الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire
وزارة التعليم العالي و البحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Mohamed Khider – Biskra
Faculté des Sciences et de la technologie
**Département : Génie Electrique**
**Ref :……**

جامعة محمد خيضر بسكرة
كلية العلوم و التكنولوجيا
**قسم:الهندسة الكهربائية**
**المرجع:……**

Mémoire présenté en vue de l'obtention
du diplôme de

## Magister en : Electronique

**Option : Architecture des systèmes**

# SYSTEMES CHAOTIQUES POUR LA TRANSMISSION SECURISEE DE DONNEES

Présenté par :

## Kihal Ahmed Ridha

Soutenu publiquement le 26/11/2013

## Devant le jury composé de :

| Nom & Prénom | Grade | Qualité | Etablissement |
|---|---|---|---|
| Dr. Abdelhamid Benakcha | Maître de conférences | Président | Univ . de Biskra |
| Dr. Mohamed Boumehraz | Maître de conférences | Rapporteur | Univ . de Biskra |
| Dr. Latifa Abdou | Maître de conférences | Examinateur | Univ . de Biskra |
| Dr. Tahar Guesbaya | Maître de conférences | Examinateur | Univ . de Biskra |

*Dédicaces*

*A*

*ma très chère mère qu' Allah la protège ,*

*la mémoire de mon père qu'Allah lui accorde ses miséricordes et son vaste paradis,*

*ma femme et mes enfants Yasmine et Moade ,*

*mes frères et sœurs ,*

*mes enseignants ,*

*mes amis ,*

*mes collègues,*

*je dédie ce modeste travail .*

# *Remerciements*

Je remercie avant tout DIEU Allah tout puissant pour la volonté, la santé et la patience qu'il m'a donné afin de réaliser ce modeste travail.

J'exprime ma plus grande reconnaissance et mon respect à mon encadreur Dr Boumehraz Mohamed pour avoir accepté de diriger ce travail , de m'avoir guidé et soutenu avec patience et indulgence ,pour ces lectures enrichissantes de mon mémoire et pour les précieux conseils qu'il n'a cessé de me prodiguer .

Je tiens également à remercier tous les membres du jury , de l'honneur qu'ils m'ont fait en acceptant d'être membres du jury de ce mémoire et pour l'intérêt qu'ils ont bien voulu porter à mon travail.

Mes sincères remerciements s'adressent aussi à tous mes enseignants à l'université de Biskra depuis l'ingéniorat jusqu'à mes études en poste graduation .

Mes remerciements vont de même à Mr Touba Mostefa Mohamed ,Dr Brima Abdelhafid **,** Dr Sbaa Salim et Mr Ahmide Abderrahmane pour m'avoir si bien reçu dans leurs bureaux et de leur aide administrative .

Merci et reconnaissance à ma très cher sœur Faiza pour sa disponibilité et son aide surtout en matière de traitement de texte .

Un grand merci à mon beau père Mr Djarou Omar et mon collègue à l'INSFP Hassani Bounab de Biskra Mr Khedri d'avoir lu mon mémoire et avoir enlevé les fautes d'orthographe que j'avais laissées.

Je n'omettrai pas de remercier mes collègues de la promotion chacun par son nom pour leurs soutien et conseils .

Merci à mes amies et collègue à l'INSFP Hassani Bounab de Biskra pour leurs encouragements .

Et enfin merci et pardon à tous ceux que je ne peut citer qui m'ont aidé de prés ou de loin .

# Résumé

Les systèmes chaotiques sont des systèmes déterministes non linéaires et très sensibles aux conditions initiales .Les signaux qui évoluent dans ces systèmes sont en général à large bande, ce qui fait apparaître leurs trajectoires comme du bruit pseudo aléatoire .Depuis la découverte de Pecorra et Carroll que deux systèmes chaotiques peuvent se synchroniser, un intérêt significatif a été donné à l'usage de ces systèmes pour sécuriser la communication .Cet intérêt est dû a leur imprévisibilité qui est supérieure à celle des systèmes de sécurité de communications conventionnelles et à leur simplicité d'implémentation . Notre travail est une contribution qui se situe dans le cadre de ce contexte. Ainsi dans ce mémoire après avoir donné un état de l'art sur les systèmes conventionnels de sécurisation de la communication, une étude théorique simulée par ordinateur sur le phénomène chaotique et sa synchronisation sera présentée . Pour aboutir enfin à une application de la sécurisation de la communication par chaos qui est l'objectif de notre travail. Simulations et tests sur deux techniques seront exposées avec analyse des résultats.



**Mots clefs :** Chaos, sécurisation de la communication, synchronisation du chaos, cryptographie, cryptosysteme, cryptage par addition, cryptage par décalage chaotique.



# ملخص

تعتبر أنظمة الفوضى أنظمة معلومة ، غير خطية وتتأثر بصورة ملحوظة بالشروط الابتدائية. الإشارات الناتجة في هذه الأنظمة تكون في أغلب الأحيان ذات مجال واسع من الموجات ،لهذا فهي تشبه الضوضاء الشبه عشوائية. منذ أن إكتشف العالمان "باكورا " و كارول" امكانية 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 ألكلاسيكية سوف نقدم دراسة نظرية حول أنظمة الفوضى وتزامنها وذلك باستعمال ألحاسوب لنصل في الأخير إلى محاكات تطبيق نظرية الفوضى في تأمين الاتصالات. و في هذا الإطار سوف نعرض طريقتين.



**الكلمات ألمفتاح** الفوضى , تأمين الاتصال ، تزامن الفوضى كريبتوغرافيا ،نظام كريبتوغرافيا ،كريبتوغرافيا بالجمع ، الكريبتوغرافيا بالانسحاب الفوضوي.

# SOMMAIRE

## CHAPITRE IV
## Utilisation du chaos pour la sécurisation des communications

# LISTES DES FIGURES

# LISTE DES TABLEAUX

# NOTATIONS ET ACRONYMES

| | | |
|---|---|---|
| **M** | : | L'ensemble des messages clairs |
| **m** | : | Message en clair |
| $C$ | : | L'ensemble des messages chiffrés |
| $K$ | : | L'espace de paramètres appelés clefs cryptographiques |
| $k$ | : | Clé de cryptage |
| $k^i$ | : | Clé de cycle |
| $T_k$ | : | Transformation mathématique de chiffrage tel que $C = T_k(M)$ |
| $E_k$ | : | Pour tout $k \in K$ ,une transformation de chiffrement $M \xrightarrow{E_k} C$ |
| $D_k$ | : | Pour tout $k \in K$ ,une transformation de déchiffrement $C \xrightarrow{D_k} M$ |
| $D_k o E_k$ | : | Fonction composée de la fonction $E_k$ suivi de la fonction $D_k$ |
| **U** | : | L'ensemble cryptosysteme |
| **DES** | : | Data Encryptions Standard |
| **AES** | : | Advancer Encryption Standard |
| **RSA** | : | Système de cryptage asymétrique (Rivest Shamir Adleman) |
| $\sigma$ | : | Un nombre sans dimension qui porte le nom de l'allemand Ludwig Prandtl |
| $\rho$ | : | Un nombre sans dimension qui porte le nom de l'anglais Lord Rayleigh |
| $x_0, y_0, z_0$ | : | Conditions initiales d'un système d'équations différentielles |
| $x, y, z$ | : | Les variables d'états d'un système d'équations différentielles |
| **T** | : | Le temps symbole d'un signal numérique |
| $T_s$ | : | Le temps de synchronisation de deux systèmes chaotiques |
| **r** | : | Paramètre d'une suite logistique |
| $\mathbb{R}$ | : | L'ensemble des nombres réels |
| $\lambda_i$ | : | L'exposant de Lyapunov |
| $\delta x_0$ | : | Faible variation de la condition initiale $x_0$ |
| $\mathbf{N_R}$ | : | Résistance équivalente de deux résistances négatives du circuit de Chua |
| $\mathbf{N_{R1}}$ ,$\mathbf{N_{R2}}$ | : | Résistances négatives d'un circuit de Chua |
| $X(0)$ | : | Vecteur d'états initiaux d'un système dynamique continu |
| $X(t)$ | : | Vecteur d'états d'un système dynamique continu |
| $X_n$ | : | Vecteur d'états d'un système dynamique discret |
| $X_0$ | : | Vecteur d'états initiaux d'un système dynamique discret |
| $\|.\|$ | : | Valeur absolue |
| **Ln** | : | Logarithme népérien |
| $\sum$ | : | Somme algébrique |
| **a,b** | : | Paramètres du système de Hénon |
| **SG** | : | Synchronisation généralisée |
| **lim** | : | Limite |
| **SNR** | : | Rapport signal sur bruit |
| **PSK** | : | Modulation à décalage de phase |
| **FSK** | : | Modulation à décalage de fréquence |
| **ASK** | : | Modulation à décalage d'amplitude |
| **CSK** | : | Masquage par décalage chaotique (Chaotic shift keying) |
| **BER** | : | Taux d'erreur binaire |

# INTRODUCTION GENERALE

L'échange de données (paroles, images, signes, signal etc. ….) pour l'homme est une nécessité. La sécurité de cette opération devient parfois plus qu'une exigence. Ainsi depuis César à l'ère de l'informatique, le chiffrement de certains messages a toujours été un besoin afin de les cacher à tout intrus non autorisé de façon à s'abriter d'un éventuel usage malveillant. De nos jours, l'ensemble de ces méthodes a été regroupé dans une branche appelée la cryptographie. Parallèlement, une autre branche ennemie à la cryptographie appelée la cryptanalyse a été développée, qui est l'art de révéler les textes en clair qui ont été l'objet d'un chiffrement sans connaître la clé de déchiffrement.

Ces 20 dernières années ont été marquées par une révolution de la technologie de l'information avec l'avènement de l'Internet, la miniaturisation des moyens de communication , comme le téléphone et l'ordinateur portables et la prolifération des réseaux sans fil. Cette banalisation d'échange d'informations à n'importe quels lieu et moment et de n'importe quelle manière, a causé l'engouement du grand public et même les organismes de pouvoir culturel ,financier, politique ,militaire et scientifique pour les nouvelles technologies de l'information .Entraînant la circulation d'un flux grandissant de données, a travers des canaux généralement qui ont un aspect public. La valeur de la donnée transmise est intrinsèque à son contenu qui peut être une simple lettre de bonjours, ou un signal de commande d'un réacteur nucléaire à tel point qu'il est souvent nécessaire de le protéger. D'où vient l'importance spéciale assumée par la cryptographie. En conséquence la cryptographie est devenue aujourd'hui pour tous un moyen quotidien de protection des données qui doivent être communiquées ou stockées à longue période et de protéger des transferts de fonds électroniques et des communications classifiées.

Les premiers principes de base de la cryptographie moderne reviennent à Auguste Kerkhoffs, énoncés dans son article intitulé " La cryptographie militaire " publié en 1883 et dont l'idée la plus importante est que la sécurité du chiffre ne doit pas dépendre de ce qui ne peut être facilement changer. En d'autres termes, aucun secret ne doit résider dans l'algorithme de cryptage mais plutôt dans la clé.

Ces principes ont été reformulés par Claude Shannon en posant également le problème de sécurité des cryptosystèmes avec l'introduction de la notion de sécurité parfaite, qui est une approche irréalisable en pratique. D'où sont fondés les algorithmes de cryptage utilisés

actuellement, en profitant astucieusement de la puissance des mathématiques et en utilisant adéquatement des techniques de substitutions, de permutations et d'itérations.

Bien que l'efficacité de ces algorithmes soit reconnue, leur temps de calcul est long, ce qui entraîne une diminution du débit des messages transmis .Il y'a aussi la question de réduction du niveau de confidentialité dans ces algorithmes avec le développement sans cesse des techniques de cryptanalyses, causées par la puissance croissante des calculateurs disponibles. Ces failles ont poussé les recherches vers le développement de nouveaux systèmes. L'usage du chaos a été une des alternatives proposées.

Les systèmes dynamiques chaotiques sont des systèmes déterministes non linéaires qui montrent souvent un comportement non divergent, apériodique et éventuellement borné. Les signaux qui évoluent dans ces systèmes sont en général ,à large bande , ce qui fait apparaître leur trajectoire comme du bruit pseudo aléatoire. En raison de ces propriétés et à cause de la fragilité des cryptosystèmes classiques , les signaux chaotiques fournissent potentiellement une classe importante des signaux qui peuvent être utilisés pour masquer les informations dans une transmission sécurisée, il suffit donc de les mélanger de manières appropriées au messages en clair qu'on souhaite transmettre confidentiellement .

La difficulté dans l'utilisation de cette procédure réside dans la restitution du message original. Ainsi ce n'est qu'à partir de 1990 après la découverte de Carroll et Pécora de la synchronisation du chaos, que la communication sécurisée chaotiquement a fait l'objet d'un intérêt croissant dans la littérature.

Le travail présenté dans ce mémoire se situe dans le cadre des approches qui proposent l'usage du chaos pour sécuriser la transmission des données. Ainsi il est organisé comme suit :

- Le premier chapitre est un exposé général de la cryptographie, dans lequel on analyses ses limites et on expose les motivations, qui poussent à chercher des techniques alternatives.
- Le deuxième chapitre est une présentation théorique du phénomène chaotique.
- Le troisième chapitre est consacré au concept de la synchronisation entre systèmes chaotiques. Des résultats de simulation sont aussi présentés.
- -Le quatrième chapitre présente les résultats obtenus en simulant deux modèles de cryptosystèmes chaotiques accompagnés par des interprétations et des analyses des performances.
- Enfin , la conclusion présente le bilan du travail réalisé et les perspectives envisagées .

# CHAPITRE I

# Généralité sur la sécurisation de la communication

## I.1. Introduction

La cryptographie ou la sécurisation de la communication est une science aussi vieille que l'existence de l'humanité .Des premiers signes de celle-ci datant de 4000 ans ont été trouvés en Egypte [12] , ainsi que chez les grecs [18] . On a découvert plusieurs méthodes de masquage de messages, citons celle qui consistait a enrouler une bande de papyrus autour d'un support cylindrique en bois et d'écrire un message à sa surface de façon à rendre le message incompréhensible une fois déroulé, dans ce cas la clé de cryptage est le diamètre du cylindre [18].

Etymologiquement la cryptographie veut dire écriture secrète mais sa définition générale qu'on peut donner est : l'art de rendre les messages échangés entre deux entités communicantes à travers un canal non sécurisé, incompréhensibles sauf par leur destination légitime qui possède la clé de déchiffrage de ces messages [12] .

En parallèle de la cryptographie, s'est développée la cryptanalyse ; c'est en quelque sorte l'opposée de la cryptographie .En effet, si déchiffrer consiste à retrouver le clair au moyen d'une clé, cryptanalyser c'est tenter de briser le message crypté ou tester la robustesse d'un cryptosystème . Ces deux domaines sont regroupés sous la dénomination de la cryptologie qui désigne la science des messages secrets [12].

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

De nos jours, les principaux services offerts par la cryptographie moderne sont : intégrité -authentification -identification - signature.

Actuellement les deux types de cryptosystèmes les plus utilisés dans les applications pratiques, sont les systèmes à clés symétriques, le DES (*Data Encryption*

*Standard* ) et l' AES (*Advanced Encryption Standard*) et les systèmes asymétriques ou à clefs publiques, largement popularisés par le système RSA (*Rivest Shamir Adleman*) [12].

L'objectif de ce chapitre est d'exposer d'une part, l'état de l'art sur les techniques de cryptage actuelles , et d'autre part leurs limites.

## I.2. Principe de la cryptographie

La cryptographie peut être illustrée par le schéma de principe de la figure (1.1) [37] :

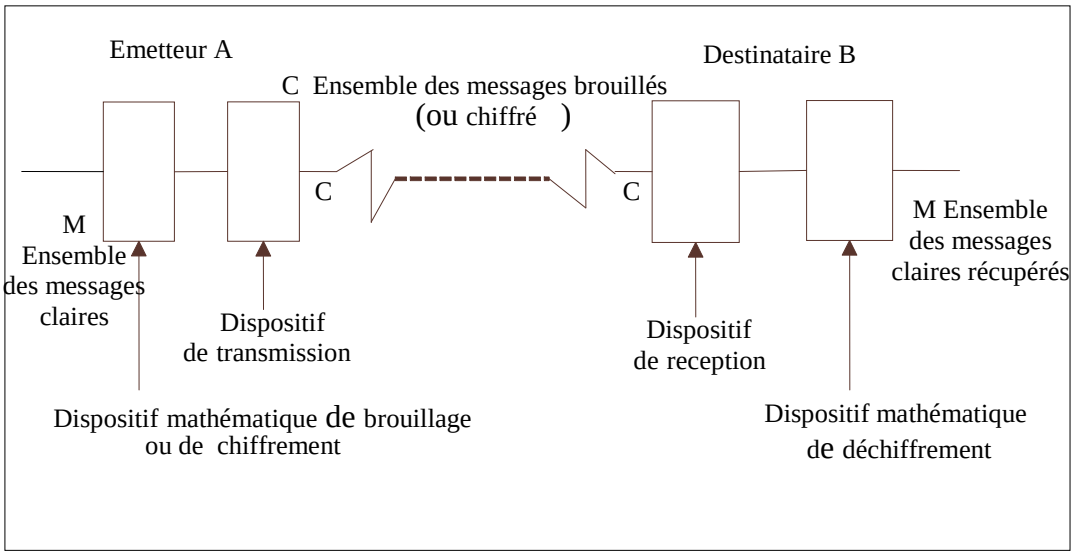



*Figure (I.1) Schéma général de la communication chiffrée entre un émetteur et un récepteur*

### I.2.1. Terminologie

- **Cryptologie :** Science des messages secrets . Elle englobe la cryptographie et la cryptanalyse.
- **Cryptographie :** Procédé (signes conventionnels, modification de l'ordre, de la disposition des signes, remplacement des signes) permettant de rendre un message inintelligible afin de le protéger [32], c'est ce qu'on appelle le chiffrement ou le cryptage. Sa fonction réciproque est l'opération de décryptage, c'est-à-dire rendre le message chiffré clair en utilisant un paramètre qui s'appelle clef de décryptage.

- **Cryptanalyse :** C'est l'inverse de la cryptographie, c'est-à-dire l'étude des méthodes de cassation des secrets du message crypté sans posséder la clef de décryptage.
- **Cryptosystème :** C'est l'ensemble des clés possibles (espace de clés), des textes clairs et chiffrés associés à un algorithme donné [10].
- **Cryptogramme :** Message rendu inintelligible par une opération de cryptage [32].

### I.2.2. Principes de Kerckhoffs pour la cryptographie

Les cryptosystèmes civils utilisés actuellement, sont basés sur le principe fondamental suivant :

La sécurité du chiffre ne doit pas dépendre de ce qui ne peut être facilement changé. En d'autres termes, aucun secret ne doit résider dans l'algorithme mais plutôt dans la clé. Sans celle-ci, il doit être impossible de retrouver le texte clair à partir du texte chiffré. Par contre, si on connaît la clé, le déchiffrement est immédiat [10].

Ce principe est l'un des six principes publiés par Kerckhoffs dans son traité de cryptographie militaire et dont l'énoncé est [18] :

- Une information codée ne doit en aucun cas pouvoir être déchiffrée sans la connaissance de sa clé.
- Les interlocuteurs ne doivent pas subir de dégâts au cas où le système de codage serait dévoilé.
- La clé doit être simple et modifiable à souhait.
- Les cryptogrammes doivent être applicables à la correspondance télégraphique.
- L'appareil de codage et les documents doivent être transportables.
- Le système doit être simple d'utilisation.

L'interprétation de ces principes est que le secret d'un message crypté doit se reposer sur le paramètre le moins cher à changer si celui-ci est dévoilé , c'est-à-dire la clé de déchiffrage.

### I.2.3. Principe de Shannon pour la cryptographie

Le principe de Claude Shannon peut être considéré comme une reformulation de celui de Kerckhoffs [6] [33]. Ainsi Shannon a énoncé que :

- Pour qu'un crypto système soit inconditionnellement sûr, il faut que la clé secrète soit aussi longue que le texte clair et tous les autres systèmes sont théoriquement cassables .
- La confusion doit cacher les structures algébriques et statistiques.
- La diffusion doit permettre à chaque bit de texte clair d'avoir une influence sur une grande partie du texte chiffré. Ce qui signifie que la modification d'un bit du bloc d'entrée doit entraîner la modification de nombreux bits du bloc de sortie correspondant.
- La sécurité pratique d'un crypto système repose sur le fait que la connaissance du message et de certains couples clairs chiffrés ne permet pas de trouver ni la clé ni le message clair en un temps humainement raisonnable.

Shannon a défini un cryptosystème comme étant un ensemble [37] :

$$U = \left(M, C, K\{E_k\}_{k\in K}, \{D_k\}_{k\in K}\right) \quad \text{(I.1)}$$

Ou : ▫ $M$ : représente l'ensemble des messages clairs.

▫ $C$ : représente l'ensemble des messages chiffrés.

▫ $K$ : représente un espace de paramètres appelés clefs cryptographiques.

▫ $E_k$ : représente, pour tout $k \in K$ , une transformation de chiffrement :

$M \xrightarrow{E_k} C$

▫ $D_k$ : représente, pour tout $k \in K$ , une transformation de déchiffrement

$C \xrightarrow{D_k} M$ telle que, pour tout message M, on ait :

$$D_k o E_k(M) = M \quad \text{(I.2)}$$

Tout cryptosystème moderne peut être décrit par ce modèle à la fois simple, élégant et puissant [37].

## I.3. Cryptanalyse

L'opération de transmission d'une information sécurisée peut être victime d'une cryptanalyse au niveau d'un canal public comme il est représenté sur le schéma de la figure (I.2) .

Cette opération consiste à reconstituer les messages originaux $M$, sur la base d'un message reçu $C = T_k(M)$ où $T_k$ est une transformation mathématique, connue ou

inconnue, dépendant du paramètre clé k qui est toujours inconnu . Pratiquement la cryptanalyse c'est le dépistage de la clé de décryptage [37].

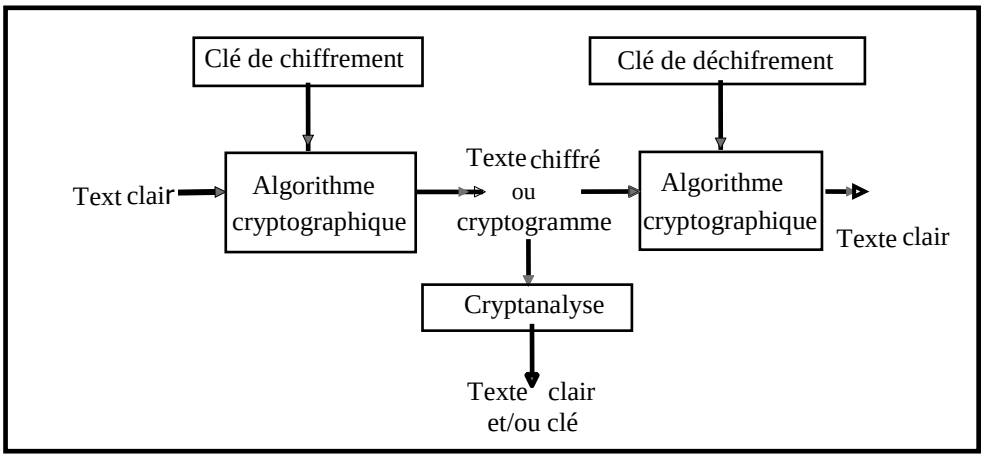



*Figure (1.2) : Schéma de principe d'une transmission sécurisée*

Construire un cryptosystème incassable passe toujours par la vérification qu'il résiste aux attaques de la cryptanalyse ; donc un cryptographiste expérimenté doit nécessairement être un bon cryptanalyste [37].

Une attaque cryptanalytique se caractérise selon des données dont elle dispose , ainsi on peut trouver quatre situations de cryptanalyse :

- Attaque sur texte chiffré seul : disposition seulement d'un nombre fini de textes chiffrés pour retrouver la clef de déchiffrage.
- Attaque à texte clair connu : disposition de couple de message (clairs, chiffrés).
- Attaque à texte clair choisi : l'attaquant a accès à l'algorithme de chiffrement et il l'utilise pour générer le couple (clairs, chiffrés).
- Attaque a texte chiffré choisi : Le cryptanalyste peut choisir les textes à déchiffrer sans connaître la clef.

Ainsi Le cryptanalyste va s'adonner d'une manière scientifique en exploitant les ressources qu'il a pu regrouper pour divulguer le message crypté et en utilisant des méthodes de cryptanalyse, qui n'ont pas cessé de se métamorphoser parallèlement avec la cryptographie et qui peuvent être groupés en [33]:

- Attaque par force brute : Le cryptanalyste essaie toutes les combinaisons de clés possibles jusqu'à l'obtention du texte clair [6] , [33].
- L'attaque par canaux auxiliaires : toutes les façons d'analyser les propriétés inattendues d'un algorithme sont prises en compte pour réussir à casser le crypto système [33].

- Attaque par cryptanalyse fréquentielle : dans cette méthode si nous avons par exemple comme message crypté un texte rédigé dans une langue quelconque , alors le cryptanalyste doit examiner les fréquences des répétitions et d'usage des lettres dans cette langue , puis il doit projeter les résultats de cet examen sur le message crypté afin de trouver la clé .Cette méthode est principalement utilisée contre les chiffrements mono alphabétiques qui substitue chaque lettre par une autre et elle est inefficace contre les chiffrements modernes .
- Attaque par cryptanalyse linéaire : Proposée par M. Matsui un cryptologue japonais et chercheur à Mitsubishi Electric .Elle nécessite une quantité n de couples (texte clair, texte chiffré), cryptés avec la même clef. Le principe est que le même message soit chiffré plusieurs fois avec des clefs différentes pour construire une immense table qui contient toutes les versions chiffrées de ce message. Lors d'une interception d'un message chiffré, on peut le retrouver dans la table et obtenir la clef qui avait été utilisée pour le cryptage. Le problème dans cette technique est le besoin d'une table trop importante .Ainsi le moyen de la réduire consiste à faire une approximation linéaire de l'algorithme de chiffrement pour le simplifier.
- Attaque par cryptanalyse différentielle: Proposée par Biham et Shamir. Elle permet de trouver la clef en utilisant plusieurs textes clairs. L'idée est de fournir comme entrée des textes clairs avec de légères différences. Ensuite, il y'aura l'analyse statistique du comportement des sorties selon les entrées pour retrouver la clef. Cette méthode est considérée comme relativement menaçante pour quelques cryptosystèmes modernes.

## I.4. Evolution de la cryptographie

### I.4.1. Cryptographie classique

Cette partie traite quelques cryptosystèmes célèbres, avant l'ère des ordinateurs qui ont été les bases pour l'évolution de plusieurs algorithmes de cryptographie utilisés actuellement. Les cryptosystèmes classiques sont regroupés en chiffrement monoalphabétique et polyalphabétique [33],[37].

#### 1.4.1.1. Système de César (par décalage)

C'est un cryptosystème a substitution monoalphabétique. Son modèle, au sens de Shannon est :

- pour Alphabet français : $Z_{26}$ (I.3)
- espace des messages : $M = (Z_{26})^n$

  (I.4)
- espace des cryptogramme: $C = (Z_{26})^n$ (I.5)
- espaces des clefs : $K = Z_{26}$ (I.6)

Un message $M = [X_1, X_2, .... X_n]$ est crypté par un entier représentant la clef $k \in K$ , en le cryptogramme :

$$C = [E_k(X_1), E_k(X_2), ....., E_k(X_n)] = [Y_1, Y_2, ....., Y_n] \quad (I.7)$$

Ce modèle peut être représenté mathématiquement en utilisant les congruences . Ainsi chaque lettre X peut être affecté par un nombre entier indiquant sa position dans l'alphabet (A=0 , B=1 …. Z=25) . Donc on aura 25 manière de coder un message . Alors pour crypter une lettre X avec une clé k ,on applique la formule :

$$E_k(X) = (X + k) \bmod 26 = Y \quad (I.8)$$

Le décryptage est : $D_k(Y) = (Y - k) \bmod 26 = X$ (I.9)

**Exemple I.1**

Pour k = 4 si nous avons le message clair :

JE SUIS EN PHASE DE REDACTION DE MON MEMOIRE (I.10)

donne le texte chiffré suivant :

NI WYMW IR TLEWI HI VIHEGXMSR HI QSR QIQSMVI (I.11)

**Remarque I.1**

La cryptanalyse du système de César peut se faire facilement par la méthode exhaustive [37].

### I.4.1.2. Système de Vigenère

Ce système utilise la notion de substitution polyalphabétique. Le modèle de Shannon pour ce système est [37] :

- Pour l'alphabet français : $Z_{26}$

- espace des messages : $M = (Z_{26})^n$
- espace des cryptogrammes : $C = (Z_{26})^n$
- espaces des clefs : $K = (Z_m)^r$ (I.12)

Un message $M = [X_1, X_2, .... X_n]$ est crypté par la clef $k = [k_1, ...., k_r] \in K$, en le cryptogramme $C = [Y_1, Y_2, ....., Y_n]$ .

Pratiquement le cryptage est réaliser en utilisant le tableau représenté sur la figure (I.3) .Pour le texte clair, on écrit immédiatement au dessous la clef, autant de fois que nécessaire par périodicité . Le cryptage de la i$^{eme}$ lettre se fait en repérant l'intersection de la colonne de la table, correspondante à la lettre du texte claire et de la ligne de la table , correspondante à la lettre de la clef .

**Exemple I.2**

Si k = BISKRA avec le message clair :

JE SUIS EN PHASE DE REDACTION DE MA THESE (I.13)

on aura le cryptogramme suivant :

KM KEZS FV HRRSF LW BVDBKLSFN EM EK KHFAW (I.14)

**Remarque I.2**

La cryptanalyse du système de Vigenére peut se faire grâce à des attaques statistiques [6].

| | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | O | R | S | T | U | V | W | X | Y | Z |
| B | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | O | R | S | T | U | V | W | X | Y | Z | A |
| C | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B |
| D | D | E | F | G | H | I | J | K | L | M | N | O | P | O | R | S | T | U | V | W | X | Y | Z | A | B | C |
| E | E | F | G | H | I | J | K | L | M | N | O | P | O | R | S | T | U | V | W | X | Y | Z | A | B | C | D |
| F | F | G | H | I | J | K | L | M | N | O | P | O | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E |
| G | G | H | I | J | K | L | M | N | O | P | O | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F |
| H | H | I | J | K | L | M | N | O | P | O | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G |
| I | I | J | K | L | M | N | O | P | O | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H |
| J | J | K | L | M | N | O | P | O | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I |
| K | K | L | M | N | O | P | O | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J |
| L | L | M | N | O | P | O | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K |
| M | M | N | O | P | O | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L |
| N | N | O | P | O | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M |
| O | O | P | O | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N |
| P | P | O | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O |
| O | O | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P |
| R | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | O |
| S | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | O | R |
| T | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | O | R | S |
| U | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | O | R | S | T |
| V | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | O | R | S | T | U |
| W | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | O | R | S | T | U | V |
| X | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | O | R | S | T | U | V | W |
| Y | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | O | R | S | T | U | V | W | X |
| Z | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y |

*Figure (I.3) : Table du chiffre de Vigenére*

### I.4.1.3. Autres crypto systèmes classiques

- ✓ **Système de Playfair :** Imaginé en 1854 par le physicien inventeur anglais C. Wheatstone, mais porte le nom de Lord Playfair qui concrétisa son utilisation .Ce système illustre la notion de chiffrement par polygrammes , alors le cryptage se fait en chiffrant 2 lettres par 2 autres , selon un algorithme spécifique à ce crypto système [37] .La cassation de ce crytosystéme peut être facile si l'on dispose de suffisamment d'échantillons de textes claires et chiffrés .
- ✓ **Système ADFG(V)X :**Ce système n'utilise dans le texte chiffré que les six lettres A,D,F,G,V et X d'où vient sa nomination .Ces lettres ont été choisis a cause de leur représentation très différente les uns des autres dans le code Morse . L'intention par la création de ce système était de réduire la possibilité d'erreur de l'opérateur. Inventé par l'Allemand F.Nobel ,cette méthode présente la particularité de mixer astucieusement transposition et substitution . La sécurité de ce crypto système a été étudiée par A. Konheim [37].
- ✓ **La machine Enigma :** C'est une machine à crypter électromécanique, inventée en 1919 par un ingénieur Hollandais. Son principe est que chaque lettre est remplacée par une autre, mais la substitution change d'une lettre à l'autre. Parmi ses points forts le nombre très important de clés ou encore la réversibilité [6 ] . Cette machine a été utilisée par les Allemands pendant la deuxième guerre mondiale. Cependant les anglais ont pu déchiffrer beaucoup de messages, qui avaient été chiffrés a l'aide de cette machine.

On peut conclure que les moyens de sécurisation des communications s'adaptent au cours des temps à l'évolution des forces d'attaque, d'où l'aboutissement aux procédés de cryptage actuels.

### I.4.2. Cryptographie actuelle

De nos jours pratiquement, la cryptographie est englobée par deux grands algorithmes de chiffrement. On distingue les algorithmes à clef secrète et les

algorithmes à clef publique. La sécurité de ces systèmes est calculatoire [33] . Ainsi leur puissance réside dans l'incapacité des calculateurs à les casser dans un temps humainement raisonnable.

### I.4.2.1. Système de chiffrement symétrique

Le principe du chiffrement symétrique est que l'émetteur et le récepteur partagent une même clé secrète c'est-à-dire les clés de chiffrement et de déchiffrement sont identiques .Le schéma de principe est illustré dans la figure (I.4). Les cryptosystèmes symétriques les plus utilisés pratiquement sont le DES et le AES.

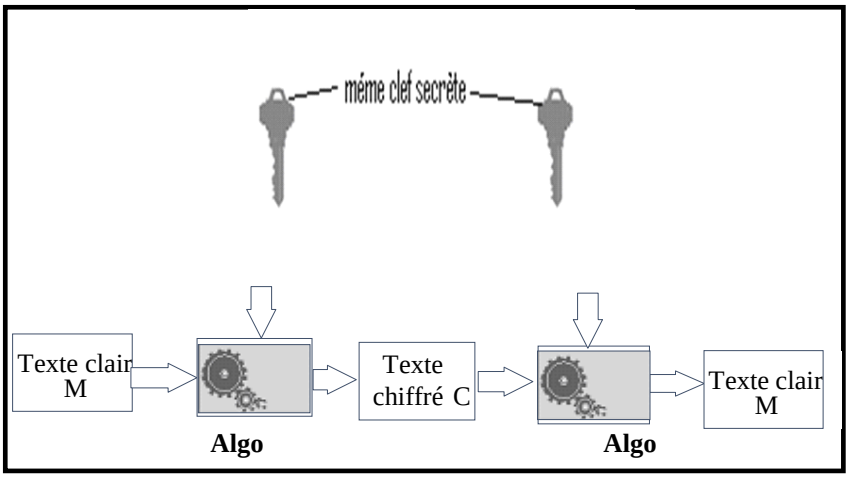



*Figure (I.4) : Schéma de principe d'un cryptosystème symétrique*

- **Le DES**

Cet algorithme doit sa conception à la société IBM, sa révision a NSA (National Security Agency) et sa publication a NBS (National Bureau of Standard) en 1977 .On note que la date exacte de l'adoption de ce système comme standard est le 23 novembre 1976 [12] .

- **Description de l'algorithme de chiffrement**

Le principe du DES est de découper le message clair en blocs de 64 bits et d'utiliser une clé k de 56 bits pour les chiffrer, afin d'obtenir des blocs de textes chiffrés de 64 bits. L'algorithme du DES est basé sur la structure de Feistel a 16 cycles figure (1.5) [12]. Il est a noter qu'au début et la fin du DES, est appliquée respectivement une permutation IP (permutation initiale) et FP (permutation finale).

Dans cette structure, un bloc du message est devisé en deux sous blocs égaux gauche $(G)$ et droit $(D)$ , puis la fonction de chiffrement $(F)$ paramétrée par une clé de cycle $(k^i)$ est appliquée sur le sous bloc droit $(D)$ et après une opération binaire (ou exclusif ) $\oplus$ est appliquée sur la sortie de l'opération $(F)$ et le sous bloc gauche $(G)$. Ensuite les deux sous blocs sont permutés et un nouveau cycle commence.

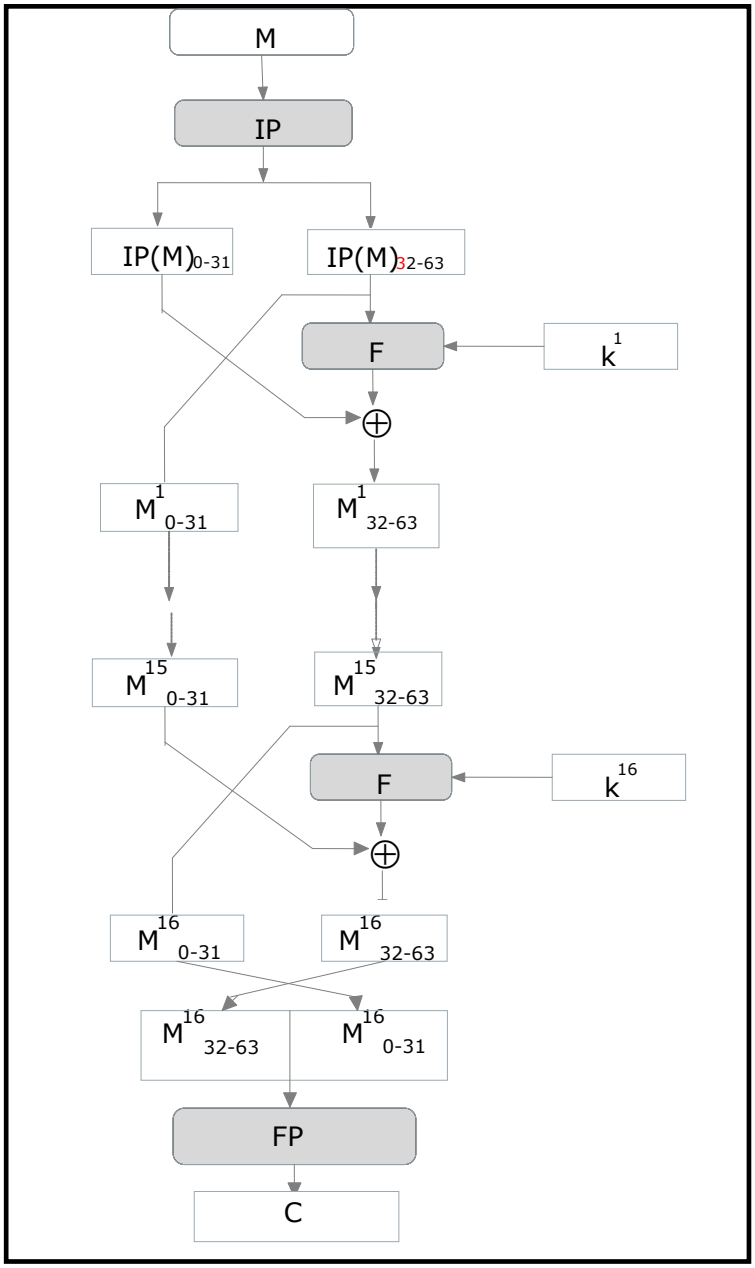


*Figure (I.5) : Structure du DES*

La fonction $(F)$ se décompose en quatre transformations, figure (1-6) :

- Une permutation expansive $(EP)$ qui prend en entrée un bloc de 32 bits et fait ressortir un bloc de 48 bits.
- Un ou exclusif avec la clé de cycle $(k^i)$ .
- Un appel aux 8 boites $(S)$ du DES qui agit non linéairement sur les blocs de 6 bits pour faire sortir des blocs de 4 bits.
- Une permutation $(P)$ de 32 bits. Les 16 clés de cycle $(k^i)$ sont les dérivés de la clé $(K)$ du DES, la procédure de leur génération est sur la figure (I.7) :
- Une permutation compressive PC-1 qui prend les 56 bits de k plus 8 bits de contrôle d'erreur (de parité) en entrée et fait retourner une valeur codée sur 56 bits.
- Des rotations vers la gauche d'un ou deux bits appliqués à des blocs de 28 bits.
- Une permutation compressive PC-2 qui prend en entrée une valeur sur 56 bits et fait retourner une valeur codée sur 48 bits qui sera utilisée comme clé de cycle .

