeur parfaitement définie du paramètre r où il y en a deux états d'équilibre (doublement de période), s'appel "bifurcation".

Lorsque r tend vers 4, on voit clairement que l'évolution de x_{n+1} donne un comportement totalement chaotique du fait de la succession de bifurcation.

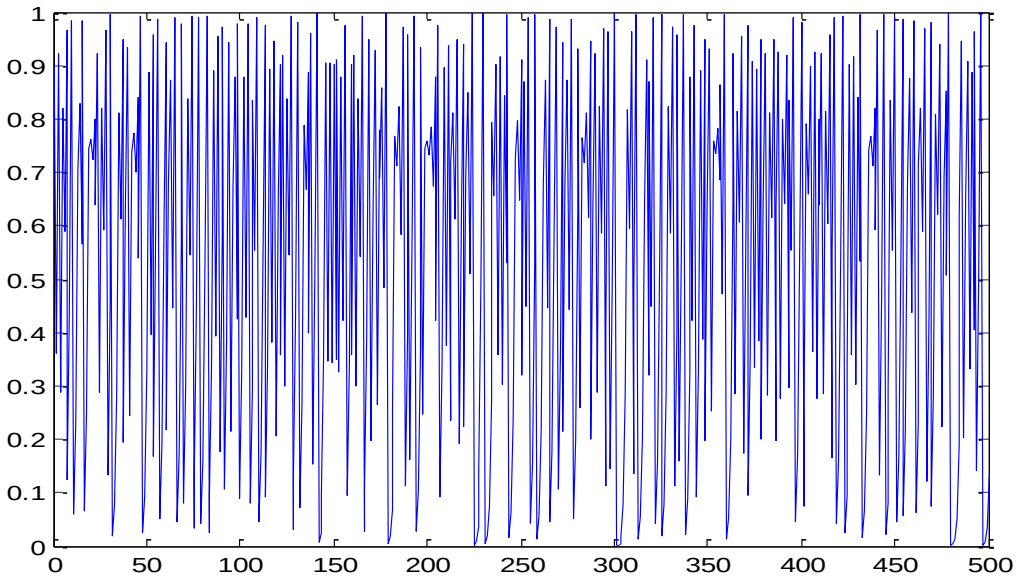


Figure III.6. Signal chaotique généré par une carte logistique avec x(0)=0.8999, $\mu = 3.9998$

On remarque bien que le signal est parfaitement aléatoire. la **Figure (III.7)** est un zoom du signal x(t) pour mieux voir le caractère aléatoire du signal

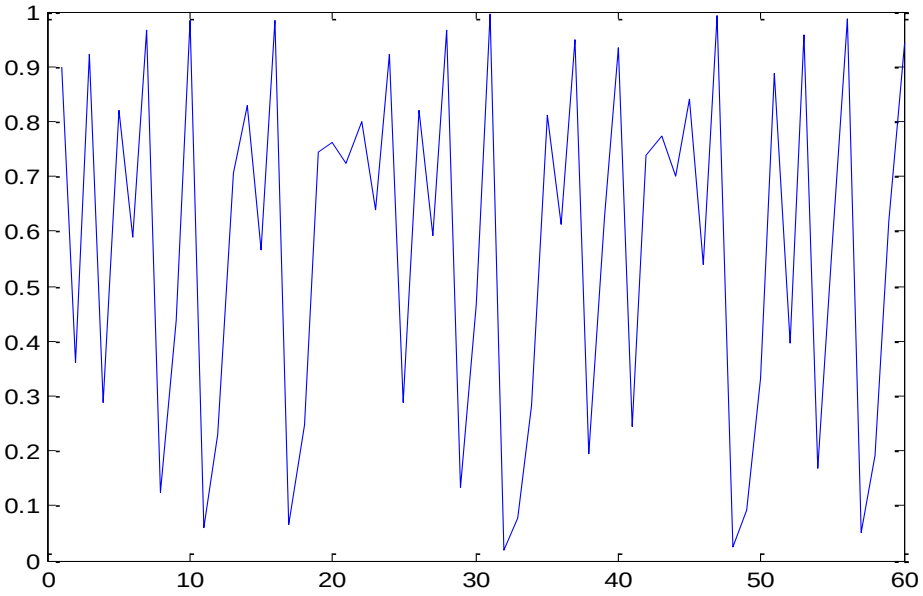


Figure III.7. Signal chaotique généré par une carte logistique après zoom avec x(0)=0.8999, $\mu = 3.9998$

La valeur moyenne du signal chaotique est calculée en utilisant la fonction mean de MATLAB, ce qui donne :

Valeur moyenne = 0.5315

Cette valeur très proche de 0.5 montre que le générateur chaotique utilisé est très sécurisé, les valeurs ainsi généré ont tous la même probabilité d'occurrence.

