الجمهورية الديمقراطية الشعبية الجزائرية
وزارة التعليم العالي والبحث العلمي

People's Democratic Republic of Algeria
Ministry of Higher Education and Scientific Research
University of Jijel Mohamed Seddik BenYahia

Faculté des Sciences et Technologies
Département d'Electronique

Mémoire de fin d'étude pour l'obtention du diplôme de
Master en Electronique
Spécialité : Electroniques des Systèmes Embarqués

Présenté par :
Mlle. BENAYACHE Hadjer
Mlle. ROUIKHA Oumayma

Thème

Compression de l'information à l'aide de systèmes chaotiques

Encadré par :
Dr. YAHIA Moussa

Année universitaire : 2019-2020

Remerciement

Grace à la volonté d'Allah le tout puissant et bienveillant que ce travail s'est accompli.

Nos remerciements le plus sincères vont à Monsieur M.YAHIA pour ses conseils précieux et son suivi qu'il nous a prodigués durant tout notre travail.

Nos vifs remerciements vont aux membres de jury d'avoir accepté l'évaluation notre présent travail.

En fin toute personne qui a participé de près ou de loin à l'accomplissement de ce mémoire soit sincèrement remerciée

Dédicace

Je dédie ce travail À :

Ma mère, qui a œuvré pour ma réussite, de par son amour, son soutien, tous les sacrifices consentis et ses précieux conseils, pour toute son assistance et sa présence dans ma vie.

Mon père, qui peut être fier et trouver ici le résultat de longues années de sacrifices et de privations pour m'aider à avancer dans la vie.

Puisse Dieu, le tout puissant, vous préserver et vous accorder santé, longue vie et bonheur.

Mon chère frère Oussama.

Mes chères sœurs : Dr.Kenza, Besma, Oumaima et Anfel.

À ma copine Lyna pour ses conseils et son encouragement, Je t'aime ma puce.

À chaque cousins et cousines

Toute la famille Benayache

Toutes mes chères amies.

À tous ceux qui ont une place dans mon cœur, et tous ceux qui m'ont aidé
de près ou de loin. Et tous ceux que j'ai omis de citer.

Hadjer

Dédicace

Ce travail est dédié

A ma chère mère et mon cher père

A mes sœurs : Roqiya et Boutheyna
Et mes frères : Zakaria ; Lokman ; et Yahya

A tous mes proches de la famille tout à son nom

A tous ceux que j'aime et ceux qui m'aiment
Merci

ROUIKHA Oumayma

Sommaire

Table des figures

Chapitre I : Généralité sur les systèmes dynamique chaotique

Chapitre II : Transmission sécurisée à base du chaos

Chapitre III : compression de l'information à l'aide de systèmes chaotiques

Table des tableaux

Nomenclature

$\dot{\boldsymbol{x}} = \frac{\boldsymbol{dx}}{\boldsymbol{dt}}$ **:**	Dérivée de la variable x par rapport au temps
$\mathbb{R}^+$ **:**	Ensembles des nombres réels positifs
$\mathbb{Z}^+$ **:**	Ensembles des nombres entiers positifs
CI :	Conditions initiales
CSK :	Chaos Shift Keying
$\cup$ **:**	Opération ‘réunion d’ensemble’
$\cap$ **:**	Opération ‘intersection d’ensemble’
$\boldsymbol{x_0}$ **:**	L’état initial
$\boldsymbol{x_k}$ **:**	L’état x au temps t=k
$\boldsymbol{f^{-1}}(.)$ **:**	Inverse de la fonction $f(.)$
$\boldsymbol{b_k}$ **:**	Variable associée aux symboles informationnels à l’ instant k
$\boldsymbol{H}$ **:**	Entropie d’un alphabet source
$\boldsymbol{S}$ **:**	Alphabet des symboles disponibles $S_{\{n\}}$
$\boldsymbol{P_n}$ **:**	Probabilité d’apparition du symbole $S_{\{n\}}$
$\boldsymbol{card}\{.\}$ **:**	Cardinal d’un symbole

Introduction générale

D'un point de vue historique, la théorie des systèmes dynamiques est née avec les travaux de Poincaré autour des années 1881-1890, notamment avec les deux grandes mémoires (sur les courbes définies par des équations différentielles, sur le problème des trois corps et les équations de la dynamique) et prolongée par quelques mathématiciens et physiciens théoriciens autour des années 1930[1].

Par la suite, dans les années 1920, avec les travaux de Birkhoff et d'autres, s'est dégagée la notion de système dynamique abstrait, de flot, d'ensemble limites [1].

Depuis 1920 jusqu' à présent les systèmes dynamiques (surtout les systèmes dynamiques en temps discret ou bien les systèmes donnés par des suites récurrentes) jouent un rôle très important puisque il y a des applications dans beaucoup de disciplines scientifiques par exemple : La physique (mécanique céleste, météo), la biologie (dynamique de population), la chimie (cinétique chimique) , l'électronique (les circuits électroniques) , l'informatique (traitement de l'images) , cryptographie (chiffrement des messages, images) , l'économie,…, etc. [1]

Depuis quelques années, la théorie des systèmes chaotiques a été appliquée dans le domaine des communications. La synchronisation des systèmes chaotiques semble impossible dans un premier temps, notamment à cause de la sensibilité de ces systèmes aux conditions initiales. De plus, un système chaotique n'est pas asymptotiquement stable, c'est-à-dire que les trajectoires issues des conditions initiales voisines (légèrement différentes) divergent exponentiellement avec le temps. En effet, on peut dire que pour les systèmes réels, il n'est pas facile de produire et de reproduire les mêmes conditions de démarrage. D'après ce point de vue, tout changement de paramètre dans un système chaotique pourrait conduire à une divergence entre ces trajectoires. Pourtant ce raisonnement n'est pas correct. Il peut exister des conditions sous lesquelles les trajectoires de deux systèmes chaotiques différents peuvent convergé l'une vers l'autre, si certaines informations (énergie) pertinentes sont échangées [2].

La transmission chaotique est un mode de communication à clé secrète. La connaissance de cette clé est nécessaire du côté de l'émetteur du message ainsi que du récepteur pour le chiffrement et le déchiffrement du message. On doit alors disposer au niveau du récepteur, d'un signal chaotique identique à la porteuse pour pouvoir récupérer le message masqué [3].

L'emploi du chaos pour la transmission sécurisée de l'information a été considéré dans les dernières années comme une solution très prometteuse pour augmenter les performances des systèmes de transmission actuels. Ainsi on trouve dans la littérature une multitude d'applications et d'études réalisés concernant plusieurs aspects de la transmission. Grâce à ses caractéristiques quasi-stochastiques le chaos offre une solution possible pour les systèmes à probabilités réduites de détection et d'interception ainsi que des applications dans l'accès multiple [4].

Dans ce contexte, notre travail vise à présenter une méthode de compression de l'information à l'aide du chaos.

Notre étude se focalise sur l'usage du chaos pour transmettre de l'information. Pour cela notre mémoire de fin de cycle s'articulera sur trois chapitres :

- ✓ Le premier chapitre aborde une étude sur les systèmes dynamiques en général et chaotique en particulier. Ainsi quelques définitions et concepts sur le chaos seront présentés.
- ✓ Le deuxième chapitre, présente les principales méthodes de transmissions sécurisées à base du chaos, qu'elle soit analogique ou numérique.
- ✓ Dans le troisième chapitre on va introduire un générateur particulier dénommé générateur probabiliste de Bernoulli, ainsi on va démontrer l'existence d'une relation entre ce générateur particulier et l'alphabet des symboles (séquence informationnelle). Malgré la similarité des performances de compression, une nouvelle application du chaos sera présentée.

Chapitre I

Généralités sur les systèmes dynamiques chaotiques

I.1 Introduction

Les systèmes dynamiques chaotiques sont inclus dans des applications effectives depuis la dernière décade malgré qu'elles soient connues depuis longtemps dans le domaine mathématique.

Dans ce chapitre nous nous intéressons aux systèmes dynamiques chaotiques, il est compté faire à introduire quelques outils de base associes au chaos.

Ce chapitre est structuré comme suit. Premièrement on commence par une présentation des différents aspects des systèmes dynamiques, continuons par l'exposition des différentes définitions et propriétés des systèmes chaotiques.

I.2 Systèmes dynamiques

I.2.1 Définition du système dynamique

On définit un système dynamique comme un système physique qu'il peut évoluer dans le temps. Les systèmes dynamiques se divisent en deux types : continu et discret.

I.2.2 Systèmes dynamiques à temps continu

Un système à temps continu est représenté par un système d'équations différentielles :

$$\frac{dx}{dt} = \dot{x}(t) = f(x(t), t) \qquad \textbf{(1.1)}$$

Dans lequel $f : \mathbb{R}^n \times \mathbb{R}^+ \to \mathbb{R}^+$ designe la dynamique du système continu.
On peut identifier une solution unique du système définie à l'aide de l'équation (1.1) si on associe à cette dynamique pour chaque couple choisie (x_0, t_0) un état initial: $x_0 = x(t_0)$.