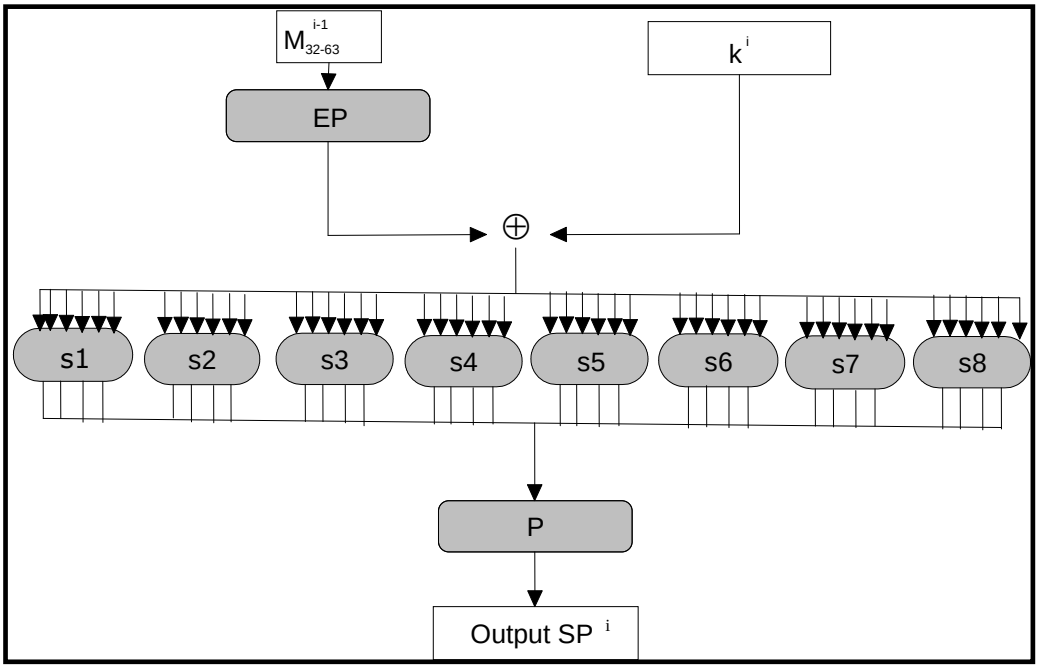


*Figure (I.6) : La fonction $(F)$ du DES*

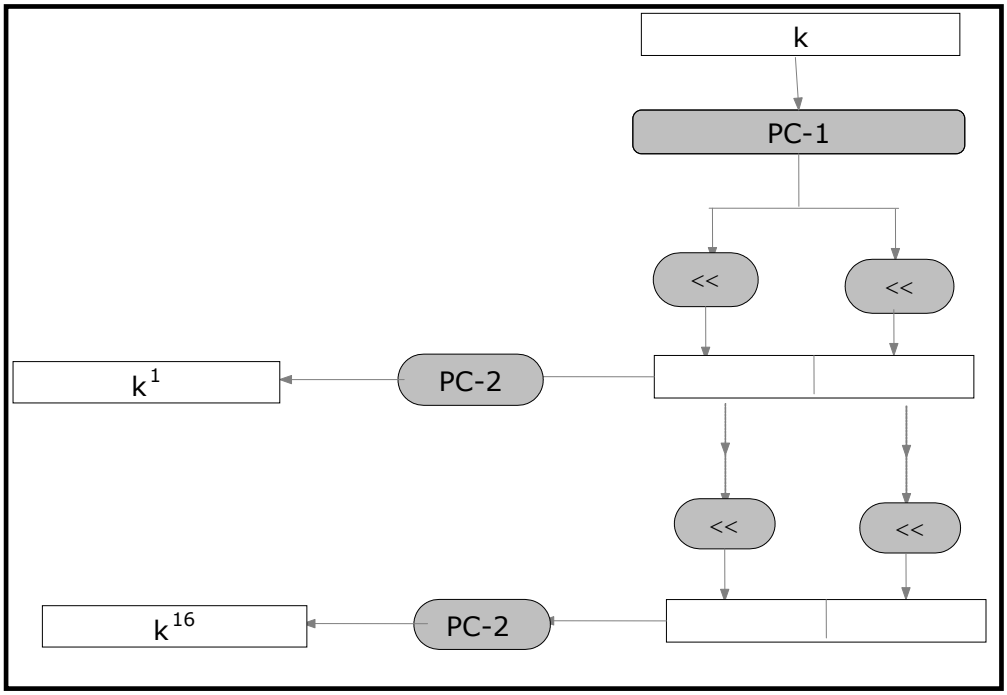



*Figure (I.7) : Génération des clés pour le DES $(k^i)$*

- **Le déchiffrement**

C'est l'application inverse du même algorithme de chiffrement en tenant bien compte que chaque itération du déchiffrement traite les mêmes paires de blocs Utilisées dans le chiffrement.

**Remarque I.3**

Une attaque exhaustive sur le DES en 1998 a permis de le casser en 56 heures ce qui a entraîné la recherche d'un remplaçant plus robuste. Ce successeur a été choisi en 2000 et son nom est AES (Advancer Encryption Standard).

- **Le AES**

Appelé aussi l'algorithme de Rijndael , sa conception revient aux deux cryptographes belge V.Rijmen et J.Daemen .Choisi par les américain pour être le nouveau standard en octobre 2000, le AES est un algorithme de chiffrement par blocs

utilisant une structure parallèle et il est disponible en trois versions pour trois tailles de clés différentes (128, 192 ou 256 bits). Cette diversification de la longueur de la clé k de l'AES permet d'obtenir respectivement un nombre Nc de 10, 12 ou 14 sous clés de cycle $k^i$ . Les blocs intermédiaires pendant les cycles sont conservés dans des tableaux d'états dont chaque case contient 1 octet, comme il est représenté sur la figure (I.8).

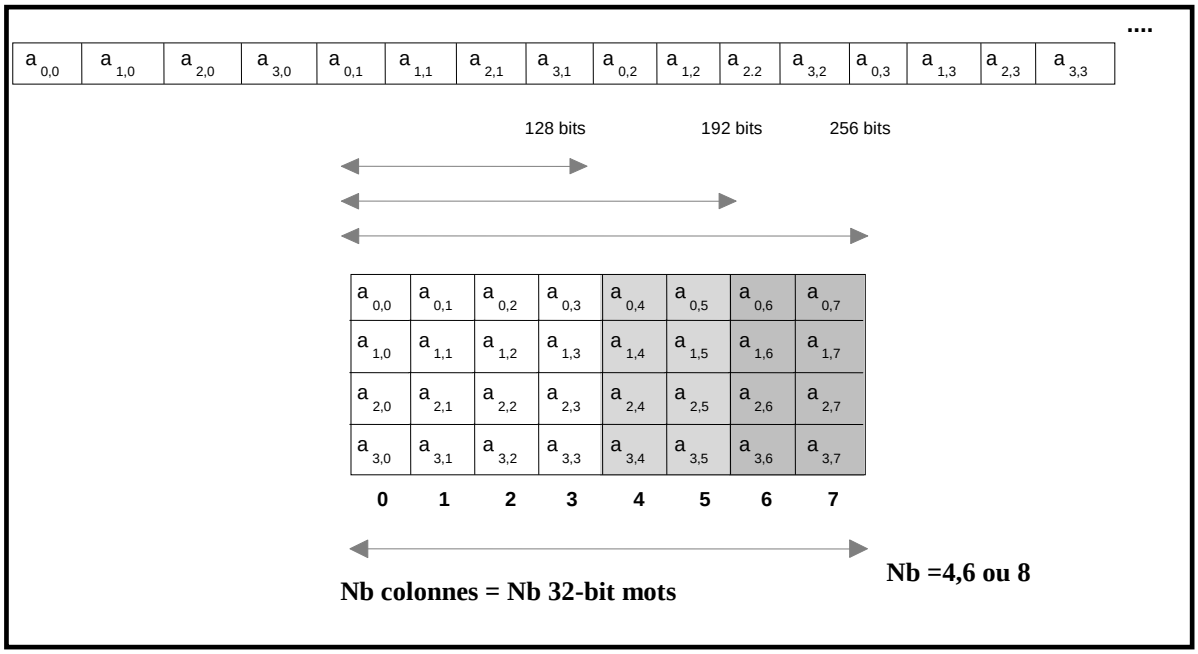



*Figure (I.8) : Représentation des clés et des blocs sur des tableaux d'états*

Pour les sous clés $k^i$ de 128 bits , numérotés de 0 à 10 , sont des dérivés de la clé secrète k (128 bits) de la manière suivante : $k^0$ correspond à k et $k^i$ est obtenue a partir de $k^{i-1}$ suivant l'algorithme décrit dans la figure (I.9) .

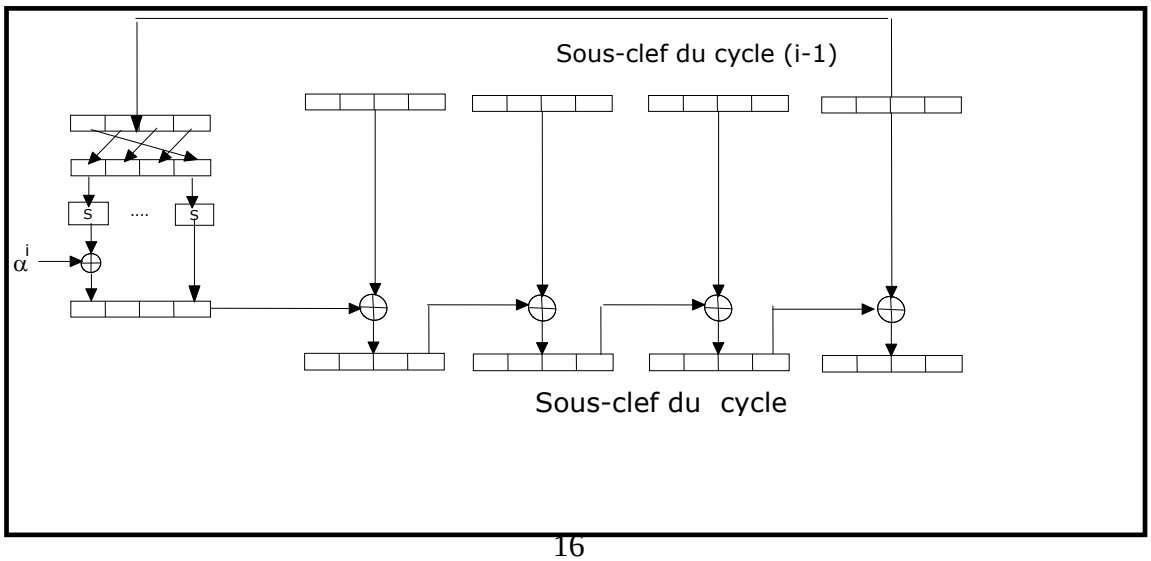


*Figure (I.9) : Génération des clés $k^i$ pour le AES*

On permute les quatre derniers octets de la sous clé $k^{i-1}$, puis on leur applique la fonction S. Apres avoir ajouté une constante (dépendante de i) au premier octet, on effectue un ou exclusif bit a bit entre les quatre octets ainsi obtenus et les quatre premiers octets de la sous-clé précédente.

Les trois autres blocs de quatre octets de la clef $k^i$ sont ensuite simplement le résultat d'un ou exclusif entre le bloc correspondant de la sous-clé $k^{i-1}$ et le bloc précédent de la sous-clé $k^i$.

Pour le chiffrement à chaque cycle, quatre transformations sont appliquées [12] :

a- SubByte (SB) qui est une fonction de substitution non linéaire et qui s'applique indépendamment à chaque octet du tableau du bloc intermédiaire.

b- ShiftRow (SR) qui effectue une rotation sur chacune des lignes dans le tableau du bloc intermédiaire .La ligne 0 n'est pas modifiée, la ligne 1 subit une rotation de 1 octet vers la gauche, la ligne 2 subit une rotation de 2 octets vers la gauche et la ligne 3 subit une rotation de 3 octets vers la gauche.

c- MixColumns (MC) qui effectue le déplacement de colonnes dans le tableau du bloc intermédiaire (sauf pour le dernier cycle).

d- Un ou exclusif $\oplus$ bit à bit avec la sous clé de cycle.

Le déchiffrement consiste à appliquer les opérations inverses , dans l'ordre inverse et avec des sous clés également dans l'ordre inverse .

Les algorithmes de chiffrement et de déchiffrement par l'AES sont représentés sur la figure (I.10).

**Remarque I.4**

On rapporte que ce système résiste encore aux attaques cryptanalytiques mais sa résistance n'est pas absolue car avec le développement du matériel de calcul ,ce système peut probablement être cassé par une attaque exhaustive, alors la recherche d'alternatifs devient une nécessité.

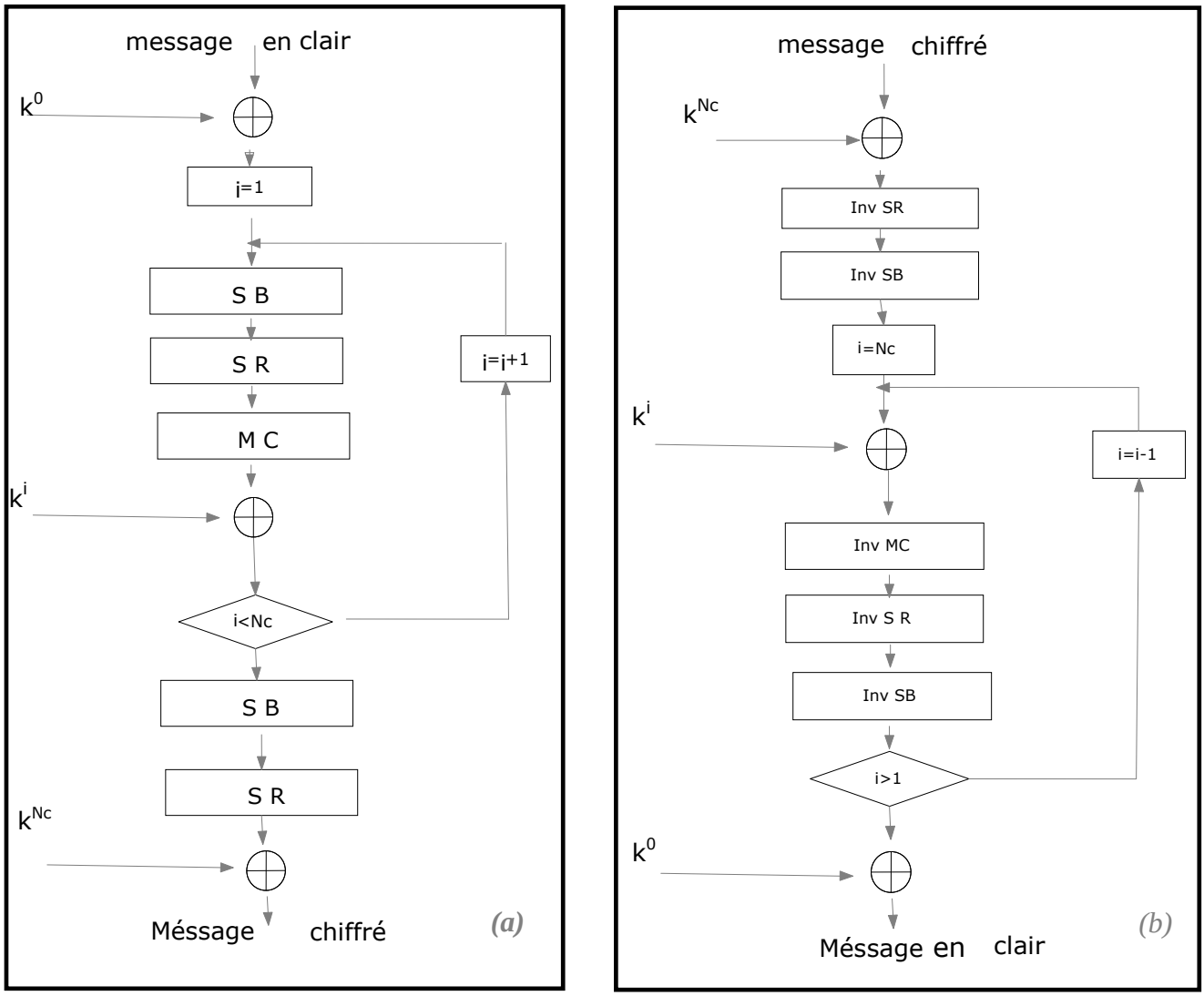



*Figure (I.10) : Algorithmes de chiffrement et de déchiffrement de l'AES*

### I.4.2.2 Système de chiffrement à clé publique ou asymétrique

Dans ces cryptosystèmes , chaque acteur de la communication sécurisée possède 2 clés distinctes (une privée, une publique) avec l'impossibilité de déduire la clé privée à partir de la clé publique qui est distribuée librement. Ce principe est illustré sur la figure (1.11).

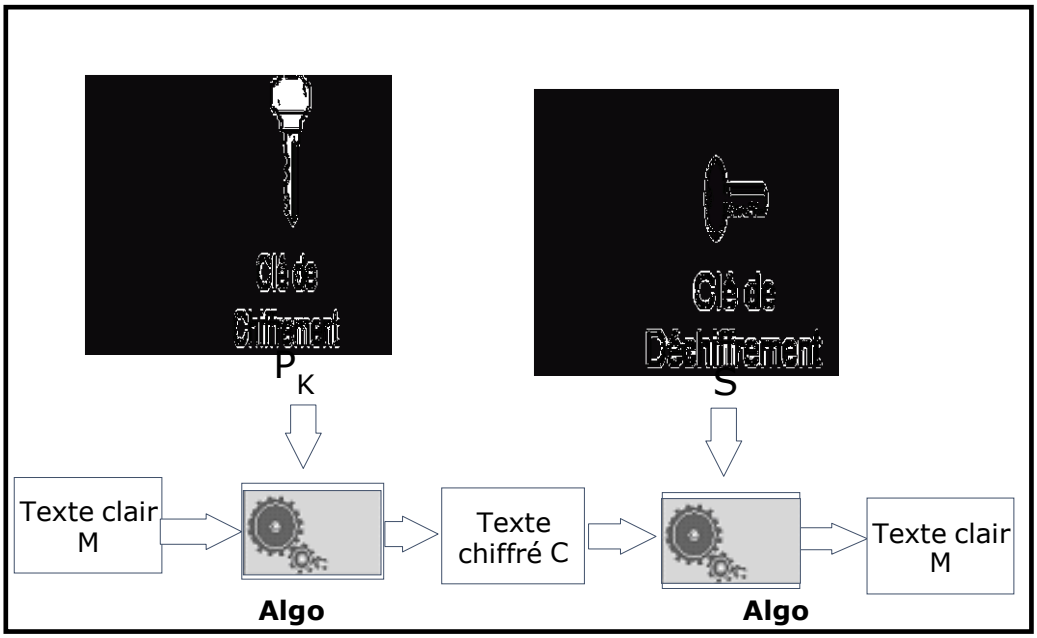



*Figure (I.11) : Schéma de principe d'un crypto système a clé publique*

**Exemple I.3**

Pour envoyer un message confidentiel à Bob, Alice chiffre le message clair à l'aide de la clé publique de Bob et lui ,à l'aide de sa clé secrète , est le seul en mesure de déchiffrer le message reçu.

Cette idée a été proposée dans un article fondamental de Diffie et Hellman en 1976 [12] , [33], [37]. Sa première implémentation a eu lieu en 1978 par Rivest , Shamir et Adleman d'où la naissance de l'algorithme (RSA) .

❖ **Le système de chiffrement RSA**

C'est le système à clé publique le plus utilisé. Ce système n'a pas d'agrément de standard mais son usage est recommandé dans un grand nombre de standards officiels.

Le fonctionnement de ce système repose sur des résultats classiques d'arithmétique, ainsi son processus est :

a- Confections de clés :

-Choix de deux grands nombres premiers $p$ et $q$. (I.15)

- $n = p \times q$ (I.16)

-Choix d'un entier $e$ premier avec le produit $(p-1)\times(q-1)$. (I.17)

-Détermination d'un entier $d$ tel que : $e \times d \equiv 1[(p-1)\times(q-1)]$. (I.18)

On aura donc :

- $(n;e)$ Comme clé publique. (I.19)

- $(p;q;d)$ Comme clé privée. (I.20)

b- Numérisation du message.

c- Découpage du message en fragments de taille égale à $n$.

d- Cryptage d'un fragment $n$ du message :

- $m^e \equiv c(\text{mod } n)$ (I.21)

alors $c$ est un fragment du message crypté.

e- Décryptage de $c$ :

- $c^d \equiv m(\text{mod } n)$ (I.22)

alors $m$ est un fragment du message décrypté.

Ce principe est illustré sur la figure (I.12).

**Remarque I.5**

Casser le système RSA consiste à retrouver la clé secrète $d$ à partir du texte chiffré $c$ et la clé publique $(e;n)$. Pour résoudre ce problème, on a affaire à factoriser $n$. L'inexistence de solution rapide a ce problème constitue sa fiabilité, mais cette fiabilité est limitée par l'évolution des moyens de cryptanalyse, donc le remplacement de ce système est la demande du futur.

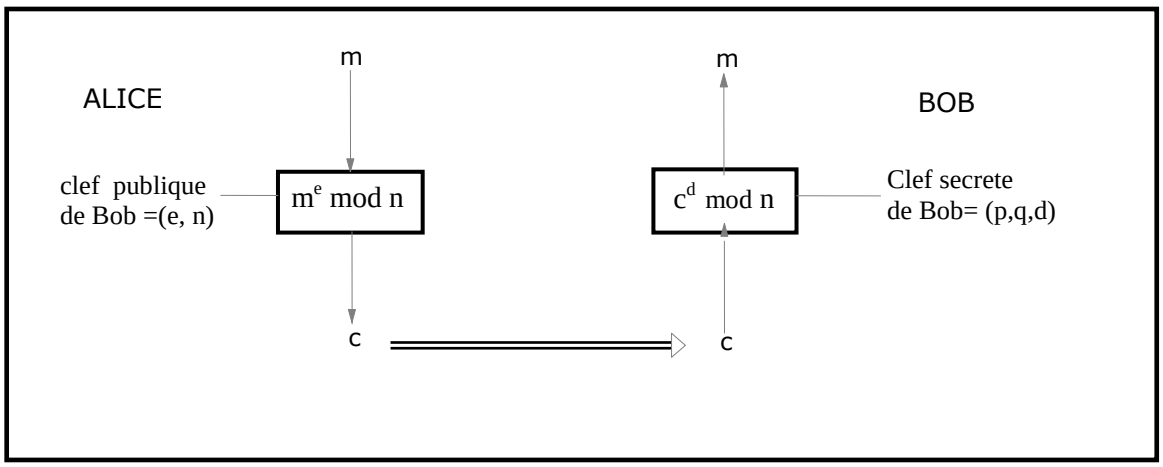


*Figure (I.12) : Le chiffrement a clé publique RSA*

## I.5. Conclusion

Ce chapitre a pour objectif de se rendre compte que les cryptosystèmes actuels sont basées sur des algorithmes de calcul qui devient de plus en plus fragiles face à la montée en puissance des calculateurs , car si leur rapidité de calcul est très efficace pour chiffrer ou déchiffrer l'information , elle l'est aussi pour la cryptanalyse ; puisqu'un très bon moyen de casser un code peut se réduire selon les cas à chercher toutes les combinaisons .De plus l'annonce des capacités de calcul très prometteuses , de l'ordinateur quantique , ainsi que la constante avancée de la théorie des nombres font apercevoir la chute brutale du cryptage algorithmique . Deux alternatives très prometteuses ont alors été développées durant la dernière décennie, la cryptographie quantique et la cryptographie chaotique. La première résout de manière radicale le problème de confidentialité puisque par principe, elle offre une clé incassable (liée au principe d'incertitude d'Heisenberg), mais son débit est très limité (de l'ordre de quelques dizaines de kbits/s) et son coût de mise en œuvre reste très élevé . La cryptographie par chaos quant à elle, a déjà donné la preuve de sa faisabilité et de sa puissance de chiffrage (>1Gbits/s) , c'est cette technique qu'on va traiter par la suite.

# CHAPITRE II

# La théorie du chaos

## II.1 Introduction

Dans ce chapitre après avoir donné brièvement des notions sur la modélisation mathématique d'un système dynamique, nous allons exposer une étude sur la transition de son comportement vers le chaos, en fonction des variations de ses paramètres, avec un test quantifié de cette transition , et enfin nous présentons des résultats de simulation de réponses de quelques systèmes chaotiques célèbres.

## II.2. Systèmes dynamiques

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

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

Dans ces représentations mathématiques interviennent des paramètres qui vont conditionner l'évolution de ce système, ainsi il peut avoir un comportement périodique, pseudopériodique ou chaotique [25] [35**]**.

### II.2.1.Modèle mathématique des systèmes dynamiques en temps continu

Un exemple d'un système dynamique dans lequel le temps $t$ est une variable continue est le système de n équations différentielles de premier ordre ordinaire et autonome [29] :

$$\begin{cases} \dfrac{dx_1}{dt} = F_1(x_1, x_2, \ldots, x_n) \\ \dfrac{dx_2}{dt} = F_2(x_1, x_2, \ldots, x_n) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \dfrac{dx_n}{dt} = F_n(x_1, x_2, \ldots, x_n) \end{cases} \quad \text{(II-1)}$$

Ce système peut être écrit sous la forme vectorielle comme suit :

$$\frac{dX}{dt} = F[X(t)] \quad \text{(II-2)}$$

Où $X$ est un vecteur à $n$ éléments. C'est un système dynamique car, pour n'importe quel état initial du système $X(0)$ , nous pouvons en principe résoudre l'équation pour obtenir le futur vecteur d'état $X(t)$ du système pour $t > 0$ .Si nous considérons un exemple concret d'un système dynamique continu , celui de Lorenz dans lequel il a résumé l'ensemble des prévisions météorologiques en trois équations différentielles qui sont [25] :

$$\begin{cases} \dfrac{dx}{dt} = \sigma.(y - x) \\ \dfrac{dy}{dt} = x.(\rho - z) - y \\ \dfrac{dz}{dt} = x.y - \beta.z \end{cases} \quad \text{(II-3)}$$

Où $\sigma$ représente le nombre de Prandtl du fluide, $\rho$ est proportionnel au nombre de Rayleigh et $\beta$ est relié au vecteur d'onde convectif. Les variables $x$ et $y$ sont respectivement proportionnelles aux amplitudes du champ de vitesse et du champ de température, alors que $z$ est relié au mode vertical de température et $t$ est le temps. On remarque que le système d'équation différentiel (II-3) est non linéaire car il comporte les termes $xy$ et $yz$.

L'outil informatique et l'usage de logiciels de calcul appropriés, faciliteront considérablement la résolution du système (II-3).

Alors pour $\sigma = 10, \rho = 28, \beta = 8/3$ et avec les conditions initiales $x_0 = 8, y_0 = 3, z_0 = 33$ , le résultat de la résolution du système (II-3) dans l'espace des phases est représenté sur la figure (II-1-a) et la représentation de la variable x en fonction du temps t sur la figure (II-1-b).

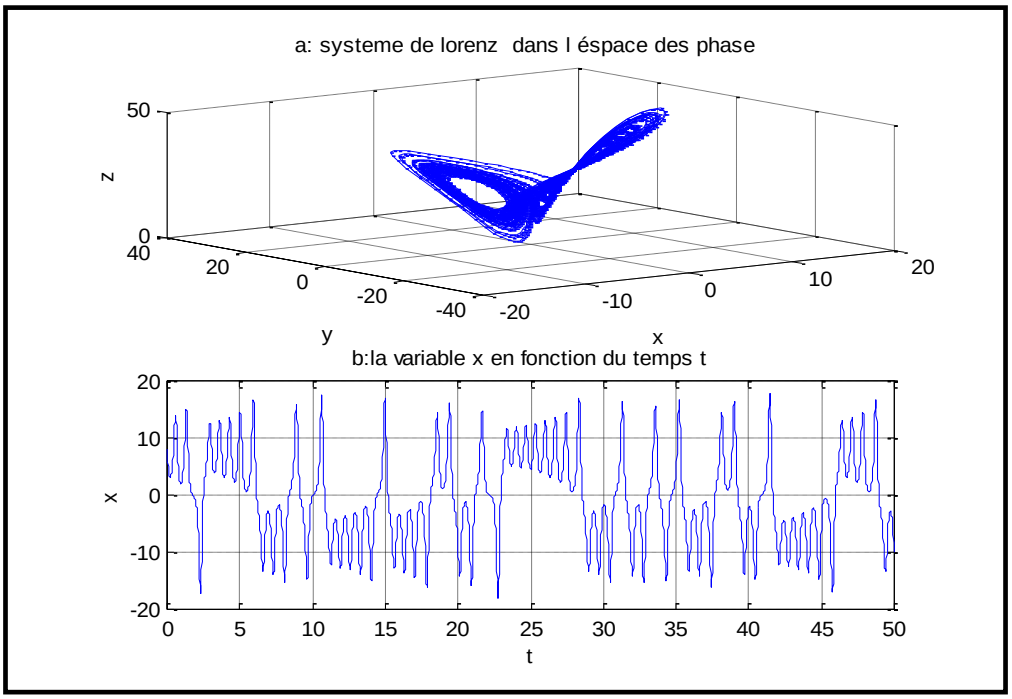



*Figure II.1 : représentation graphique de la résolution du système (II-3)*

**Remarque II.1**

Pour étudier complètement un système dynamique on ne doit pas se contenter de l'évolution d'une seule variable au cours du temps figure (II.1.b) , car son évolution est trop complexe, pour cela on a intérêt à considérer le système dans un espace mathématique appelé espace des phases ,représenté sur figure (II.1.a). Cet espace, bien qu'abstrait, contient sous forme géométrique une information concrète. Les variables qui sont à la base de la construction de cet espace sont des grandeurs réelles et à chaque point correspond une situation physique bien déterminée. Ainsi, l'espace des phases du système (II.3) est construit à partir des variables $x, y, z$ .

Le choix de ces variables n'est pas arbitraire. L'espace doit contenir toutes les informations sur la dynamique du système étudié. Les grandeurs doivent être indépendantes pour que chacune apporte sa propre information. Ce qui implique un certain nombre de variables nécessaires et introduit la notion de degré de liberté du système que nous prendrons égal à la dimension de l'espace des phases.

### II.2.2. Modèle mathématique des systèmes dynamiques en temps discret

Dans le cas discret, le système dynamique est représenté par des équations à différences finies ; le temps est évalué par un nombre entier $k$ (avec $k$ qui désigne la variable temps, $k = 0,1,2\ldots$), un exemple de ce système dynamique est la carte logistique qui peut être écrite sous une forme vectorielle comme :

$$X_{k+1} = F(X_k) \tag{II-4}$$

Où $X_k$ est à dimension $n$ et $X_k = (X_k^{(1)}, X_k^{(2)}, \ldots, X_k^{(n)})$ . Pour un état initial $X_0$, on obtient l'état du système pour le temps $k = 1$ par $X_1 = F(X_0)$ et de cette manière l'on peut déterminer les états suivants du système [29].

## II.3. Le chaos : définition et propriétés

Le terme chaos a été introduit avec sa signification actuelle en 1976 par Jim Yorke, un mathématicien de l'université du Maryland , mais le début des études du chaos peut être imputé a Henri Poincaré au début du XXe siècle , puis elles ont été ressuscitées en 1961 par le météorologue américain Edward Lorenz , professeur de mathématiques au MIT (Massachusetts Institute of Technology) qui est considéré après ses recherches sur le chaos , en tant que père officiel. Et depuis, ce concept a envahi beaucoup de domaines qu'ils soient physiques, mathématiques, politiques ou religieux [13] .

La définition qu'on peut donner au chaos est que c'est un phénomène qui peut apparaître dans les systèmes dynamiques déterministes non linéaires. Il présente un

aspect fondamental d'instabilité appelé sensibilité aux conditions initiales, ce qui le rend imprédictible en pratique à long terme. Une autre caractéristique du système chaotique est son évolution qui semble aléatoire.

### II.3.1. La route vers le chaos dans les systèmes dynamiques

La trajectoire d'un système dynamique à partir d'un vecteur de conditions initiales $X_0$ et en passant par un régime transitoire, arrive à une région permanente de l'espace des phases. Ce comportement asymptotique obtenu pour $t$ (en continu) ou $k$ (discret) qui tendent vers l'infini est une des caractéristiques essentielles à étudier pour tout système dynamique. Pour les systèmes linéaires la solution asymptotique est unique et ne dépend pas des conditions initiales. La non linéarité engendre une plus grande variété de régimes permanents, parmi lesquels on trouve, par ordre de complexité : points d'équilibre, solutions périodiques, solutions quasi-périodiques et chaos, respectivement [25]. Ces comportements peuvent être illustrés dans un exemple de systèmes dynamiques unidimensionnels discrets, connu dans la théorie des systèmes non linéaires sous le nom de la carte logistique, qui est une fonction itérative définie par la fonction :

$$f : [0,1] \to [0,1] \quad x_{k+1} = f(x_k) = r.x_k.(1 - x_k) \tag{II.5}$$

Le paramètre $r$ défini dans $[0,4]$ , est responsable du type de comportement de cette dynamique.

La figure (II.2) représente le comportement du système (II-5) en fonction du paramètre $r$ . Ainsi on trouve pour $r = 2$, la tendance de la suite logistique vers un point d'équilibre, pour $r = 3.2$ la suite logistique oscille entre deux valeurs ,pour $r = 3.5$ la suite logistique oscille entre plus de deux valeurs et pour $r = 3.9$ la suite logistique a un comportement qui semble aléatoire : c'est le comportement chaotique.

La figure (II-3) représente un diagramme dit de bifurcation de Feigenbaum [27] , qui décrit la transition de la suite logistique vers le chaos.

Dans notre représentation on a choisi le temps discret $k = 0,1,2...100$ et le nombre de valeurs de $r$ égal à 500 définies dans l'intervalle $[0,4]$ . On remarque dans le diagramme de bifurcation de Feigenbaum que :

- pour $1 \le r < 3$ , le système possède un point fixe attractif qui devient instable lorsque $r = 3$ comme il est représenté sur la figure (II-3) .
- pour $3 \le r < 3.373$ le système se comporte périodiquement, de période $2^m$ où $m$ est un entier qui tend vers l'infini lorsque $r$ tend vers 3.57, comme il est représenté sur la figure (II-3) .
- pour $3.57 \le r < 4$ le système présente une succession de bifurcations (doublement de période), alors on aura un comportement chaotique, comme il est représenté sur la figure (II-3) .

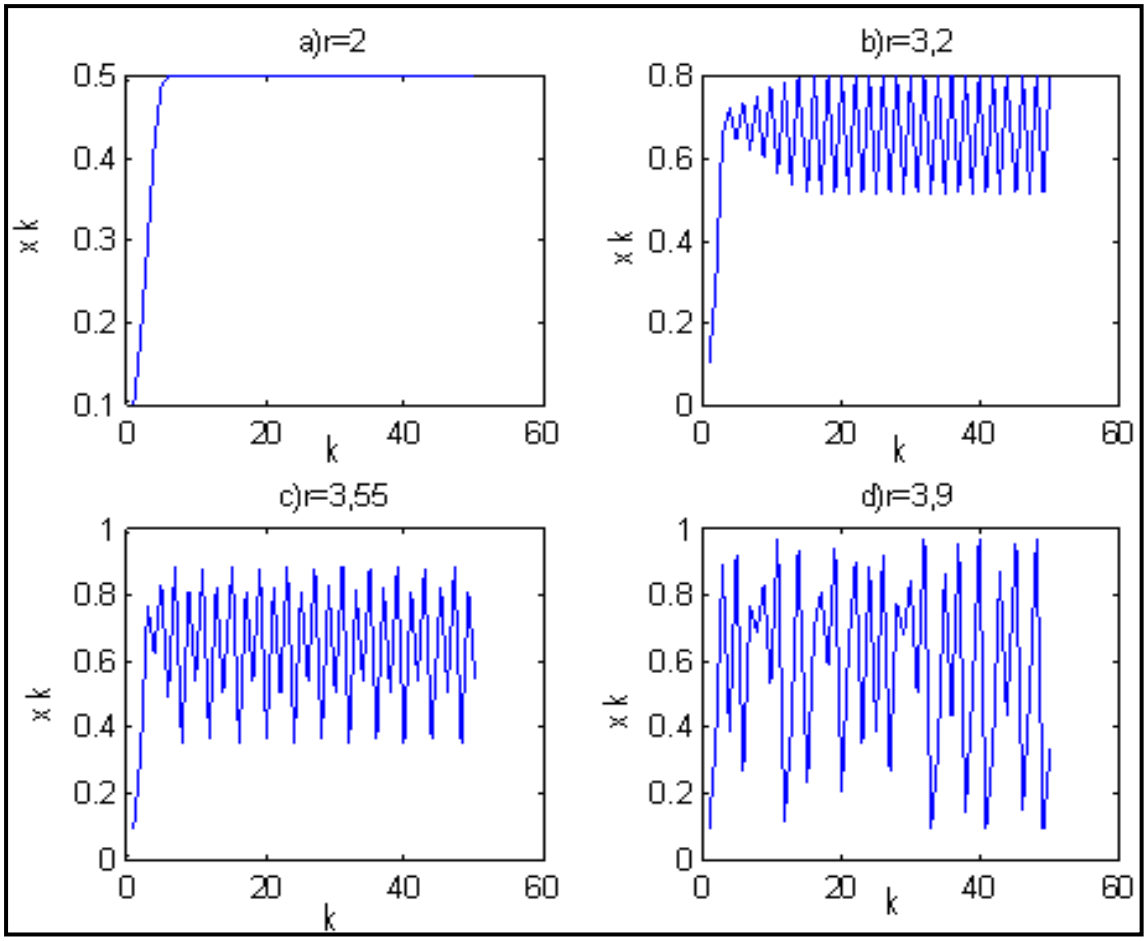



*Figure (II.2) Séquences générées par la fonction logistique pour* $x_0 = 0.1$ *pour : a)* $r = 2$ *;b)* $r = 3.2$ *; c)* $r = 3.55$ *; d)* $r = 3.9$

**Remarque II.2**

Dans la région de comportement chaotique du système on peut trouver une fenêtre où il peut présenter des oscillations périodiques ,voir figure (II.3).