III.4.3.Cryptage par fonction logistique :

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 est le suivant :

Considérons les deux systèmes suivants :

$$\dot{x} = f1(x,u)$$
$$\dot{\hat{x}} = f2(\hat{x},u) \qquad \textbf{(III.4)}$$

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 $e$est :

$$e = |\hat{x}(t) - x(t)| \rightarrow 0 \; quand \; t \rightarrow \infty \qquad \textbf{(III.5)}$$

III.4.4 Simulation et résultats :

Pour tester la synchronisation d'une communication sécurisée par carte logistique, nous avons utilisés un signal carré présenté dans la **Figure (III.8)** suivante :

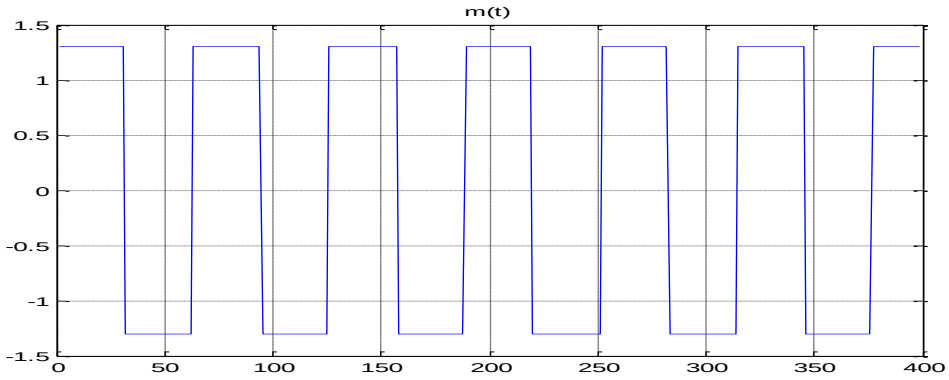


Figure III.8. Signal émis m(t) original

Figure (III.9) donne l'allure du signal chaotique x(t), le signal émis m(t) et le signal crypté s(t) :

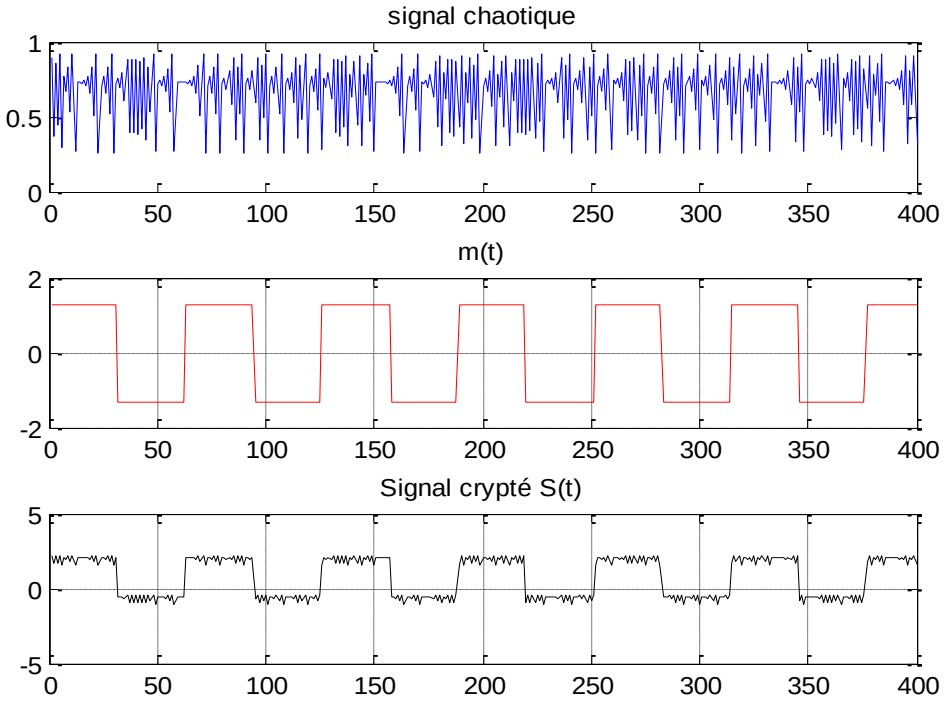


Figure III.9. Allure du signal chaotique x(t), le signal émis m(t) et le signal crypté s(t)

Au niveau de la réception, l'erreur entre le signal original et le signal reçu est donné par les **Figures (III.10)** et **(III.11)** suivantes. La première figure concerne le cas où il n'y a pas une synchronisation et dans la deuxième figure, les deux signaux sont synchronisés.