La solution unique qui fournit l'ensemble d'états successifs servie par le système à chaque instant t s'appelle généralement trajectoire.

Parmi les systèmes dynamiques chaotiques les plus connus on prend le célèbre système de Lorenz comme exemple, il est donné par les équations suivantes [5] :

$$\begin{cases} \dot{X} = -\sigma X + \sigma Y \\ \dot{Y} = -XZ + \gamma X - Y \\ \dot{Z} = XY - bZ \end{cases} \qquad \textbf{(1.2)}$$

Oú X, Y et Z sont les variables d'états du système, σ , γ et b sont les paramètres réels. Les paramètres et la condition initiale ont été choisis comme suit: $\sigma = 10;\ \gamma = 28; b = 2.5$ avec $(X_0, Y_0, Z_0) = (2{,}5{,}20)$.

On peut dire par observation que la dynamique du système de Lorenz exprimée par l'équation (1.2) est indépendante de l'instant t considéré, et généralement ce type de système est compétent d'autonome.

La trajectoire particulière du système de Lorenz est illustrée dans la figure suivante:

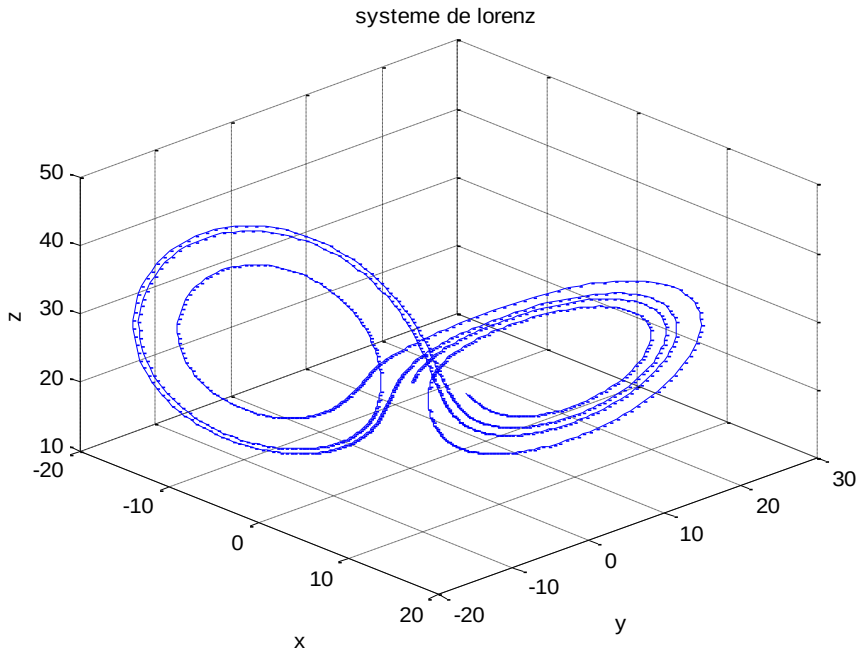

Figure 1.1: Exemple de trajectoire pour le système de Lorenz

I.2.3 Systèmes dynamiques à temps discret

Comme le système à temps continu est représenté par des équations différentielles, le système à temps discret est décrit par un système d'équations aux différences finies:

$$\boldsymbol{x(k+1) = g(x(k), k)} \qquad \textbf{(1.3)}$$

Où g: $\mathbb{R}^n \times\ \mathbb{Z}^+ \rightarrow \mathbb{R}^n$ indique la dynamique du système en temps discret.

De la même manière qu'en temps continu, si on associe un état initial a cette dynamique nous pouvons identifier une solution unique.

I.2.4 Systèmes autonome et non autonome

Un système dynamique est dit autonome quand sa dynamique ne dépend pas absolument du temps, et dit non autonome dans le cas contraire [6].

I.2.5 Comportements d'un système dynamique

La trajectoire d'un système dynamique accès à une région limitée de l'espace des phases, à partir d'un état initial x_0 et après un régime transitoire.

L'une des plus importantes caractéristiques à étudier pour tout système dynamique est ce comportement asymptotique obtenu pour $t, k \to \infty$. Dans un système linéaire la solution asymptotique est unique et indépendante de la condition initiale, mais il existe une plus grande variété de régimes permanents en présence de non linéarité.

Parmi ces variétés on trouve, respectivement et par ordre de complexité : point d'équilibre, solution périodiques, solution quasi-périodiques et chaos. C'est une obligation de préciser que le comportement développé par un système dynamique particulier cette fois est fortement dépendant de la condition initiale choisie [7].

On prend l'équation logistique définie par l'équation (1.4) comme exemple pour illustrer le comportement précèdent :

$$\boldsymbol{x_{k+1} = r(1 - x_k)x_k} \qquad \textbf{(1.4)}$$

Le mécanisme de construction d'une séquence est tout d'abord montré sous la forme d'un diagramme en toile (web diagram [4] figure (1.2)). Cette méthode permet de générer la séquence choisie, en utilisant la projection des états successifs par rapport à la diagonale principale.

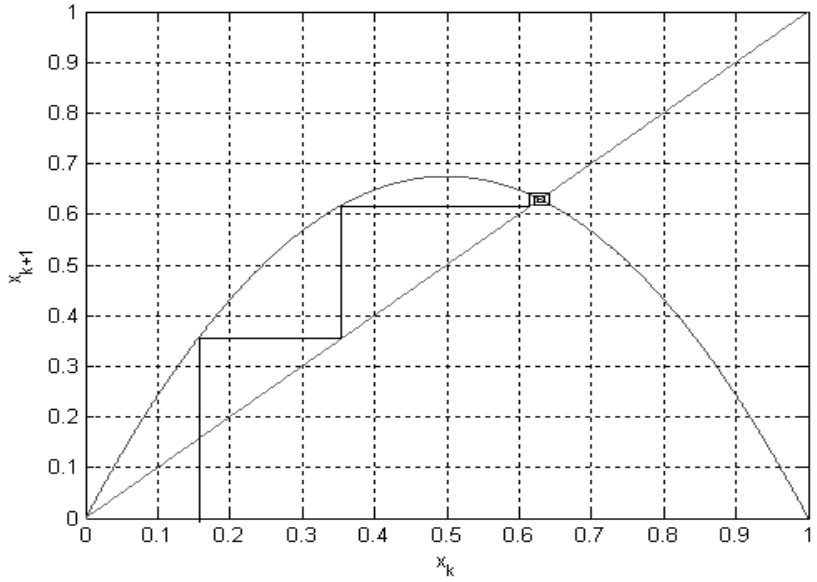

Figure 1.2: Diagramme d'évolution pour la fonction logistique, r=2.7 [7]

Des comportements très différents se présentes suivants les valeurs de r et de la condition initiale x_0 de la suite x_k. L'étude de l'évolution de la dynamique du système vers un comportement chaotique consiste à analyser le changement de la valeur du paramètre r ou

paramètre de bifurcation figure (1.3). Cette présentation s'appelé diagramme de bifurcation car le comportement asymptotique subit une bifurcation de l'ensemble d'états pour des valeurs du paramètres de r bien déterminée. La bifurcation se manifeste comme multiplication des trajectoires possibles dans le cas continu [4].

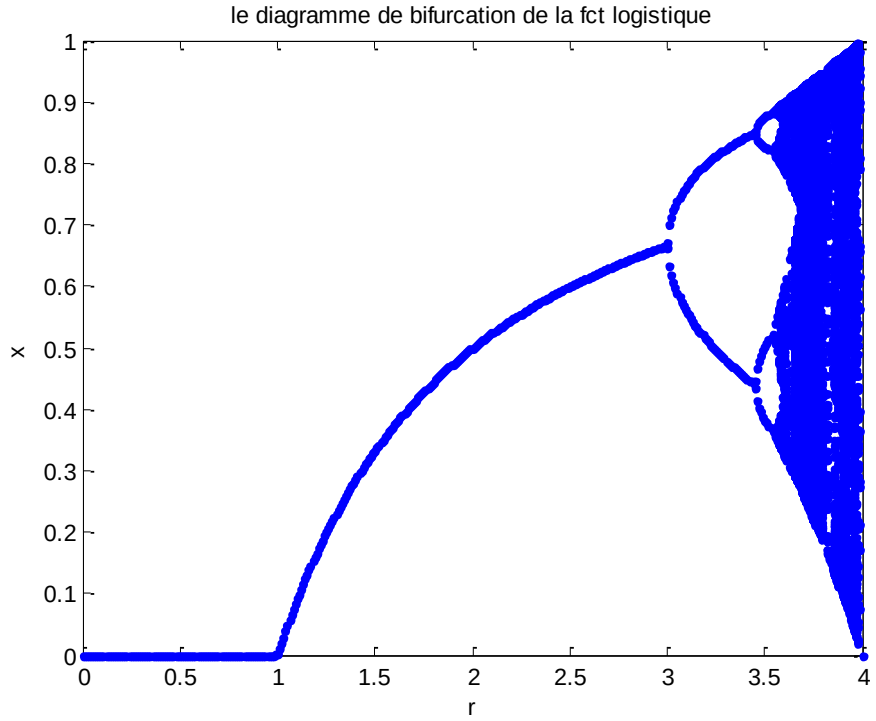

Figure 01.3: Diagramme de bifurcation pour la fonction logistique

Pour chaque type de régime permanent on a:

- ***Points d'équilibres***: dans ce cas, on représente la solution asymptotique par un point, sa valeur étant déterminée selon la condition initiale choisie. Ainsi, on peut identifier plusieurs points d'équilibre pour des conditions initiales différentes. De même, ces points peuvent être stables ou instables suivant que les trajectoires voisines convergent ou divergent entre-elles. Dans le cas de la dynamique logistique, on observe que pour toute valeur $r \in [1,3]$ un point limite stable façonne le régime permanent, la valeur de cet point est sa dépend du choix de paramètre r. la figure (1.4) nous présente une vue générale d'une telle trajectoire pour r =2. Donc,

par observation on peut dire que la séquence se stabilise après une période de transition autour du point fixe qui cette fois est: $x_\infty = 0{,}5$

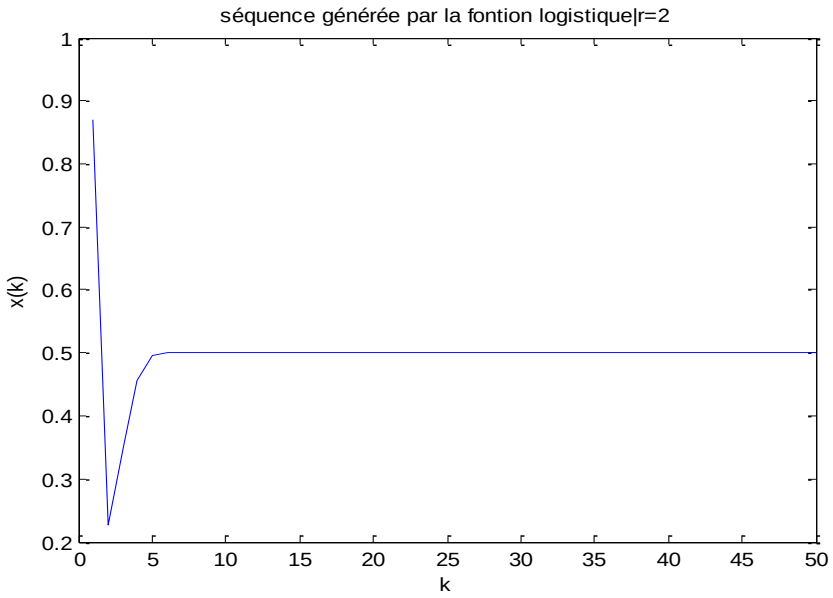

Figure 1.4 *:* Séquence générée et états limites pour $r = 2$

- ***Régime périodique:*** Le régime asymptotique permanent périodique correspond à une trajectoire dont les répliques d'une portion élémentaire sont espacées à des intervalles $nT \in \mathbb{N}^+$, T désignant la période. Pour la fonction logistique par exemple le choix de $r = 3.2$ nous garantit que l'ensemble des états limites est formé par deux points, et la période correspond à deux échantillons (figure 1.5).

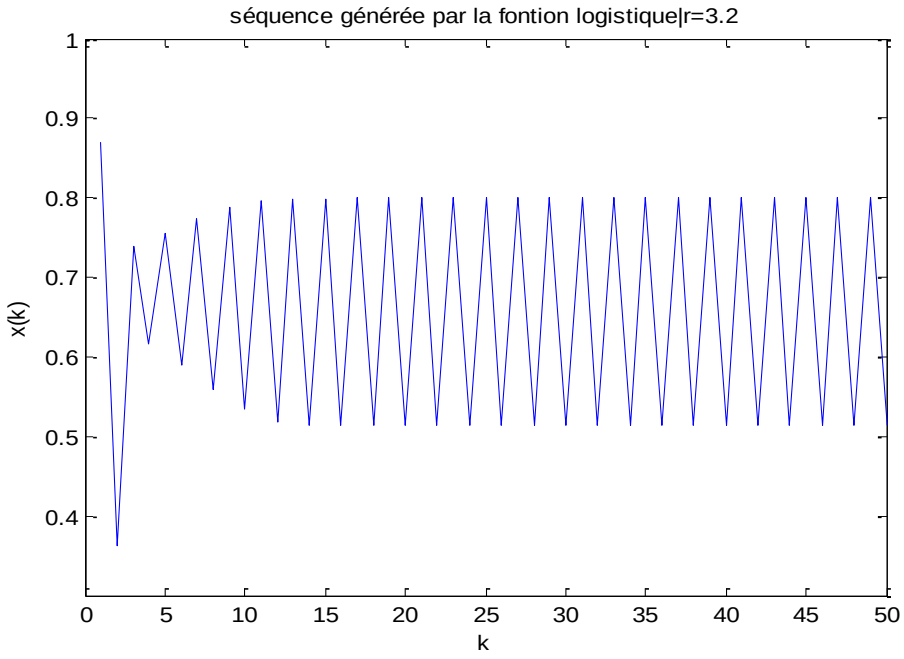

Figure 1.5 : Séquence générée et états limites pour $r = 3.2$

- ***Régime quasi-périodique:*** correspond à une somme de solutions périodiques dont le rapport des périodes est un nombre irrationnel. Un régime quasi-périodique peut être représenté dans l'espace d'état par un tort.
- ***Régime chaotique:*** Tout régime permanent qui n'appartient à aucune des classes présentées précédemment est un régime chaotique. La présentation d'une telle solution est par une trajectoire asymptotique bornée avec une extrême sensibilité aux conditions initiales. Ainsi deux trajectoires générées à partir de CI (conditions initiales) très proches, vont diverger très vite l'une par rapport à l'autre. Le comportement en apparence stochastique des générateurs chaotiques est traduit par cette sensibilité aux conditions initiales, de telle sorte d'une prévision à long terme du comportement de système est impossible. L'exemple donnée dans la figure (1.6) est pour deux CI espacées par une valeur de 10^{-4}, on observe que juste après quelques itérations les deux trajectoires divergent et deviennent non-corrélées.

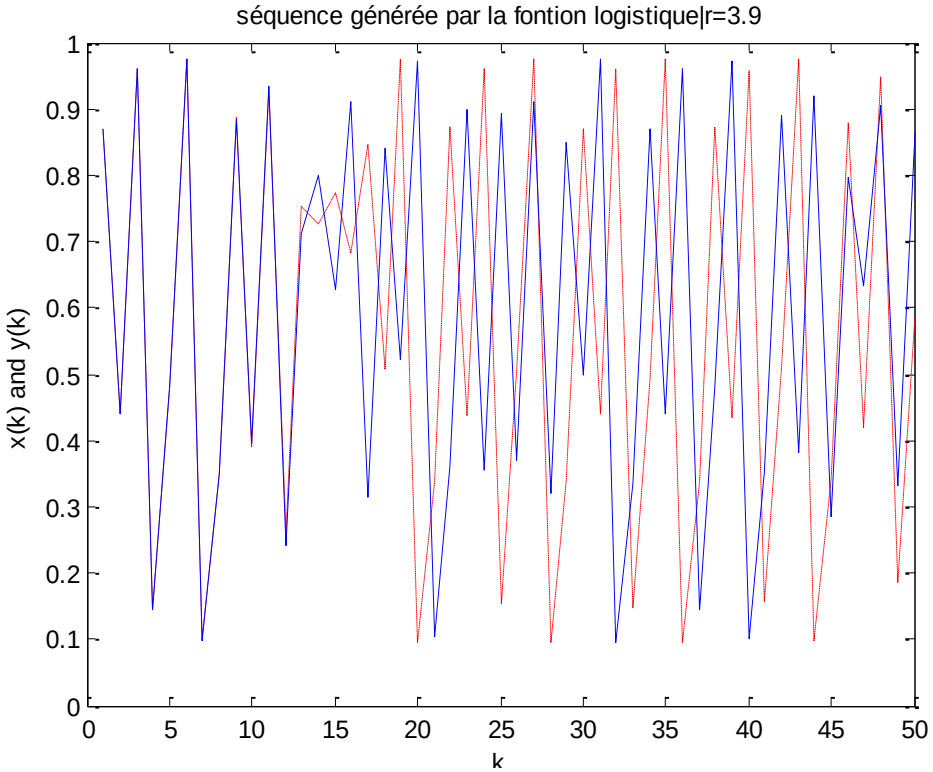

Figure 1.6 : Séquences générées et sensibilité aux CI pour $r = 3.9$.