En conclusion un système dynamique chaotique est caractérisé par un comportement sensible aux conditions initiales et un aspect semblable à l'aléatoire.

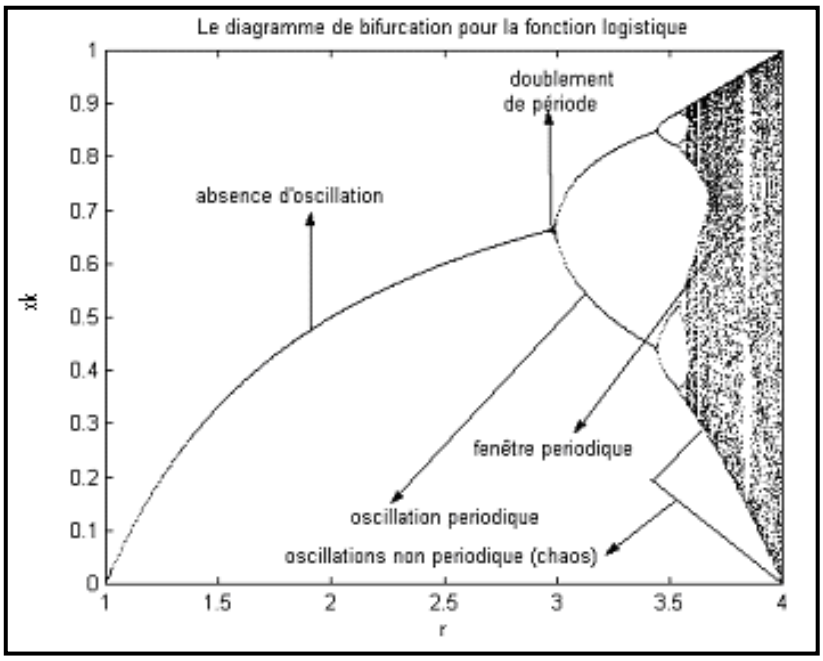



*Figure (II.3) La route vers le chaos de la suite logistique*

**II.3.2. Test du chaos dans un système dynamique**

Tester le chaos dans un système dynamique peut être procédé par élimination des comportements que nous avons vus au paragraphe (II.3.1). C'est-à-dire , si le comportement d'un système dynamique n'est pas un point fixe, ni périodique ou quasi périodique, on conclut alors qu'il est chaotique. Mais dans le cas d'un système affecté par un bruit, et la séquence qu'il génère n'est pas connue , cette méthode est alors à rejeter . En conséquence les scientifiques ont proposé des solutions basées sur une approche statistique dont la plus utilisée pratiquement est celle des exposants de Lyapunov, vu sa performance et son coût de calcul relativement réduit. On peut ainsi quantifier la divergence des trajectoires d'un système dynamique issues des conditions initiales différentes en calculant son exposant de Lyapunov ,dont la valeur est un

indicateur utilisé pour tester le chaos dans le système.

Nous allons traiter tout d'abord le calcul des exposants de Lyapunov pour un système unidimensionnel, puis pour un système de dimension supérieure à 1.

❖ **Exposants de Lyapunov pour un système de dimension égale a 1**

Soit un système dynamique unidimensionnel modélisé par une fonction discrète $f$ de $\mathbb{R} \longrightarrow \mathbb{R}$ qui applique [27] :

$$x_k = f(x_{k-1}) \tag{II.6}$$

Si on choisit deux conditions initiales très proches :

$$x_0 \qquad \text{et} \quad x_0 + \delta x_0 \tag{II.7}$$

Si on suppose que l'écart entre les trajectoires du système issues des conditions initiales (II.7), après $k$ itération et avec l'existence d'un réel $\lambda$ peut être quantifié par :

$$\left| f^k(x_0 + \delta x_0) - f^k(x_0) \right| \approx \delta x_0 e^{k\lambda} \tag{II.8}$$

d'où $$k\lambda \approx \ln \frac{\left| f^k(x_0 + \delta x_0) - f^k(x_0) \right|}{\delta x_0} \tag{II.9}$$

pour $\delta x_0 \to 0$ on aura :

$$\lambda \approx \frac{1}{k} \ln \frac{\left| f^k(x_0 + \delta x_0) - f^k(x_0) \right|}{\delta x_0} = \frac{1}{k} \ln \left| \frac{df^k(x_0)}{dx_0} \right|$$

$$\approx \frac{1}{k} \ln \left| \frac{df^k(x_0)}{df^{k-1}(x_0)} . \frac{df^{k-1}(x_0)}{df^{k-2}(x_0)} \ldots . \frac{df^1(x_0)}{dx_0} \right|$$

$$\approx \frac{1}{k} \ln \left| \frac{df(x_{k-1})}{dx_{k-1}} . \frac{df(x_{k-2})}{dx_{k-2}} \ldots . \frac{df(x_0)}{dx_0} \right| = \frac{1}{k} \sum_{i=0}^{k-1} \ln \left| \frac{df(x_i)}{dx_i} \right| \tag{II.10}$$

ainsi on aura : $$\lambda = \lim_{k \to +\infty} \frac{1}{k} \sum_{i=0}^{k-1} \ln \left| f'(x_i) \right| \tag{II.11}$$

$\lambda$ est appelé exposant de Lyapunov , il représente le taux de divergence .

➪**Pour** $\lambda \leq 0$ **:** la trajectoire de l'évolution du système peut tendre vers un point fixe, avoir un comportement périodique ou quasi-périodique.

➪**Pour** $\lambda > 0$ **:** le système est chaotique .

**Exemple II.1**

Si on applique l'expression (II.11) pour le calcul de l'exposant de Lyapunov de la fonction logistique (II.5) on aura alors :

$$\lambda = \lim_{k \to +\infty} \frac{1}{k} \sum_{i=0}^{k-1} \ln \left| \left( r - 2.r.x_i \right) \right| \qquad \text{(II.12)}$$

On peut ainsi visualiser la transition vers le chaos pour ce système en ajoutant sur la figure (II.3) la variation de l'exposant de Lyapunov $\lambda$ en fonction de r, ceci est représenté sur la figure (II.4), qui est une simulation pour 100 itérations de $x_k$ et 500 valeurs de $r$ .

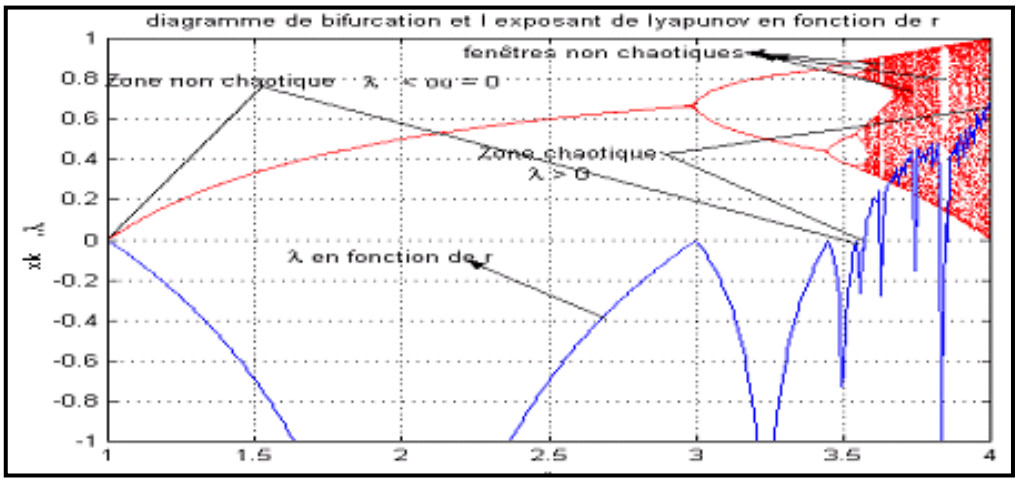



*Figure (II-4) Diagramme de bifurcation et exposant de Lyapunov*

❖ **Exposants de Lyapunov pour un système de dimension supérieure à1**

Pour un système de dimension supérieure à 1 on parle de spectre d'exposants de Lyapunov dont le nombre est égal à cette dimension. Ainsi si nous avons par exemple un système dynamique continu dans un espace de phase de dimension $n$ , son spectre d'exposants de Lyapunov peut être défini par un ensemble ;

$$\{\lambda_1, \lambda_2, \ldots\ldots \lambda_n\} \qquad \text{(II.13)}$$

Géométriquement si on choisit pour étudier ce système un ensemble de conditions initiales dans une sphère infiniment petite (de diamètre $\delta(0)$); la sphère va se déformer en ellipsoïde au cours du temps. Le i$^{eme}$ exposant de Lyapunov se définit en fonction de la déformation subie sur la $i^{éme}$ direction [25] [38] comme

$$\lambda_i = \lim_{t\to\infty} \frac{1}{t} \ln\left(\left|\frac{\delta_i(t)}{\delta_i(0)}\right|\right), i = 1..n \qquad \text{(II.14)}$$

La classification des comportements des systèmes dynamiques selon les exposants de Lyapunov est représentée sur le tableau (II.1) [25] :

| **Régime permanent** | **Attracteur** | **Spectre** | **Exposants de Lyapunov** |
|---|---|---|---|
| point d'équilibre | point | composante continue | $\lambda_n \le \lambda_{n-1} \le \ldots\ldots \le \lambda_1 < 0$ |
| périodique | courbe fermée | fréq. fondamentale + harmoniques entières | $\lambda_n \le \lambda_{n-1} \le \ldots\ldots \lambda_2 < \lambda_1 = 0$ |
| quasi-périodique | tore | composantes fréquentielles en rapport irrationnel | $\lambda_1 = \ldots = \lambda_i = 0$<br>$\lambda_n \le \lambda_{n-1} \le \ldots\ldots \le \lambda_{i+1} < 0$ |
| chaotique | fractale | spectre large | $\lambda_1 > 0$<br>$\lambda_n \le \lambda_{n-1} \le \ldots . \lambda_2 \le 0$ |

*Tableau (II.1) : Classification du comportement du système dynamique en fonction des exposants de Lyapunov*

**Remarque II.3**

Dans le tableau ci dessus on a cité une notion importante qui est la notion d'attracteur, qui représente par définition la limite asymptotique des solutions partant de toute condition initiale située dans un bassin d'attraction qui est un domaine de volume non nul.

Ainsi pour un système chaotique l'existence d'un attracteur nécessite que la dynamique de ce système soit globalement dissipative. Cela signifie que le système doit être caractérisé par une stabilité globale qui correspond à la condition suivante sur le

spectre de Lyapunov :

$$\sum_{i=1}^{n} \lambda_i < 0 \qquad \text{(II.15)}$$

**Exemple II.2**

Si on veut calculer le spectre d'exposants de Lyapunov du système de Lorenz décrit par le système d'équations différentielles (II.3) ,avec les mêmes paramètres et les mêmes conditions initiales ; on utilise pour cela l'algorithme de A.Wolf et al publié en 1985 [38].

Cet algorithme est conçu essentiellement pour estimer les exposants de Lyapunov des systèmes expérimentaux, ainsi on procède par observer le système à étudier et on mesure à chaque unité de temps, les variables d'états qui le caractérisent, ensuite en fonction de ces variables et du temps passé on calcule les exposants de Lyapunov . Les évolutions des exposants de Lyapunov pour le système de Lorenz sont représentées sur la figure (II.5).

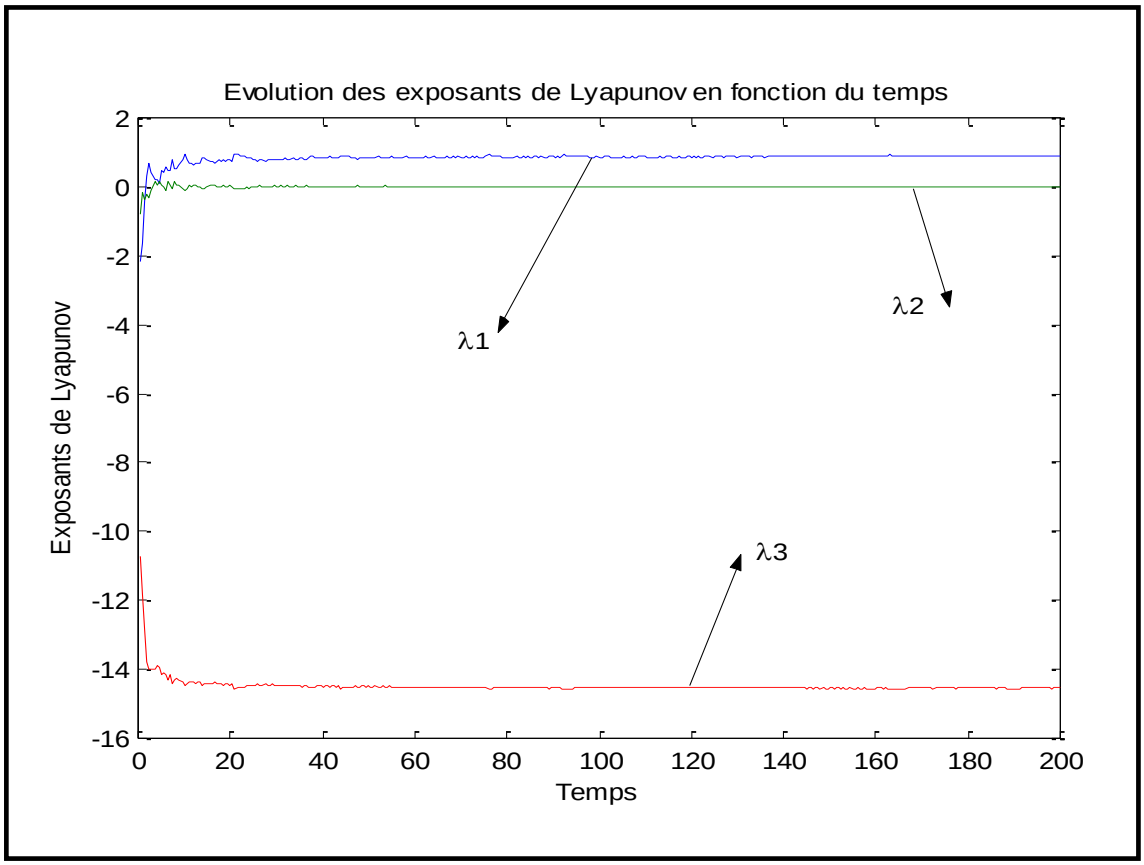



*Figure (II.5) : Evolution des exposants de Lyapunov du système de Lorenz en fonction du temps*

Sur la figure (II.5) les limites asymptotiques de $\lambda_1, \lambda_2 et \lambda_3$ sont données par :

$$\begin{cases} \lambda_1 \longrightarrow 0.7895 \\ \lambda_2 \longrightarrow -0.0526 \\ \lambda_3 \longrightarrow -14.5263 \end{cases} \quad \text{(II.16)}$$

Alors , on conclut que le système est chaotique car $\lambda_1$ est supérieur a 0 et que le système est globalement dissipatif car $\sum \lambda_i = -13.7894 < 0$, alors ce système peut être utilisé dans un cryptosysteme chaotique.

## II.4. Exemples de systèmes chaotiques

Dans cette partie, nous exposons les exemples les plus connus et les plus étudiés des systèmes chaotiques.

### II.4.1. Systèmes chaotiques à temps continu

Pour les systèmes chaotiques à temps continu, on peut considérer : le système de Lorenz, le système de Rössler et l'oscillateur de Chua.

❖ **Système chaotique de Lorenz**

On rapporte que la théorie du chaos ne s'est véritablement développée qu'à partir de 1960 après les travaux du mathématicien et passionné de la météorologie ,l'américain Edward Lorenz, qui représentent une révolution dans la théorie des mathématiques en prouvant qu'il existe des modèles mathématiques déterministes de phénomènes physiques, qui aboutissent après plusieurs itérations à des résultats imprévisibles en variant d'une manière infinitésimale leurs conditions initiales. Le phénomène physique étudié par Lorenz est l'imprévisibilité à longue durée des fluctuations climatiques dans la nature, ainsi par la suite de ses recherches en 1972, Lorenz a organisé une conférence à l'American Association for the Advancement of Science , intitulée: «Prédictibilité : le battement d'ailes d'un papillon au Brésil peut-il provoquer une tempête au Texas ?» [6]. Cette hypothèse veut dire que l'imprévisibilité est devenue une caractéristique essentielle du chaos. Le modèle mathématique de Lorenz est celui qu'on a donné par l' équation (II.3). La représentation graphique de

ce système est donnée à la figure (II.6), où on voit l'attracteur de Lorenz, la coordonnée x en fonction du temps et la sensibilité aux conditions initiales de la coordonnée $x$ pour $[x_0 = 8, y_0 = 3, z_0 = 33]$ et $[x_0 = 8.001, y_0 = 3.001, z_0 = 33.001]$ .

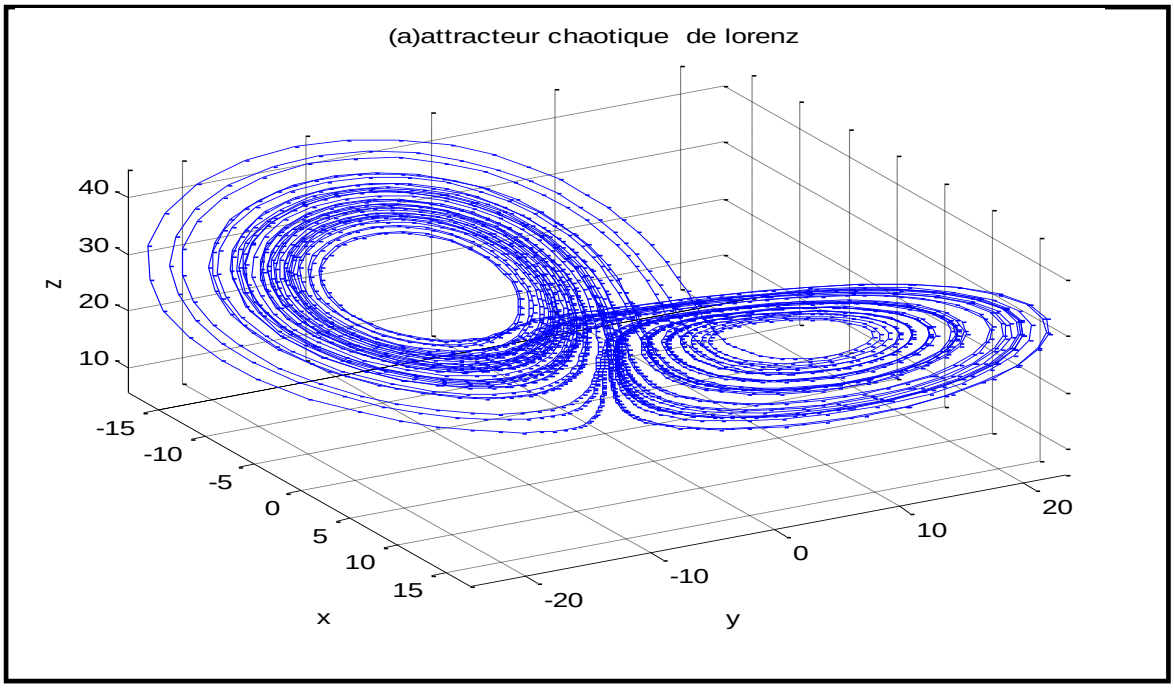



*Figure (II.6.a)*

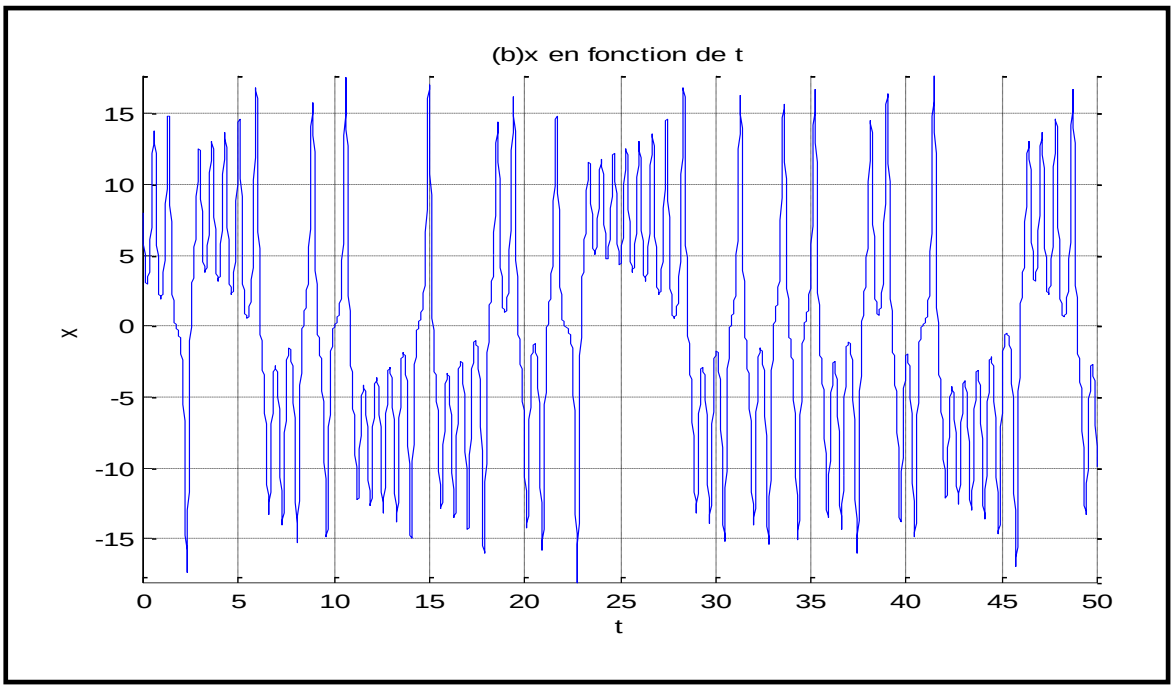



*Figure (II.6.b)*

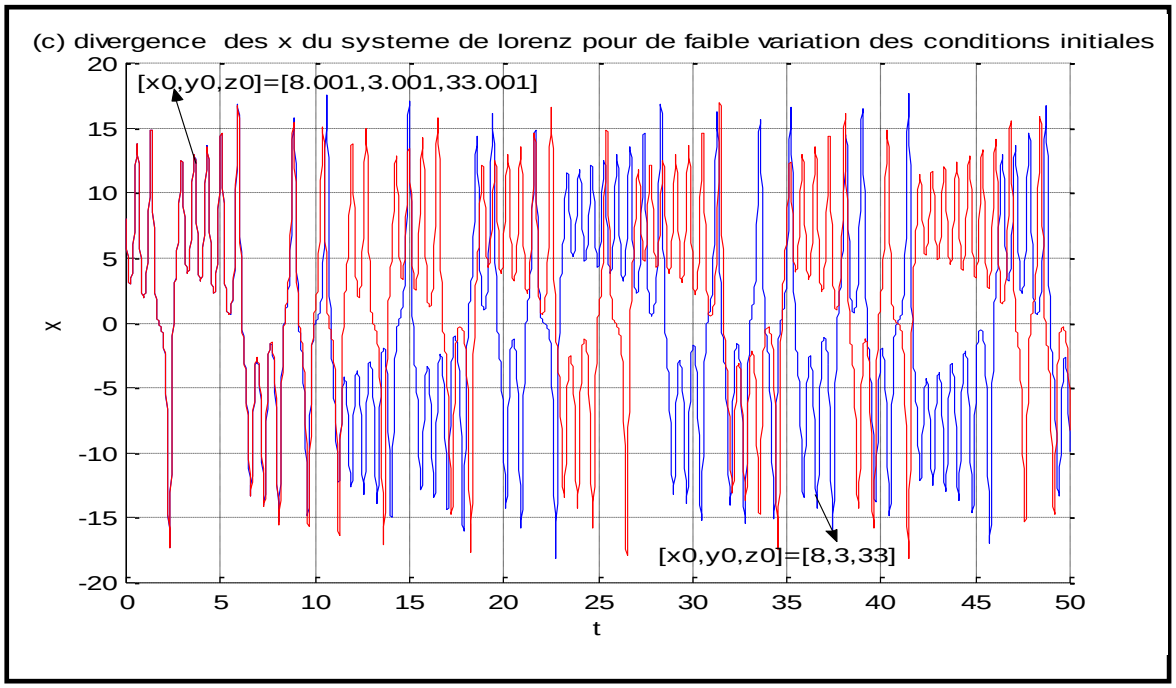



*Figure (II.6.c)*

*Figure (II.6) : Réponse du système chaotique de Lorenz*

❖ **Système chaotique de Rössler**

Ce système semblable à celui de Lorenz, a été proposé par le biochimiste Allemand Otto Rössler en 1976, il découle des équations de Navier Stokes, ainsi il est lié à l'étude de l'écoulement des fluides. Le modèle mathématique résultant est[6], [43] :

$$\begin{cases} \dfrac{dx}{dt} = -(y+z) \\ \dfrac{dy}{dt} = x + a.y + 0.01.x.\ln(z) \\ \dfrac{dz}{dt} = c + z.(x-b) \end{cases} \qquad \text{(II.17)}$$

La représentation graphique de ce système est donnée par la figure (II.7) ,où on voit l'attracteur de Rössler , les coordonnées (x,y,z) en fonction du temps et la

sensibilité aux conditions initiales pour $[x_0 = 0.01, y_0 = 0.01, z_0 = 0.01]$ et $[x_0' = 0.011, y_0' = 0.011, z_0' = 0.011]$ pour les paramètres $[a = 0.2, b = 5.7, c = 0.2]$ .

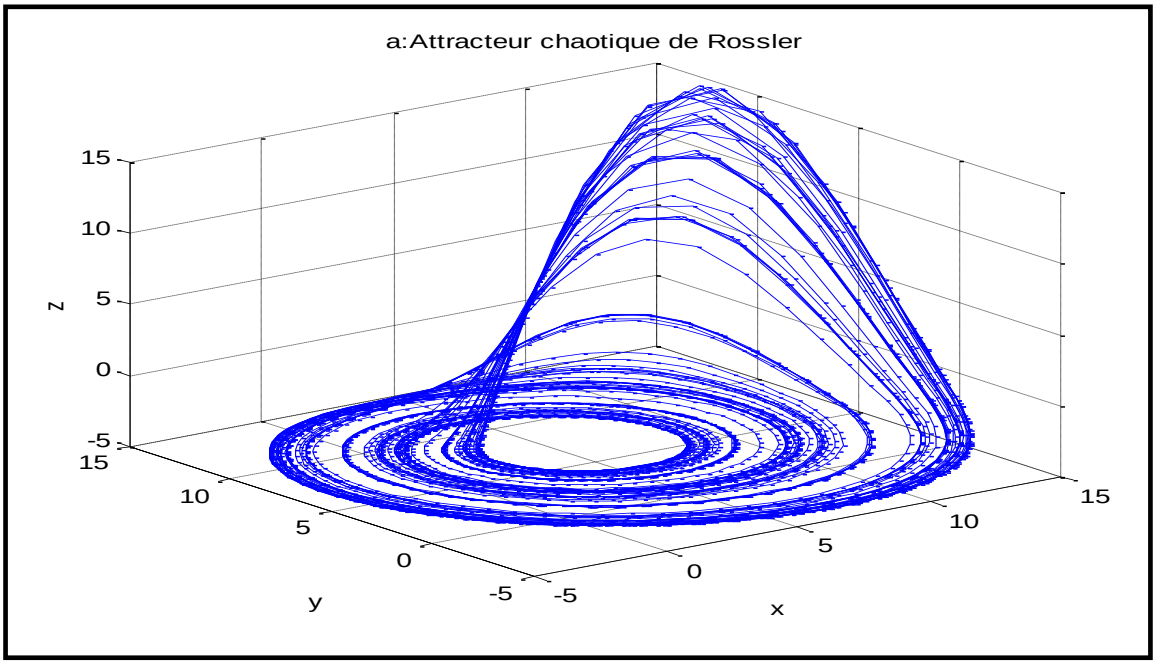



*Figure (II.7.a)*

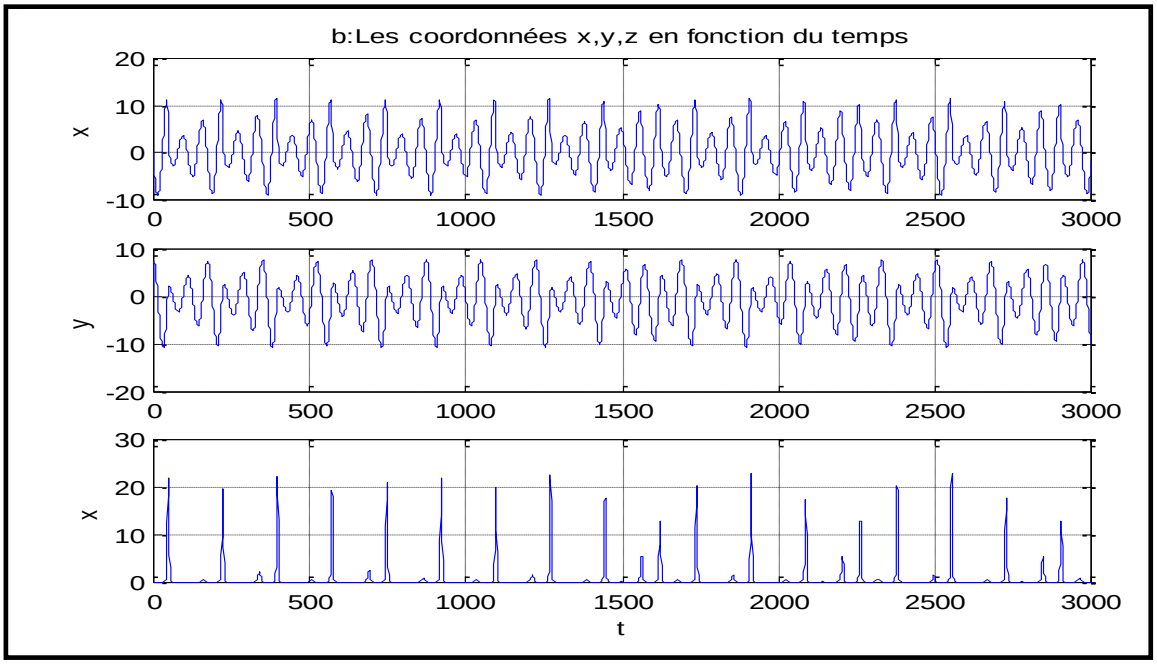



*Figure (II.7.b)*

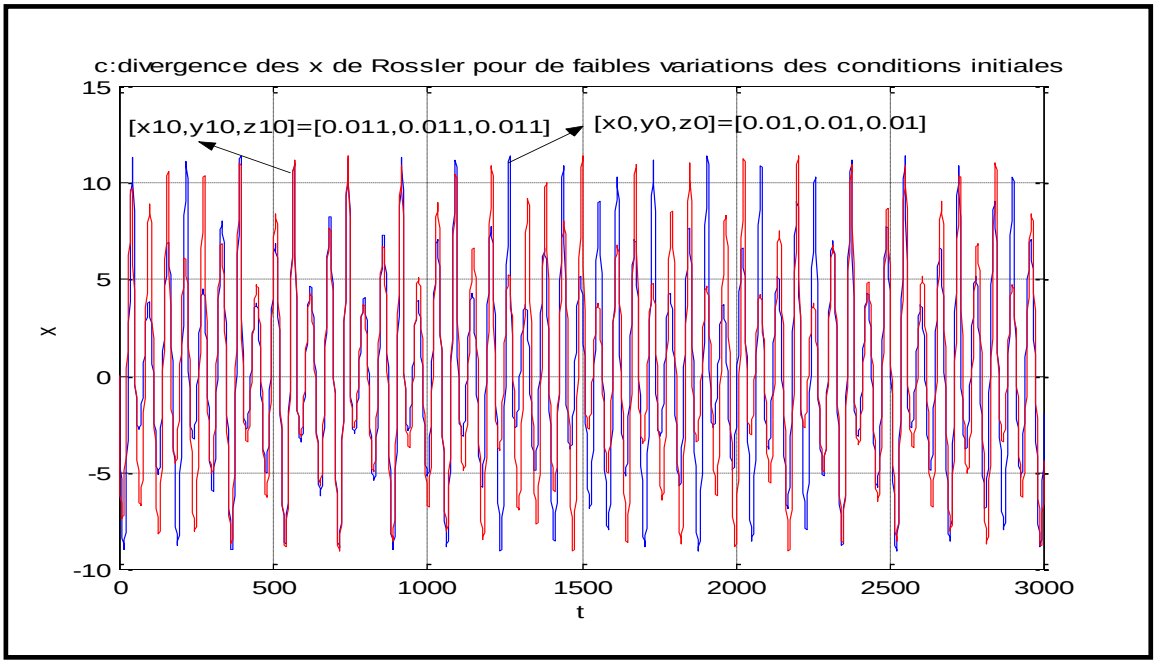



*Figure (II.7.c)*

*Figure (II.7) : Réponse système chaotique de Rössler*

❖ **Oscillateur chaotique de Chua**

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

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

L'existence des attracteurs chaotiques du circuit de Chua avait été confirmée numériquement par Matsumoto [28] et expérimentalement observée par Zhong et Ayrom [44].

La figure (II.8) présente le circuit de Chua [17] , constitué de deux condensateurs, une résistance, une inductance et une résistance négative non linéaire.

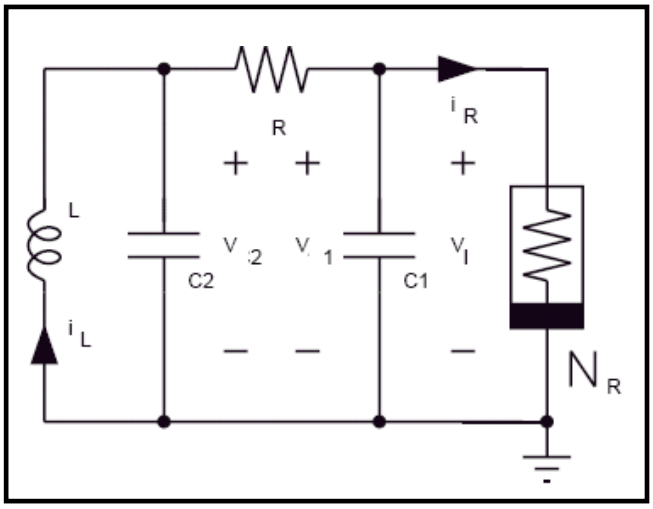



*Figure (II.8) : Le circuit électrique de l'oscillateur de Chua[17]*

Ce circuit est décrit par le système d'équations différentielles suivant :

$$\begin{cases} C1.\dfrac{dv_1}{dt} = \dfrac{1}{R}.(v_2 - v_1) - f(v_1) \\ C2.\dfrac{dv_2}{dt} = \dfrac{1}{R}(v_1 - v_2) + i_L \\ L.\dfrac{di_L}{dt} = -v_2 \end{cases} \qquad \text{(II.18)}$$

Où la fonction non linéaire de Chua $f(v_1)$ , représentée dans la figure (II.9), est la caractéristique courant–tension de la résistance équivalente $N_R$ de deux résistances négatives en parallèle $N_{R1}$ et $N_{R2}$ , dont leurs fonctions sont données par [17] :

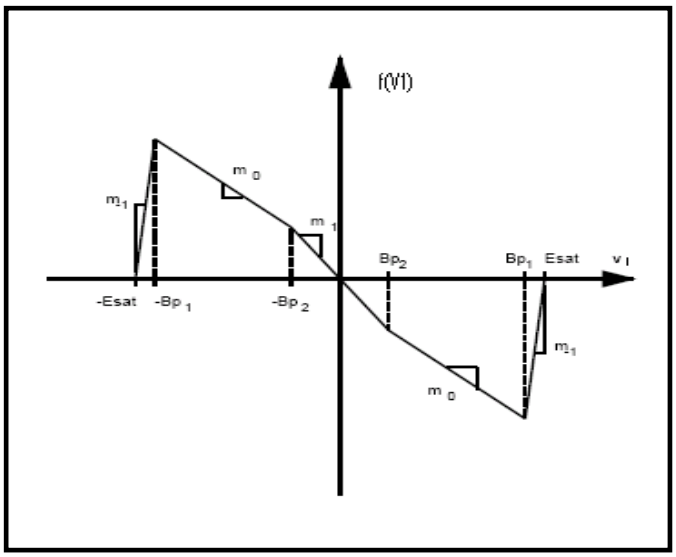



*Figure (II.9) : Fonction non linéaire de Chua[17]*

Les caractéristiques courant–tension des deux résistances négatives $N_{R1}$ et $N_{R2}$ sont données par la figure (II.10). Ainsi :

$$f(v_1) = g_1(v_1) + g_2(v_2) \qquad \text{(II.19)}$$

(a) (b)

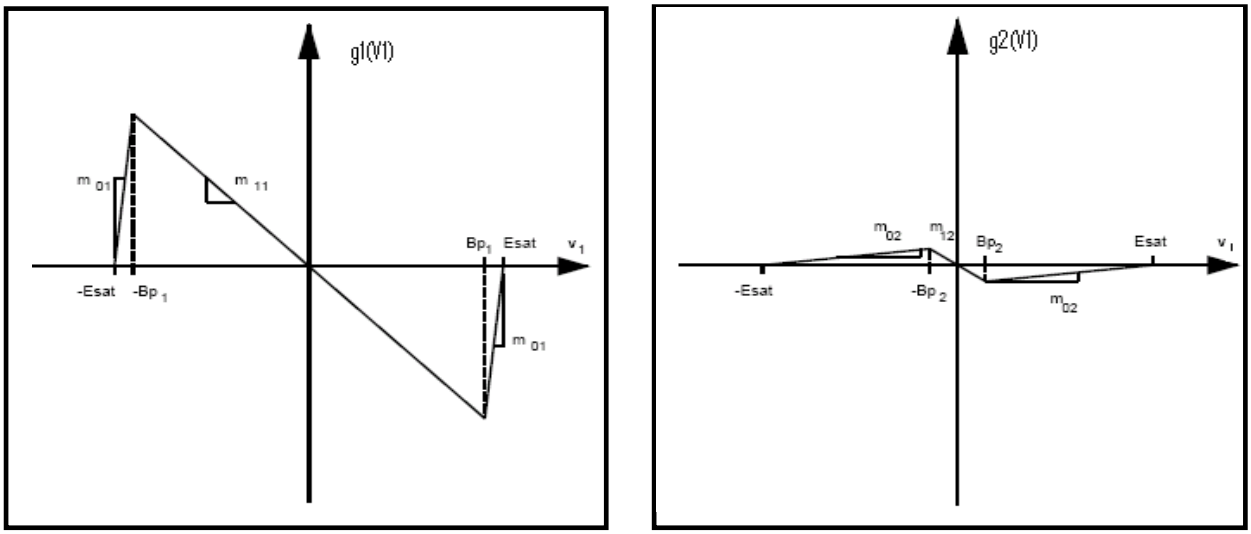



*Figure (II.10) : (a) Caractéristique de $N_{R1}$ ; (b) Caractéristique de $N_{R2}$ [17]*

Le courant dans la résistance négative équivalente est :

$$i_{NR} = i_{NR1} + i_{NR2} \tag{II.20}$$

avec :

$$i_{NR} = f(v_1)\ ,\ i_{NR1} = g_1(v_1)\ ,\ i_{NR2} = g_2(v_2) \tag{II.21}$$

d'où $$f(v_1) = m_0.v_1 + \frac{1}{2}.(m_1 - m_0).\left[\left|v_1 + B_{p1}\right| - \left|v_1 - B_{p1}\right|\right] \tag{II.22}$$

Le circuit complet de l'oscillateur de Chua est représenté sur la figure (II.11), La résistance de Chua est réalisée en utilisant des amplificateurs opérationnels .