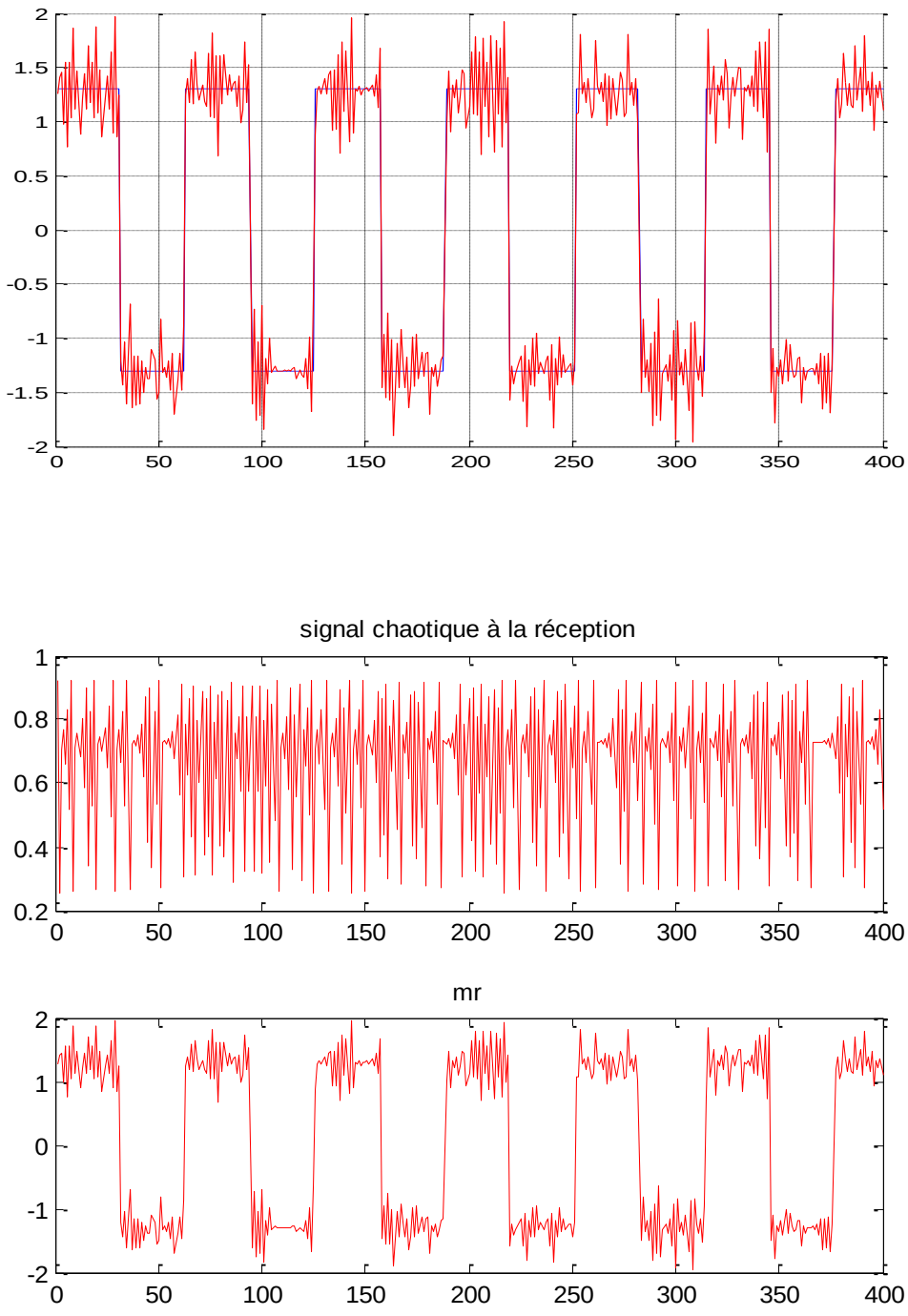


Figure III.10. Signal chaotique généré par la fonction logistique et Le signal reçu sans synchronisation