Généralement, l'ensemble des solutions asymptotiques stables décrites ci-dessus est qualifié d'attracteur; il représente la région de l'espace d'état au voisinage de laquelle les trajectoires restent confinées lorsque, $t, k \to \infty$ .En parallèle avec la définition de l'attracteur apparait la notion de bassin d'attraction qui est défini comme la région de l'espace d'état formée par l'ensemble des CI à partir desquelles l'attracteur sera atteint.

I.3 Chaos?

I.3.1 Définition du chaos

Il existe plusieurs définitions du chaos, parmi lesquelles on mentionne les suivantes:

- Un mouvement irrégulier d'un système dynamique qui est déterministe, sensible aux conditions initiales, et impossible de prédire à long terme avec rien moins qu'une représentation infinitive et parfaite des valeurs analogiques.
- Le chaos est une évolution à long terme se tenue et désordonnée qui satisfait certains critères mathématiquement spéciaux et qui se produit dans un système déterministe non linéaire.
- La propriété qui caractérise un système dynamique dont la plupart des orbites présentent dépendance sensible [8].

I.3.2 Système dynamique chaotique

Un système dynamique chaotique est un système qui dépend de plusieurs paramètres et caractérisés par une extrême sensibilité aux conditions initiales, ils ne sont pas déterminés ou modélisés par un système d'équation linéaire ni par les lois de la mécanique classique, ils ne sont pas nécessairement aléatoire, relevant du seul calcul des probabilités.

I.3.3 Caractéristiques des systèmes chaotiques

Les définitions et les propriétés suivantes nous servent une meilleure compréhension des systèmes chaotiques [9]:

I.3.3.1 La non-linéarité

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

I.3.3.2 Le déterminisme

La capacité de «prédire» le futur d'un phénomène à partir d'un évènement passe ou présent est la signification de la notion de déterminisme. La non-linéarité entraine l'évolution irrégulière du comportement d'un système chaotique. Donc un système déterministe est un système dont l'état présent est complètement déterminé par les conditions initiales. Ainsi le système chaotique a des règles fondamentales déterministes et non probabilistes.

I.3.3.3 Aspect aléatoire

Tous les états d'un système chaotique présentent des aspects aléatoires. La figure (1.7) illustre l'état chaotique x_1 du système de Rössler:

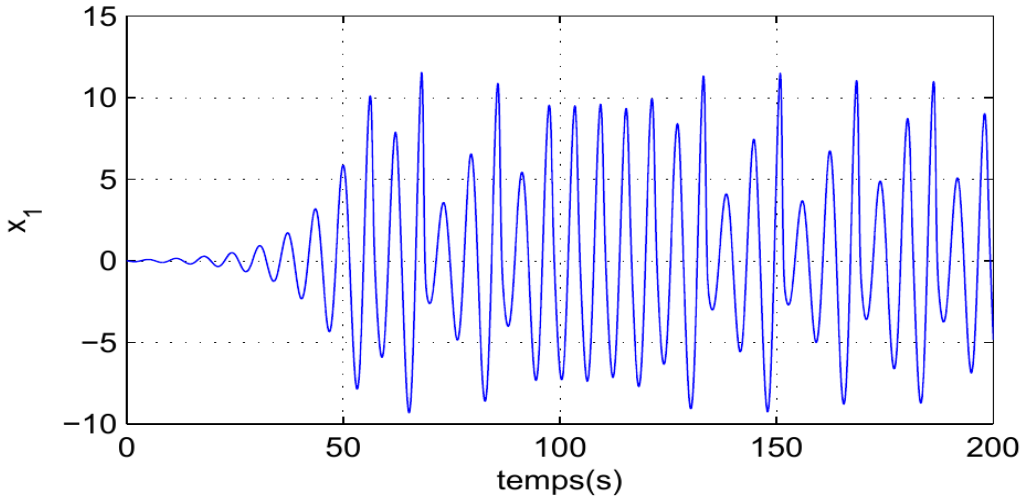

Figure 1.7 : Etat chaotique x_1 du système de Rössler [9]

I.3.3.4 Sensibilité aux conditions initiales

La sensibilite aux conditions initiales signifie que chaque point dans un système chaotique est arbitrairement prés approchée par l'autre point avec sensiblement voie d'avenir, ou trajectoire. Ainsi que la moindre erreur ou petit changement sur les conditions initiales conduit a une mauvaise decision sur la trajectoire effectivement suivie a tout temp, en consequence il est impossible de faire predire sur l'evolution a long terme du système.

La sensibilite aux conditions initiales est donc l'une des propriétés essentielles du chaos. On peut la caractérise par le mesure des taux de divergences des trajectoires.

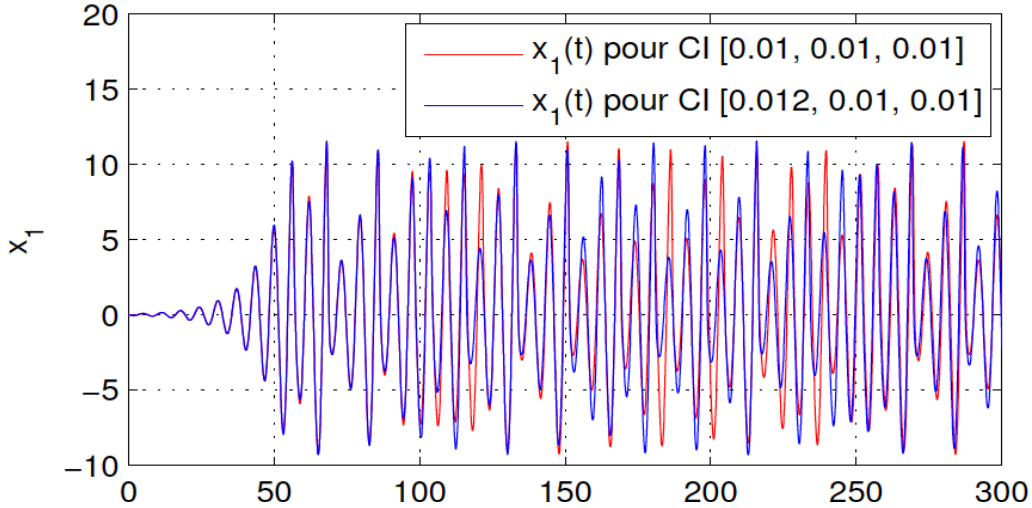

Figure 1.8 : Illustration de la propriété de sensibilité aux conditions initiales sur l'état x_1 [9]

I.3.4 Application du chaos

Le chaos peut s'appliquer dans des diverses applications, on peut mentionner les applications suivantes:

- Contrôle: la première application du chaos est le contrôle du comportement irrégulier dans les circuits et les systèmes.
- Synchronisation: communication sécurisé, cryptage, radio.
- Traitement d'information: codage, décodage et le stockage d'information dans des systèmes chaotiques tel que les éléments de mémoires et les circuits. Reconnaissance de forme.
- Prédiction à court terme: les maladies contagieuses, température, économie [10].

I.3.4.1 Domaines d'application du chaos

Parmi les nombreux domaines d'application du chaos, on cite les suivants :

- **Engineering:** contrôle de vibration, stabilisation des circuits, réactions chimiques, turbines, étages de puissance, lasers…
- **Ordinateurs:** communications des paquets dans des réseaux informatiques. Cryptage, contrôle du chaos dans les systèmes robotique.
- **Communications:** compression et stockage d'image, conception et management des réseaux d'ordinateurs.
- **Médecine et biologie:** cardiologie, analyse et rythme du cœur(EEG), prédiction et contrôle d'activité irrégulière du cœur.
- **Management et finance:** prévision économiques, analyses financières, et prévision des marché.

I.4 Attracteurs

Dans un système dynamique, on appelle un attracteur tout ensemble de condition initial qu'appartient à un volume donné peut converger vers un ensemble. Un attracteur est définit comme un ensemble dans lequel le système se développe de manière irréversible en absence de perturbation [11].

Un attracteur peut se classées dans une des catégories suivantes:

- Point fixe: le système tend à se comporter de manière statique.

- Cycle limite: le système présente un comportement oscillatoire qui se maintient sur le long terme.
- Attracteur quasi-périodique: est identifié avec un tore dans l'espace de phase.
- Attracteur étrange: la trajectoire sur l'attracteur est complexe et manifeste la propriété de sensibilité aux conditions initiales.

Les attracteurs se divisent en deux types: attracteur réguliers et attracteur étrange (chaotique). Nous intéressons aux attracteurs chaotiques.

I.4.1 Attracteurs chaotiques

Les attracteurs chaotique sont une des découvertes les plus spectaculaire des dernières années. Ces objets géométriques issus de l'évolution de système chaotique. Un attracteur est dit chaotique ou étrange lorsqu'il est contenu dans un espace fini, son volume nul, sa structure est fractale, et sa trajectoire est complexe. La propriété remarquable qui possède notamment à l'attracteur chaotique est que la trajectoire ne repasse jamais par un même état ce qui signifie que cette trajectoire se passe par une infinité d'états. Cela traduit la sensibilité aux conditions initiales. Toute condition initiale appartenant au bassin d'attraction.