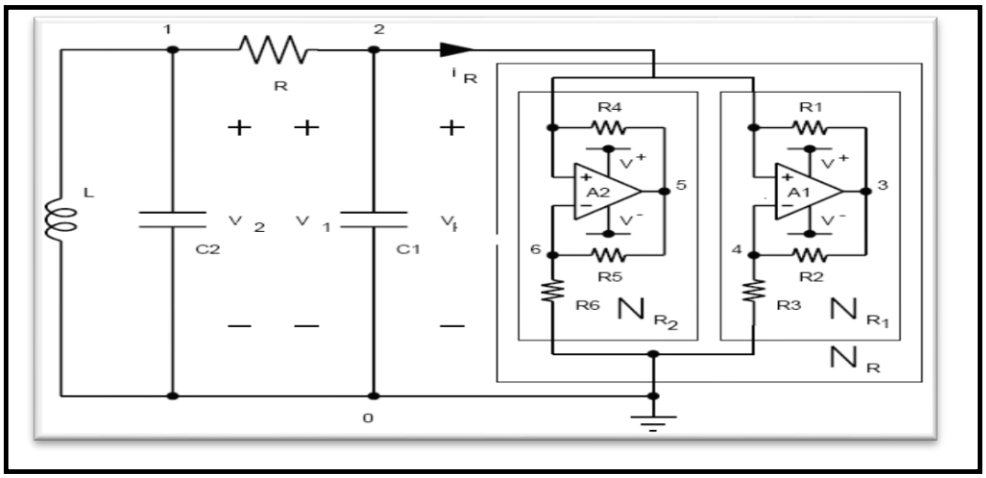



*Figure (II.11) : Circuit complet de l'oscillateur de Chua [17]*

Avec $R_1 = R_2$ et $R_5 = R_4$ Les paramètres de la fonction $f(v_1)$ sont donnés par :

$$m_{01} = \frac{1}{R_1}, m_{11} = -\frac{1}{R_3}, m_{02} = \frac{1}{R_4}, m_{12} = -\frac{1}{R_6}, B_{p1} = \frac{R_3.E_{sat}}{(R_2 + R_3)}, B_{p2} = \frac{R_6.E_{sat}}{(R_5 + R_6)} \tag{II.23}$$

et pour la combinaison des deux résistances négatives représentée sur la figure (II.9) :

$$m_{11} + m_{02} = m_0, m_{11} + m_{12} = m_1 \quad \text{(II.24)}$$

Pour la réalisation pratique du circuit, Kennedy [17] a choisi deux alimentations $V^+ = +9V et V^- = -9V$ et il a choisi l'amplificateur opérationnel AD 712 pour la réalisation de la résistance non linéaire ainsi $E_{sat} = +8.3V$ . Aussi, il a trouvé pour les paramètres de la caractéristique de la résistance non linéaire :

$$m_0 = -0.409\,mS, m_1 = -0.756\,mS, B_p = 1.08V$$

En suivant cette stratégie de conception, Kennedy [17] a dérivé une liste complète de composants pour le circuit de Chua représenté sur le tableau (II.2):

| Composants | Description | Valeur | Tolérance |
|---|---|---|---|
| Amplificateur opérationnel | AD 712 ou le TL082 | | |
| $R1$ | Résistance de $\frac{1}{4}W$ | $220\Omega$ | 5% |
| $R2$ | Résistance de $\frac{1}{4}W$ | $220\Omega$ | 5% |
| $R3$ | Résistance de $\frac{1}{4}W$ | $2.2k\Omega$ | 5% |
| $R4$ | Résistance de $\frac{1}{4}W$ | $22k\Omega$ | 5% |
| $R5$ | Résistance de $\frac{1}{4}W$ | $22k\Omega$ | 5% |
| $R6$ | Résistance de $\frac{1}{4}W$ | $3.3k\Omega$ | 5% |
| $R$ | Potentiomètre | $2k\Omega$ | |
| $C1$ | Capacité | $10nF$ | 5% |
| $C2$ | Capacité | $100nF$ | 5% |
| $L$ | Inductance | $18mH$ | 10% |

*Tableau (II.2) : Liste des composants pour la réalisation du circuit de Chua[17]*

Plusieurs articles ont été publiés sur l'étude du chaos dans le circuit de la figure (II.10) en fonction de la variation d'un de ses paramètres (L, $C_1$, $C_2$, R et la tension de polarisation de l'amplificateur opérationnel). La figure (II.12) représente le comportement du circuit de Chua en

variant la résistance R pour une simulation avec le logiciel Multisim 7 [15] ,[17],[26],[28].

La figure (II.12) interprète la route vers le chaos de la réponse du circuit de Chua en fonction de la variation de la résistance R. Ainsi pour (a) R= 2kΩ , génération d'un signal sinusoïdal qui tend vers une tension continue ; (b) R=1.95kΩ , génération d'un signal périodique sinusoïdal ;(c) R =1.94 kΩ , génération d'un signal périodique avec dédoublement de la période ; (d) R= 1.8999 kΩ ,génération d'un signal qui a un aspect qui semble aléatoire et ressemblance avec le système de Rössler donc c'est un système chaotique ;(e) R =1.88 kΩ , génération d'un signal qui a un aspect qui semble aléatoire et ressemblance avec le système de Lorenz donc c'est un système chaotique .

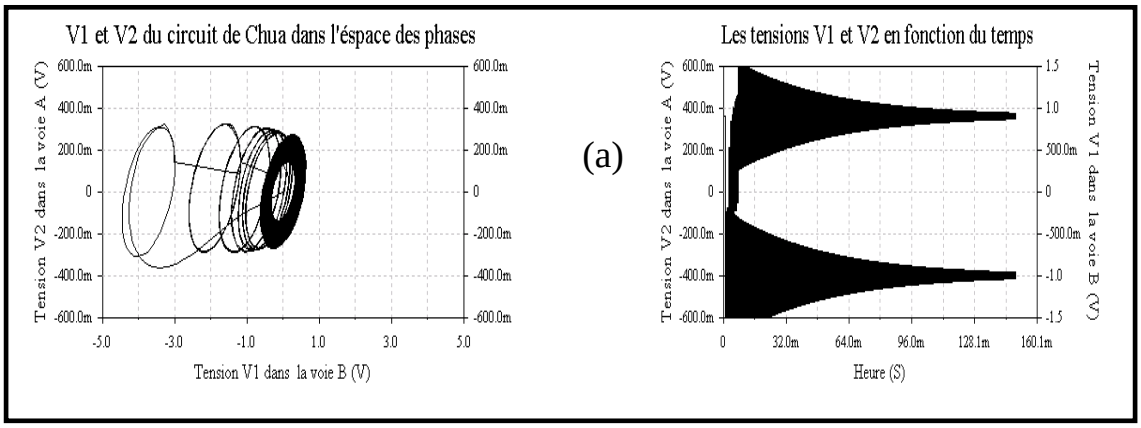



*Figure (II.12.a)*

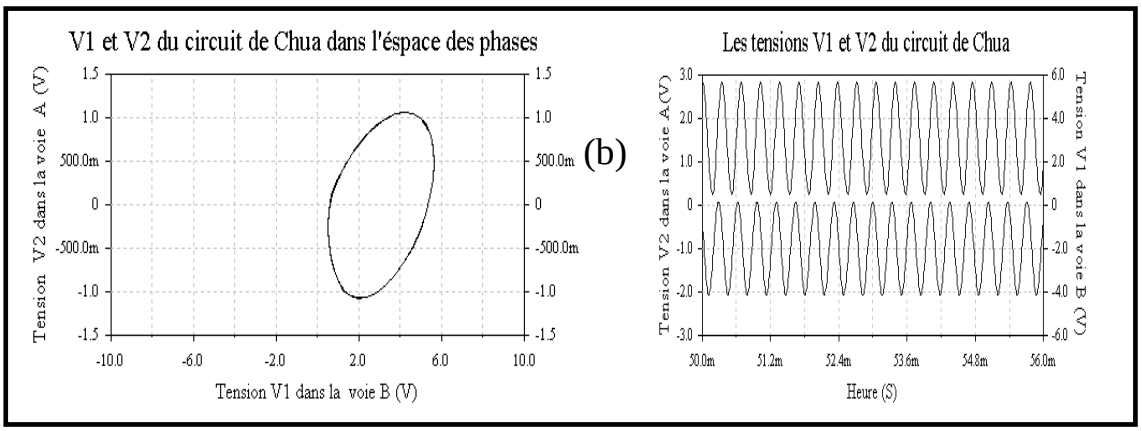



*Figure (II.12.b)*

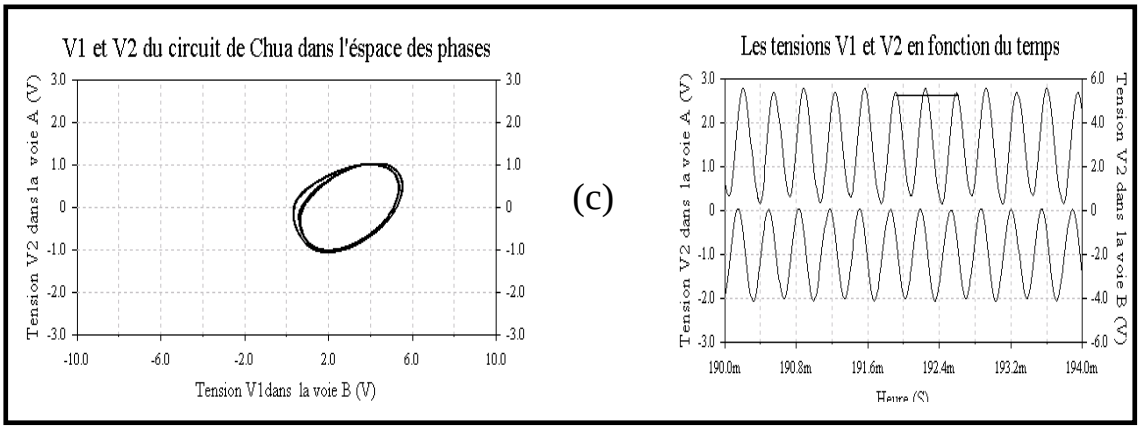



*Figure (II.12.c)*

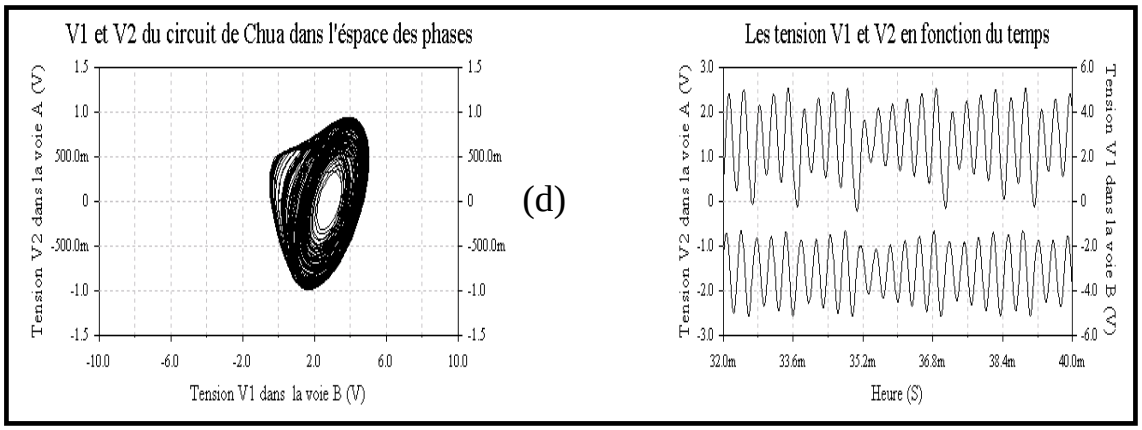



*Figure (II.12.d)*

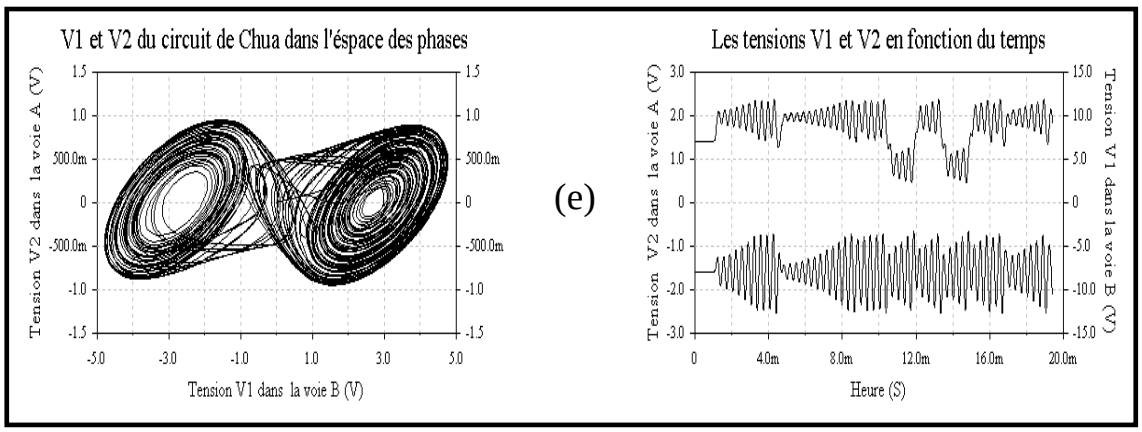



*Figure (II.12.e)*

*Figure (II.12) : Résultat de simulation de l'oscillateur de Chua par le logiciel Multisim7*

### II.4.2. Systèmes chaotiques à temps discrets

Pour les systèmes chaotiques à temps discret on peut considérer le système unidimensionnel de la suite logistique , que nous avons vu au paragraphe (II-2-2) et le système bidimensionnel de Hénon.

❖ **Système de Hénon**

Ce système est un modèle proposé en 1976 par le mathématicien Michel Hénon [43] .L'intérêt de ce modèle est l'étude de certaines propriétés d'une section de Poincaré de l'attracteur de Lorenz par l'introduction d'itérations dans le plan. Le modèle mathématique de ce système est donné par :

$$\begin{cases} x_{k+1} = a - x_k^2 + b.y_k \\ y_{k+1} = x_k \end{cases} \qquad \text{(II.25)}$$

Les valeurs des paramètres proposées par Michel Hénon pour observer le phénomène chaotique sont : $a = 1.4 et b = 0.3$ . Pour simuler l'attracteur de Hénon on a pris pour conditions initiales $(x_0 = 0, y_0 = 0)$ . Ainsi la figure (II.13) représente l'attracteur de Hénon et la figure (II.14) montre l'évolution qui semble aléatoire de la coordonnée $X_n$ en fonction du temps.

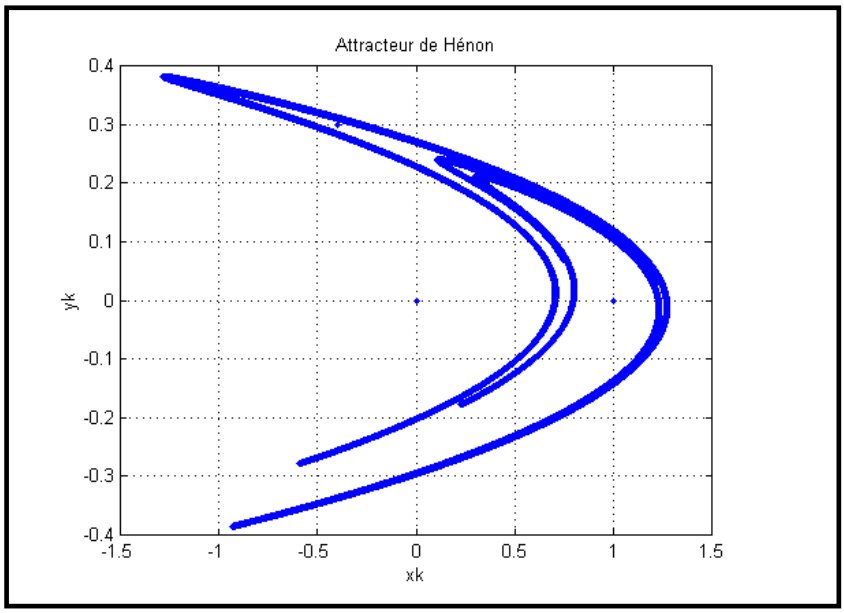



*Figure (II.13) :Attracteur chaotique de Hénon*

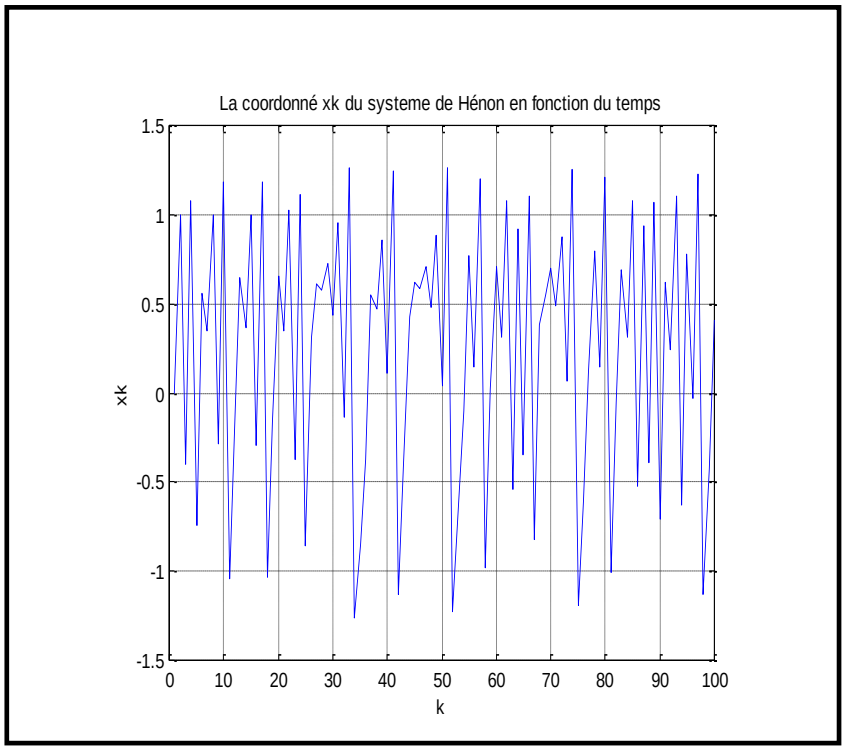



*Figure (II.14) : Evolution chaotique de la coordonnée $x_k$ en fonction du temps discret k*

## II.5. Conclusion

Dans ce chapitre, on a présenté une étude théorique du phénomène chaotique. En décrivant comment le distinguer, comment le quantifier et comment le changement des paramètres d'un système dynamique peut l'amener vers le chaos.

# CHAPITRE III

# La synchronisation du chaos

## III.1. Introduction

L'usage du chaos pour la sécurisation de la télécommunication pose directement le problème de synchronisation du récepteur afin de suivre le signal chaotique employé à l'émetteur. Alors c'est quoi la synchronisation ?

Le mot "synchronisation" vient du grec " *συν* " (syn) qui veut dire "ensemble " et "*χρνος* " (chronos) qui veut dire "temps. " De plus le dictionnaire la définit en tant qu'action de faire se produire ou s'accomplir simultanément (plusieurs faits, plusieurs actions appartenant à des séries différentes).

Dans les relations humaines se synchroniser est l'une des premières choses que nous avons appris, car un bébé qui répond au sourire de sa mère, ne fait rien d'autre que de se synchroniser sur les expressions du visage de sa mère.

L'histoire de la synchronisation revient au $17^{eme}$ siècle quand le célèbre scientifique hollandais Christian Huygens a rapporté son observation, que deux horloges à pendule supportées par une même planche en bois, finissaient par avoir les mêmes oscillations périodiques (même phase et même fréquence). En outre, il a remarqué que si l'oscillation d'une des pendules était perturbée par une force externe, elle reviendrait à son état initial.

C'était la première découverte de la synchronisation. La conclusion de Huygens sur la cause de cette synchronisation est le mouvement de la planche en bois ,malgré qu'il soit à peine perceptible [31]. Ce mouvement représente donc un faible accouplement des deux horloges. Par conséquent, dans le contexte classique la synchronisation n'est réservée qu'aux mouvements périodiques. Par ailleurs le concept moderne couvre également les systèmes chaotiques.

En résumé la synchronisation est le changement du rythme des oscillateurs (périodique ou non) dûs aux interactions faibles. Selon Pikovsky [31], il y a trois conditions qui doivent être rassemblées pour qu'un phénomène soit considéré synchrone [24] :

- Les systèmes oscillent indépendamment.

- Le changement du comportement est dû à un accouplement faible.
- Le changement du comportement se produit dans une certaine gamme de disparité. Si un oscillateur change lentement, le second devrait suivre cette variation.

L'aspect pseudo aléatoire du chaos nous amène à penser qu'il est impossible de le synchroniser. Cette hypothèse a été proposée par Fujisaka et al en 1983 [11].

Ce n'est qu'en 1990 que les deux chercheurs Pecora et Carroll [30] ont montré,que deux systèmes chaotiques identiques peuvent se synchroniser. Cette découverte a ouvert la voie pour des applications du chaos aux télécommunications et encore d'autres méthodes pour synchroniser le chaos .Ainsi, après la méthode de Pecora et Carroll d'autres propositions pour synchroniser le chaos ont été proposées, comme la méthode de synchronisation généralisée dont Rulkov et al ont posé les bases [34] et la synchronisation impulsive [42]. Dans ce chapitre nous présentons une étude sur ces 3 méthodes principales de synchronisation.

## III.2. Synchronisation identique ou approche de Pécora et Carroll

Comme il a été dit précédemment, les systèmes chaotiques sont des systèmes dynamiques qui défient la synchronisation à cause de leur sensibilité aux conditions initiales.

L'évolution de deux systèmes chaotiques identiques, qui commencent presque aux mêmes points initiaux, devient non corrélative au cours du temps. D'où l'impossibilité pratique de construire des systèmes chaotiques identiques, synchronisés dans le laboratoire.

En 1990 Pecorra et Carroll ont exposé, dans un article [30], leur découverte que deux systèmes chaotiques identiques se synchronisent sous certaines conditions. Alors ils ont considéré un système chaotique autonome de dimension $n$ :

$$\dot{U} = f(U) \tag{III.1}$$

Ce système peut être décomposé en deux sous-systèmes $U=(V,W)$ tel que $\dot{V}=g(V,W)$ et $\dot{W}=h(V,W)$ de dimensions $(m$ et $k)$ respectivement avec $n=k+m$ . Ensuite Pécora et Carroll ont dérivé de ce système un sous-système $W'$ identique au sous -système $W$ , tel que $\dot{W}'=h(V,W')$ .

On aura donc la configuration de Pécora et Carroll pour la synchronisation identique du chaos :

$$\left.\begin{aligned}\dot{V}&=g(V,W)\\ \dot{W}&=h(V,W)\end{aligned}\right\} \text{ Système maître} \qquad \text{(III.2)}$$

$$\left.\dot{W}'=h(V,W')\right\} \text{ Sous- système esclave} \qquad \text{(III.3)}$$

On remarque que l'accouplement entre les systèmes se produit par la variable $V$ du système maître (III.2), qui est substituée à son analogue $V'$ dans le sous- système esclave (III.3). Ainsi la synchronisation des deux sorties $W$ et $W'$ implique :

$$\Delta W=\lim_{t\to\infty}\|W-W'\|\to 0 \qquad \text{(III.4)}$$

La vérification de ce résultat se fait comme suit :

$$\Delta W=W-W'\to\Delta\dot{W}=h(V,W)-h(V,W') \qquad \text{(III.5)}$$

$$\text{Qui est égal à} \quad D_W h(V,W)\times\Delta W \qquad \text{(III.6)}$$

Où :

$$D_W h=\frac{\partial h(V,W)}{\partial W} \quad \text{le Jacobien du sous- système } W \qquad \text{(III.7)}$$

On déduit que l'étude de la convergence de $\Delta W$ vers 0 revient à l'étude des exposants de Lyapunov du sous-système $W$ . En conséquence Pécora et Carroll ont énoncé le théorème suivant [30] :

**Théorème III.1**

Les systèmes maître et esclave sont synchronisés si et seulement si tous les exposants de Lyapunov du système esclave , appelés les exposants de Lyapunov conditionnels ,sont négatifs.

**Exemple III.1**

Pour clarifier ce concept et illustrer la technique de Pécorra-Carroll on reprend un exemple sur la synchronisation identique du système de Lorenz donné dans la référence [5] . Le modèle mathématique de ce système est :

$$\begin{cases} \dot{x} = \sigma(y - x) \\ \dot{y} = -xz + rx - y \\ \dot{z} = xy - bz \end{cases} \quad \text{avec } \sigma = 16; r = 45{,}92; b = 4 \qquad \text{(III.8)}$$

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

$$\begin{cases} \dot{x}' = \sigma(y' - x') \\ \dot{y}' = -x'z + rx' - y' \end{cases} \text{ configuration } (x, y) \text{ avec } z \text{ entrée d'accouplement} \qquad \text{(III.9)}$$

$$\begin{cases} \dot{x}' = \sigma(y - x') \\ \dot{z}' = x'y - bz' \end{cases} \text{ configuration } (x, z) \text{ avec } y \text{ entrée d'accouplement} \qquad \text{(III.10)}$$

$$\begin{cases} \dot{y}' = -xz' + rx - y' \\ \dot{z}' = xy' - bz' \end{cases} \text{ configuration } (y, z) \text{ avec x entrée d'accouplement} \qquad \text{(III.11)}$$

Suivant le théorème III.1, la synchronisation identique nécessite la recherche d'une configuration du sous-système esclave qui donne des exposants de Lyapunov conditionnels négatifs.

En utilisant l'algorithme de A.Wolf et al [38], on a obtenu le tableau (III.1) qui donne les valeurs approximatives des exposants de Lyapunov conditionnels pour les configurations précédentes.

| Système | Signal maître | Configuration du sous système esclave | Exposants de Lyapunov |
|---|---|---|---|
| Lorenz $\sigma = 16; r = 45{,}92; b = 4$ | $z$ | $(x, y)$ | $(0.0002; -17.0036)$ |
| | $y$ | $(x, z)$ | $(-4.0007; -16.0033)$ |
| | $x$ | $(y, z)$ | $(-2.4125; -2.5885)$ |

*Tableau (III.1) : Les exposants de Lyapunov conditionnels pour les différentes configurations du sous- système esclave du système (III.8)*

- **Vérification du théorème III.1**

Dans les figures (III.1) on montre graphiquement que la garantie de la synchronisation maître esclave est donnée par les valeurs négatives des exposants de Lyapunov associées au système esclave. Ainsi on remarque, dans les figures (III.1b) et (III.1c), que les états du système esclave convergent asymptotiquement vers les états correspondant au système maître, alors que la figure (III.1a) représente une divergence d'états.

En conclusion, le choix d'un sous système esclave candidat pour la synchronisation est limité par les conditions du théorème III.1. En plus pour un éventuel usage de cette méthode pour la sécurisation de la communication entre émetteur et récepteur, la réalisation du sous-système esclave , dans le récepteur ,dupliqué d'un sous-système du système maître de l'émetteur ne semble pas très facile à mettre en pratique a cause des disparités des paramètres [6]. Ces contraintes ont poussé les chercheurs à trouver d'autres méthodes de synchronisation qui cassent relativement les limites posées dans le cas de la synchronisation identique, la synchronisation

généralisée est une des alternatives proposés que nous allons étudier dans le paragraphe suivant.

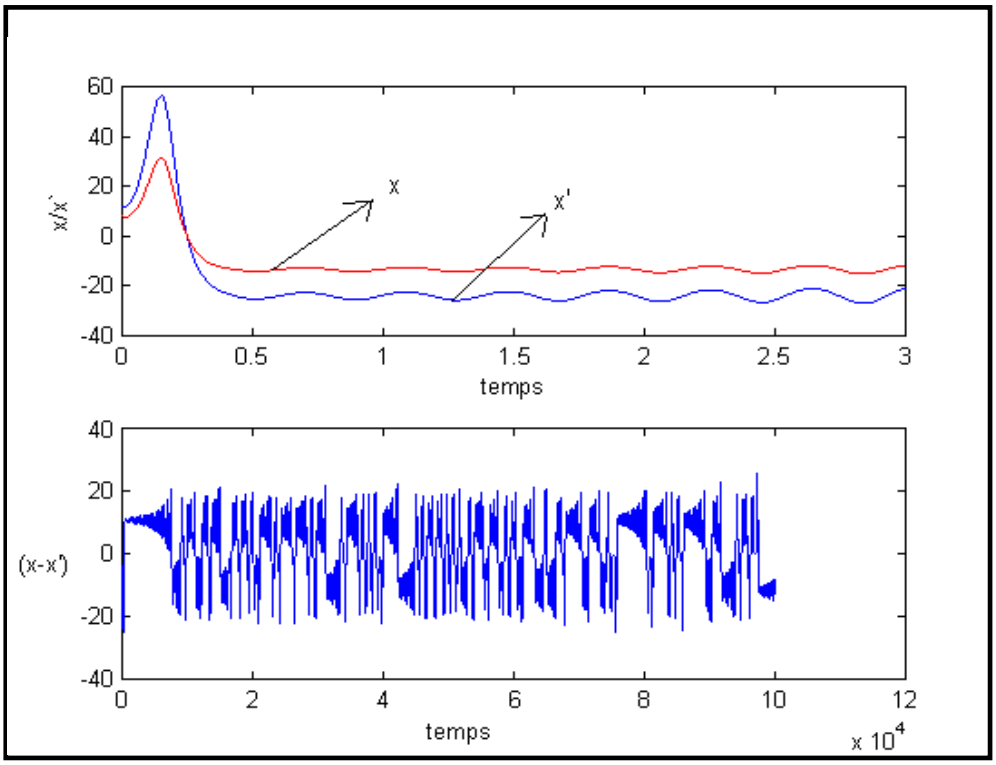



*Figure (III.1.a1)*

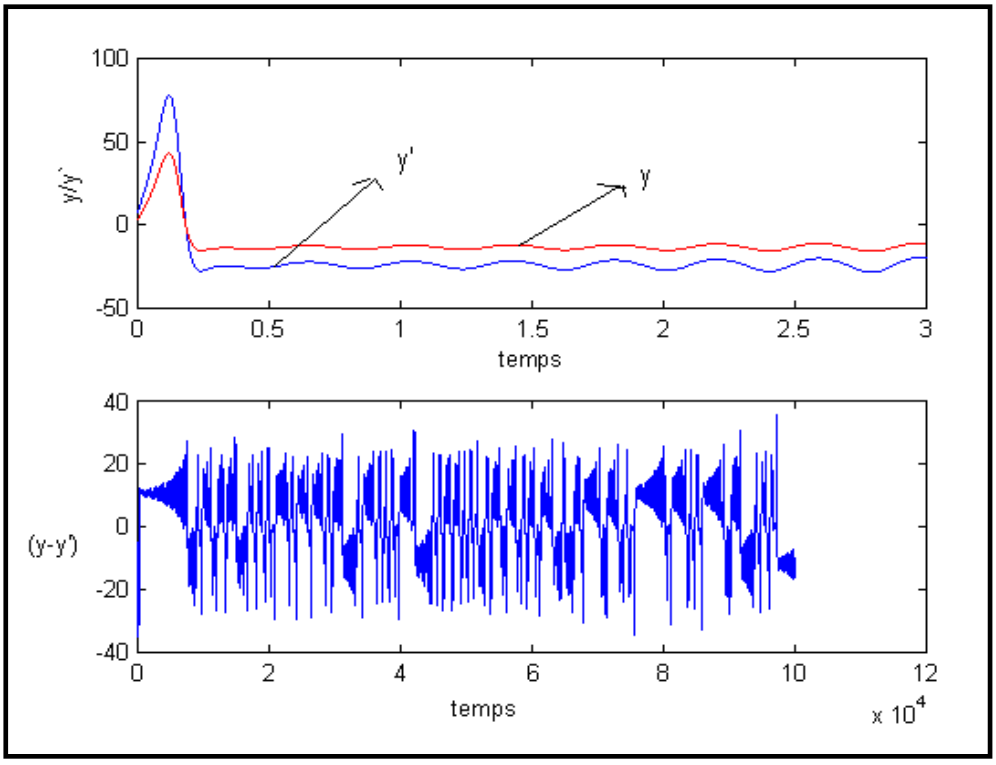



*Figure (III.1.a2)*

*Figure (III.1.a) : Test de la synchronisation pour un sous- système esclave* $(x, y)$

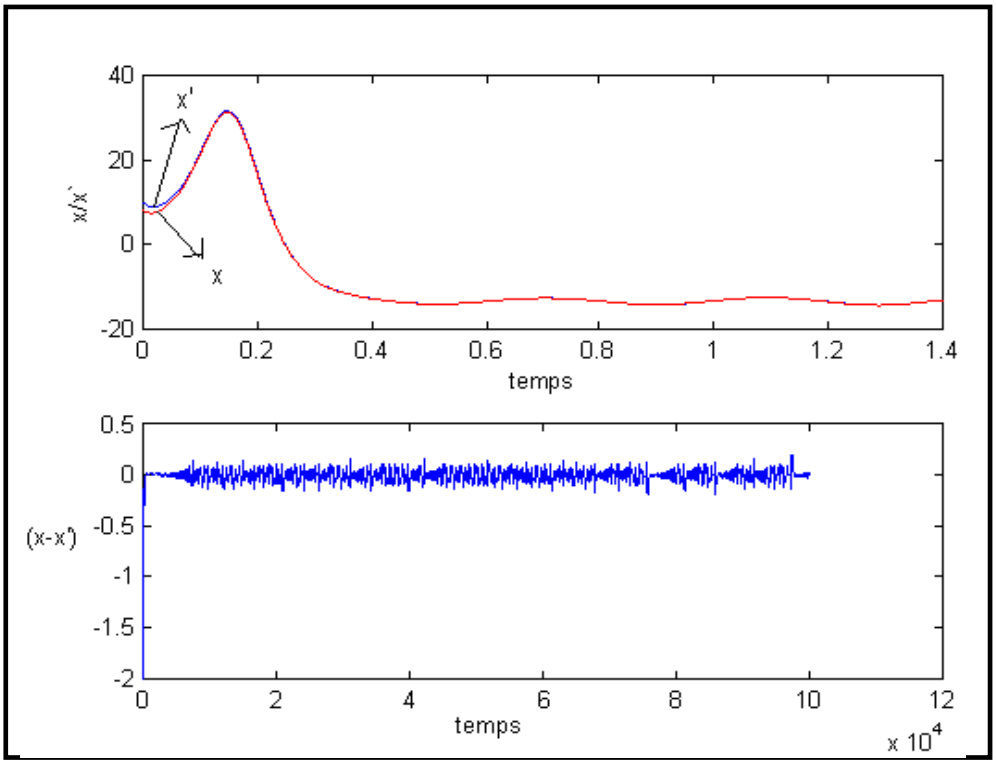



*Figure (III.1.b1)*

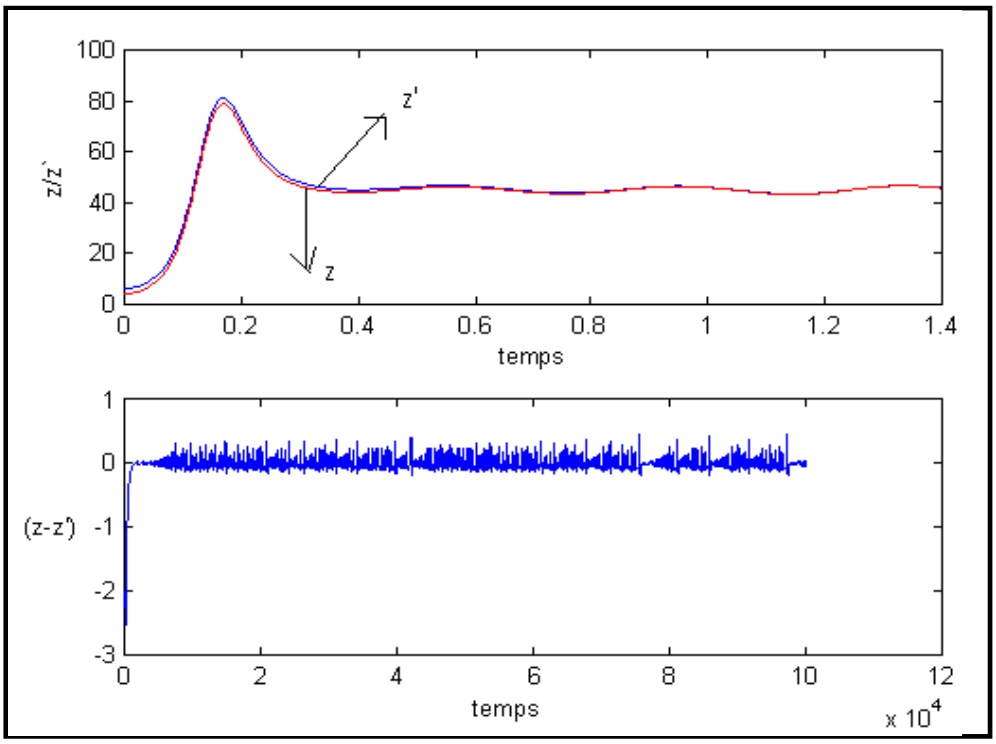



*Figure (III.1.b2)*

*Figure (III.1.b) : Test de la synchronisation pour un sous- système esclave* $(x, z)$