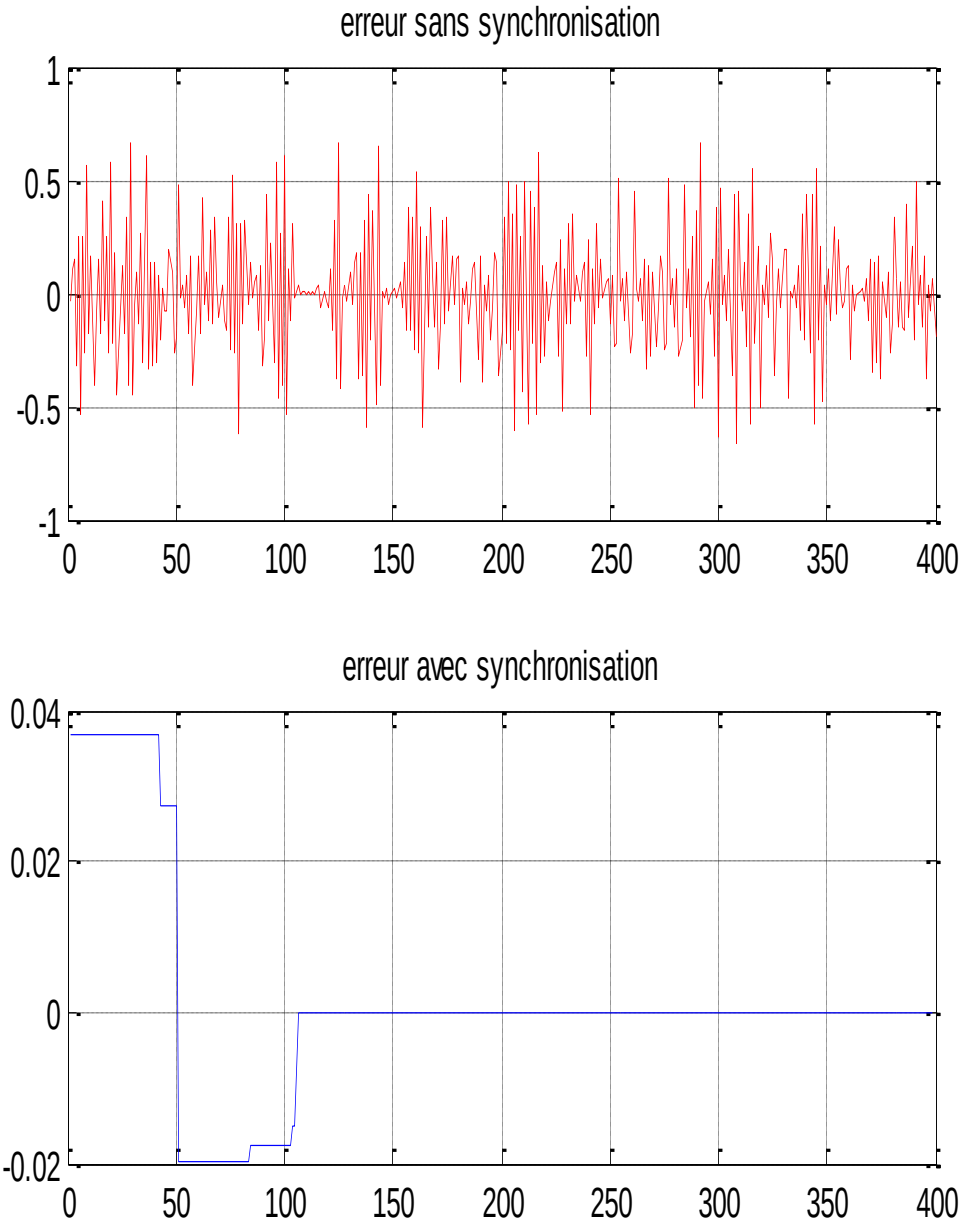


Figure III.11. L'erreur avant et après synchronisation

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, voir **Figure (III.12).**

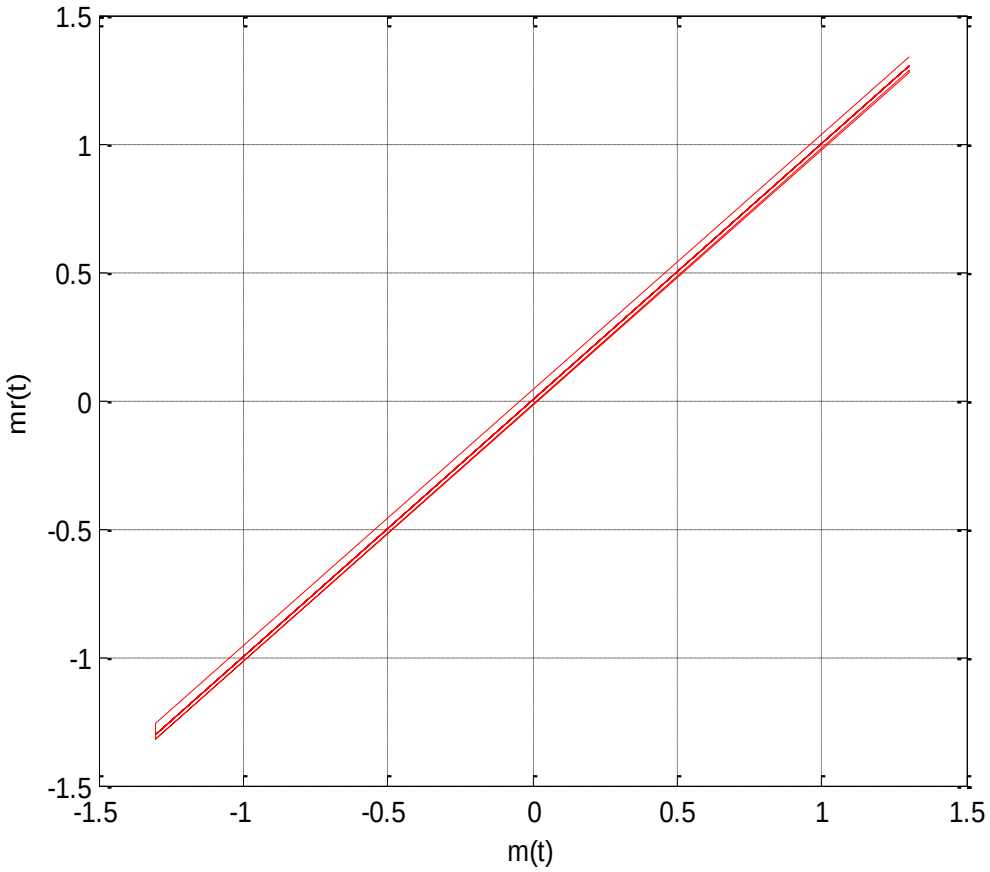


Figure III.12.Synchronisation des deux circuits

$$m(t) = 0.5\cos(0.1t) * \cos(0.01t) * (cos0.01t)$$

2 éme cas.