Ce dernier est l'ensemble des points des phases qui donne une trajectoire évoluant vers l'attracteur considéré [12].

On observe dans la figure (1.9) un objet géométrique relativement complexe et qui dégage une extrême quantité d'information qu'il contient le système.

Parmi les exemples d'attracteurs on cite les suivants: attracteur de Rössler, attracteur de Henon, attracteur de Lorenz… .

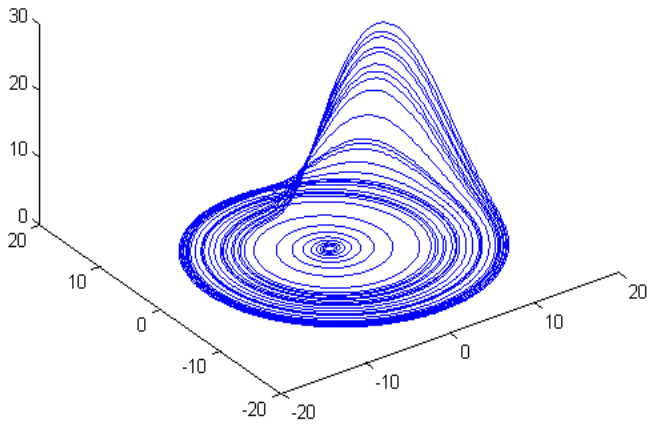

Figure 1.9 : Attracteur de Rössler

I.5 Conclusion

Dans ce chapitre une présentation de quelques notions élémentaires concernant les systèmes dynamiques chaotiques est réalisée, dans un premier temps on a commencées par des définitions des systèmes dynamiques à temps continu et discret, ainsi que les systèmes autonome et non-autonome, le comportement des systèmes dynamiques ont été données.

Par la suite on a défini le chaos, ces caractéristiques et on a cité quelques applications du chaos.

Finalement on a terminé par la présentation des attracteurs et les attracteurs étranges (chaotiques).

Chapitre II

Transmission sécurisée à base du chaos

II.1 Introduction

Comme il a été déjà mentionné dans le chapitre précèdent, le chaos qui est un signal déterministe peut être vu comme des comportements dynamiques d'apparences aléatoires. Il serait donc intéressant de l'utiliser comme porteuses d'informations en télécommunication [3].

Le chaos est obtenu à partir des systèmes non linéaires, sensible aux conditions initiales ; il correspond à un comportement stable, apériodique et éventuellement borné, de ces systèmes ce qui fait apparaitre comme du « bruit » pseudo-aléatoire [13].

Dans ce présent chapitre les principales méthodes de transmission seront exposés, que ce soit analogique ou numérique.

II.2 Transmission par chaos analogique

Différentes technique d'injection de l'information dans un système chaotique ont été proposées dans la littérature. Nous allons présenter par la suite les principales méthodes proposées pour l'exploitation du chaos dans les transmissions analogiques [13].

II.2.1 Synchronisation des systèmes chaotiques

Comme il a été mentionné précédemment, les systèmes chaotiques sont des systèmes dynamiques qui défient la synchronisation à cause de leur sensibilité aux conditions initiales [14].

Dans les systèmes de transmission, la synchronisation est une clé très importante pour une transmission réussie. A la différence de la synchronisation classique employée dans les systèmes de transmission ou l'on cherche à reproduire juste une période d'oscillation, la synchronisation chaotique au niveau du récepteur cherche à dupliquer le signal chaotique généré par l'émetteur selon les travaux de Pecora et Caroll en [2], [14].

Les méthodes traditionnelles de synchronisation sont en général basées sur l'utilisation des circuits identiques. Supposons deux systèmes chaotiques identiques oscillant de façon totalement indépendante. Si par un moyen quelconque, on leur permet d'échanger de l'énergie, action que l'on nomme "couplage", les deux systèmes finiront par céder la place à un comportement commun : ils se synchronisent. Il est possible de coupler les systèmes chaotiques dans un sens (couplage unidirectionnel) ou dans les deux sens (couplage bidirectionnel) [2].

Il existe plusieurs méthodes proposées qui combine la synchronisation du chaos avec la communication sécurisée, elles sont souvent basées sur le masquage, la commutation ou la modulation des signaux chaotiques [3].

II.2.2 Technique de transmission par chaos analogique

Pour l'injection de l'information dans un système chaotique différent technique ont été proposées dans la littérature. Nous allons présenter par la suite les principales méthodes proposées pour l'exploitation du chaos dans les transmissions analogiques [15].

II.2.2.1 Masquages chaotiques

La modulation par masquage chaotique est l'une des premières méthodes appliquées aux communications chaotiques [16].

Cette technique est basée sur le principe de synchronisation par couplage entre deux générateurs chaotiques. Le transmetteur additionne le signal chaotique $c(t)$ avec un signal d'information $m(t)$, possédant une amplitude beaucoup plus petite, cachant ainsi le signal d'information.

Au récepteur, le signal reçu $r(t)$ sert à synchroniser un générateur chaotique avec celui du transmetteur. Le message d'information reçue $m(t)$ est décodé par la différence entre le signal $r(t)$ reçu et une copie du signal chaotique $c(t)$ généré localement [17].

L'ordre de grandeur du signal message, doit être impérativement très faible par rapport à celui du signal chaotique $c(t)$, pour éviter le risque d'être piraté, sans savoir le signal $c(t)$ exact et pour avoir une bonne synchronisation au niveau du récepteur autorisé.

La figure suivante illustre le principe du masquage d'information par chaos :

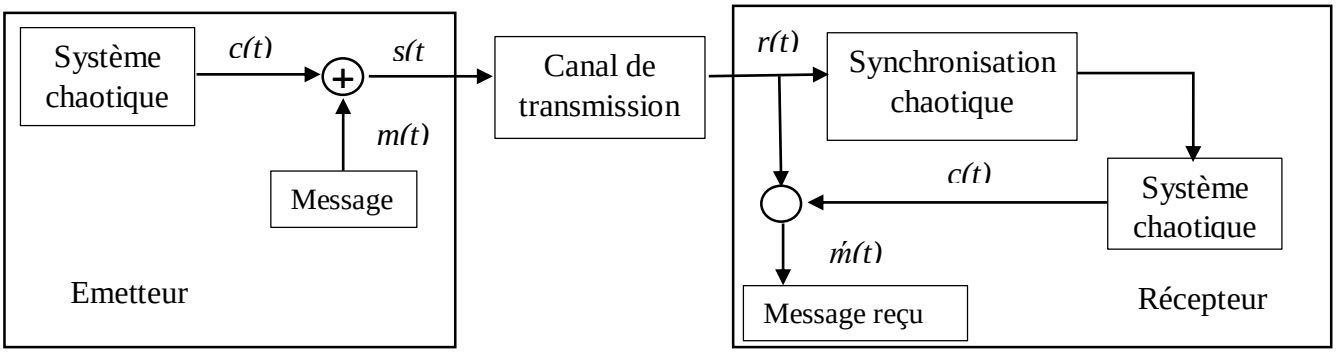

Figure 2.1 : Système de communication par masquage chaotique

Les avantages du masquage chaotique par addition résident dans sa simplicité de réalisation, inversement on souligne des inconvénients qui limitent l'application de cette technique en pratique, tels que :

- La synchronisation non parfaite entre l'émetteur et le récepteur.

- Le faible degré de sécurité démontré.
- La sensibilité à la disparité des paramètres entre les systèmes chaotiques [13].
- la grande sensibilité au bruit de l'unité de synchronisation et de son effet sur la faible amplitude du signal d'information.

II.2.2.2 Méthodes de modulation chaotique

La modulation chaotique consiste à assigner les bits d'informations aux états d'un signal qui varie chaotiquement. Plusieurs méthodes ont été proposées pour moduler un signal informationnel par un signal chaotique.

1) Chaos shift keying « CSK »

La modulation de type chaos shift keying (CSK) est une autre technique basée sur la synchronisation par couplage [18].Un signal d'information binaire encode les bits "0" et "1" sur deux signaux chaotiques statistiquement similaires $c1(t)$ et $c2(t)$ respectivement. Les signaux $c1(t)$ et $c2\ (t)$ peuvent être générés par une fonction chaotique définie par des paramètres différents résultant ainsi en deux générateurs chaotiques $f1$ et $f2$.

Le récepteur cohérent contient une copie des deux générateurs du transmetteur. Le signal reçu $r(t)$ sert à synchroniser un des deux générateurs chaotiques afin de générer les signaux chaotiques $c1(t)$ et $c2(t)$ en fonction de la transmission d'un bit "0" ou "1". Le message original est décodé soit en calculant l'erreur ou par corrélation entre le signal reçu et les signaux $c1(t)$ et $c2(t)$ générés localement.

Contrairement au système CSK cohérent, un système de communication CSK non cohérent n'a pas besoin de générer les séquences chaotiques localement pour démoduler l'information.