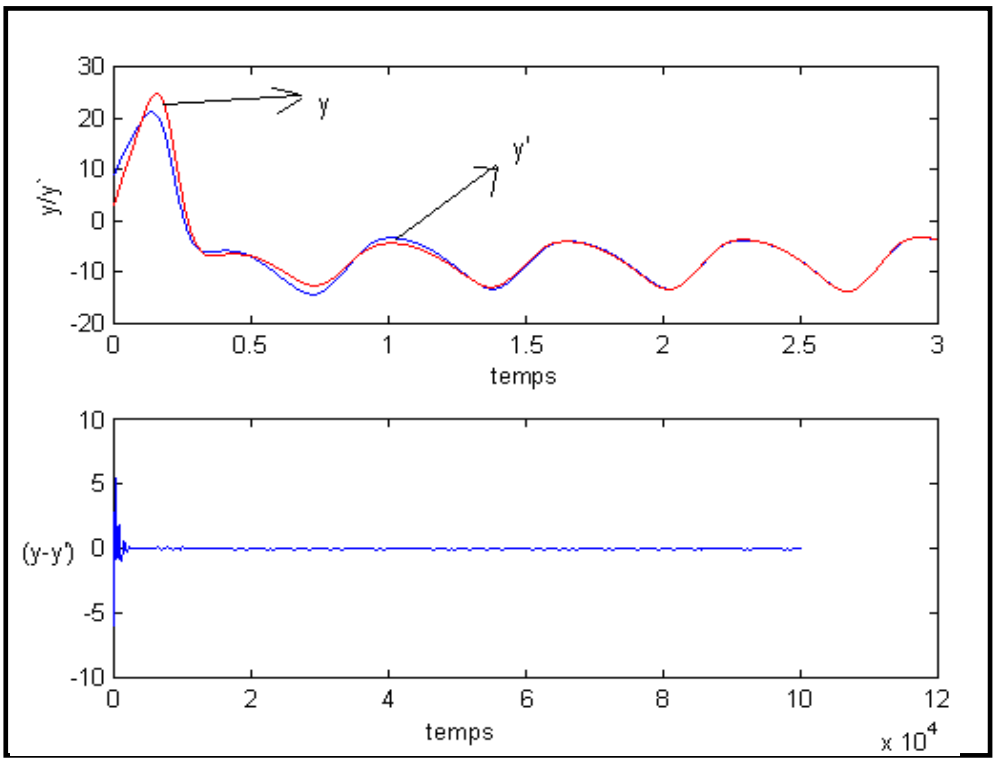



*Figure (III.1.c1)*

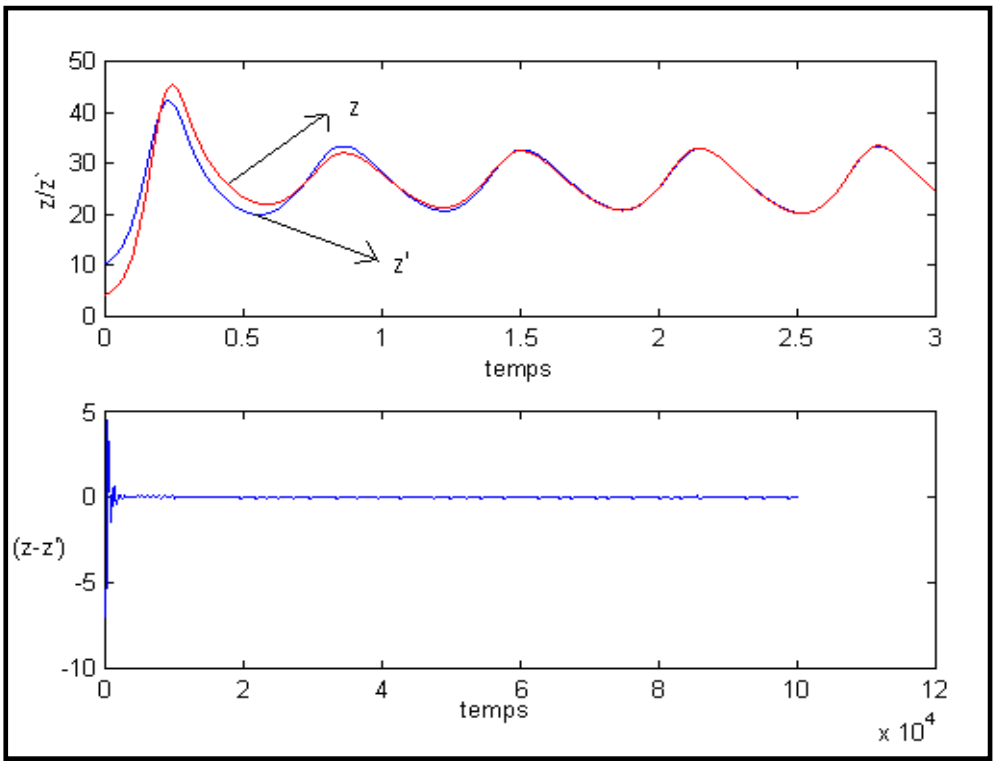



*Figure (III.1.c2)*

*Figure (III.1.c) : Test de la synchronisation pour un sous- système esclave* $(y, z)$

## III.3. Synchronisation généralisée

Il est clair que la contrainte de l'application de la synchronisation identique réside dans la difficulté de réaliser pratiquement un sous-système esclave tout à fait identique à un autre sous-système issu d'une décomposition du système maître [6] .

Ainsi les recherches se sont penchées pour affranchir cet obstacle, d'où la proposition d'une méthode de synchronisation plus générale qui est la synchronisation généralisée (SG en abrégé). Parmi Les premières publications sur cette méthode on cite celle de Rulkove et al [34] et de Kocarev et al [20].

En comparaison avec la synchronisation identique [41], la SG peut donner une dynamique plus riche car elle peut aussi envisager certains cas désynchronisés, dus aux disparités des paramètres, aux déformations des canaux de transmission et autres.
En conséquence les possibilités d'appliquer la SG pratiquement, peuvent être plus large que la synchronisation identique.

### III.3.1. Analyse de la littérature sur la synchronisation généralisée

Tous les travaux sur la synchronisation généralisée traitent deux issues centrales qui sont les bornes du sujet. La première est la généralisation du concept de la synchronisation pour inclure la non identité entre les systèmes chaotiques couplés. La deuxième est la conception d'essais pour la détecter [5],[20],[34],[41],[46].

### III.3.2. Définition générale de la synchronisation généralisée

Si on considère les deux systèmes dynamiques couplés suivants [5],[20],[34],[41],[46] :

système maître $$\dot{x} = F(x) \tag{III.12}$$

système esclave $$\dot{y} = G(y, h_g(x)) \tag{III.13}$$

Tel que x est le vecteur d'état du système maître de dimension n et y est le vecteur d'états du systèmes esclave de dimension m. F et G sont des fonctions vectorielle telles que $F : R^n \to R^n$ et G : $R^m \to R^m$ . L'accouplement entre les systèmes maître et esclave est assuré par le vecteur de fonctions $h_g(x)$ : $R^n \to R^m$ , où la dépendance de ces fonctions du paramètre g est considérée explicitement . Si g=0, le système esclave évolue indépendamment du système maître, et on suppose que les deux systèmes sont chaotiques. Si $g \neq 0$, les trajectoires chaotiques des deux systèmes sont synchronisés dans le sens généralisé, si il existe une transformation $\varphi : x \to y$ , telle que :

$$y = \lim_{t \to +\infty} \varphi(x) \tag{III.14}$$

Indépendamment des conditions initiales dans le bassin de la variété de synchronisation $M = \{(x, y) : y = \varphi(x) \}$.

Plus spécialement, si $\varphi$ est égale à l'identité, les systèmes se synchronisent identiquement .Ainsi on conclut que la synchronisation identique est un cas particulier de la synchronisation généralisée SG .

### III.3.3. Détection de la synchronisation généralisée

Vu sa facilité d'application on a adopté l'approche des systèmes auxiliaires pour détecter la synchronisation généralisée [1] .Son principe est de considérée un autre système :

$$\dot{z} = G(z, h_g(x)) \tag{III.15}$$

copie exacte du système esclave (III.13) mais de conditions initiales différentes et couplé de la même façon avec le système maître (III.12). La règle est que si les réponses des deux accouplements sont identiques, alors on conclut qu'il y a synchronisation généralisée entre les deux systèmes (III.12) et (III.13). Sinon les deux systèmes ne sont pas synchronisés.

**Exemple III.2**

Soit à vérifier la synchronisation de deux systèmes de Rössler suivants [5],[34] :

Système maître
$$\begin{cases} \dot{x}_1 = -(x_2 + x_3) \\ \dot{x}_2 = x_1 + 0{,}2.x_2 \\ \dot{x}_3 = 0{,}2 + x_3.(x_1 - \mu) \end{cases} \quad \text{(III.16)}$$

Système esclave
$$\begin{cases} \dot{y}_1 = -(y_2 + y_3) - g.(y_1 - x_1) \\ \dot{y}_2 = y_1 + 0{,}2.y_2 \\ \dot{y}_3 = 0{,}2 + y_3.(y_1 - \mu) \end{cases} \quad \text{(III.17)}$$

avec $\mu = 5{,}7$ .

Pour les conditions initiales des deux systèmes $x_1(0)=0.01$, $x_2(0)=0.01$, $x_3(0) = 0.01$ ; $y_1(0) =1$, $y_2(0) =1$, $y_3(0) =1$. On constate sur la figure (III.2) que pour g=0.20 , $x_2(t)$ et $y_2(t)$ tendent vers une évolution confondue, ce qui implique la synchronisation identique des deux systèmes (III.16) et (III.17), tandis que sur la figure(III.3) , pour g = 0.10, on remarque une divergence des trajectoires et non stabilité de la relation (x=y) . Donc les systèmes ne synchronisent pas. Dans ce cas on remarque que la synchronisation est évidente en comparant tout simplement les évolutions des réponses des deux systèmes.

Pour l'étude de la synchronisation généralisée, les auteurs [5],[34] ont proposé un nouveau système esclave qui exhibe la synchronisation généralisée, à partir d'une transformation non linéaire du système esclave (III.17) .Cette transformation est donnée par :

$$\begin{cases} z_1 = y_1 \\ z_2 = y_2 + a.y_3 + b.y_3^{\,2} \\ z_3 = y_3 \end{cases} \quad \text{(III.18)}$$

avec a =0,4 et b = -0.008 .

Les équations du nouveau système esclave deviennent :

$$\begin{cases} \dot{z}_1 = -[z_2 + (1-a).z_3 - b.z_3^{\,2}] - g.(z_1 - x_1(t)) \\ \dot{z}_2 = z_1 + 0{,}2.(z_2 - a.z_3 - b.z_3^{\,2}) + (a + 2.b.z_3).[0{,}2 + z_3.(z_1 - \mu)] \\ \dot{z}_3 = 0{,}2 + z_3.(z_1 - \mu) \end{cases} \quad \text{(III.19)}$$

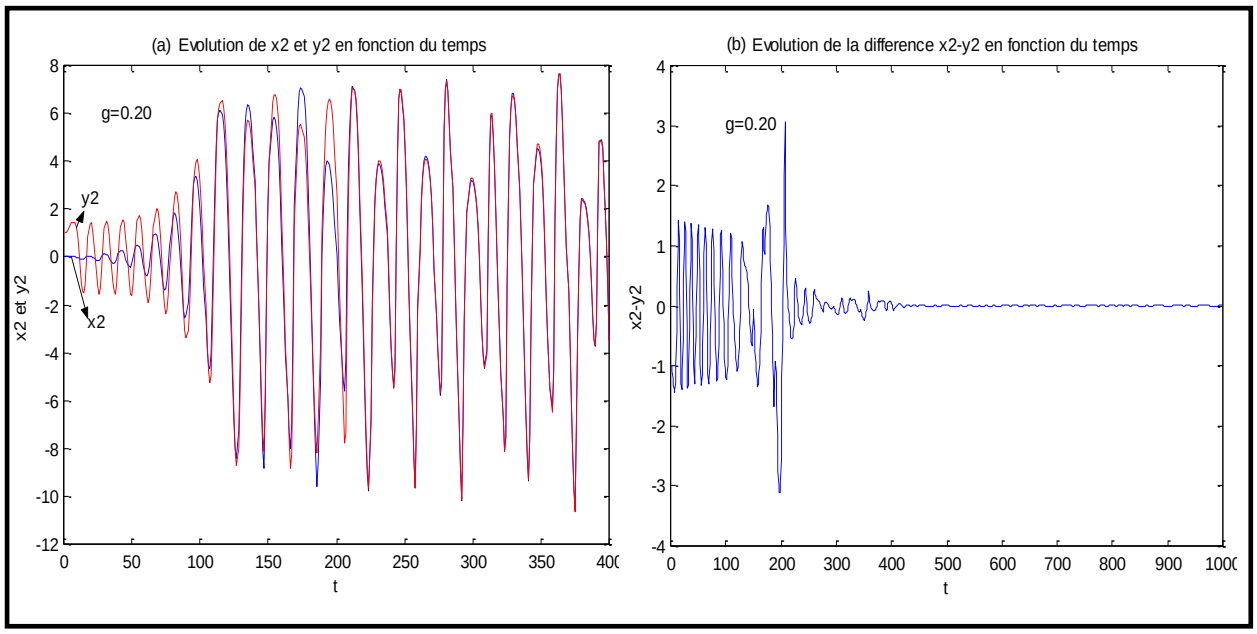



*Figure (III.2) : Synchronisation des deux systèmes (III.16) et (III.17)*

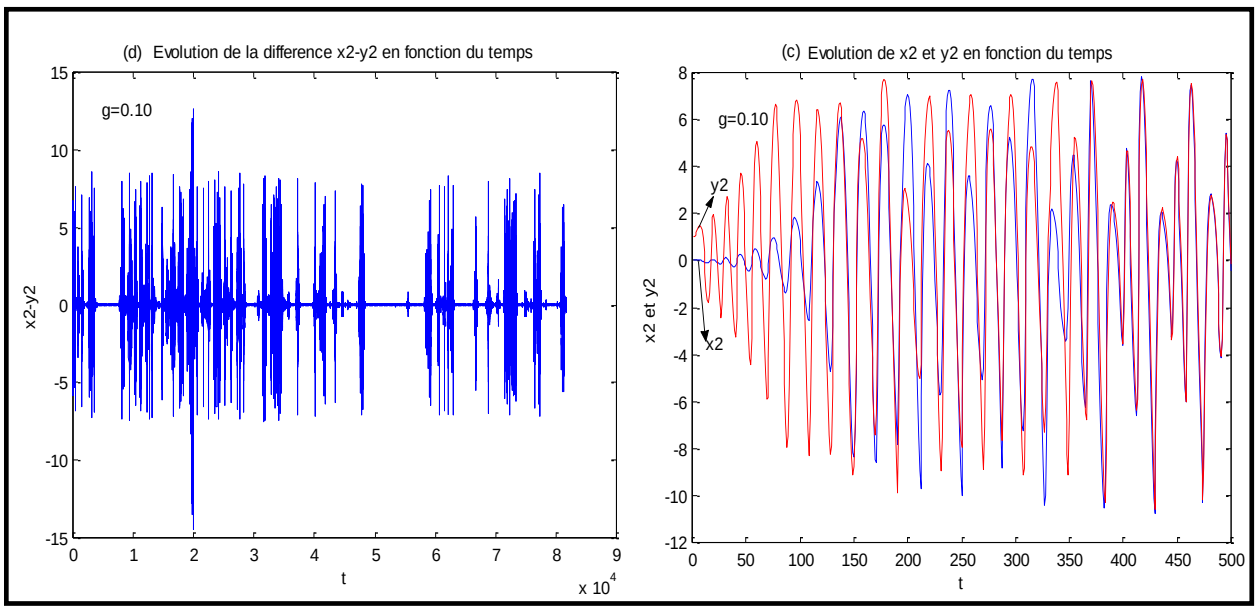



*Figure (III.3) : La non synchronisation des deux systèmes (III.16) et III.17)*

La détection de la synchronisation généralisée est plus compliquée que dans le cas de la synchronisation identique. En conséquence pour tester la synchronisation entre les systèmes (III.16) et (III.19) on a utilisé la méthode du système auxiliaire exposée dans le paragraphe III.3.3 .Alors si on considère le système auxiliaire suivant :

$$\begin{cases} \dot{w}_1 = -[w_2 + (1-a).w_3 - b.w_3^{\,2}] - g.(w_1 - x_1(t)) \\ \dot{w}_2 = w_1 + 0{,}2.(w_2 - a.w_3 - b.w_3^{\,2}) + (a + 2.b.w_3).[0{,}2 + w_3.(z_1 - \mu)] \\ \dot{w}_3 = 0{,}2 + w_3.(w_1 - \mu) \end{cases} \quad \text{(III.20)}$$

ce système et le système esclave (III.19) sont accouplés avec le même système maître (III.16).

Pour les conditions initiales suivantes des trois systèmes (III.16) , (III.19) et (III.20) $x_1(0)=0.1$, $x_2(0)=0.1$, $x_3(0)=0.1$ ; $z_1(0)=0.5$, $z_2(0)=0.5$, $z_3(0)=0.5$ ; $w_1(0)=1$, $w_2(0)=1$, $w_3(0)=1$.On peut donc vérifier la synchronisation dans le sens généralisé des deux systèmes ( III.16) et (III.19) en testant si les systèmes esclave (III.19) et auxiliaire (III.20) tendent à devenir identique pour $t \to \infty$ , ce qui revient à dire que :

$$\lim_{t\to\infty}(z(t) - w(t)) = 0 \quad \text{(III.21)}$$

inversement :

$$\lim_{t\to\infty}(z(t) - w(t)) \neq 0 \quad \text{(III.22)}$$

D'où la non synchronisation des systèmes [1]. La figure (III.4) montre la synchronisation des systèmes pour g=0.20 et la figure (III.5) montre la non synchronisation des systèmes pour g=0.10.

**Exemple III.3**

Dans ce cas le système maître est le système (III.16) et le système esclave est un système de Lorenz défini par les équations suivantes [1] :

$$\begin{cases} \dot{y}_1(t) = \sigma[y_2(t) - y_1(t)] - g.[y_1(t) - x_1(t)] \\ \dot{y}_2(t) = -y_1(t).y_3(t) + r.y_1(t) - y_2(t) \\ \dot{y}3(t) = y_1(t).y_2(t) - b.y_3(t) \end{cases} \quad \text{(III.23)}$$

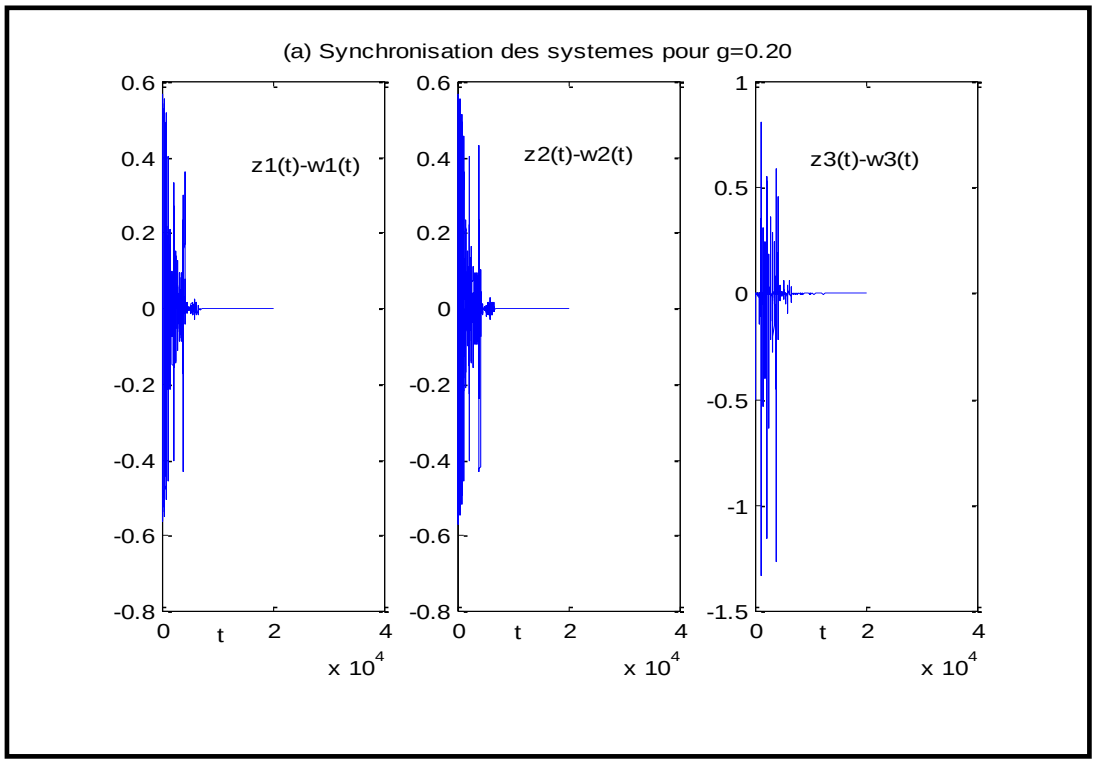



*Figure (III.4) : Synchronisation des systèmes (III.16) et (III.19)*

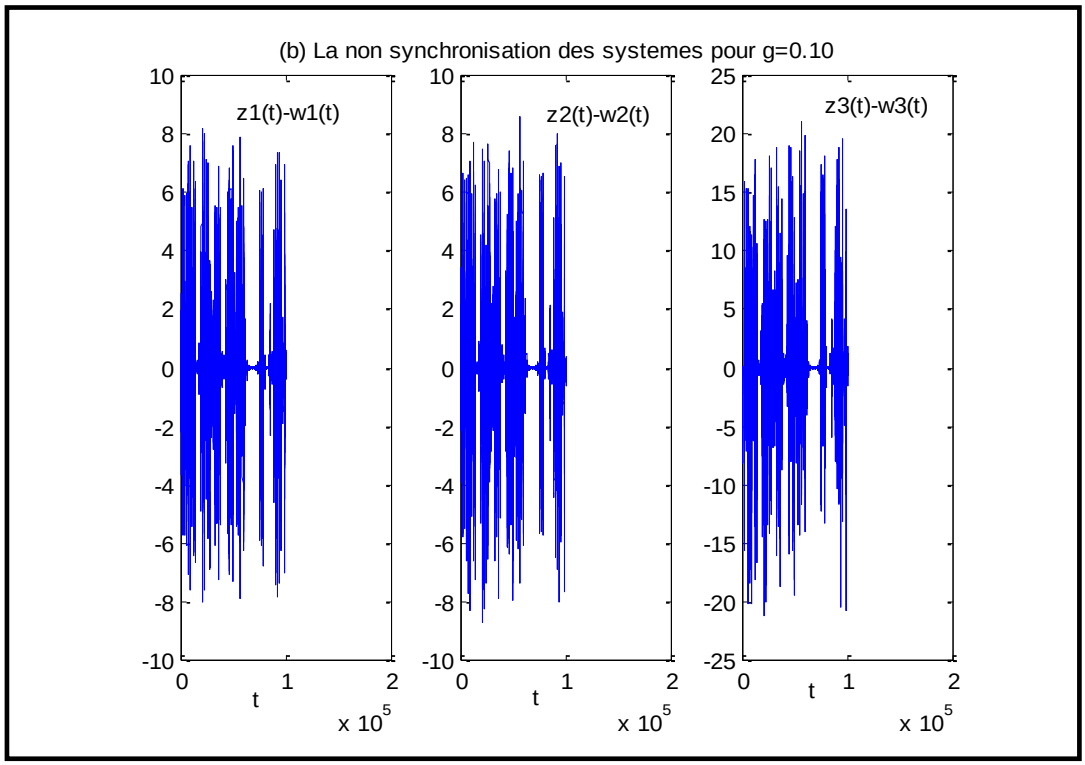



*Figure (III.5) : La non synchronisation des systèmes (III.16) et (III.19)*

Avec $\mu = 5{,}7$ dans le système de Rössler et $\sigma = 16, b = 4$ et $r = 45{,}92$ dans le système de Lorenz . Le système esclave est couplé au système maître seulement par le terme $x_1(t).g$ , qui caractérise la force de l'accouplement unidirectionnel et puisque les systèmes couplés sont différents il est évident que l'égalité x (t)=y (t) est impossible, ainsi la synchronisation ne peut être identique. Cependant, ces systèmes peuvent être synchronisés dans le sens généralisé. Pour détecter cette synchronisation les auteurs de l'article [1], ont raisonné avec la méthode du système auxiliaire exposée dans le paragraphe III.3.3.

Le système de Lorenz auxiliaire est :

$$\begin{cases} \dot{z}_1(t) = \sigma[z_2(t) - z_1(t)] - g.[z_1(t) - x_1(t)] \\ \dot{z}_2(t) = -z_1(t).z_3(t) + r.z_1(t) - z_2(t) \\ \dot{z}_3(t) = z_1(t).z_2(t) - b.z_3(t) \end{cases} \quad \text{(III.24)}$$

Qui représente une reproduction exacte de la réponse du système (III.23). Alors la synchronisation est réalisée entre les systèmes (III.16) et (III.23) si les deux systèmes (III.23) et (III.24) tendent vers une égalité stable y (t) = z (t) et cela ne se réalise que si le terme d'accouplement $x_1(t).g$ est suffisamment grand . Pour les conditions initiales suivantes des trois systèmes (III.16), (III.23) et (III.24) : $x_1(0)=0.5$, $x_2(0)=0.2$, $x_3(0)=0.9$) ; ($y_1(0)=0.5$, $y_2$ (0)=0.5, $y_3$ (0)=0.5) ; ($z_1$ (0)=2, $z_2$ (0)=2, $z_3$ (0)=2. En utilisant l'approche du système auxiliaire [1]. La figure (III.6) représente l'évolution de (y (t)-z (t)) en fonction du temps dans les deux cas. Ainsi :

- Pour la figure (III.6a), g=4.9, (y (t)-z (t)) tend vers 0 lorsque le temps t augmente, donc la synchronisation des systèmes (III.16) et (III.23).

- Pour la figure (III.6b) g= 4.8, (y (t)-z (t)) ne tend pas vers 0 lorsque le temps t augmente, donc la non synchronisation des systèmes (III.16) et (III.23).

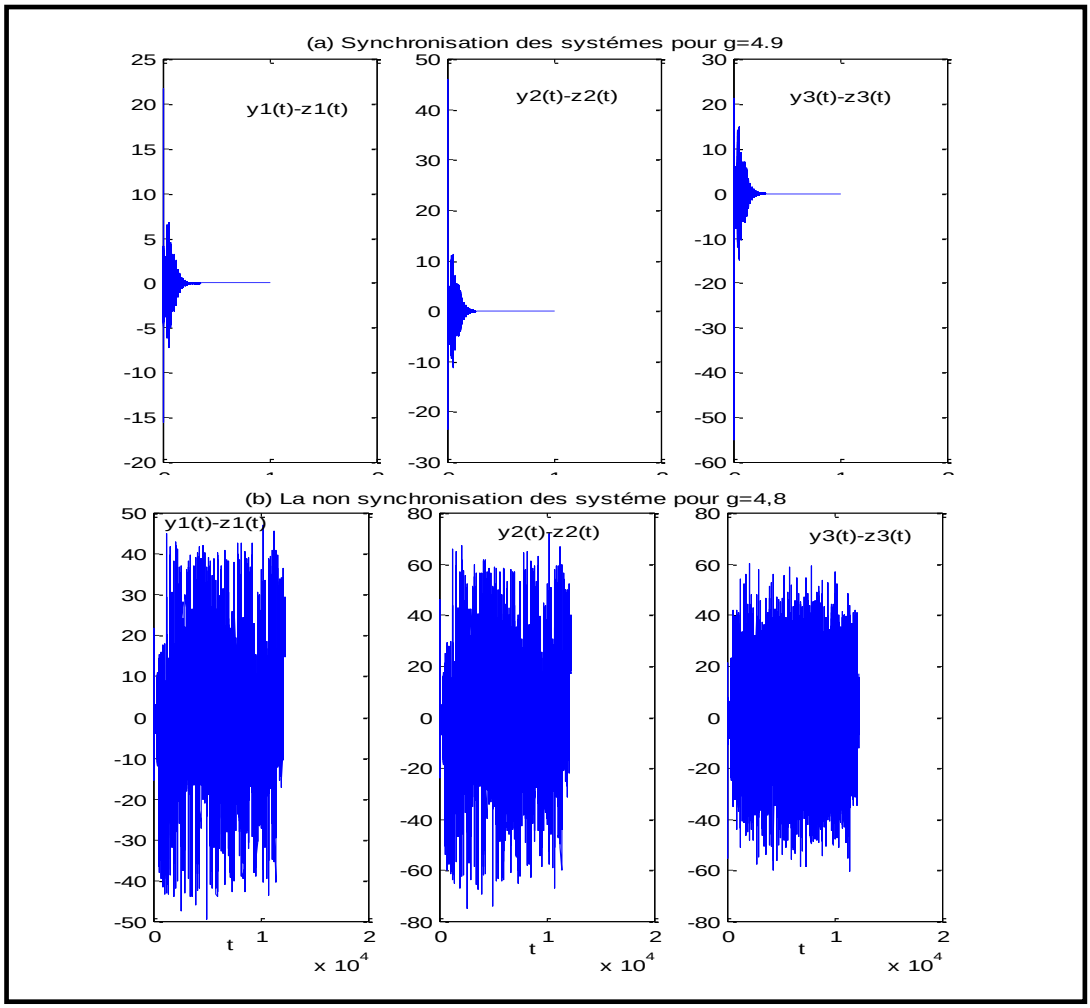



*Figure (III.6) :(a) Synchronisation des systèmes (III.16) et (III.23) , (b) la non synchronisation des systèmes (III.16) et (III.23)*

**Remarque III.1**

La synchronisation généralisée entre deux systèmes chaotiques x et x' peut être exprimée par l'existence d'une transformation φ telle que :

$$\lim_{t\to\infty}\|x'(t)-\varphi(x(t))\|=0 \qquad \text{(III.25)}$$

et ce, indépendamment des conditions initiales .Si la fonction φ est inversible, alors $\varphi^{-1}(x')$ fournit une estimation de l'état x. Mais cette transformation n'est pas toujours inversible [6], on ne peut pas estimer x. Cela représente un inconvénient majeur pour certaines techniques de communication qui utilisent l'état de l'émetteur pour décrypter le message transmis ; alors une autre méthode de synchronisation, dite la

synchronisation impulsive du chaos a été proposée et qui est considérée comme plus robuste aux disparités des paramètres par rapport aux méthodes précédentes [42].

## III.4. La synchronisation impulsive du chaos

En 1997, une nouvelle technique de la synchronisation chaotique appelée la synchronisation impulsive a été proposée. La commande impulsive basée sur la théorie de contrôle impulsif a été largement utilisée pour stabiliser et synchroniser les systèmes chaotiques. Son utilité réside dans les cas où certains systèmes ne peuvent pas être contrôlés par un contrôle continu. Par exemple, un gouvernement ne peut pas changer des taux de l'épargne de sa banque centrale chaque jour [39]. En plus, le contrôle impulsif est plus efficace pour traiter les systèmes qui ne peuvent pas supporter des perturbations continues. En outre, la méthode impulsive peut également réduire considérablement le coût de contrôle.

### III.4.1. Contrôle impulsif des systèmes non linéaires

Soit le système chaotique dont la forme générale est la suivante [39] :

$$\dot{x} = f(x,t) \tag{III.26}$$

Où $t \in J = [t_0, \infty]$ $(t_0 \geq 0)$ , $x \in R^n$ est le vecteur d'état et $f : J \times R^n \to R^n$ le vecteur de fonctions continues. Une loi de contrôle impulsif du système (III.26) est donnée par une séquence $\{t_k, u_k(x(t_k))\}$, $u_k(x(t_k))$ ayant l'effet de changer soudainement l'état du système aux instants $t_k$ , où $t_1 < t_2 < ..... < t_k$ , $\lim_{k\to\infty} t_k = \infty$ et $t_1 > t_0$ telle que :

$$\Delta x|_{t_k} = x(t_k^{+}) - x(t_k) = u_k(x(t_k)) \tag{III.27}$$

Où $x(t_k^+) = \lim_{t\to t_k^+} x(t)$ et $x(t_k) = \lim_{t\to t_k^-} x(t)$ (III.28)

En général pour simplifier on pose $x(t_k^-) = x(t_k)$ . En outre, $u_k(x(t_k))$ peut être choisi comme $B_k x(t_k)$ , avec $B_k$ sont des matrices de dimension $n \times n$ . Le système contrôlé impulsivement peut être exprimé par :

$$\begin{cases} \dot{x} = f(t,x), t \neq t_k \\ \Delta x = B_k x, t = t_k \\ x(t^+{}_0) = x_0 \,/(k = 1,2,.....) \end{cases} \quad \text{(III.29)}$$

appelé aussi un système différentiel impulsif.

**Exemple III.4**

Soit le système chaotique dont l'expression est la suivante [39] :

$$\begin{cases} \dot{x}_1 = a(x_2 - x_1) \\ \dot{x}_2 = -x_1 x_3 + c x_2 \\ \dot{x}_3 = x_1 x_2 - b x_3 \end{cases} \quad \text{(III.30)}$$

Avec a =36, b = 3, c = 20.

Ce système est appelé le système de Lu .Si on choisi ce système comme système maitre et si nous réécrivons ce système sous la forme :

$$\dot{x} = Ax + \Phi(x) \quad \text{(III.31)}$$

Où A est une matrice qui représente la partie linéaire du système correspondant et $\Phi(x) = [0, -x_1 x_3, x_1 x_2]^T$ le système esclave sera modélisé par l'équation impulsive suivante:

$$\begin{cases} \dot{y} = Ay + \Phi(y), t \neq t_k \\ \Delta y = B_k e, t = t_k \\ y(t^+{}_0) = y_0 \,/(k = 1,2,.....) \end{cases} \quad \text{(III.32)}$$

Où $y = [y_1, y_2, y_3]^T$ , si on pose $e = [e_1, e_2, e_3]^T = [y_1 - x_1, y_2 - x_2, y_3 - x_3]^T$ comme erreur de synchronisation et on définit :

$$\Psi(x,y)=\Phi(y)-\Phi(x)=\begin{pmatrix}0\\-y_1y_3+x_1x_3\\y_1y_2-x_1x_2\end{pmatrix} \tag{III.33}$$

alors le système erreur de la synchronisation impulsive est décrit par :

$$\begin{cases}\dot{e}=Ae+\Psi(x,y), t\neq t_k\\ \Delta e=B_k e, t=t_k\\ e(t^{+}{}_0)=y(t_0)-x(t_0)(k=1,2,.....)\end{cases} \tag{III.34}$$

On note qu'il existe une constante positive M pour le système chaotique (III.30) telle que $|x(t)|\leq M$ pour tout t.

Pour simplifier l'analyse ,on utilise la notation suivante :

$$\lambda_2=\frac{1}{2}\lambda_{\max}(A+A^T), \beta_k=\lambda_{\max}\left[(I+B_k)^T(I+B_k)\right] \tag{III.35}$$

Avec I la matrice identité et $\lambda_{\max}(D)$ la valeur propre maximale de la matrice D. Les conditions de synchronisation sont données par le théorème suivant [39] :

**Théorème III.2**

1) Si $2\lambda_2+M=\lambda<0$ ($\lambda$ est une constante) et il existe une constante $0\leq\alpha<-\lambda,$ telle que $\ln\beta_k-\alpha(t_k-t_{k-1})\leq 0, k=1,2,.....$ alors la solution du système (III.34) est globalement exponentiellement stable, ce qui implique que le système (III.31) est globalement exponentiellement synchronisé avec le système (III.29) .

2) Si $2\lambda_2+M=\lambda\geq 0$ ($\lambda$ est une constante) et il existe une constante $\alpha\geq 1$ , telle que $\ln\alpha\beta_k+\lambda(t_k-t_{k-1})\leq 0, k=1,2,.....$ alors le système (III.31) est globalement asymptotiquement synchrone avec le système (III.29).

Ainsi la vérification de la synchronisation impulsive entre les systèmes (III.29) et (III.31), revient à vérifier que la réponse du système erreur (III.34) tend

asymptotiquement vers le point (0, 0,0) et ce résultat est conditionné par le choix adéquat de la période d'excitation τ du système esclave par le système maître. Alors suivant le théorème III.2 , à partir de la simulation du système (III.29), on trouve la valeur de M =40 donc $\lambda$ =90.5733, si on choisit B = $B_k$=la matrice diagonale constante [-0.58,-0.68,-0.78] pour tout k, alors $\beta = 0.1764$ et si on prend $\alpha = 1.01$ alors $t_{k+1} - t_k = \tau < \frac{-\ln \alpha\beta}{\lambda} = 0.019$ .Ainsi le système (III.29) est globalement asymptotiquement synchrone avec le système (III.31) pour $\tau < 0.019$.