Pour ce 2éme cas, on utilise le signal informationnel émis,

Avec A : amplitude du signal, f : fréquence du signal voir **Figure (III.13)**

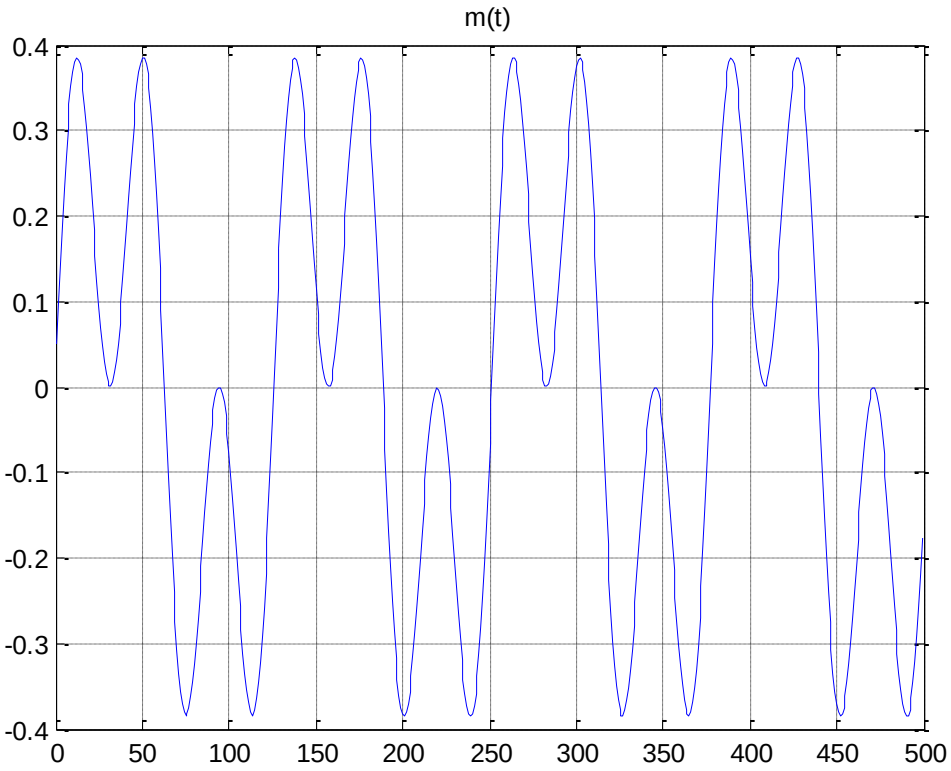


Figure III.13. Signal émis

la **Figure (III.14)** représente le signal chaotique généré par la carte logistique

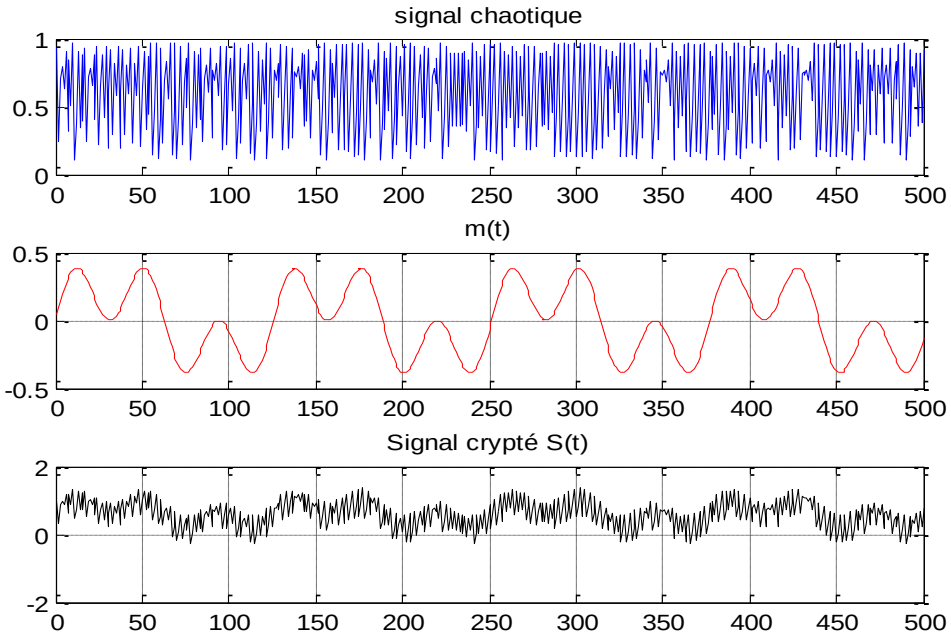


Figure III.14. Signal chaotique généré par une carte logistique avec x(0)=0.8999, $r = 3.89$