Il se base plutôt sur la différence en énergie des séquences chaotiques reçues pour distinguer les différents symboles transmis [19]. À chaque bit d'information "0" ou "1" est associée une séquence chaotique d'énergie différente $c1(t)$ et $c2(t)$. Les séquences $c1(t)$ et $c2(t)$ sont générées à partir de deux générateurs chaotiques ayant des énergies différentes ou par un générateur avec un gain d'énergie différent pour les bits "0" ou "1". L'énergie du signal reçu est estimée par un processus de corrélation intégration et le message original est décodé en comparant l'énergie de chaque symbole avec un seuil.

Malgré sa grande robustesse au bruit sauf que la sécurité faible de la modulation CSK est son principal inconvénient parce qu'il serait facile de distinguer la différence en distribution de

$f1$ et $f2$ pour le système cohérent et la différence en énergie pour le système non cohérent. La figure suivante montre le schéma bloc d'un système de communication CSK cohérent [20].

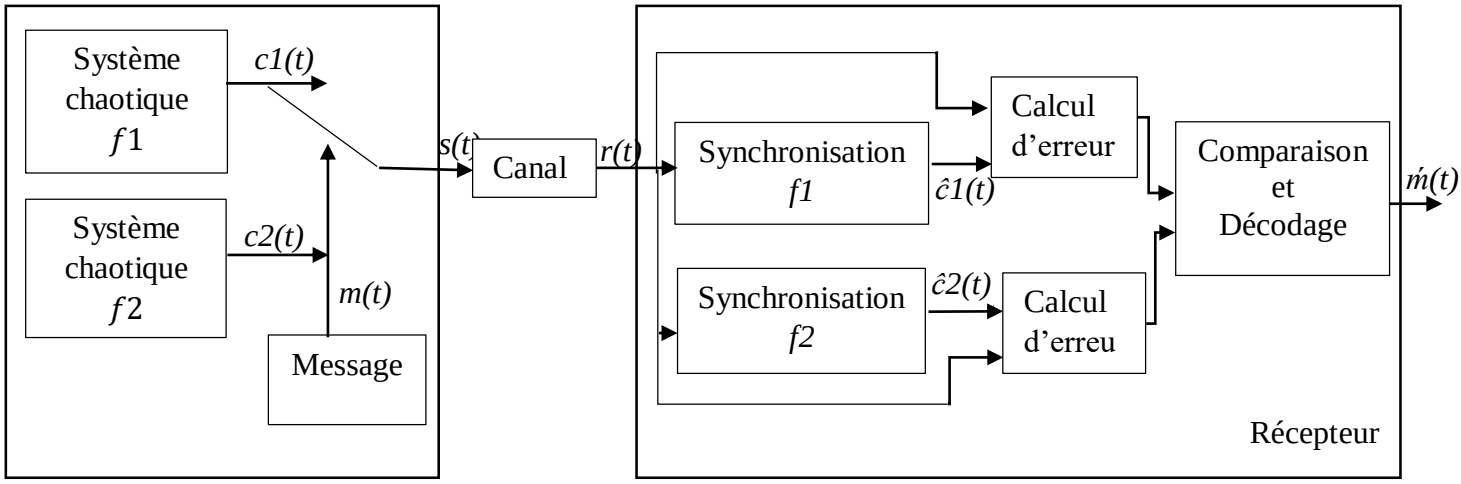

Figure 2.2 : Schéma illustrant le principe de modulation CSK cohérent

2) Modulation paramétrique

Le principe de cette méthode consiste à utiliser le signal d'information, généralement de nature binaire, pour moduler l'un des paramètres du système chaotique émetteur. Le système récepteur synchronise d'une manière adaptative avec l'émetteur chaotique et le signal d'information est restauré par l'intermédiaire d'une loi d'adaptation. Le schéma descriptif de cette technique est représenté dans la figure (2.3) [21].

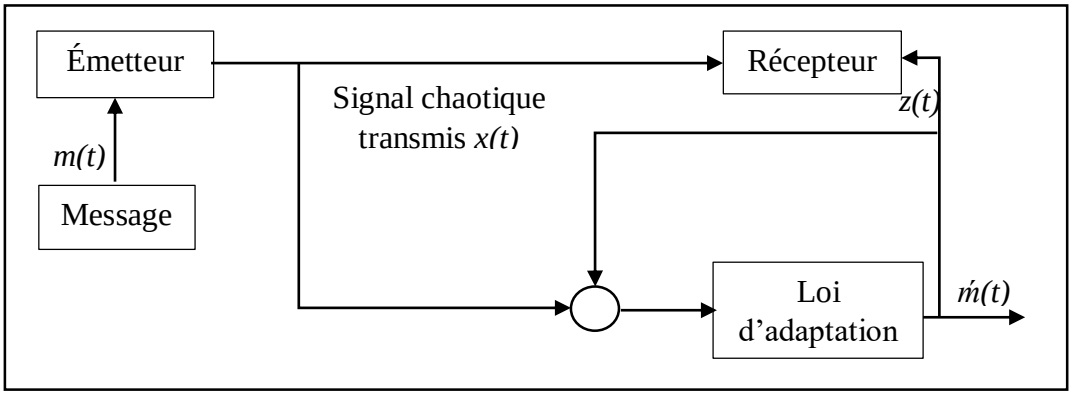

Figure 2.3: Schéma illustrant le principe de la modulation paramétrique

La modulation paramétrique apporte quelques avantages par rapport aux techniques précédentes, notamment concernant le niveau de sécurité. Elle offre aussi des capacités de multiplexage chaotique, de sorte que plusieurs messages peuvent moduler différents paramètres

d'un même système chaotique et par conséquent être envoyés et récupérés en utilisant un seul signal de transmission [22].

Cependant, l'inconvénient majeur de cette méthode s'agit du mécanisme de synchronisation adaptative employé, qui nécessite un temps de convergence pendant lequel les paramètres et l'information sont construits de manière erronée, ce qui dégrade la qualité de la transmission [13].

3) Modulation par inclusion

Cette technique consiste à injecter le message dans la dynamique chaotique d'émetteur. La synchronisation et la restauration de l'information côté récepteur peut être établie suivant deux techniques, reposant soit sur les observateurs à entrées inconnues, soit sur l'inversion du système émetteur. La figure (2.4) illustre la méthode d'inclusion [2].

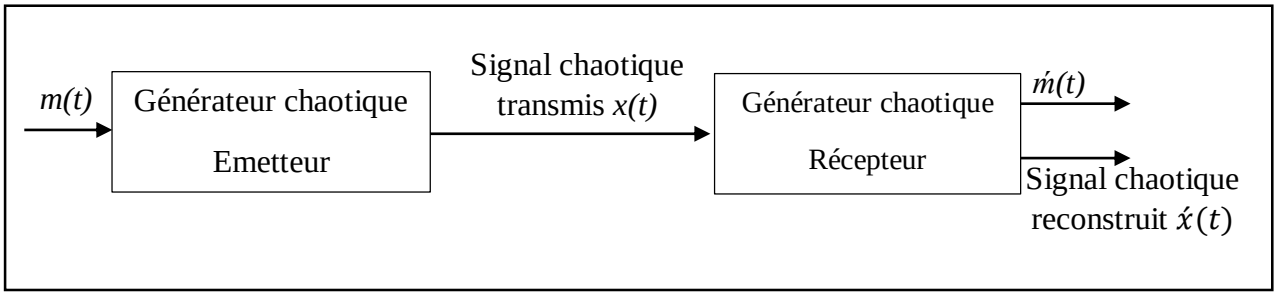

Figure 2.4: Schéma illustrant le principe du chiffrement par inclusion

La modulation par inclusion chaotique offre un niveau de sécurité nettement plus élevé par rapport aux techniques précédentes, puisque le signal confidentiel est injecté dans la dynamique du système chaotique émetteur. De ce fait, le signal chaotique disponible dans le canal de transmission public ne porte pas l'information d'une manière directe à propos le signal confidentiel. Ainsi, contrairement au chaos qui lui est déterministe, l'information ne répond à aucun critère de prévisibilité et évolue de façon complètement aléatoire ce qui va ajouter un degré de complexité supplémentaire à la procédure du chiffrement. Cependant, le principal inconvénient de la méthode de chiffrement par inclusion c'est qu'elle est moins sensible aux variations des paramètres, ce qui pose le problème du choix des clés secrètes valides [23].

II.2.2.3 Etalement de spectre

L'étalement de spectre désigne en général un ensemble de techniques de transmission de l'information utilisées pour combattre les effets nuisible de l'interférence produite par un brouillage. L'étalement de spectre est utilisé aussi pour masquer le signal en utilisant une faible

puissance d'émission, et par conséquence le signal sera difficile à intercepter par un utilisateur non-autorisé [21].