La figure (III.7) montre la réponse du système erreur pour $\tau = 0.01$ et pour les conditions initiales suivantes des systèmes maître (III.29) et esclave (III.31) ($x_1(0)=3$, $x_2(0)=4$, $x_3(0)=5$) et ($y_1(0)=7$, $y_2(0)=8$, $y_3(0)=9$) on remarque que les 2 systèmes sont synchronisés.

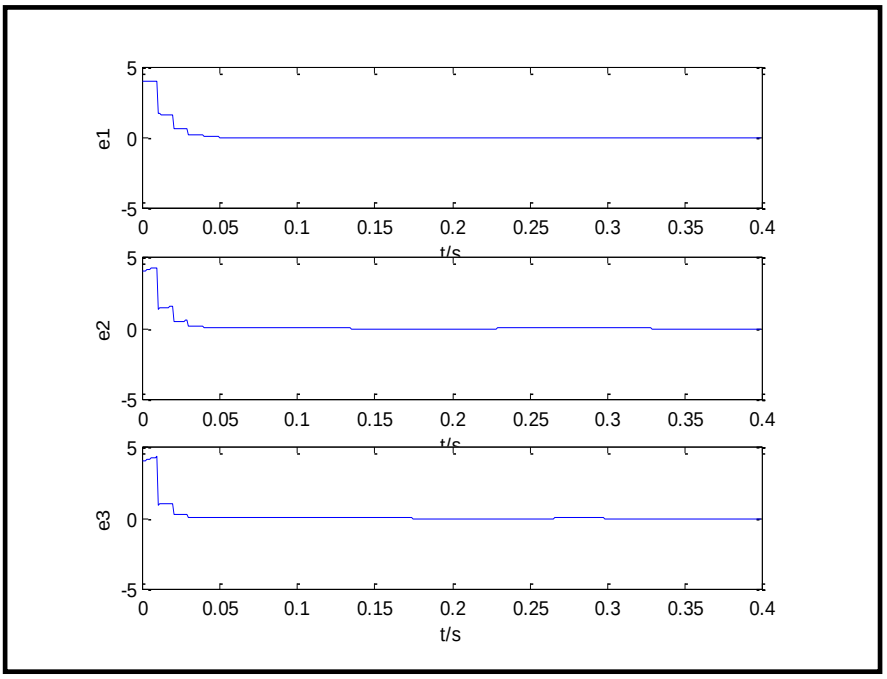



*Figure (III.7) Erreurs de synchronisation impulsive de 2 systèmes de Lu*

## III.5. Autres techniques de synchronisation du chaos

Il existe plusieurs autres formes de synchronisation qui ont été proposées dans la littérature, parmi lesquelles [6] :

### III.5.1. La synchronisation de phase

Ce type de synchronisation vient de la notion classique de synchronisation pour deux systèmes périodiques dont les phases sont $\theta_1$ et $\theta_2$, qui est exprimée par la relation $|n.\theta_1 - m.\theta_2| < c$ ou m, n sont des entiers naturels et c est une constante positive. Ainsi pour exprimer la phase d'un système en représentant son signal analytique $\varphi(t)$ sous la forme d'une fonction complexe définie par :

$$\varphi(t) = s(t) + j\tilde{s}(t) = A(t).e^{j\theta(t)} \tag{III.36}$$

Où $\tilde{s}(t)$ est la transformée de Hilbert de la série temporelle $s(t)$ par :

$$\tilde{s} = \frac{1}{\pi} V.P.\left(\int_{-\infty}^{+\infty} \frac{s(\tau)}{t-\tau} d\tau\right) \tag{III.37}$$

Avec V.P, la valeur principale de Cauchy de l'intégrale. Par analogie avec les systèmes périodiques dans l'expression (II.50) A (t) est l'amplitude du signal $\varphi(t)$ et $\theta(t)$ sa phase. Donc il se produit une synchronisation de phase entre les deux systèmes chaotiques couplés si $|n.\theta_1 - m.\theta_2| < c$ .

### III.5.2. La synchronisation retardée

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

$$\lim_{t\to\infty} \|x'(t) - x(t-\tau)\| = 0 \tag{III.38}$$

## III.6. Conclusion

Pour mettre en application un système de sécurisation de la communication par synchronisation du chaos trois problèmes techniques critiques devraient être d'abord résolus. Le premier est la disparité des paramètres entre l'émetteur et le récepteur

chaotiques, le deuxième est la non linéarité et le bruit additif au niveau du canal de liaison et le troisième est la robustesse du système. Ainsi ce chapitre a été consacré pour la présentation par ordre d'évolution des trois méthodes de synchronisation en critiquant leurs limites .Actuellement il n'existe évidemment pas de méthodes sans inconvénients. Cependant la synchronisation impulsive présente des qualités plus avantageuses par rapport aux autres méthodes, surtout concernant les limites dues aux disparités des paramètres.

# CHAPITRE IV

# Utilisation du chaos pour la sécurisation des communications

## IV.1. Introduction

Les systèmes chaotiques ont plusieurs caractéristiques significatifs favorables pour sécuriser les communications, telles que l' ergodicité , la sensibilité aux conditions initiales , l'aspect ressemblant à l'aléatoire , qui peuvent être associés à certaines propriétés conventionnelles de la cryptographie comme confusion/diffusion .

Ainsi la découverte par Pecora et Carroll [30] que deux systèmes chaotiques peuvent être synchronisés , a déclenché un certain intérêt pour le développement des systèmes de communication sécurisés basés sur le chaos dans les trois décennies passées .

L'idée de base est de brouiller un message adéquatement avec le chaos au niveau de l'émetteur, afin de le dissimuler des intrus , avant de le transmettre à sa destination qui sera la seule capable de le déchiffrer.

Ainsi dans ce chapitre on va exposer deux essais sur deux méthodes pour la sécurisation de la communication par le chaos .La première est le masquage par addition et la deuxième est le masquage par commutation.

## IV.2. Masquage par addition

### IV.2.1. Présentation de la technique

Cette technique est considérée comme la première proposition d'utiliser le chaos pour sécuriser la communication [6],[25] . Elle est présentée dans les références [8] ,[19],[42] .Son principe est de brouiller le signal message m (t) dans un signal chaotique c (t) , par une opération d'addition directe avant de le transmettre ,afin d'avoir un signal crypté s(t) . Pour récupérer le signal message au niveau du récepteur autorisé , le même système générateur du chaos est utilisé à la fois à l'émission et à la réception , avec la différence que dans le récepteur , ce système est contrôlé par le signal reçu $r(t)$ (égal

au signal s(t) affecté par les perturbations dans le canal ) pour obtenir la synchronisation .

L'ordre de grandeur du signal message, doit être impérativement très faible par rapport à celui du signal chaotique c (t), pour ne donner aucun espoir de le récupérer par les intrus, sans savoir le signal c (t) exact et pour avoir une bonne synchronisation au niveau du récepteur autorisé. La clef de cryptage et de décryptage est égale aux valeurs des paramètres d'accouplement entre l'émetteur et le récepteur et des paramètres caractérisant les systèmes chaotiques utilisés.

Alors le signal message est reconstitué par la différence entre le signal reçu $r(t)$ et le signal $\hat{c}(t)$ proche de $c(t)$ résultat de la synchronisation, voir la figure(IV.1).L'exemple de simulation suivant illustre ce principe :

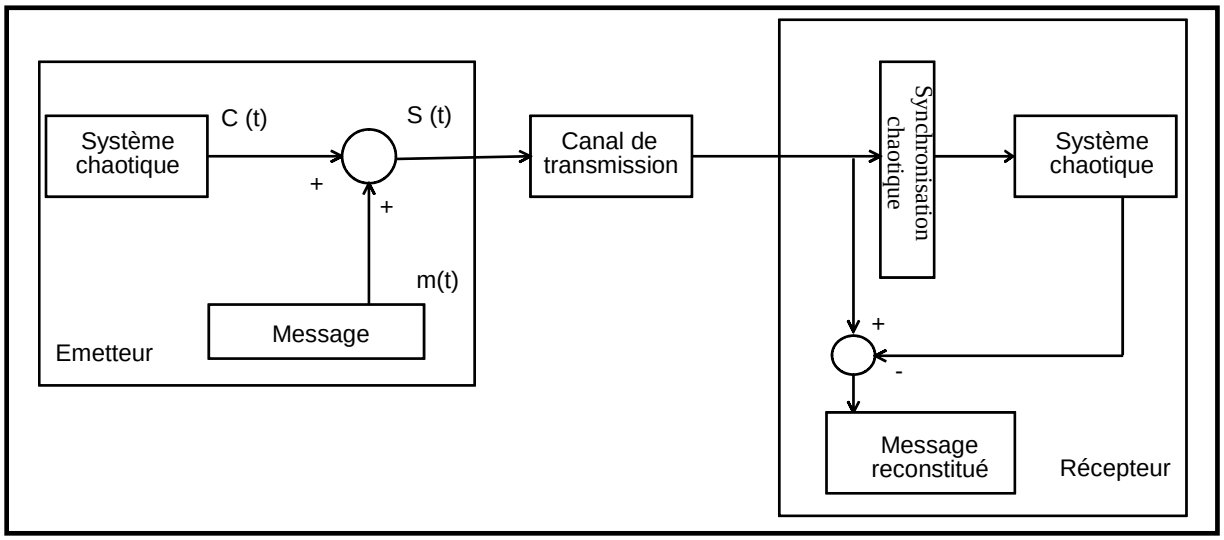



*Figure (IV.1) : Schéma du masquage chaotique par addition*

### IV.2.2. Exemple de simulation

Ainsi dans cette simulation, on utilise la synchronisation identique entre deux systèmes de Rossler qu'on a vérifié dans l'exemple III.2 du chapitre III. De cette façon on prend le système (III.16) comme générateur d'un signal chaotique (on a choisi c (t)=$x_1$(t) une variable d'état du système (III.16) dans l'émetteur) .Au niveau du récepteur la synchronisation est faite en utilisant le système (III.17) avec les mêmes

conditions initiales que celles données dans l'exemple III.2, mais contrôlé par le signal r (t) reçu.

On aura alors le système suivant :

$$\begin{cases} \dot{y}_1 = -(y_2 + y_3) - g.(y_1 - r(t)) \\ \dot{y}_2 = y_1 + 0{,}2.y_2 \\ \dot{y}_3 = 0{,}2 + y_3.(y_1 - 5.7) \end{cases} \quad \text{(IV.1)}$$

Si on suppose que les perturbations dues au canal sont négligeables et que la transmission ne nécessite pas de modulation on aura alors :

$$r(t) = s(t) = c(t) + m(t) \quad \text{(IV.2)}$$

Avec m(t) le signal message et g de valeur 0.2 le paramètre d'accouplement.

La clé de cryptage et de décryptage est le paramètre d'accouplement g et les paramètres du système émetteur. Si on choisit pour m (t) un signal carré d'amplitude égale a 0.0001 et de fréquence égale 1 Hz, comme le montre la figure (IV.2). Au niveau de l'émetteur on aura alors le message crypté représenté sur la figure (IV.3) et à la sortie du récepteur, on aura alors le message reconstitué représenté sur la figure (IV.4).

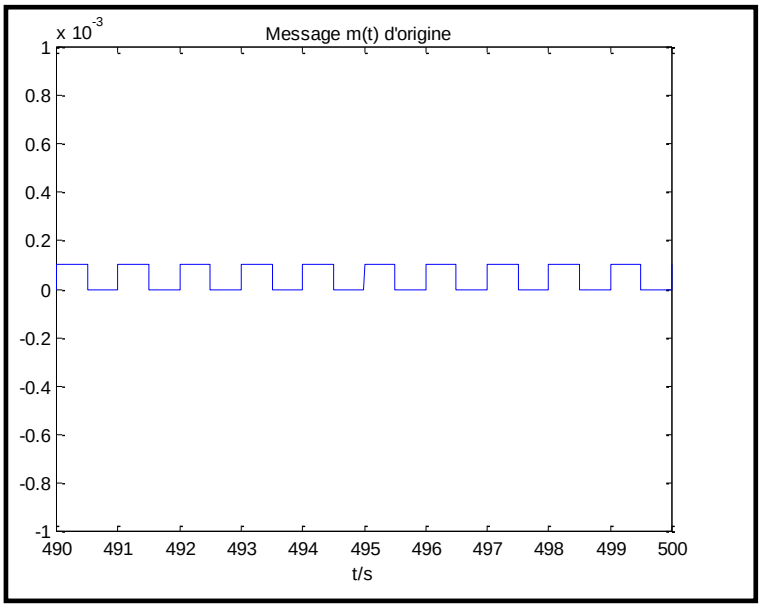



*Figure (IV.2) : Message m (t) d'origine*

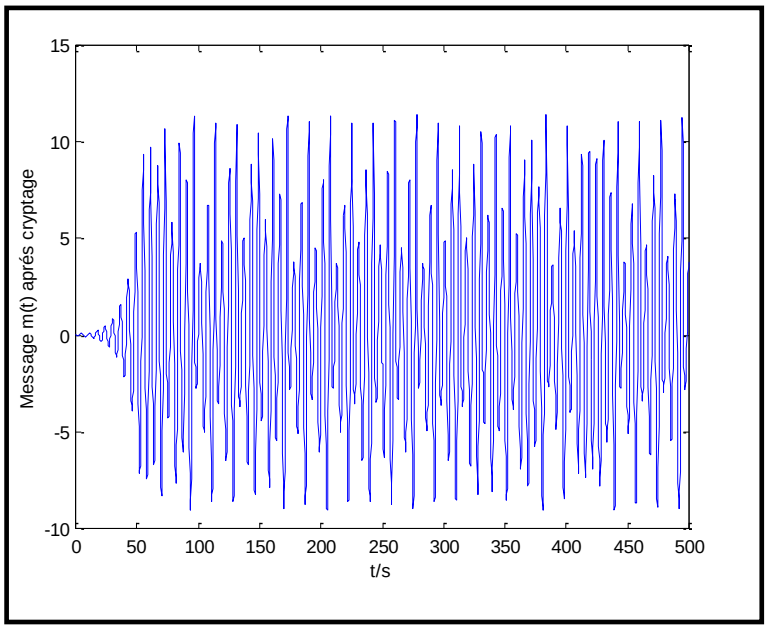



*Figure (IV.3) : Message m (t) après cryptage*

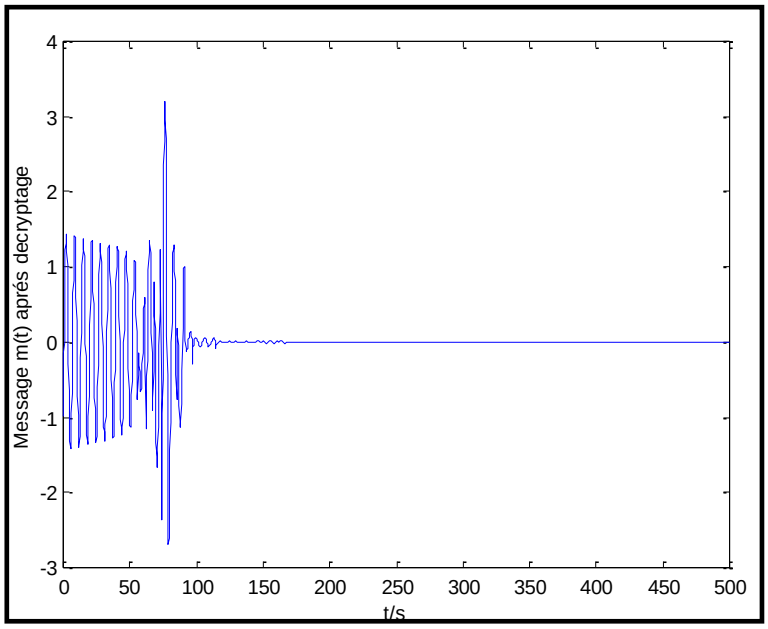



*Figure (IV.4) : Message reconstitué après cryptage et décryptage par la méthode du masquage par addition*

Pour vérifier la qualité du résultat on diminue l'échelle de l'axe des ordonnées de la représentation du signal reconstitué on aura alors la figure suivante :

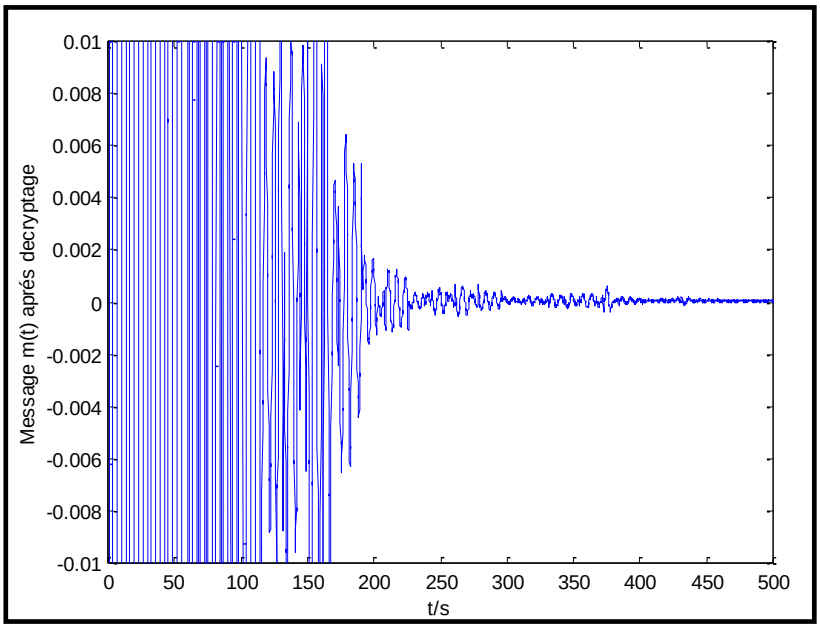



*Figure (IV.5) : Message reconstitué après cryptage et décryptage par la méthode du masquage par addition après diminution de l'échelle de la représentation*

Si on visualise notre signal entre les deux points d'abscisses respectivement 490s et 500s, alors on aura la figure suivante :

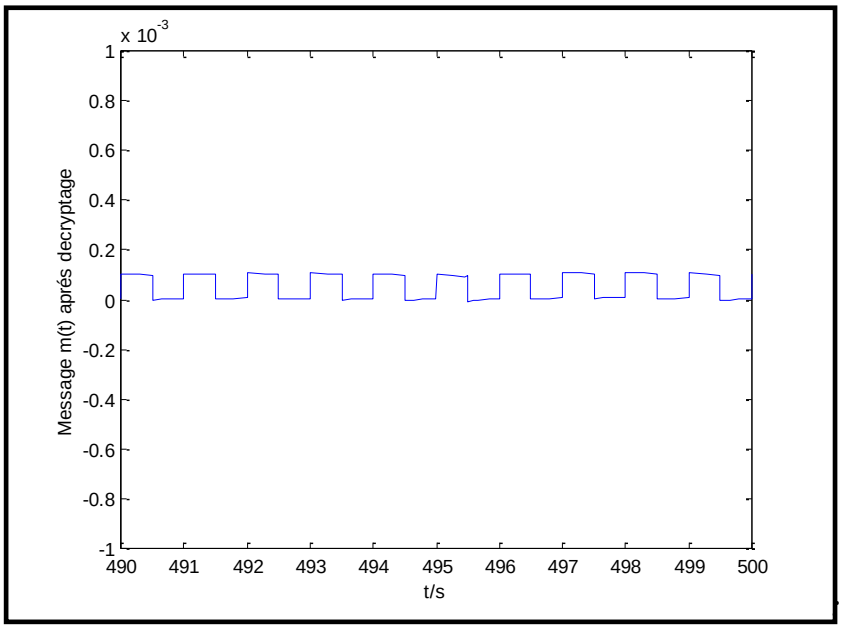



*Figure IV.6 :Visualisation du message décrypté entre deux points d'abscisses 490 s et 500 s*

On constate dans la figure (IV.6) qu'on a une forme similaire à notre signal message m(t) d'origine (amplitude 0.0001 et période de 1s).

### IV.2.3. Discussion des résultats

Les avantages du masquage chaotique par addition résident dans sa simplicité de réalisation et la possibilité de l'utiliser pour masquer l'analogique ou le numérique avec des canaux à fort SNR , comme c'est le cas des fibres optiques [25] . Inversement on souligne des inconvénients qui limitent l'application de cette technique en pratique tels que :

-La synchronisation non parfaite au niveau du récepteur, même avec une amplitude très faible du signal message devant le signal chaotique, ce qui implique la sensibilité au bruit du canal.

-Sensibilité à la disparité des paramètres, entre les systèmes chaotiques dans l'émetteur et le récepteur.

-Le faible degré de sécurité démontré, en testant cette technique par des méthodes de cryptanalyse exposées dans les articles [2],[36] ,[40] .

## IV.3. Masquage par décalage chaotique

### IV.3.1. Présentation de la technique

L'apparition de cette technique, est considérée comme une conséquence des problèmes d'application pratique du masquage par addition [9]. Elle a été proposée pour la première fois par le groupe de Kocarev [19] , et sa dénomination actuelle connue par '' Chaos shift keying : CSK'' revient à l'article du groupe de Dedieu [9] .

La CSK définie comme une modulation numérique est inspirée des techniques de modulation classique telle que la FSK (frequency shift keying) la ASK (amplitude shift keying ) et la PSK (phase shift keying).Alors le système de masquage par CSK est constitué par un modulateur CSK au niveau de l'émetteur et d'un démodulateur CSK au niveau du récepteur raccordés par un canal routeur du signal comme il est représenté sur la figure (IV.7).

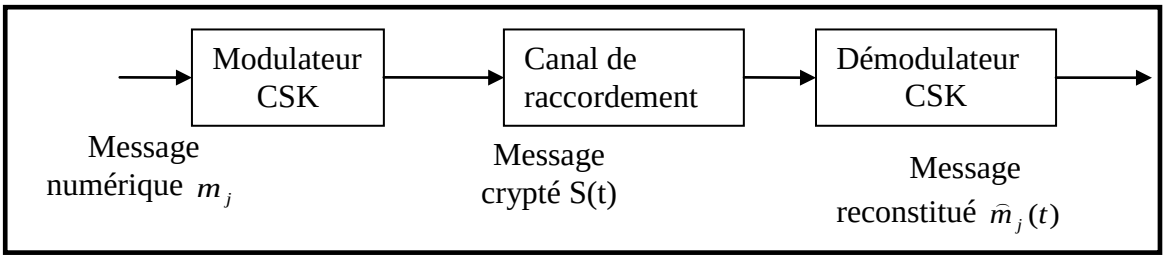



*Figure (IV.7) : Schéma de principe simplifié d'un système de cryptage CSK*

#### 4.3.1.1. Le modulateur CSK

Son idée de base est la même que celle de la modulation numérique classique, c'est-à-dire associer à chaque symbole du message à transmettre non pas une porteuse sinusoïdale , mais une porteuse chaotique différente [21],[22] ,en se déplaçant dans une période de durée T . Ainsi en utilisant la notation la plus générale introduite dans [23], les éléments de l'ensemble d'un signal message numérique incluent dans un espace de symboles à M niveaux modulé par CSK sont définis par :

$$S(t) = \sum_{j=1}^{N} m_j g_i(t) \qquad \text{(IV.3)}$$

Où $m_j$ sont les éléments du vecteur signal message et $g_i(t)$ sont les porteurs chaotiques. Avec $j = 1,2.....N$ ; $i = 1,2.....M$ ; $N \le M$ et $m_j = 1$ si $i = j$ et $m_j = 0$ si $i \neq j$. Le signal $S(t)$ peut être généré comme il est représenté dans la figure(IV.8) [23] .

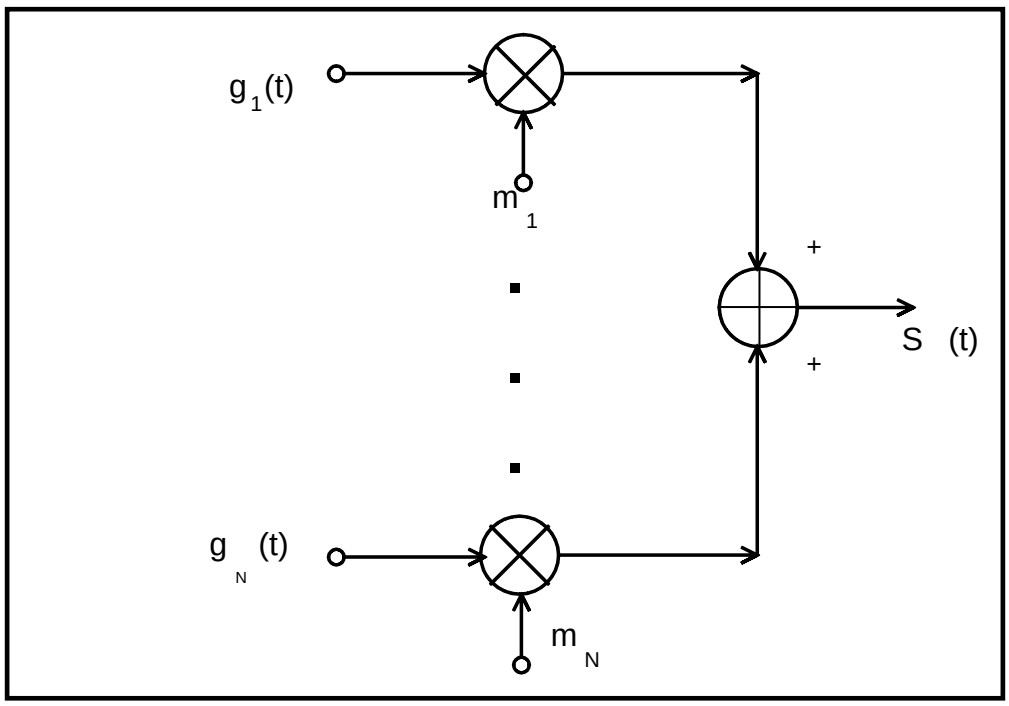



*Figure (IV.8) : Principe de la modulation par CSK*

#### 4.3.1.2. Le Démodulateur CSK

Du côté du récepteur autorisé si on suppose que le signal est reçu par bande de base, on peut citer deux types de schémas qui ont été proposés [16] :

**-Démodulation basée sur la synchronisation et le calcul d'erreur :** A ce niveau les porteurs chaotiques $g_i$ , utilisés pour la modulation, seront reconstruits en utilisant des unités de synchronisation chaotiques. Le nombre de ces unités est égal au nombre des porteurs chaotiques $g_i$ , figure (IV.9). Ainsi dans cette configuration, le signal reçu va essayer de synchroniser toutes les unités de synchronisation. Alors si on suppose que le signal transmis $S(t) = g_i(t)$ , on n'aura donc la synchronisation qu'avec la i-ème unité. De cette façon on va avoir une convergence de $g_i(t)$ vers la sortie de l'unité $\hat{g}_i(t)$ et une divergence pour les autres unités. L'estimation des symboles $m_j$ du message sera faite après le calcul des erreurs de synchronisation dans le bloc de

décision. Les paramètres des unités de synchronisation et le temps symbole peuvent être considérés comme la clé de décryptage .

**-Démodulation basée sur la synchronisation et la corrélation :** Dans ce modèle, la reconstitution des porteurs chaotiques $g_i(t)$ est aussi nécessaire, ainsi elle se fait de la même manière que pour le modèle précèdent. Comme la corrélation est un processus générique dans les systèmes de communication qui est employé pour évaluer la similarité entre deux signaux, alors la différence de ce système par rapport au précédent est que chaque unité de synchronisation chaotique est cascadée par un bloc corrélateur . De cette manière, si les porteurs chaotiques $\hat{g}_i(t)$ reconstitués par synchronisation pendant un temps $T_s$ convergent vers $g_i(t)$ , le symbole transmis peut être identifié en évaluant la corrélation entre $g_i(t)$ et $\hat{g}_i(t)$ .La prise de décision sera faite en comparant les éléments du vecteur de décision $Z = (z_1 ....., z_M)$ sorties des corrélateurs. Alors l'affirmation de la convergence de $g_i(t)$ vers $\hat{g}_i(t)$ sur un intervalle $[T_s, T]$ va nous donner une observation $z_i > z_k \forall k = 1...M \quad i \neq k$ . La figure (IV.10) illustre ce principe. Les paramètres des unités de synchronisation et le temps symbole peuvent être considérés comme la clé de décryptage .

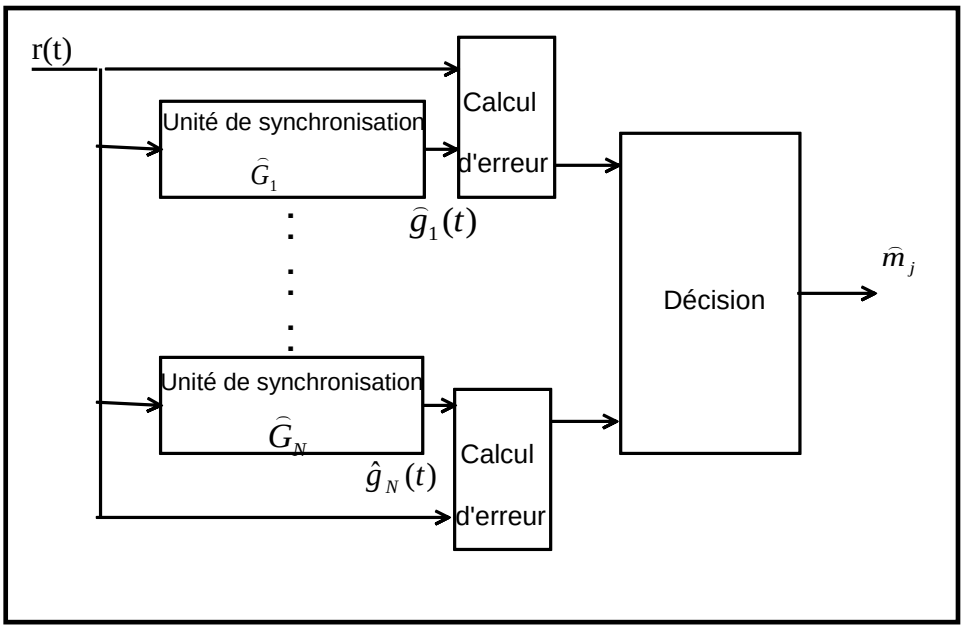



*Figure (IV.9) : Démodulation basée sur la synchronisation et le calcule d'erreur*

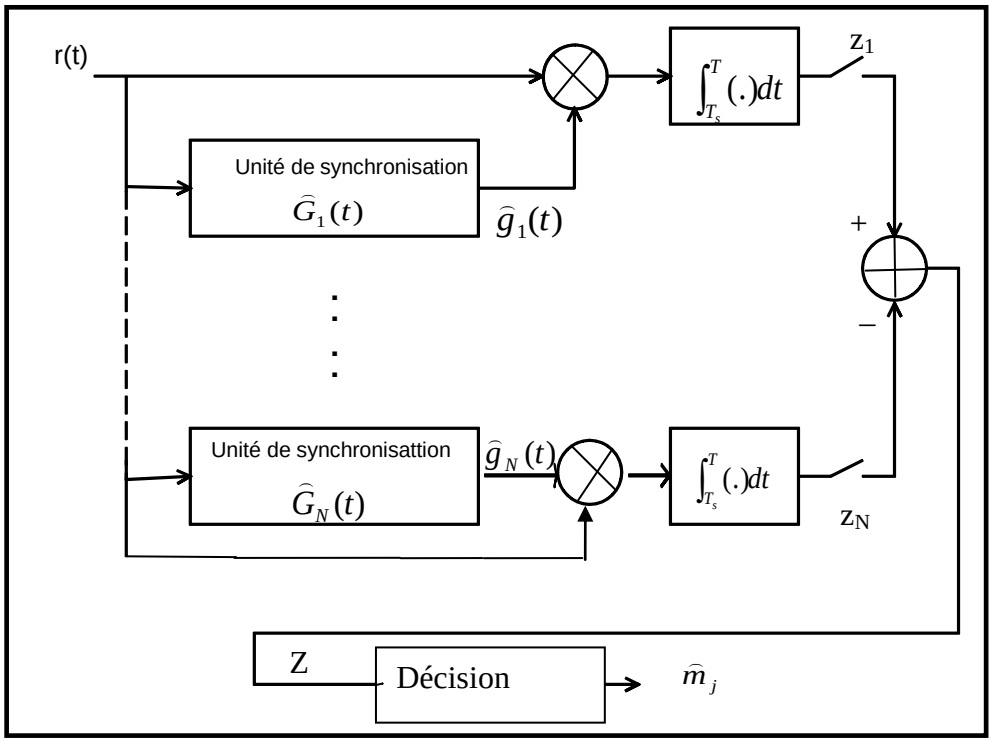



*Figure (IV.10) : Démodulation basée sur la synchronisation et la corrélation*

**Remarque IV.1**

Il est à noter que ces propositions sont basées sur la démodulation cohérente, c'est-à-dire le récepteur est capable de reproduire la même porteuse chaotique que celle émise par l'émetteur, afin que le message d'origine soit décrypté.

L'inconvénient le plus important pour ces deux techniques est que la synchronisation se perd, lorsque le symbole du signal message change. Ainsi le temps de transmission d'un seul symbole doit être supérieur ou égal à la somme du temps de synchronisation, plus le temps de décision, ce qui limite le débit de transmission du message. Des modifications de la méthode CSK pour la démodulation non cohérente, qui n'exigent pas la reproduction de la même porteuse chaotique de l'émission, ont été également proposées [22] .

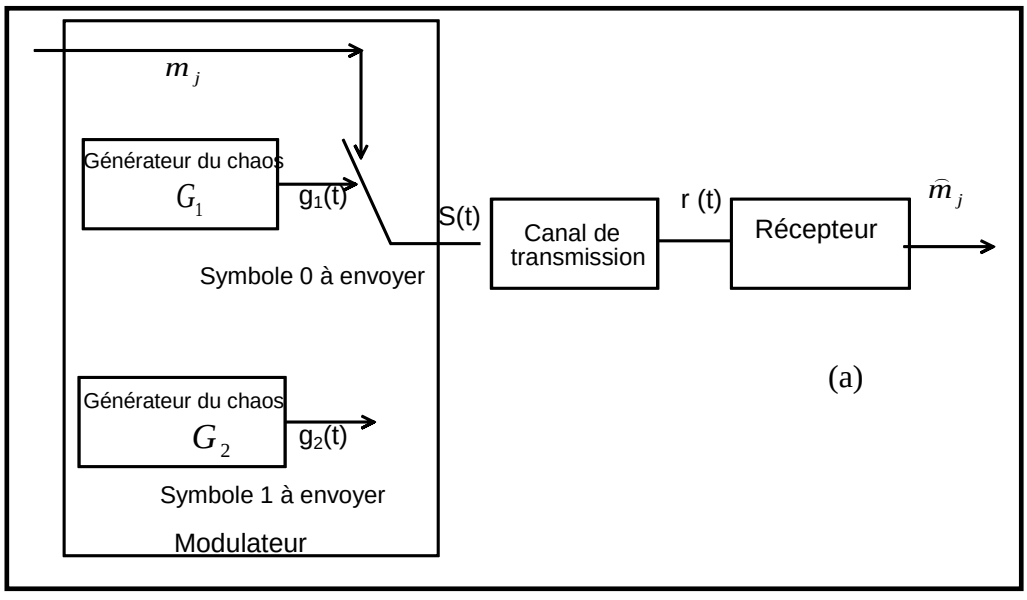
### IV.3.2. Exemple de simulation

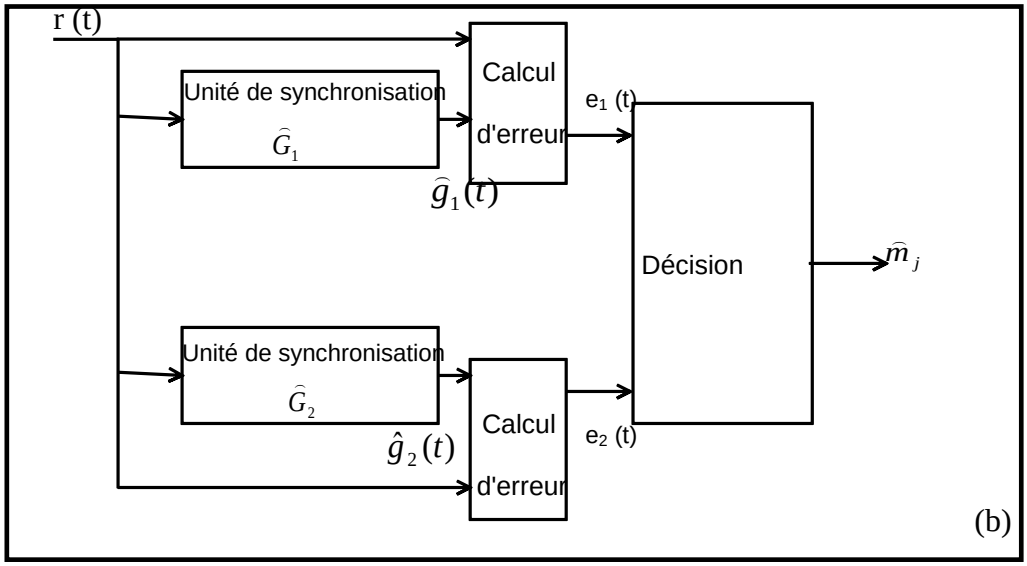
La synchronisation étant un élément clé dans l'étude des communications

sécurisées par le chaos, ainsi dans notre étude de la CSK, on a choisi de simuler un système à récepteur cohérent, dont la démodulation est basée sur la synchronisation et le calcul d'erreur représenté sur la figure (IV.9) et on a choisi comme message un signal binaire. De cette façon, au niveau de l'émetteur, notre système fait la commutation, entre deux signaux chaotiques différents $g_1(t)$ et $g_2(t)$ mais statiquement similaires, selon que la valeur du signal message, est égale à ''0'' ou ''1''. Dans ce cas, si le mot binaire à envoyer durant l'intervalle $[(l-1)T, lT]$ est 0, alors $g_1(t)$ est transmis, si le mot binaire est 1 alors $g_2(t)$ est transmis. Le schéma de la modulation et la démodulation, CSK devient alors comme il est représenté sur la figure (IV.11) [16].
Pour la CSK, le masquage d'un signal numérique, exige :

- Le choix d'une porteuse chaotique de fréquence de fluctuation plus grande, que la fréquence du signal message binaire à transmettre. Comme pour la modulation classique la fréquence porteuse est très supérieure à la fréquence du signal modulant.

- Le temps de synchronisation au niveau du récepteur doit être plus faible, que le temps nécessaire pour la transmission d'un seul bit, car elle est perdue à chaque fois que le signal reçu change (0 ou 1) selon le bit transmis [9].