L'addition des deux signaux permet d'obtenir le signal crypté qui sera transmis au récepteur, voir **Figure (III.15).**

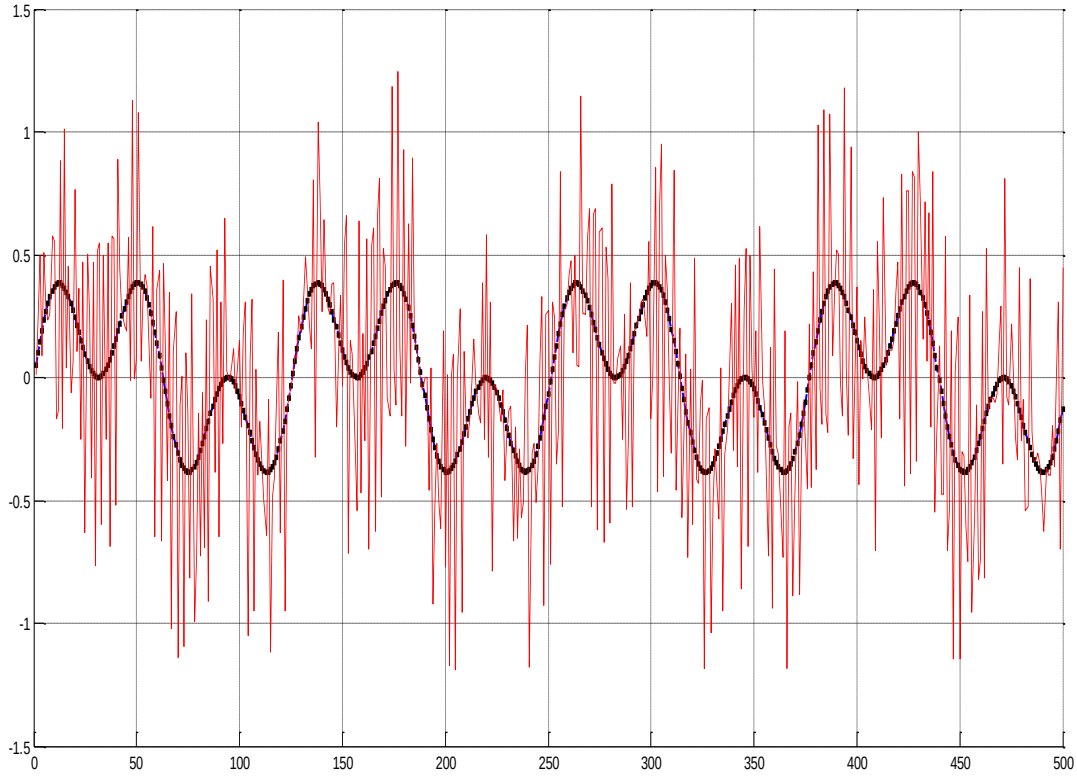


Figure III.15. Allure du signal chaotique x(t), le signal émis m(t) et le signal crypté s(t)

On remarque que le signal informationnel émis est complètement brouillé et la reconnaissance du signal original est très difficile sans connaitre les paramètres de la carte logistique utilisée pour le cryptage du signal.

Décryptage du signal reçu

Le décryptage au niveau du récepteur est très simple à réaliser. Une simple soustraction entre le signal reçu et le signal chaotique régénéré en synchronisation avec l'émetteur permet d'obtenir le signal décrypté.

La **Figure (III.16)**, représente le signal reçu, le signal chaotique et le signal décrypté respectivement avec synchronisation.