Les signaux chaotiques peuvent être employés à cet effet. L'idée de base consiste à remplacer le générateur de séquences pseudo-aléatoires employé dans les techniques d'étalement conventionnelles par une dynamique chaotique, puisque les séquences chaotiques possèdent des propriétés similaires aux séquences d'étalement.

La technique d'étalement de spectre consiste à répartir le spectre d'un signal sur une bande de fréquence très large. Cela peut être réalisé par une multiplication du signal par une séquence spécifique, nommée code ou séquence d'étalement [22].

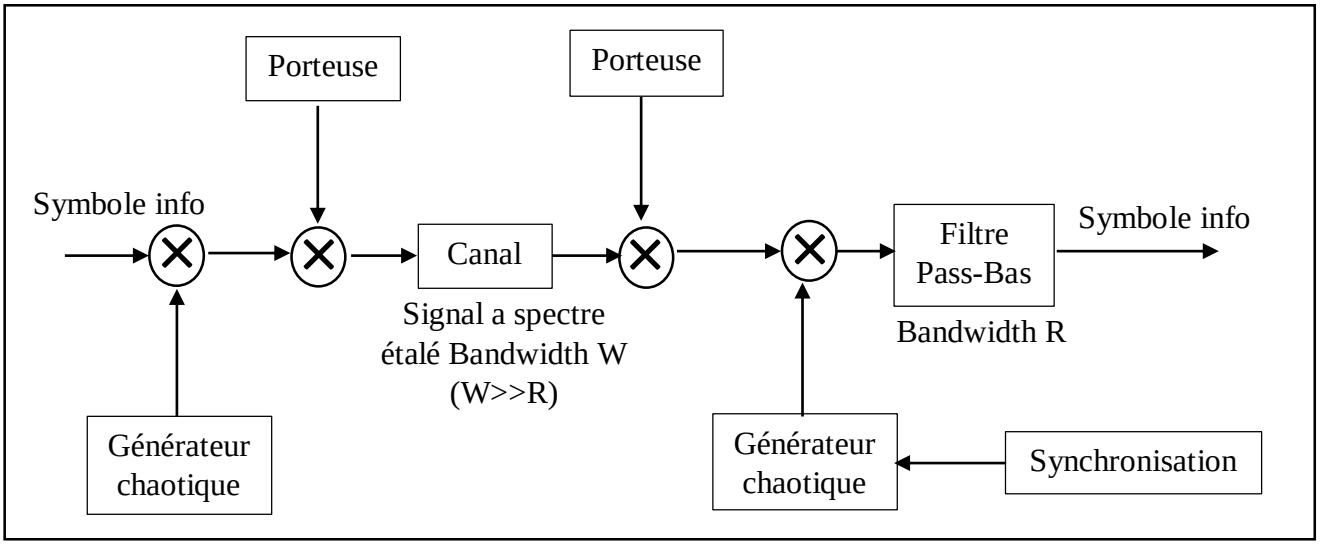

Figure 2.5 : Modèle d'un système de communication a étalement de spectre par séquence chaotique

II.2.3 Avantages et inconvénients

Les méthodes de transmission à base de chaos analogique permettent de crypter et d'étaler le spectre du signal en même temps dont les informations sont transmises et reçues en temps réel, tout en exigeant des circuits moins compliqués par rapport aux méthodes de transmission conventionnelles. Toutefois, la plupart d'entre elles présentent des inconvénients communs et partagent les mêmes difficultés de réalisation [21]:

- **Faible niveau de confidentialité:** la concurrence requise par ces techniques cryptographiques implique la transmission d'informations suffisantes sur la dynamique chaotique utilisée dans la cryptographie. Ainsi, différentes attaques peuvent agir sur le signal de synchronisation lors de la transmission. Les plus notables sont l'analyse spectrale de programme, les techniques de filtrage, la fonction de rétroaction et la synchronisation générale [23].

- **Dégradation des propriétés des systèmes chaotiques:** les termes correctifs appliqués aux systèmes chaotiques, pendant la synchronisation, servent à limiter l'effet du bruit qui s'ajoute au signal chaotique et à corriger les éventuelles perturbations dues aux incertitudes paramétriques.
- **Faible robustesse contre le bruit:** Il a été prouvé dans de nombreux travaux que les performances de synchronisation dans une transmission sûre par chaos se dégradent rapidement en présence de bruit. Ces défauts surviennent en particulier lors de la transmission et de la récupération de signaux utiles, en particulier lorsqu'il s'agit d'une appréciation partagée des états inconnus et des entrées de systèmes chaotiques. Ces transmissions il a généralement besoin d'un rapport signal sur bruit plus élevé que ses homologues conventionnels, afin de maintenir le même taux d'erreur.

II.3 Transmission par chaos numérique

Les vulnérabilités induites par les techniques de chiffrement par chaos analogique ont motivé l'extension de la cryptographie chaotique au domaine des signaux entièrement numériques, afin de créer une nouvelle génération de chiffrement par chaos indépendante des mécanismes de synchronisation analogiques.

L'intérêt majeur de numériser les signaux chaotiques est la génération plus aisée et de manière reproductible des séquences discrètes, ainsi que le contrôle pertinent de leurs propriétés naturelles:

- Initialisation efficace des systèmes chaotiques sans se soucier des problèmes liés à la synchronisation entre l'émetteur et le récepteur ;
- La binarisation des signaux chaotique implique l'utilisation d'une précision finie (32 bits ou 64 bits), ce qui simplifie la réalisation matérielle et augmente la performance de chiffrement/déchiffrement;
- Mécanismes de mise en œuvre et de contrôle des dynamiques chaotiques efficaces au niveau des calculateurs numériques. Ce qui élimine les effets des perturbations dues aux variations paramétriques;
- La possibilité d'utiliser les conditions initiales et les paramètres comme clés secrètes de tailles convenables.

Etant donné que cette catégorie de chiffrement par chaos est fortement inspirée de la cryptographie symétrique, son principe de base consiste à construire des transformations bijectives par rapport aux conditions initiales et aux paramètres de contrôle des systèmes

chaotiques employés, conformément aux deux concepts formalisés par Shannon dans le cadre de la théorie de l'information [24]:

- **La confusion:** sert à cacher la relation entre le clair et le chiffré par l'intermédiaire d'une clé secrète. La méthode la plus courante pour appliquer la confusion est la substitution, souvent non-linéaire comme celle adoptée par l'algorithme AES (Advanced Encryption Standard);
- **La diffusion:** sert à éliminer les redondances dans le message confidentiel et à diffuser l'influence du changement d'un bit de la clé ou du clair sur tout le chiffré correspondant. La diffusion est assurée par une simple transposition ou permutation.

II.4 Conclusion

Dans ce chapitre, nous avons traité plusieurs points, dont les plus importants sont :

- Génération des séquences à spectre étalé d'une manière algorithmiques.
- Un protocole de communication est présenté à l'aide d'un nouveau schéma de modulation chaotique pour la transmission de messages numériques.

Chapitre III

Compression de l'information à l'aide de systèmes chaotiques

III.1 Introduction

La compression consiste à réduire la taille physique de blocs d'informations. Un compresseur utilise un algorithme qui sert à optimiser les données en utilisant des considérations propres au type de données à compresser; un décompresseur est donc nécessaire pour reconstruire les données originelles grâce à l'algorithme inverse de celui utilisé pour la compression. La méthode de compression dépend intrinsèquement du type de données à compresser : on ne compressera pas de la même façon une image qu'un fichier audio [25].

De façon générale tous les algorithmes de compression peuvent être divisés en deux classes fondamentales : algorithmes de compression sans perte et avec pertes au niveau de l'information régénérée. Dans les deux cas le but de la compression est de supprimer la redondance dans une séquence informationnelle, le premier avec l'objectif de la reconstruction totale de la séquence initiale et le deuxième suppose d'accepter une certaine distorsion.

Le problème de la compression des données sans perte a reçu une attention accrue à la fois par les entreprises de fabrication douce, mais aussi par les chercheurs indépendants qui ont développé divers types d'algorithmes, en commençant par les statistiques les plus adaptatifs [26].

Contrairement aux algorithmes de compression des données, l'utilisation de signaux chaotiques est relativement dans le domaine des télécommunications et peu d'études ont été réalisées avec l'application des générateurs et des signaux chaotiques spécifiquement pour la compression et le codage des données. La technologie de chiffrement a reçu une grande attention et tous récemment l'introduction de la dynamique symbolique, et le système code par le canal considéré, ont vraiment ouvert l'utilisation de Piese Wise Linear Markov mappe (PWLM) à la zone des méthodes de codage [27].

Ce chapitre a pour but de montrer que la dynamique symbolique peut s'appliquer au problème de compression d'information.

III.2 Description en dynamique symbolique des systèmes chaotiques

La dynamique symbolique est un outil de description et d'analyse des systèmes dynamiques, introduit par Hadamard en 1898 pour étudier les propriétés de codage des systèmes dynamiques

et la codification des orbites périodiques, et comprendre ainsi la diversité et la complexité des trajectoires engendrées par des lois simples. Depuis 1989, cette approche a été largement considérée dans l'étude des dynamiques chaotiques [28], principalement dans le cadre des transmissions numériques.