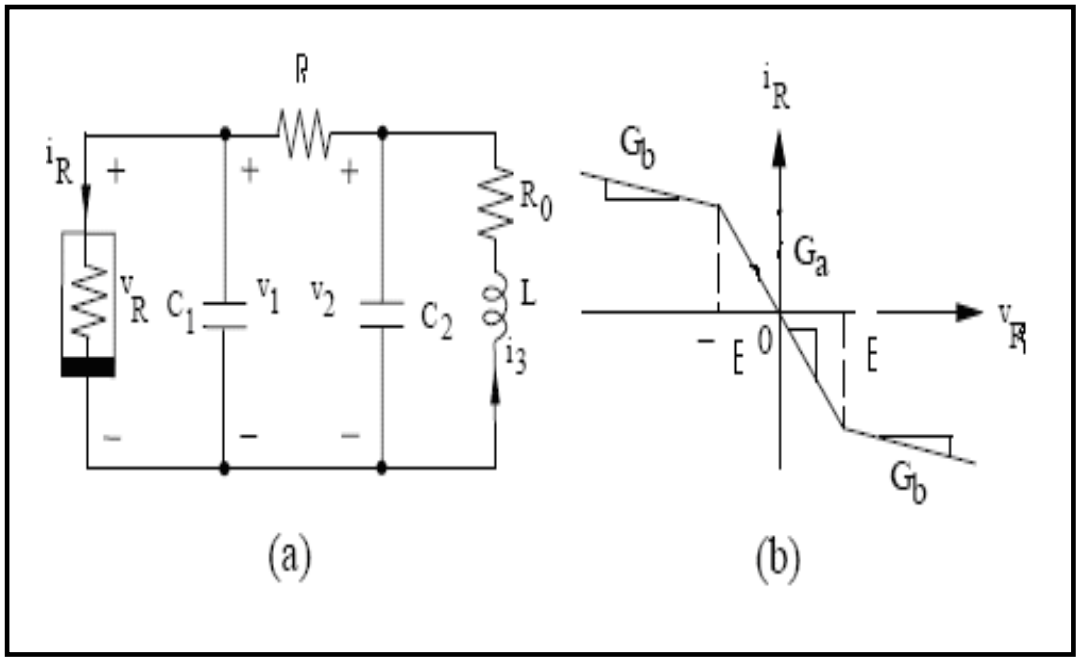

*Figure(IV.11) :(a) Modulateur CSK d'un signal binaire (b) Démodulateur CSK*

Ainsi on a utilisé l'oscillateur de Chua dont le schéma est représenté sur la figure(IV.12) comme générateur du chaos. Ses équations d'états sont données par [42] :

$$\begin{cases} \dfrac{dv_1}{dt} = \dfrac{1}{C_1}[G(v_2 - v_1) - f(v_1)] \\ \dfrac{dv_2}{dt} = \dfrac{1}{C_2}[G(v_1 - v_2) + i_3] \\ \dfrac{di_3}{dt} = \dfrac{1}{L}[-v_2 - R_0 i_3] \end{cases} \tag{IV.4}$$

Où : $v_1$ , $v_2$ et $i_3$ sont respectivement la tension aux bornes de $C_1$, la tension aux bornes de $C_2$ et le courant traversant L avec le paramètre $G = \dfrac{1}{R}$ . Le terme $R_0 i_3$ représente la tension de la résistance additionnelle au niveau de la bobine L. La caractéristique $f(v_1)$ de la diode de Chua est donnée par :

$$f(v_1) = G_b v_1 + \frac{1}{2}(G_a - G_b)(|v_1 + E| - |v_1 - E|) \tag{IV.5}$$




*Figure( IV.12) (a) L'oscillateur de Chua. (b) La caractéristique de la diode de Chua[42]*

Il a été vérifié dans la référence [42] que le système (IV.4), qui est considéré comme système maître , se synchronise identiquement avec un système esclave dont les équations d'états sont données par :

$$\begin{cases} \dfrac{d\tilde{v}_1}{dt} = \dfrac{1}{C_1}[G(\tilde{v}_2 - \tilde{v}_1) - f(\tilde{v}_1)] \\ \dfrac{d\tilde{v}_2}{dt} = \dfrac{1}{C_2}[G(v_1 - \tilde{v}_2) + \tilde{i}_3] \\ \dfrac{d\tilde{i}_3}{dt} = \dfrac{1}{L}[-\tilde{v}_2 - R_0\tilde{i}_3] \end{cases} \qquad \text{(IV.6)}$$

ou $\tilde{v}_1$ , $\tilde{v}_2$ et $\tilde{i}_3$ sont les variables d'état du système esclave.

L'accouplement entre les deux systèmes se fait par la variable $v_1$ du système (IV.4) dans la seconde équation du système (IV.6).

Avec les paramètres donnés dans la référence [42] , à l'instant t=0.005 s , on a trouvé que l'erreur de synchronisation entre les systèmes (IV.4) et (IV.6) tendant vers

0 , passe à une valeur égale à $-7.89\times10^{-9}$ .Ainsi on va considérer par la suite que le temps de synchronisation $T_s$ est aux environs de 0.005s.

Dans notre simulation, on a utilisé deux oscillateurs chaotiques $G_1$ et $G_2$ pour coder le ‘’0 ‘’ et le ‘’1’’ du signal message, dont les équations d’états sont celles du système (IV.4). Ils sont similaires mais statistiquement différents. Concernant leurs paramètres on a choisi respectivement :

- pour le système $G_1$ : R=1000 Ω, $R_0$=20 Ω, $G_a$=-1.139mS, $G_b$=-0.711mS, E=1V, L=12.2mH, $C_1$=17.2nF, $C_2$=180nF et les conditions initiales $v_1(0)=0.2, v_2(0)=0.2, i_3(0)=0.002$ .
- pour le système $G_2$ : R=1000 Ω, $R_0$=20 Ω, $G_a$=-1.139mS, $G_b$=-0.711mS,E=1V ,L=12.1mH, $C_1$=17.1nF, $C_2$=179nF et les conditions initiales $v_1(0)=0.15, v_2(0)=0.15, i_3(0)=0.0015$ .

On note que ces paramètres sont légèrement différents à ceux donnés dans la référence [42]. On a pris les deux signaux $v_1(t)$ des deux systèmes chaotiques $G_1$ et $G_2$ comme porteuses chaotiques dans notre système de cryptage . La figure (IV.13) montre les formes des attracteurs chaotiques ($v_1$, $v_2$) générés par les systèmes $G_1$ et $G_2$ .

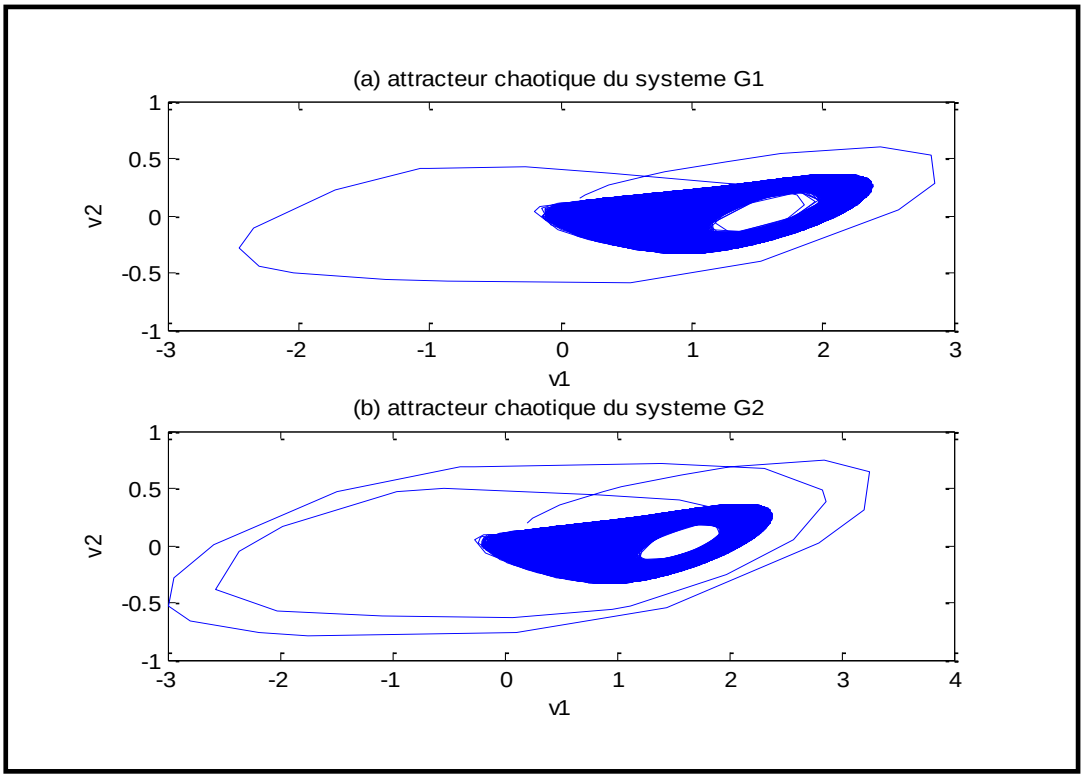



*Figure (IV.13) : Les attracteurs chaotiques des deux systèmes $G_1$ et $G_2$*

Au niveau de la réception, les blocs de synchronisation $\hat{G}_1$ et $\hat{G}_2$ dont les équations d'états sont celles du système (IV.6) et les paramètres sont identiques aux systèmes $G_1$ et $G_2$ .

Pour les conditions initiales des blocs $\hat{G}_1$ et $\hat{G}_2$ on a choisi respectivement [0.16, 0.16, 0.0016] et [0.17, 0.17, 0.0017].

Puisque le débit du signal message à masquer est limité par le temps de synchronisation $T_s$ des oscillateurs chaotiques (0.005 s dans notre cas), on a choisi dans notre simulation d'utiliser le bloc" Bernouilli Binary Generator " de simulink , qui génère des séquences 0 et 1, d'une façon aléatoire et on a réglé son débit T égale à 0.01 s supérieur au temps de synchronisation $T_s$ . Pour la probabilité d'apparition des 0 et des 1 on a choisi sa valeur égale à 0.5.

La figure (IV.14a) représente l'allure du signal message $m_j$ avant la modulation. A la sortie du modulateur CSK , le signal est représenté sur la figure (IV.14 b).

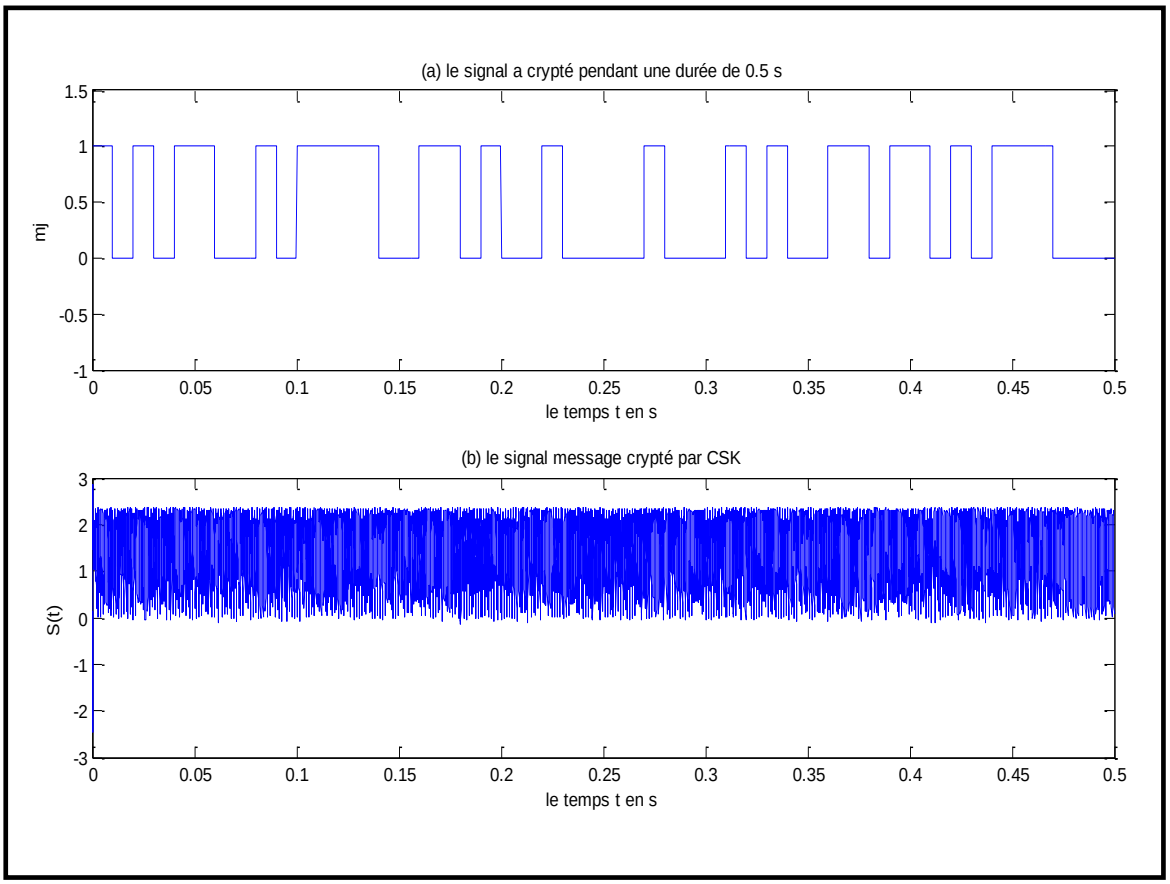



*Figure (IV.14) : (a)L'allure du signal message $m_j$ pendant une durée de 0.5 s*

*(b) L'allure du signal message après cryptage par CSK*

Si on suppose que le signal message crypté S(t) est reçu par le récepteur autorisé, représenté sur la figure (IV.11 b) , sans perturbation . A ce niveau il y'aura alors synchronisation respectivement des deux oscillateurs $\hat{G}_1$ ou $\hat{G}_2$ avec le signal S(t) reçu , selon que la valeur du signal message $m_j$ est à '0' ou '1' .

Ce résultat est identifié par l'annulation des signaux erreurs de synchronisation $e_1(t)$ ou $e_2(t)$ , comme il est représenté sur les figures (IV.15 a) et (IV.15 b).

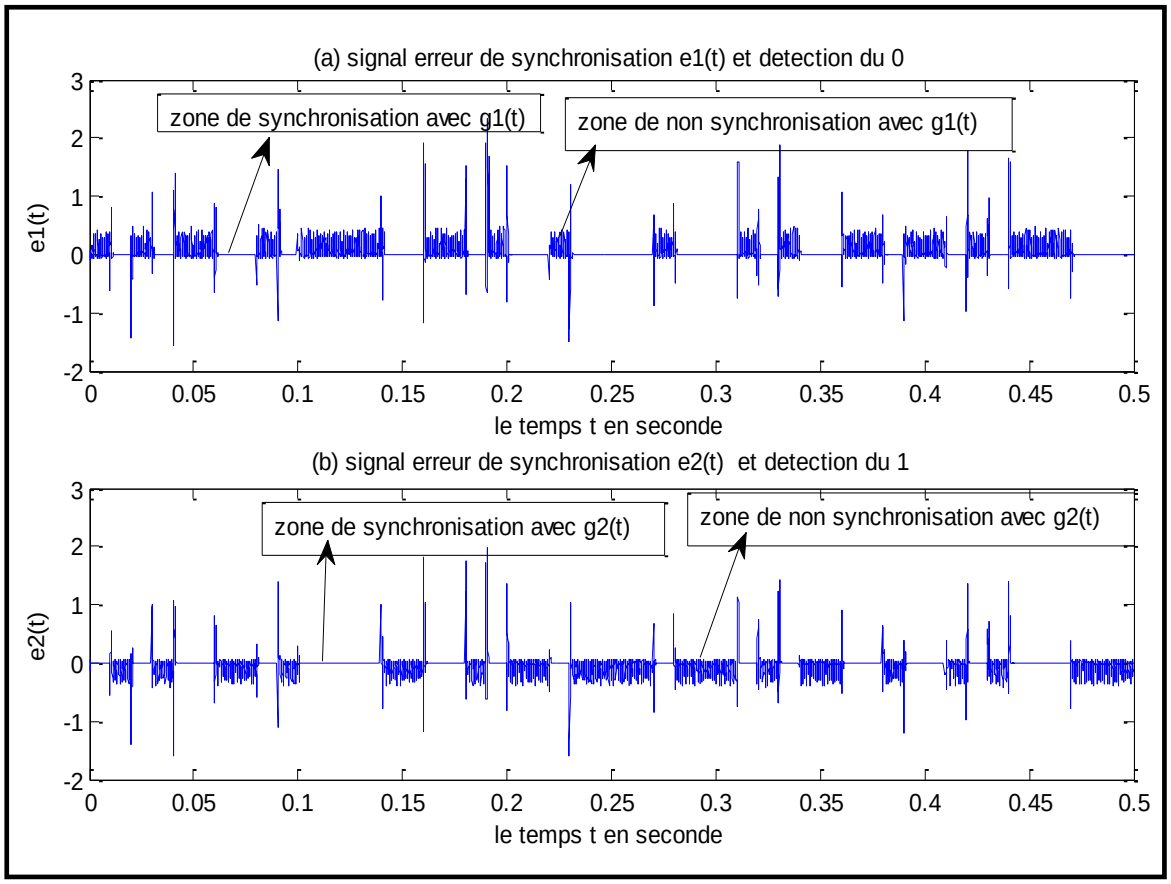



*Figure (IV.15) : (a)Signal erreur de synchronisation avec $g_1(t)$ (b) Signal erreur de synchronisation avec $g_2(t)$*

A partir de ces erreurs de synchronisation , la prise de décision pour récupérer le signal message sera alors faite dans le bloc de décision représenté sur la figure(IV.16).

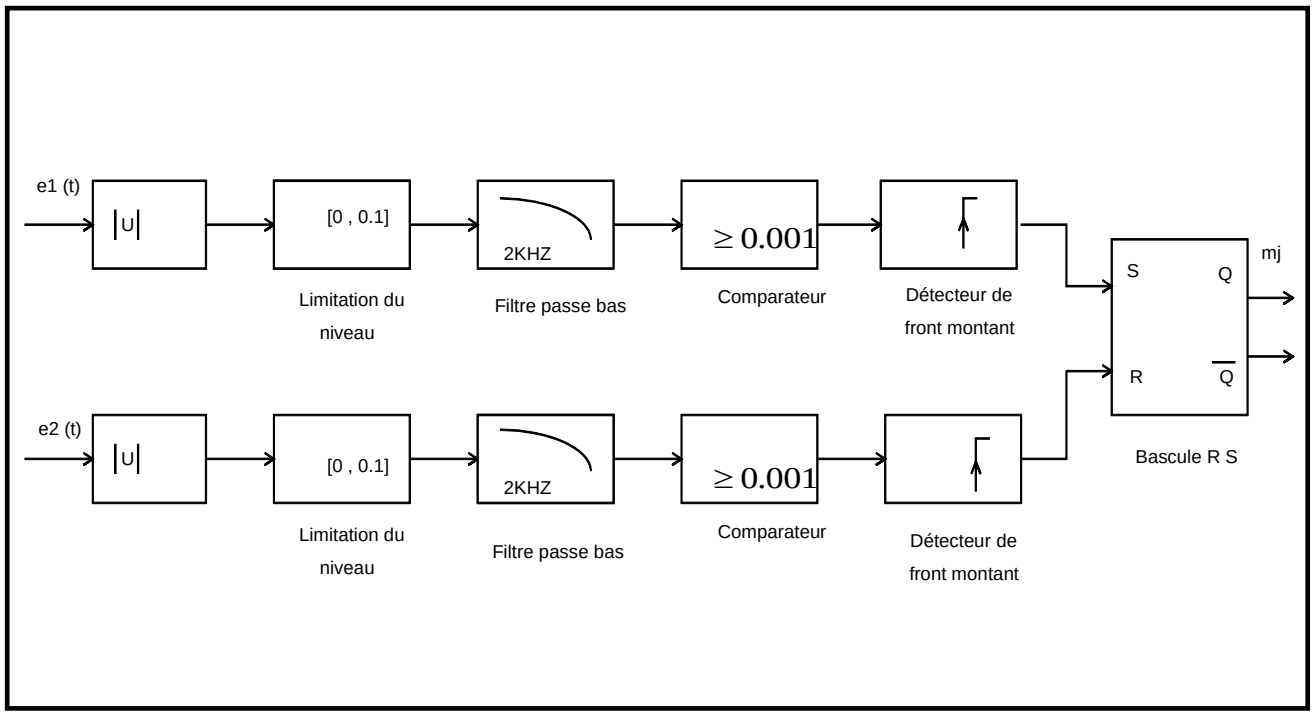



*Figure (IV.16) : Le bloc de décision*

La procédure de traitement au niveau de ce bloc peut être résumée comme suit :

1-Quelque soit le signe de l'erreur de la synchronisation identique entre deux signaux chaotiques, la règle de base est qu'une erreur nulle implique la synchronisation. Ainsi dans des situations pareilles au traitement dans le bloc de décision représenté à la figure (IV.16) , on trouve des propositions de traiter les carrés des erreurs [6]. Par un raisonnement, à titre de conséquence, dans notre simulation on a choisi de traiter les valeurs absolues des erreurs $e_1(t)$ et $e_2(t)$, figure (IV.17).

2-La figure (IV.17) représente les signaux résultants des erreurs $e_1(t)$ et $e_2(t)$, qui sont des signaux binaires enveloppant des porteuses chaotiques. Pour détecter ces enveloppes , on a procédé comme pour la démodulation AM classique , par écrêtage de notre signal dans l'intervalle [0,0.1] , par l'étage limiteur . On aura ainsi les signaux représentés sur la figure (IV.18). Ensuite ces signaux seront filtrés par des filtres passe-bas, pour atténuer les porteuses chaotiques et maintenir les enveloppes binaires. On a choisi pour cela des filtres passe bas de fréquences 2 KHz. Le signal filtré est représenté sur la figure (IV.19).

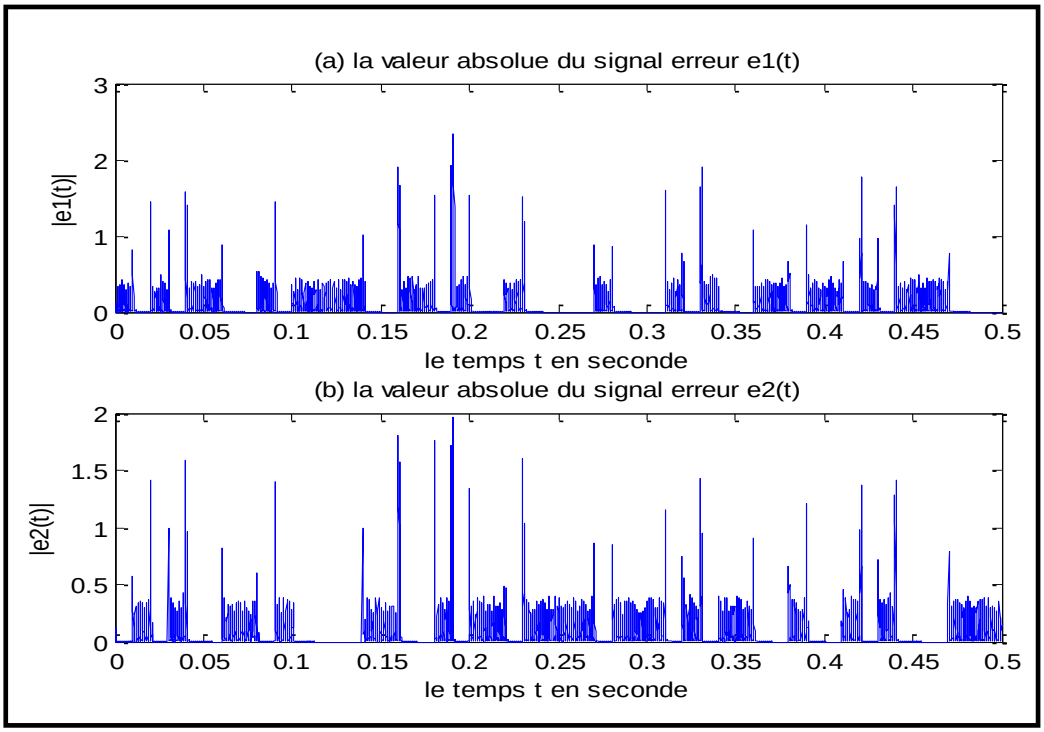



*Figure (IV.17) : Les valeurs absolues des signaux erreurs de synchronisation*

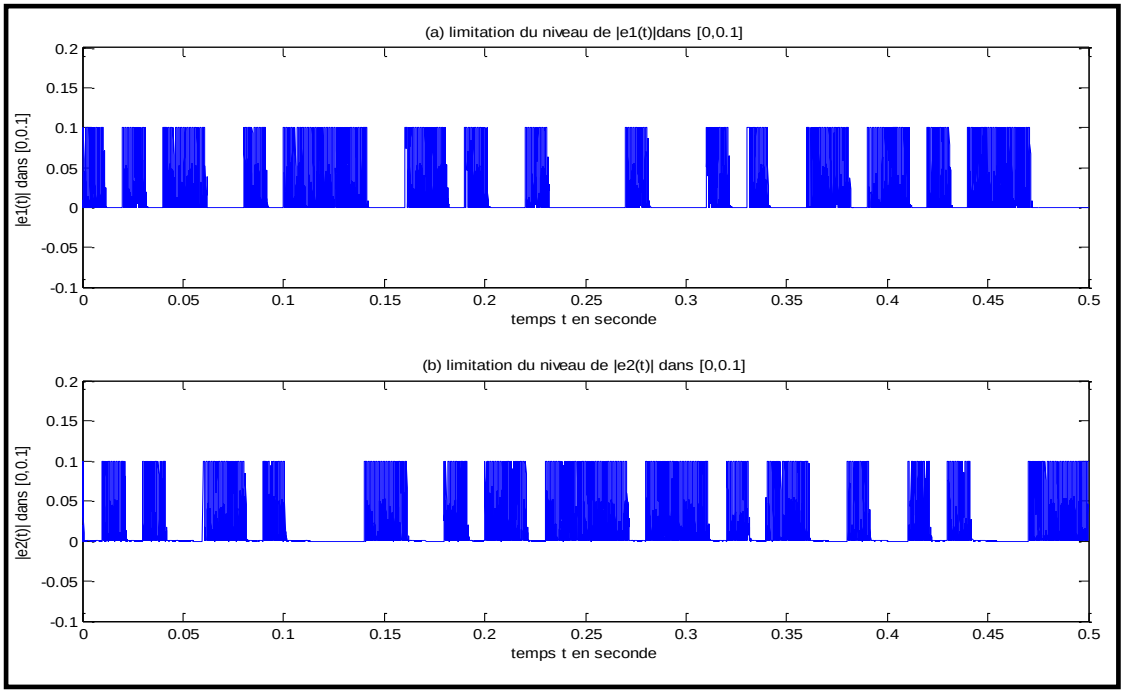



*Figure (IV.18) : Valeurs limitées des valeurs absolues des signaux erreurs de synchronisation*

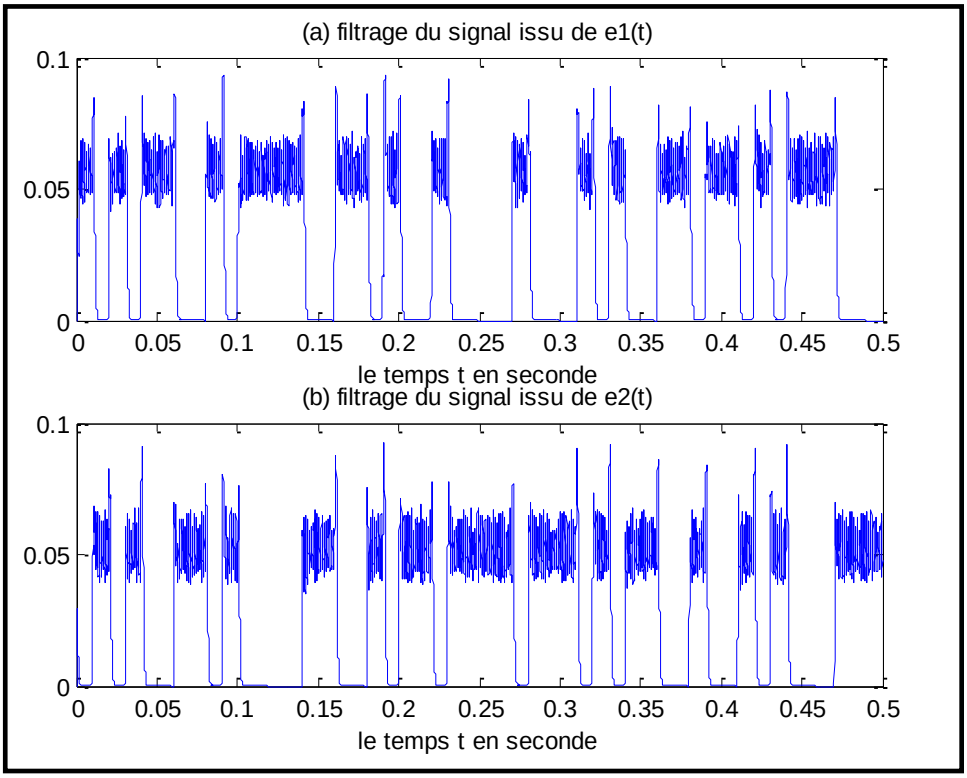



*Figure (IV.19) : Filtrage des signaux issus de* $e_1(t)$ *et* $e_2(t)$

3-Les signaux binaires résultants des signaux $e_1(t)$ et $e_2(t)$, seront tirés des signaux représentés sur la figure (IV.19), par seuillage et comparaison. On a utilisé pour cela l'étage comparateur réalisant l'opération suivante :

$$\begin{cases} 1 \Rightarrow signal \geq 0.001 \\ 0 \Rightarrow signal < 0.001 \end{cases} \qquad \text{(IV.7)}$$

On aura alors les signaux représentés sur la figure (IV.20).

4-En comparant les signaux représentés sur la figure (IV.20) avec le signal message $m_j$ d'origine , représenté sur la figure (IV.14 a), on a remarqué que, ce signal monte à un niveau haut en même temps avec un front montant du signal binaire issu de $e_1(t)$ et descend vers un niveau bas en même temps ,avec un front montant du signal issu de $e_2(t)$ .Ainsi pour reconstituer le signal d'origine, on a procédé par la détection des fronts montants des signaux représentés sur la figure (IV.20) par des étages détecteurs de fronts montants .Ces signaux deviennent comme représenté sur la figure (IV.21) .Puis

ces signaux seront injectés dans une bascule ‘RS’ pour récupérer le signal message d’origine.

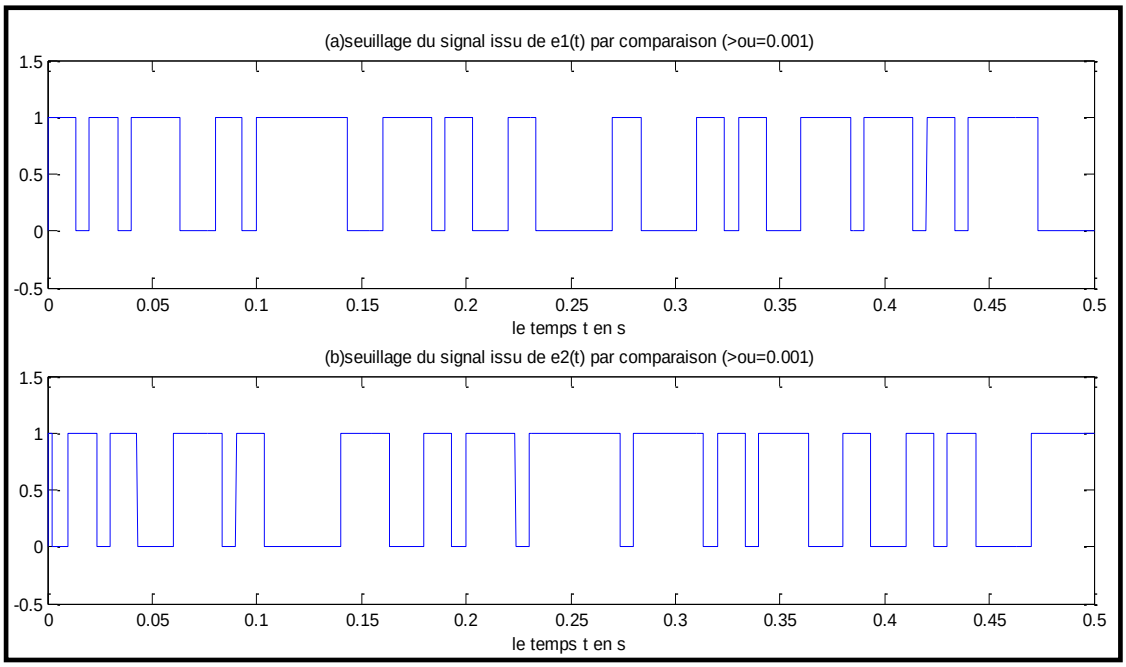



*Figure (IV.20) : Seuillage des signaux issus de* $e_1(t)$ *et* $e_2(t)$

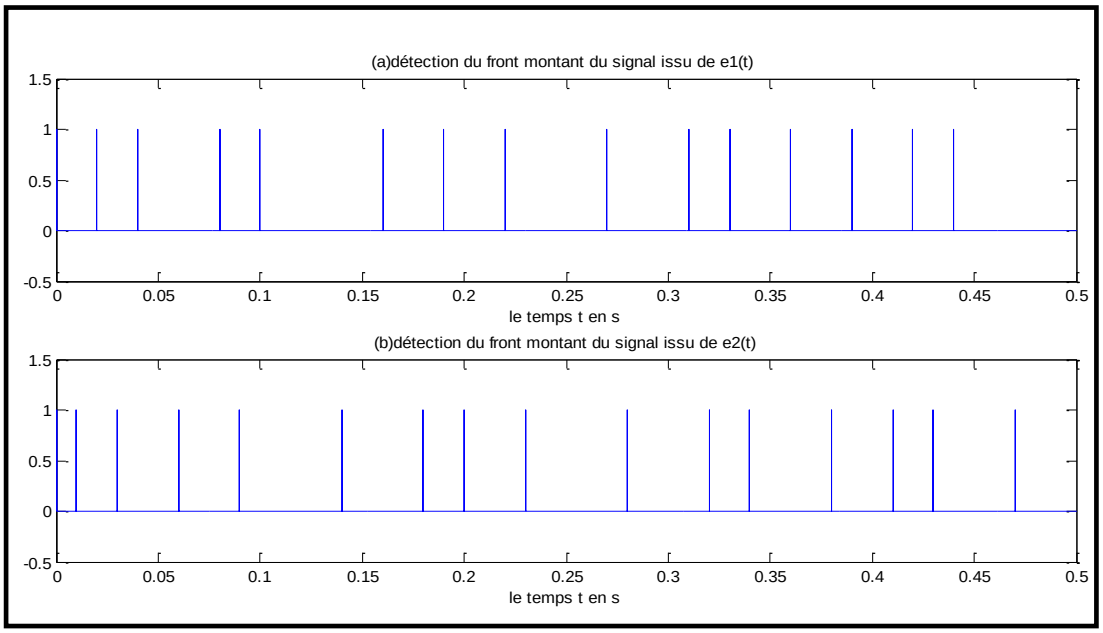



*Figure (IV.21) : Détection des fronts montants des signaux issus de* $e_1$ *(t) et* $e_2$ *(t)*

La figure (IV.22) représente le signal d'origine et le signal reconstitué par l'opération de décryptage qu'on a utilisé. Le signal reconstruit est alors tout à fait identique au signal message d'origine.

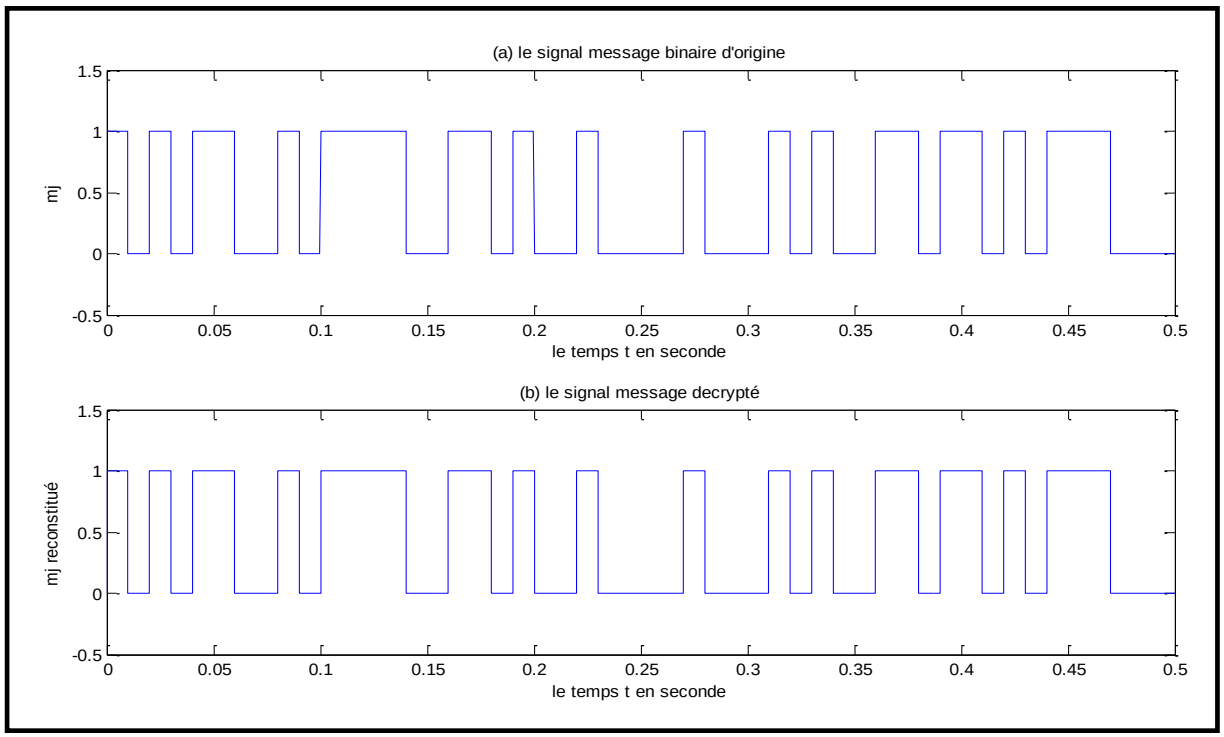



*Figure (IV.22) : Décryptage du signal message crypté et comparaison avec le signal message d'origine*

### IV.3.3. Discussion des résultats

L'analyse du cryptosysteme chaotique étudié, sera faite sur sa fiabilité de cryptage et de décryptage d'une image binaire, vis-à-vis des effets du temps symbole, des perturbations du canal et des disparités des paramètres.