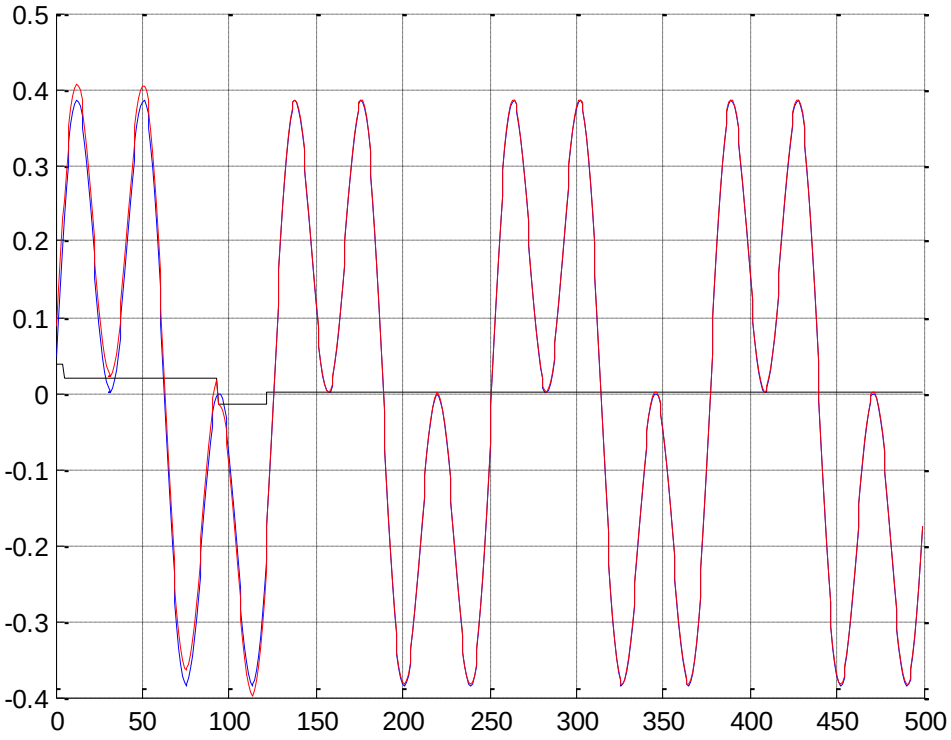
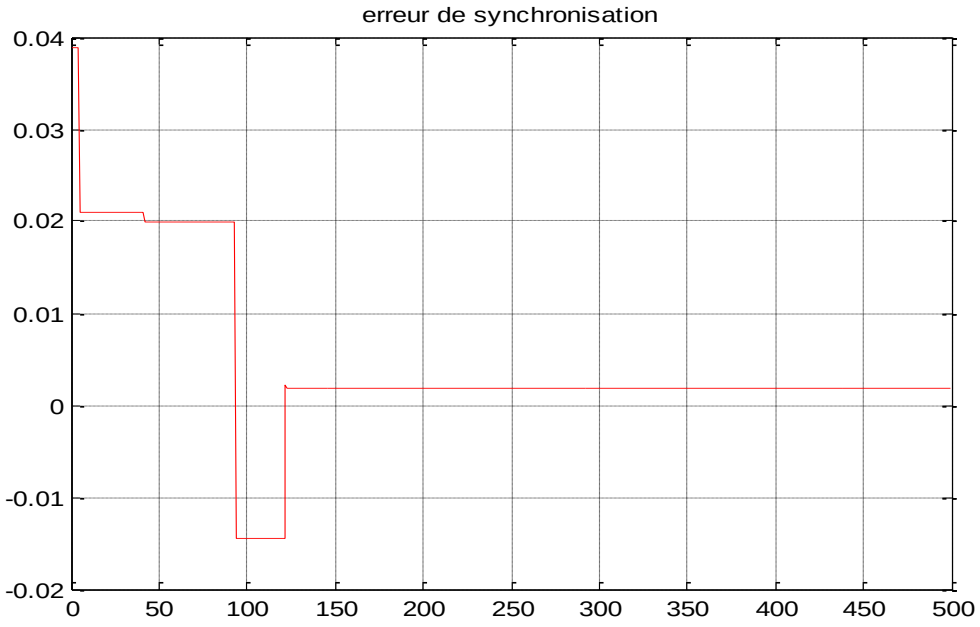


Figure III.16. L'allure du signal original m(t), le signal récupéré m(t) et l'erreur de synchronisation.

Le signal décrypté est ainsi similaire au signal émis. Dans cette simulation on n'a pas pris en considération les différents bruits introduits par le cana de transmission.



III.5. Conclusion :

A travers cette simulation, nous avons défini le circuit de la carte logistique 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 nous sommes intéressées par l'efficacité de la synchronisation. Nous avons également étudié les différentes possibilités qui offrent le chaos à travers ses propriétés adaptées au cryptage des signaux afin de sécuriser la transmission des données. Dans le cas du cryptage chaotique, l'émetteur et le récepteur ont les mêmes paramètres qui jouent le rôle de la clef de chiffrement.

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

CONCLUSION GENERALE

Conclusion générale :

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 ce chapitre, nous avons aussi 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 électronique d'une suite logistique, 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.

BIBLIOGRAPHIE

Bibliographie :

[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] O.Megherbi, " Etude et réalisation d'un système sécurisé à base de systèmes chaotiques", Thèse de magister, Université Mouloud Mammeri Tizi-Ouzou, Algérie, 2013.

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

[6] L. Kocarevet, S. Lian, «haos-BasedCryptography»: Theory, Algorithms and Applications, Springer, 2011.

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

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

[9] M. L'HERNAULT-ZANGANEH, Faisabilitè d'un système d'èmission-rèception analogique pour les communications sècurisèes par le chaos, Thèse de Doctorat ; Université de Paris 6,2007.

[10] A. R. KIHAL, Système chaotique pour la transmission sécurisée de donnée, *Mémoire de magister, Université Mohammed Khider, Biskra, 2013.*

[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 MouloudMammri de Tizi-Ouzo.

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

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

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

Canada, 2004.MEMOIRE DE MAGISTER.UNIVERSITE MOULOUD MAMMERI TIZI-OUZOU.2013.