#### IV.3.3.1. L'image utilisée pour l'analyse

Le choix a été fait sur une image à niveau de gris qui contient (256x256) pixels . Elle peut être représentée par une matrice (256x256) contenant des entiers en base 10,

représentant le degré de luminosité des pixels constituant l'image .Afin de réaliser le processus de transmission de cette image par l'intermédiaire du cryptosysteme ci-dessus , les transformations suivantes sont nécessaires :

a- Conversion des entiers représentants la matrice image en binaire , c'est-à-dire avec la transformation de chaque entier de la matrice image en son équivalent binaire sur 8 bits on aura alors une matrice de (256x256x8) éléments binaires .

b- La matrice de nombres binaires obtenue, sera transformée en un seul vecteur par concaténation de ces colonnes pour générer le signal binaire à transmettre .

c- Le choix de la temporisation de l'acquisition de l'image sera fait , par la création d'un vecteur temps de même dimension que le vecteur image, représentant les instants de l'envoi de chaque bit de l'image .

La figure suivante représente la préparation de l'image avant sa transmission :

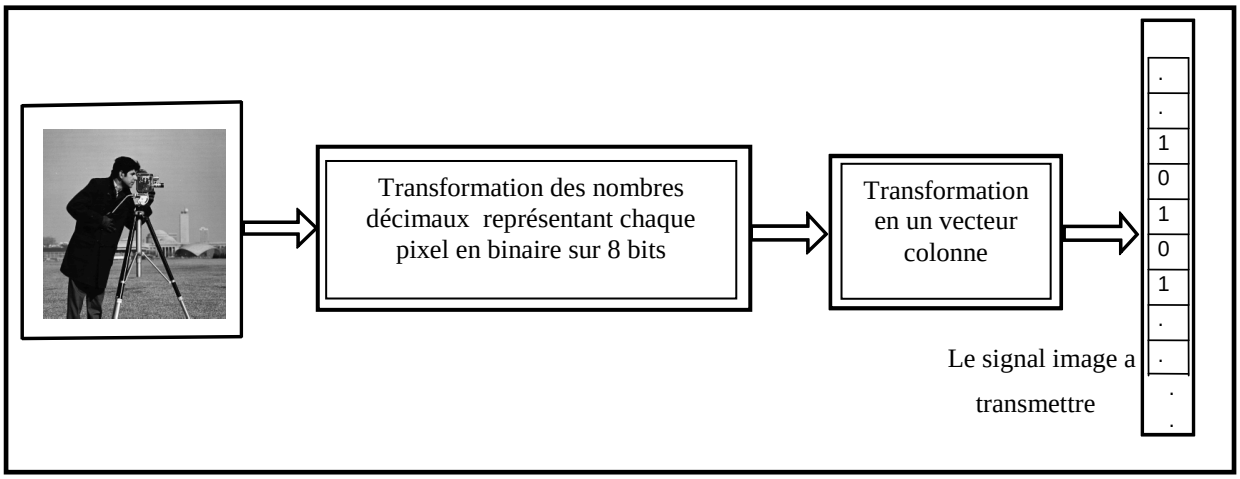



*Figure (IV.23) : Traitement du signal image avant la transmission à travers le cryptosysteme conçu*

### IV.3.3.2. Effet du débit du signal message sur le fonctionnement du système étudié

Le comportement idéal du système étudié, implique la neutralité des perturbations au niveau du canal routeur du signal transmis et l'absence de disparité de paramètres dans les unités de synchronisation chaotiques à la réception autorisée. Ces circonstances de fonctionnement ont été utilisées pour étudier l'effet de la durée du

symbole T sur le cryptage et la reproduction fidèle de l'image décrite ci-dessus. Notre étude consiste donc à mettre en évidence la variation du taux d'erreur BER entre l'image d'origine et l'image reconstituée en fonction de T. La figure (IV.24) illustre cette variation .Dans cette figure qui est une résultante des tests du système étudié sur plusieurs valeurs de T ,on remarque que le BER augmente avec la diminution de T .Cela est dû à la perte de la synchronisation au niveau du récepteur pour les durées symbole inférieures au temps de synchronisation $T_s$ .

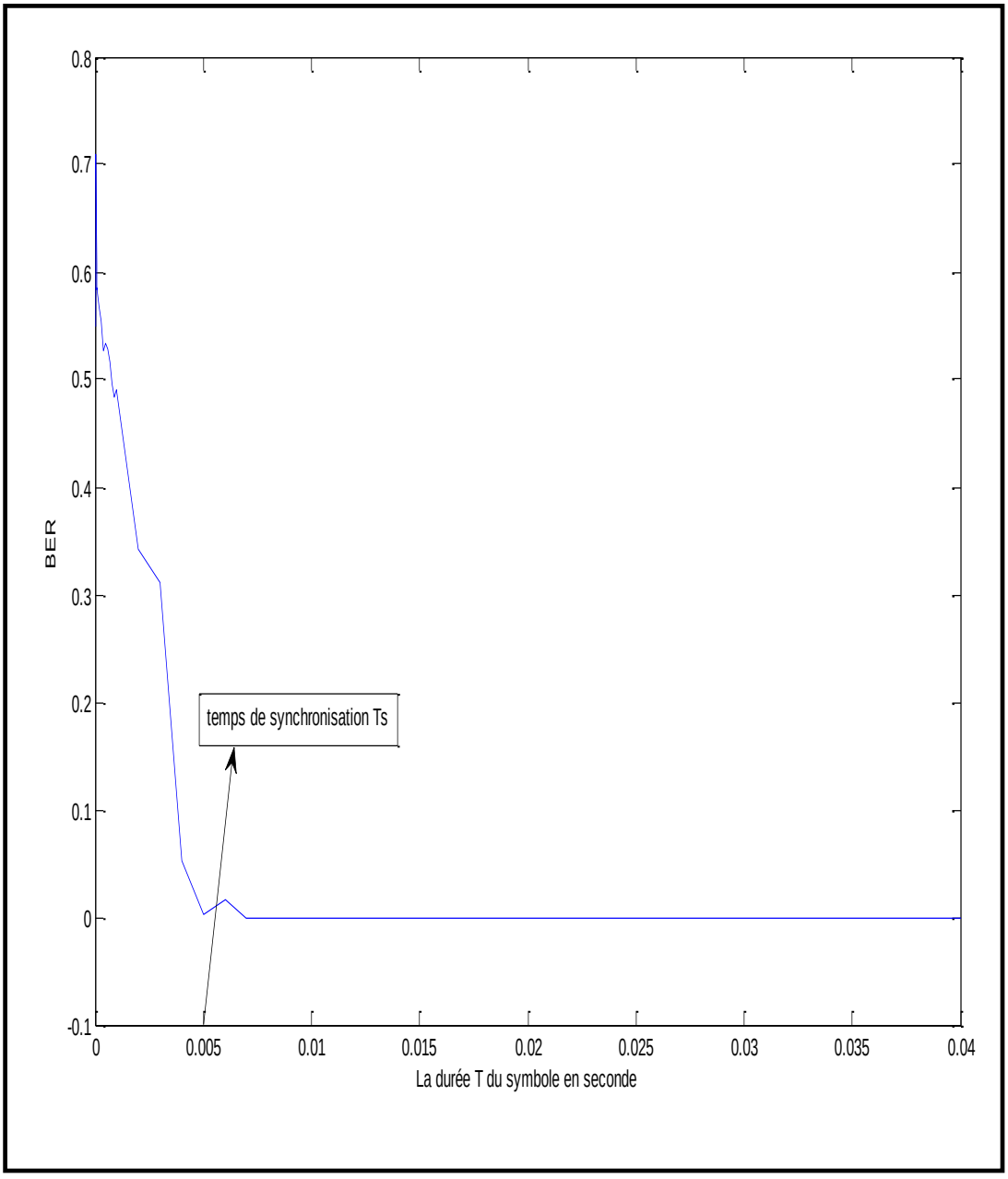



*Figure (IV.24) : La variation du BER en fonction de la durée symbole T*

La figure (IV.25) montre les changements subis sur l'image à T supérieur au temps de synchronisation $T_s$ au niveau d'un récepteur autorisé et un autre non autorisé , puis à T inférieur au temps $T_s$ au niveau d'un récepteur autorisé .

*(a)Image d'origine* *(b) Réception non autorisée a T=0.01s > $T_s$*

*(c)Image décryptée a T=0.01s > $T_s$* *(d) Image décrypté a T=0.001s < $T_s$*

*Figure (IV.25) : Changements subis sur l'image reçue et effet du temps symbole T*

### IV.3.3.3. Effet des perturbations du canal de transmission

Le problème de robustesse aux perturbations du canal se pose pour tout système de communication. Selon la nature du canal, les signaux sont de nature différente :

-Atmosphère : ondes électromagnétiques.

-Câble coaxiale : signaux électriques.

-Fibre optique : lumière.

Une modélisation simplifiée du canal peut être représentée sur la figure (IV.25) [21] . Ce canal peut affecter le signal transmis par atténuation de son amplitude, ajout de bruit et distorsion.

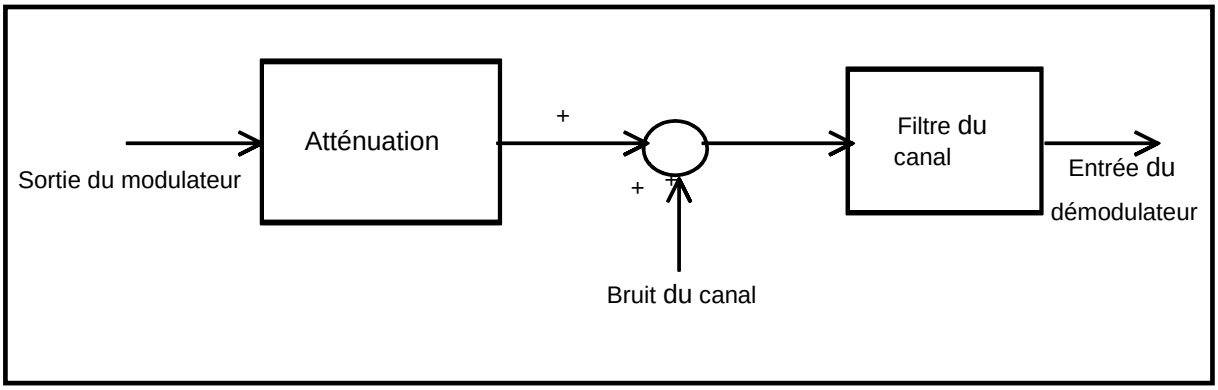



*Figure (IV.26) : Modélisation du canal de transmission*

Ces phénomènes agissent sur la qualité de la synchronisation au niveau de la réception. Avec la supposition que le canal de transmission à une bande passante infinie et que la seule perturbation qui affecte le signal est l'addition d'un bruit blanc. Notre analyse consiste alors à évaluer l'impact de l'amplitude du bruit blanc additionnel sur le taux d'erreur binaire BER de restauration de l'image décrite ci-dessus par le système CSK étudié, après modulation et démodulation. La figure (IV.26) représente la variation du BER en fonction de la densité spectrale de puissance du signal bruit en dB avec un temps symbole de 0.01s.

Ainsi l'erreur à la réception augmente avec la densité spectrale de puissance du bruit du canal jusqu'à des valeurs pratiquement inacceptables . La figure (IV.27) montre l'effet du bruit sur l'image reconstituée

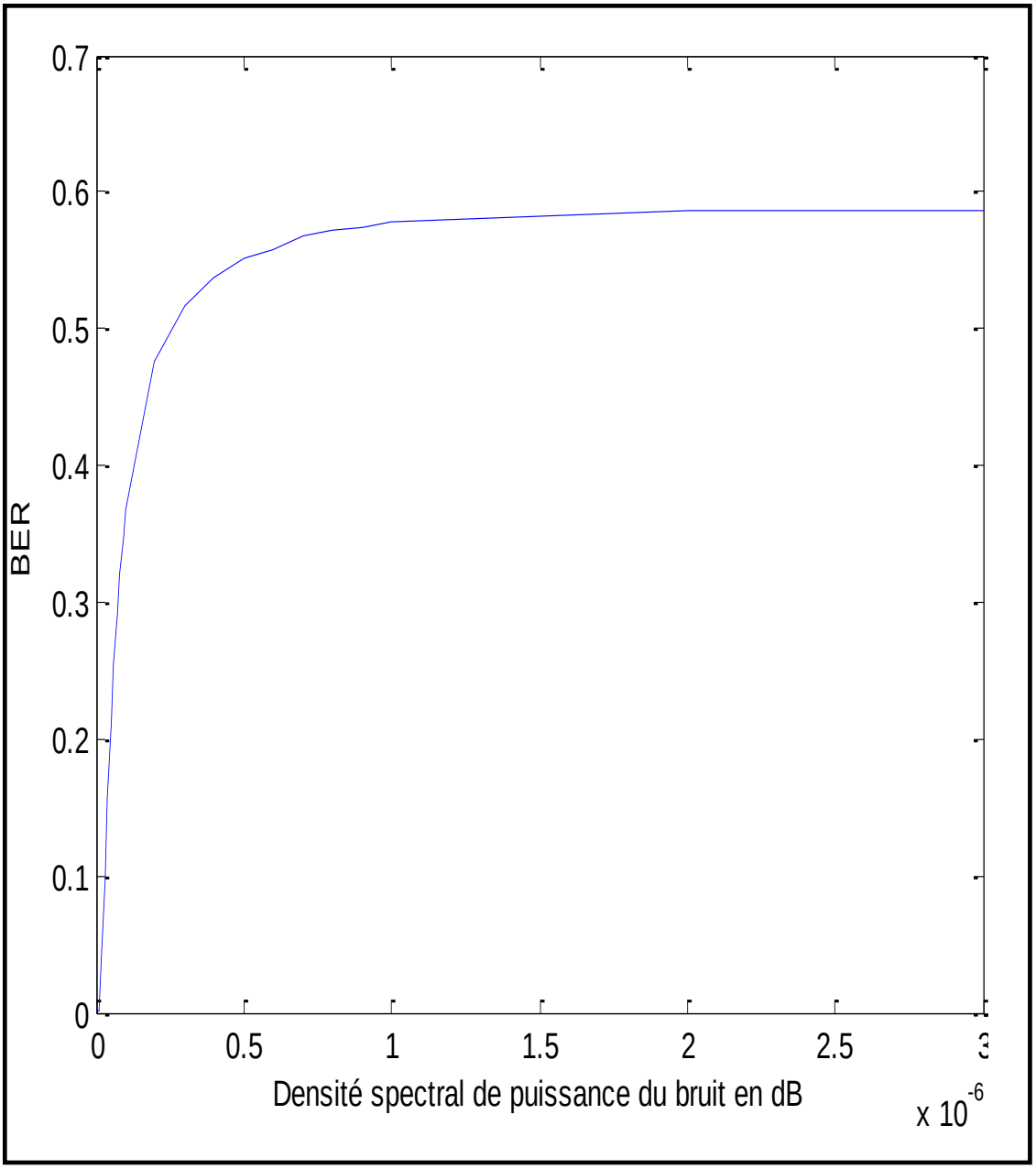



*Figure (IV.27) :L'impact du bruit du canal sur le taux d'erreur de l'image modulée et démodulée*

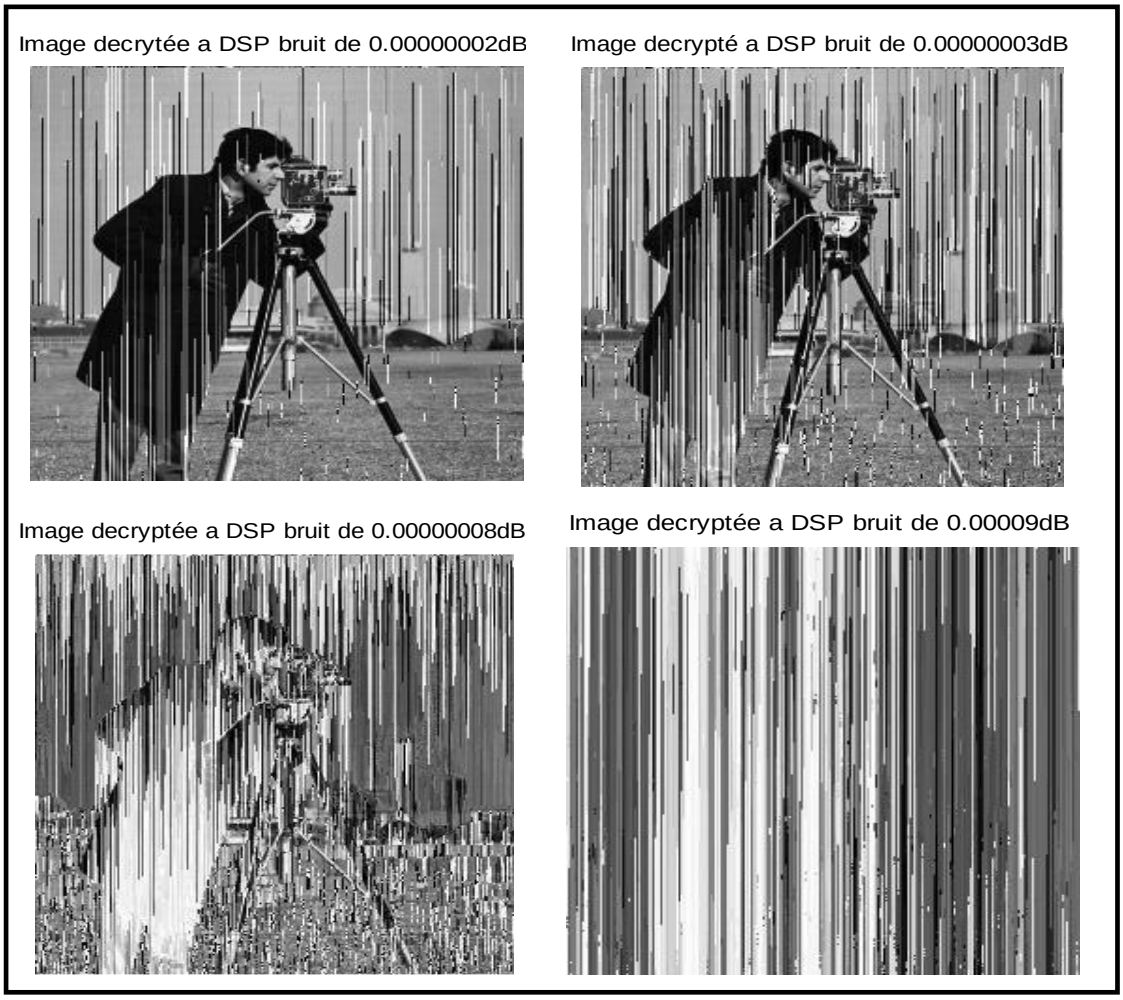



*Figure (IV.28) : Images reconstituées pour différentes valeurs de bruits*

### IV.3.3.4. Effet de la disparité des paramètres

La synchronisation chaotique parfaite entre l'émetteur et le récepteur exige que, les valeurs des paramètres constituants le récepteur soient exactement les mêmes que celles de l'émetteur. Pratiquement il est impossible de réaliser cette condition avec une erreur nulle. Il y'aura toujours un certain décalage entre les valeurs des composants des circuits d'émission et de la réception. Un test de la robustesse du système étudié a été fait par rapport à la variation de la capacité $C_1$ de l'unité de synchronisation $\hat{G}_1$ .Ainsi pour $C_1$ = 17.104 nF le BER est 0.1512 et pour $C_1$ = 17.109 nF le BER est 0.412. La figure (IV.29) illustre la déformation de l'image reconstituée en fonction de la capacité

$C_1$. La conclusion tirée est que le système étudié résiste pour de faibles variations de la capacité $C_1$.

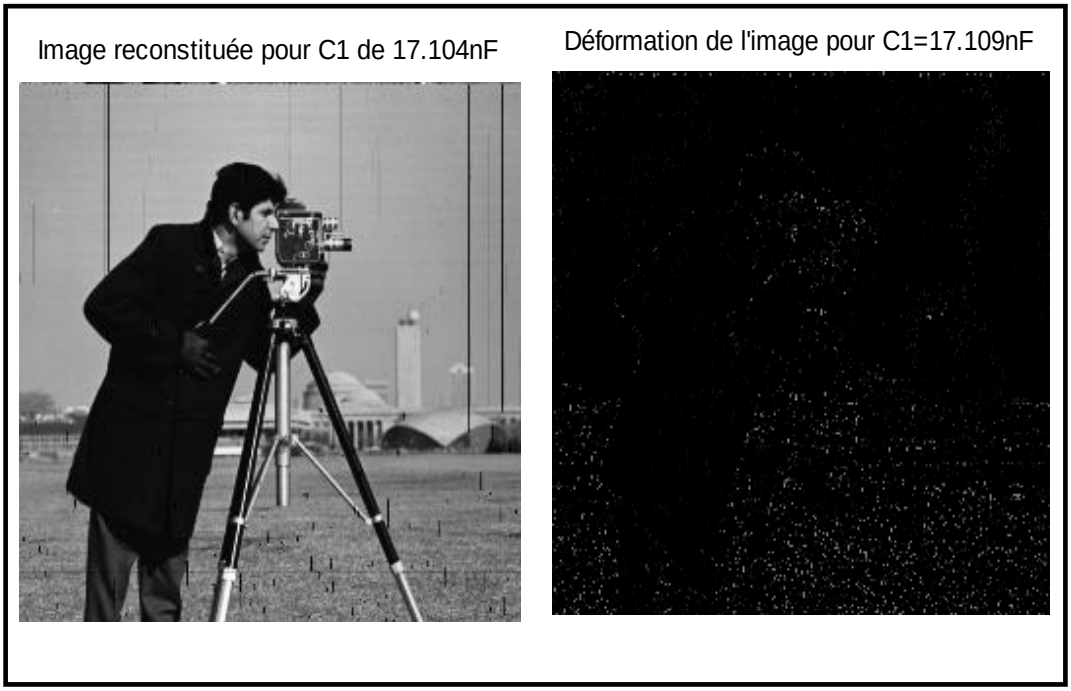



*Figure (IV.29) : Effet de la variation de $C_1$ de $\hat{G}_1$ sur l'image reconstituée*

### IV.3.3.5. Discussion de la sécurité du système

Le degré de sécurité dans le système étudié baisse, si les attracteurs chaotiques correspondant à 0 et 1 sont trop différents, car on peut observer les changements de système chaotique au niveau du signal transmis [6], [42]. Le remède à cet inconvénient est le choix d'attracteurs chaotiques similaires mais statiquement différents. En plus on trouve dans la littérature des articles traitant la possibilité de briser ce type de cryptosystemes .Par exemple la référence [45] utilise des applications de premier retour et une fonction d'auto corrélation pour reconstruire le message. T. Yang et al ont exposé dans [40], une technique de cryptanalyse en utilisant la synchronisation généralisée [6]. Une idée pour remédier relativement à ces contraintes a été proposée par T. Yang et al en 1997, appelée la 3$^{eme}$ génération de cryptage par chaos [42]. Son principe consiste à combiner la technique cryptographique classique avec celle utilisant le chaos. La projection de cette idée sur le système CSK étudié engendre

la figure (IV.30). Ainsi un choix rigoureux de règles de cryptage et de décryptage E(.) et D(.) , de clefs de cryptage et de décryptage et d'attracteurs chaotiques , permet d'augmenter la sécurité du cryptosysteme étudié .

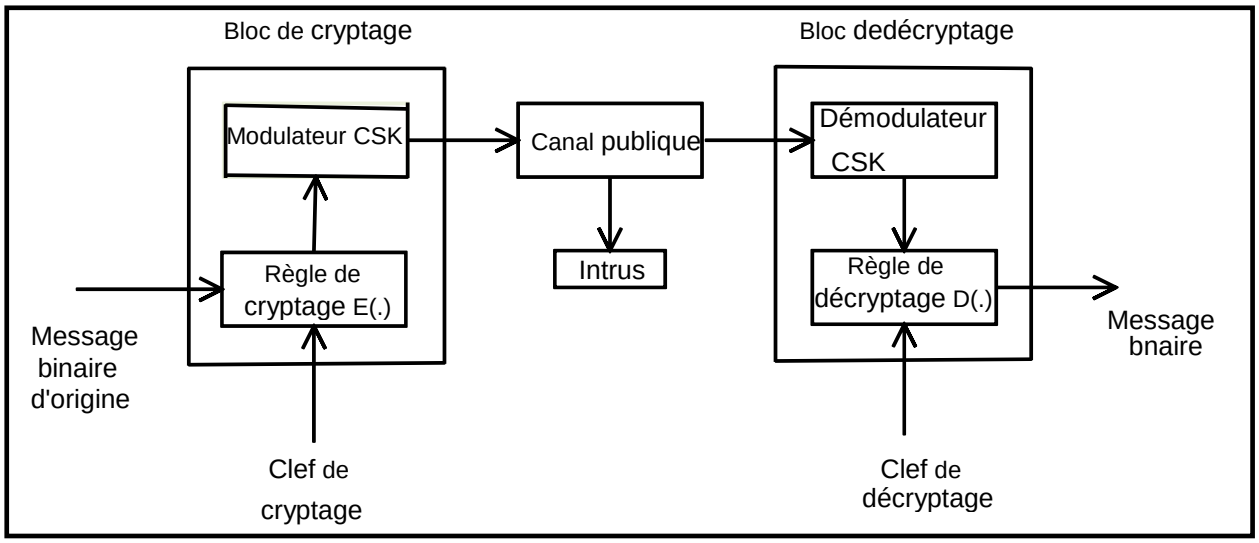



*Figure (IV.30) : Le modèle de sécurisation de données par le mixage de la CSK et la cryptographie classique*

## IV.3. Conclusion

Des exemples de simulations de l'application du chaos pour sécuriser la communication ont été présentés dans ce chapitre. Le choix a été fait sur deux techniques traitant respectivement la sécurisation de messages analogiques et numériques.

Pour simuler le masquage par addition la première technique abordée, la synchronisation des systèmes chaotiques de Rossler vérifiée dans le chapitre III a été utilisée. Les déductions tirées d'après les résultats trouvés sont la sensibilité au bruit du canal et à la disparité des paramètres entre l'émetteur et le récepteur.

Pour la simulation de la technique de cryptage par décalage chaotique CSK, un exemple de modèle illustrant le principe de la CSK basé sur la synchronisation et le calcul d'erreur a été conçu en utilisant l'oscillateur de Chua comme générateur de porteuses chaotiques. Les résultats de test du modèle en utilisant un message généré par

“ Bernouilli Binary Generator“ de simulink ont donné une parfaite similarité entre le signal message d’origine et le signal reconstitué à la réception. Des tests des effets du temps symbole, de l’immunité aux bruits du canal et de la disparité des paramètres, ont été également faits sur le système dans le cas de cryptage et de décryptage d’une image. La conclusion tirée est que sa robustesse est limitée.

# CONCLUSION GENERALE

Nous avons situé tout d'abord les problèmes rencontrés dans les crypto systèmes utilisés actuellement. Une accentuation a été faite sur les limites de sécurité de ces cryptos systèmes. Nous avons remarqué à travers notre recherche bibliographique sur les cryptosystèmes les plus utilisés actuellement tels que le AES, DES et le RAS, que cette sécurité est calculatoire , car elle est fondée sur les calculs algébriques. C'est l'une des raisons qui ont déclenché, la nécessité de chercher d'alternatif, dont l'usage du chaos sujet de notre travail, est l'une des solutions proposées.

A ce niveau notre travail a été débuté par l'exploration du phénomène chaotique en le simulant par ordinateur. Nous avons ainsi vérifié la sensibilité des systèmes chaotiques même aux faibles variations des conditions initiales, dépisté la route vers le chaos d'un système dynamique en traçant son diagramme de bifurcation, identifié le chaos dans un système dynamique par le calcul de ses exposants de Lyapunov et représenté graphiquement le comportement de quelques systèmes chaotiques célèbres dans le domaine temporel et l'espace des phases.

La découverte en 1990 de Pecora et Carroll sur la synchronisation du chaos a été un déclic, pour la possibilité de l'utiliser dans la sécurisation de la communication. D'où vient l'objectif de la deuxième phase de notre travail. Dans des conditions idéales (en négligeant la disparité des paramètres et perturbation d'accouplement entre le système maître et le système esclave) de bons résultats ont été obtenus par le test de la synchronisation du chaos en utilisant trois techniques (l'approche de Pécorra et Carroll, synchronisation généralisée et la synchronisation impulsive). On note que la robustesse de ces techniques vis-à-vis de la disparité des paramètres et les perturbations d'accouplement est limitée.

La troisième est la dernière phase de notre travail consiste dans l'étude de l'usage du chaos pour sécuriser les données. Deux techniques ont été simulées et analysées :

- Le masquage par addition est la première méthode étudiée .Les résultats obtenus dans cette méthode montrent une mauvaise reconstitution du signal message à la réception même avec des conditions idéales de fonctionnement.
- Le masquage par décalage chaotique est la deuxième méthode étudiée. On note dans cette méthode, une similarité parfaite entre le signal message d'origine et

le signal reconstitué au niveau de la réception dans un fonctionnement idéal. En revanche , cette similarité diminue avec un temps symbole inférieur au temps de synchronisation, la disparité des paramètres et l'augmentation du bruit du canal. Concernant la sécurité de cette technique, elle peut être augmentée par mixage avec les techniques de cryptographie classiques.

Plusieurs perspectives peuvent être envisagées à la suite de ce travail ,à savoir :

- Etude et estimation de toutes les techniques de synchronisation du chaos et la poursuite de la recherche dans ce domaine.
- Etude et estimation de toutes les techniques de cryptage par chaos et la poursuite de la recherche dans ce domaine.
- Usage du chaos pour sécuriser la transmission par ondes radios.

# BIBLIOGRAPHIE


[1 ] H. D. I. Abarbanel, N.F. Rulkov, et Mikhail M. Sushchik "*Generalized synchronization of chaos: The auxiliary system approach* "*Physical review E* ,vol. 53 ,pp.4528-4535, 1995 .

[2 ] G. Alvarez, L. Hernández, J. Muñoz, F. Montoya et S. Li. "*Security analysis of communication system based on the synchronization of different order chaotic systems*" *Physics Letters A*, vol. 345, pp. 245–250, 2005 .

[3 ] F. Arnault .*Théorie des nombres et cryptographie* . Cours de DEA, Université de Limoges, France, 2005 .

[4 ] X. Bavard. *Numérisation du chaos et applications aux systèmes de communication sécurisés par chaos en longueur d'onde*. Thèse de doctorat, Université de Franche -Comté, 2004 .

[5 ] S. Boccaletti ,J. Kurths, G. Osipovd et D.L. Valladares, C.S. Zhou " *The synchronization of chaotic systems*" *Physics Reports*,vol. 366, pp.1–101,2002 .

[6 ] E. Cherrier . *Estimation de l'état et des entrées inconnues pour une classe de systèmes non linéaires* .Thèse de doctorat , institut national polytechnique de Lorraine , 2006 .

[7 ] K.M. Cuomo, A.V. Oppenheim et S.H. Isabelle " *Spread spectrum modulation and Signal masking using synchronized chaotic systems*" *MIT Tech .Rep* ,vol . 570. , 1992 .

[8 ] K.M. Cuomo, A.V. Oppenheim et S.H. Strogatz. "*Synchronization of Lorenz-based chaotic circuits with applications to communications*" *IEEE Transactions on Circuits and Systems II*, vol. 40, pp. 626–633, 1993 .

[9 ] H. Dedieu, M.P. Kennedy et M. Hasler. "*Chaos shift keying: modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits* " *IEEE Transactions on Circuits and Systems I*, vol. 40, pp .634–642, 1993 .

[10 ] R. Dumont .*Introduction a la cryptographie et a la sécurité informatique*. Note de cours, université de Liége, 2006-2007 .

[11 ] H. Fujisaka et T. Yamada "*Stability theory of synchronized motion in coupled oscillator systems*" *Prog. Theor. Phys*, vol. 69, pp 32–47, 1983 .

[12 ] C. Giraud. *Attaques de crypto systèmes embarqués et contre-mesures associées*. Thèse de doctorat en informatique , université de Versailles Saint-Quentin , France , 2007 .

[13 ] J. Gleick . *La théorie du chaos – vers une nouvelle science*. Albin Michel, Paris, 1989 .

[14 ] V.Guglielmi , P-Y .Besnard , D.Fournier-Prunaret, P.Pinel, AK.Taha et L.Beneteau "*Un système numérique de cryptographie basé sur les propriétés des signaux chaotiques discrets* " *GRETSI' 03 : 19° Colloque sur le traitement du signal et des images*, France, 2003 .

[15 ] A .Huang "*A study of the chaotic phenomena in Chua's circuit* " , *proceedings of 1988 IEEE International Symposium on Circuits and Systems* vol.1, pp.273-276. 1988 .

[16 ] G. Kaddoum .*Contributions à l'amélioration des systèmes de communication Multi- Utilisateurs par chaos : synchronisation et analyse des performances*. Thèse de doctorat en électronique, université de Toulouse, 2008 .

[17 ] M.P. Kennedy, "*Robust op amp implementation of Chua's Circuit* " *Frequenz* Vol.46, pp.66-80, 1992 .

[18 ] A. Kerckhoffs "*La cryptographie militaire* "*Journal des sciences militaires*, vol.9, pp .2-38 .161-191, 1883 .

[19 ] L. Kocarev, K. S. Halle, et A. Shang, "*Transmission of digital signals by chaotic synchronization*" *International Journal of Bifurcation and Chaos*, vol. 2, pp. 973-977, 1992 .

[20 ] L. Kocarev et U. Parlitz, " *Generalized synchronization in chaotic systems* "*Chaotic circuits for communication . Proceedings of the Meeting . Philadelphia .PA* , vol.2612, pp.57-61 ,1995 .

[21 ] G. Kolumbán, M. P. Kennedy et 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*, vol. 44, pp .927–936, 1997 .

[22 ] G. Kolumbán, M. P. Kennedy et 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*, vol. 45, pp. 1129–1140, 1998 .

[23 ] G. Kolumbán, M. P. Kennedy & L. O. Chua. "*The role of synchronization in digital communications using chaos - part III Performance Bounds for Correlation Receivers* "*IEEE Transactions on Circuits and Systems I: Fundamental theory and application*, vol. 47, pp.1673-1683 , 2000 .

[24 ] Chris LeBailly " *Synchronization of chaotic oscillators* " *Evanston Township High School* , USA, 2003 .

[25 ] M. B. Luca . *Apports du chaos et des estimateurs d'états pour la transmission sécurisée de l'information* . Thèse de doctorat en electronique ,université de Bretagne Occidentale, 2006 .

[26 ] R.N. Madan "*observing and learning chaotic phenomena from Chua's circuit* " *Proceedings of the 35th Midwest Symposium on Circuits and Systems IEEE,* vol.1, pp.736-745. 1992 .

[27 ] P.Manneville .*Instabilité, chaos et turbulence* .Ecole polytechnique, Paris ,2004 .

[28 ] T. Matsumoto "*A chaotic attractor from Chua's circuit*" *IEEE Trans. Circuits Syst*, vol .31, pp .1055-1058, 1984 .

[29 ] E. Ott . *Chaos in dynamical systems* . Cambridge University press , seconde edition, university of Maryland , 2002 .

[30 ] L.M. Pecora et T.L. Carroll. "*Synchronization in chaotic systems*" *Physical Review Letters*,vol. 64, no. 8, pages 821–824, 1990 .

[31 ] A. Pikovsky, M. Rosenblum, J. Kurths .*Synchronization: A universal concept in nonlinear Sciences*. Cambridge University Press, England, 2003 .

[32 ] P.Robert et A.Rey .*Le grand Robert de la langue française : dictionnaire alphabétique analogique de la langue française* .Seconde édition , Paris ,2001.

[33 ] J.M.M. Rodrigues. *Transfert sécurisé d'images par combinaison de techniques de compression, cryptage et marquage*. Thèse de doctorat en informatique, université Montpellier II, France ,2006 .

[34 ] N.F. Rulkov, M.M.Sushchik, L.S.Tsimring et H.D.I. Abarbanel "*Generalized synchronization of chaos in directionally coupled chaotic systems* " *Physical Review E*, vol. 51, pp 980–994, 1995 .

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

[36 ] K.M. Short. "*Steps towards unmasking secure communications* " *International Journal of Bifurcation and Chaos*, vol. 4, pp. 959–977, 1994.

[37 ] J.P. Tual " *Cryptographie* " *Techniques de l'Ingénieur,* H2 248, 1996 .

[38 ] A. Wolf, J. B. Swift, H. L. Swinney, et J. A. Vastano. "*Determining lyapunov exponents from a time series*" *Physica D*, vol .16 ,pp .285–317, 1985 .

[39 ] X. Wu , J. Lu , C. K. Tse , J. Wang et J. Liu "*Impulsive control and synchronization of the Lorenz systems family* "*Chaos, Solitons and Fractals* , vol .31 ,pp .631–638 , 2007 .

[40 ] T. Yang, L.-B. Yang et C.-M. Yang. "*Cryptanalyzing chaotic secure communications using return maps*" *Physics Letters A*, vol. 245, pp. 495–510, 1998 .

[41 ] T. Yang et L.O. Chua " *Generalized synchronization of chaos via linear transformations* " *International Journal of Bifurcation and Chaos*, vol. 9, pp .215-219 ,1999 .

[42 ] T. Yang. "*A survey of chaotic secure communication systems*" *Int. J. of Comput. Cognition*, vol. 11, pp 81–130, 2004 .

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

[44 ] G. Q. Zhong et F. Ayrom, "*Experimental confirmation of chaos from Chua's circuit* ", *Int. J. Circuit Theory Appl*, Vol. 13, pp. 93-98, 1985 .

[45 ] C.S. Zhou et T.L. Chen. "*Extracting information masked by chaos and contaminated with noise: some considerations on the security of communication approaches using chaos* "*Physics Letters A*, vol. 234, pp. 429–435, 1997.

[46 ] Z. L. Zhu, S. Li et H. Yu " *A new approach to generalized chaos synchronization based on the stability of the error System* " *Kybernetika*, Vol. 44. No. 4, pp .492–500, 2008 .

.