[16]L.M. Pecora, T.L.Caroll."Synchronization in chaotic systems" *PHYSICAL REVIEW LETTERS*, February 19, 1990:821-825.MEMOIRE DE MAGISTER.UNIVERSITE MOULOUD MAMMERI TIZI-OUZOU.2013.

[17]T.Yamada, H.Fujisaka."Stabilitytheoryofsynchronizedmotionincoupledoscillator" *Progress of Theoretical Physics*, 1983: 32-47.MEMOIRE DE MAGISTER.UNIVERSITE MOULOUD MAMMERI TIZI-OUZOU.2013.

[18]K.M.Cuomo, A.V. Oppenheim, S.H. Strogatz."Synchronization of Lorenz-based chaotic circuits with applications to communications" *IEEE Transactions on Circuits and Systems II*, 1993:626-633.MEMOIRE DE MAGISTER.UNIVERSITE MOULOUD MAMMERI TIZI-OUZOU, 2013.

[19] G. Kolumbán, M.P. Kennedy, L.O.Chua."The role of synchronization in digital communications using chaos - part I: Fundamentals of digital communications"*IEEE Transactions on Circuits and Systems I*, 1997: 927-936.MEMOIRE DE MAGISTER.UNIVERSITE MOULOUD MAMMERI TIZI-OUZOU.2013.

[20] G. Kolumbán, M. P. Kennedy, L. O. Chua. "The role of synchronization in digital communications using chaos - part II: chaotic modulation and chaotic synchronization." *IEEE Transactions on Circuits and Systems I*, 1998:1129–1140. MEMOIRE DE MAGISTER.UNIVERSITE MOULOUD MAMMERI TIZI-OUZOU.2013.

[21] H. Hamiche.*Inversion à Gauche des Systèmes Dynamiques Hybrides Chaotiques, Applications à la Transmission Sécurisée de Données.* Thèse de Doctorat, Université Mouloud Mammeri de Tizi-Ouzou, 2011. MEMOIRE DE MAGISTER.UNIVERSITE MOULOUD MAMMERI TIZI-OUZOU.2013.

[22] 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.

[23] 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.*

[24] R. Tenny. "Symmetric and Asymmetric Secure Communication Schemes." Thèse de Doctorat, University of California, San Diego, 2003. MEMOIRE DE MAGISTER.UNIVERSITE MOULOUD MAMMERI TIZI-OUZOU.2013.

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

[26] 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.

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

[28] 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.*

[29] 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.*

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

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

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

[33] F. Anstett.*Les systèmes dynamiques chaotiques pour le chiffrement synthèse et cryptanalyse.*2006. MEMOIRE DE MAGISTER.UNIVERSITE MOULOUD MAMMERI TIZI-OUZOU.2013.

[34] E.N Lorenz.Deterministic non periodic flow. M. Almos sci, vol 20, N°2, pp 130-140. 1963. thèse de Doctorat en Sciences. Université LARBI BEN M'HIDI OUM El BOUAGHI.2018

[35] A. Boukabou. Méthodes de contrôle des systèmes chaotiques d'ordre élevé et leur application pour la synchronisation : Contribution à l'élaboration de nouvelles approches. Thése de doctorat. Université de Constantine.2006. Thèse de Doctorat en Sciences. Université LARBI BEN M'HIDI OUM El BOUAGHI.2018

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

[37]http://www.cmls.polytechnique.fr/perso/vlambert/fichiers/La%20suite%20logistique.PDF.

ANNEXE

Annexe :

Algorithme de runge kutta

Pour une équation donnée par :

$u_j=f_j(t, u1, u2,\ldots.. u_m)$ $j=1,2,\ldots\ldots m$

$a<= t <=b$ $u_j(a)= alpha_j j=1,2,\ldots\ldots m$

entrées : (a, b, nombres d'équations m, N, conditions initiales $alpha_1,\ldots alpha_m$)

Sorties : (approximation w_j de $u_j(t)$ pour N+1 valeurs de t)

étape1:
h= (b-a)/N
t=a

étape2: for j=1: m
$w_j=alpha_j$

étape3:sorties (t, w_1, w2,….. w_m)

étape4: for i=1: N

étape5: for j=1: m
k(1,j)=h*fj(t,W1,W2,F,gama,omega);

for j=1:m
k(2,j)=h*fj(t+h/2,W1+0.5*k(1,1),W2+0.5*k(1,2),les données);

for j=1:m
k (3,j)=h*fj(t+h/2,W1+0.5*k(2,1),W2+0.5*k(2,2), les données);

for j=1:m
k (4,j)=h*fj(t+h,W1+k(3,1),W2+k(3,2), les données);

for j=1: m
Wj=Wj+(k(1,j)+2*k(2,j)+2*k(3,j)+k(4,j))/6;

WWj0 (i) =Wj;

t=a+i*h;
end

Sorties; (t, w_1, w2… w_m)

```
tt(i)=t;
```
W1=ww10(i);
Dans notre cas : m=3 ;