III.2.1 Définition (*Description en dynamique symbolique*)

La description d'un système chaotique en dynamique symbolique consiste à convertir les valeurs réelles continues des signaux chaotiques en séquences de symboles, en partitionnant l'espace des phases en intervalles, dont chacun est un homéomorphisme.

En associant à chaque intervalle $I_{\{n\}}$, un symbole distinct $S_{\{n\}}$, une séquence symbolique peut être définie comme étant l'ensemble de régions que le signal chaotique visite durant son évolution temporelle [29]. Étant donné que chaque orbite chaotique est représentée par une infinité d'états$\{x_0, x_1, x_2, .., x_n, ..\}$ déterminés par une condition initiale x_0, il peut être démontré que pour chaque point de l'espace des phases est associée une séquence symbolique: $s = \{s_i, i = 1 \dots M | s_i \in S\}$, où S représente l'alphabet des symboles disponibles $S_{\{n\}} \in S$, $n = 1 \dots N$.

Nous considérons une application particulière de la dynamique symbolique au générateur de type Bernoulli suivant :

$$\boldsymbol{f(x)} = \begin{cases} \boldsymbol{f^{(1)}(x) = 2x} & \boldsymbol{, x \in I_1 = [0, 0.5]} \\ \boldsymbol{f^{(2)}(x) = 2x - 1, x \in I_2 = (0.5, 1]} \end{cases} \quad \textbf{(3.1)}$$

Dans l'équation ci-dessus on a considéré les intervalles juxtaposés et disjoints deux à deux $I_{\{n\}}$, avec les propriétés $\cap_{n=1}^{N} I_{\{n\}} = \emptyset$ et $\cup_{n=1}^{N} I_{\{n\}} = I$, pour le cas où $N = 2$, $n = 1 \dots N$ et $I = [0,1]$. De cette façon nous avons défini une fonction bijective entre l'ensemble $\cup_{n=1}^{N} I_{\{n\}} = I$ qui représente l'espace d'état de la fonction chaotique à l'alphabet $\cup_{n=1}^{N} S_{\{n\}} = S$. On a employé la terminologie d'alphabet pour faciliter l'explication de l'algorithme de compression présenté dans les sections suivantes.

On observe que pour chaque intervalle $I_{\{n\}}$ le générateur Bernoulli, donné par l'équation (3.1), associe une fonction linéaire$f^{(n)}: I_{\{n\}} \to I$. Cette fonction linéaire sur l'intervalle particulier $I_{\{n\}}$ est bijective et en conséquence inversible, ainsi nous pouvons affirmer qu'il existe $f^{-1(n)}: I \to I_{\{n\}}$ pour chaque $n = 1 \dots N$.

On va montrer le fonctionnement du processus de codage d'une séquence informationnelle par un exemple, et pour celle-ci on suppose que le dernier symbole est $s_M = S_{(2)}$. La conséquence que le symbole $s_M = S_{(2)}$ à l'instant M soit le dernier nous conduit à l'hypothèse qu'au rang $M - 1$ tout l'intervalle de valeurs possibles de conditions initiales (IC) pour l'état est (I).

La fonction donnée par $f^{-1(2)}$ est propage n'importe laquelle des valeurs de l'intervalle I à l'intervalle $I_{\{2\}}$, et la propriété de bijectivité nous assure que pour n'importe quelle valeur dans I lui correspondra juste une valeur dans $I_{\{2\}}$ et vice versa. Alors finalement pour le $M-$ième symbole on obtient :

$$\boldsymbol{I^{(M)} = f^{-1(2)}(I) = I_{\{2\}}} \qquad \textbf{(3.2)}$$

Où la notation $I^{(i)}$ a été choisie pour désigner l'intervalle des conditions initiales possibles et nécessaires pour que la séquence de symboles soit $\{s_i, s_{i+1}, .., s_M\}$. On va continuer l'application du même principe, cette fois pour le symbole de rang $M - 1$, choisi par exemple comme $s_{M-1} = s_{\{1\}}$. Cette fois, l'intervalle de valeurs disponible sera limité à $I^{(M)}$, et en conséquence l'intervalle des conditions initiales possibles est donné par $I^{(M-1)} = f^{-1(1)}\left(I^{(M)}\right)$. Généralement la relation (3.2) peut s'exprimée pour n'importe quel symbole s_i avec la valeur S_n , par la récurrence :

$$\boldsymbol{I^{(i)} = f^{-1(n)}(I^{i+1})} \qquad \textbf{(3.3)}$$

L'application de la relation de propagation ci-dessus au générateur Bernoulli (3.1) est illustrée à la figure (3.1) :

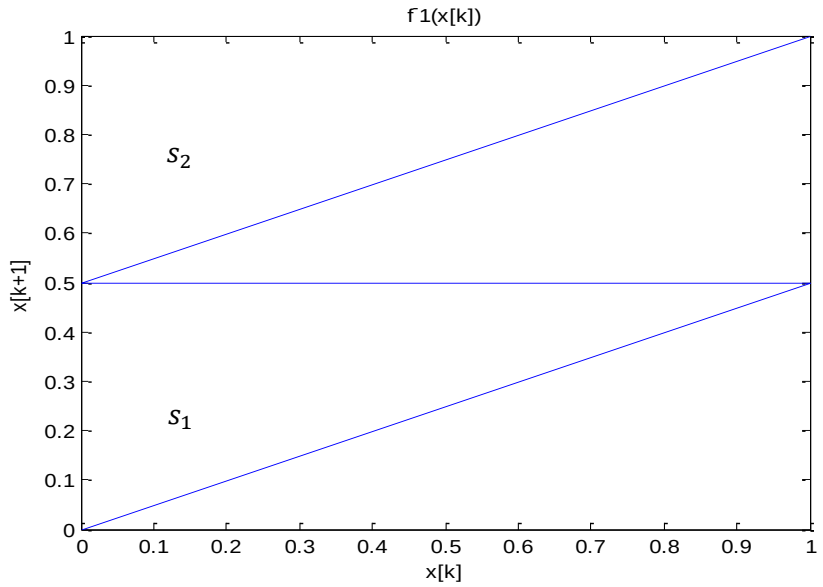

Figure 3.1: Forme de la fonction inverse $f^{-1}(.)$

Nous venons d'exposer le mécanisme de propagation inverse qui nous permet de trouver l'intervalle de conditions initiales nécessaire pour la reconstruction de la séquence informationnelle.

III.3 Générateur probabiliste de Bernoulli

Le générateur probabiliste de Bernoulli est un système dynamique chaotique particulier. Ce système est caractérisé par la forme qui prend une fonction linéaire par portions, non-uniforme, décrivant un processus de Markov d'ordre 1. La non-uniformité vient parce que les intervalles $I_{\{n\}}$ peuvent être de largeurs inégales.

La détermination du générateur se fait par la considération du même alphabet *S*, associe à la probabilité d'apparition de chaque symbole P_n , $n = 1..N$. Alors pour l'ensemble des intervalles $I_{\{n\}}$ ainsi pour les probabilités P_n , les relations suivantes peuvent s'écrites comme suit:

$$\cup_{n=1}^{N} \boldsymbol{I}_{\{n\}} = \boldsymbol{I} = [\boldsymbol{0}, \boldsymbol{1}]$$

$$\sum_{n=1}^{N} \boldsymbol{P_n} = \boldsymbol{1} \qquad \textbf{(3.4)}$$

$$\cap_{n=1}^{N} \boldsymbol{I}_{\{n\}} = \emptyset$$

P_n: Probabilité d'apparition du symbole S_n

La relation entre probabilité d'apparition et intervalles peut facilement s'obtenus avec les expressions (3.4), définissant l'espace d'état où s'appliquera la dynamique symbolique :

$$\boldsymbol{I}_{\{1\}} = [\boldsymbol{0}, \boldsymbol{P_1}]$$

$$\boldsymbol{I}_{\{i\}} = \left] \sum_{i=1}^{n-1} \boldsymbol{P_i}, \sum_{i=1}^{n} \boldsymbol{P_n} \right], \boldsymbol{n = 2 \ldots N} \qquad \textbf{(3.5)}$$

Alors la fonction caractéristique pour le générateur probabiliste de Bernoulli prendra la forme:

$$\boldsymbol{f_p(x)} = \begin{cases} \boldsymbol{f_p^{(1)}(x) = \frac{1}{P_1} x \, , x \in I_{\{1\}}} \\ \boldsymbol{f_p^{(2)}(x) = \frac{1}{P_2}(x - P_1), x \in I_{\{2\}}} \\ \cdots \\ \boldsymbol{f_p^{(N)}(x) = \frac{1}{P_N}(x - \sum_{n=1}^{N-1} P_n) \, , x \in I_{\{N\}}} \end{cases} \qquad \textbf{(3.6)}$$

La figure suivante présente la fonction caractéristique:

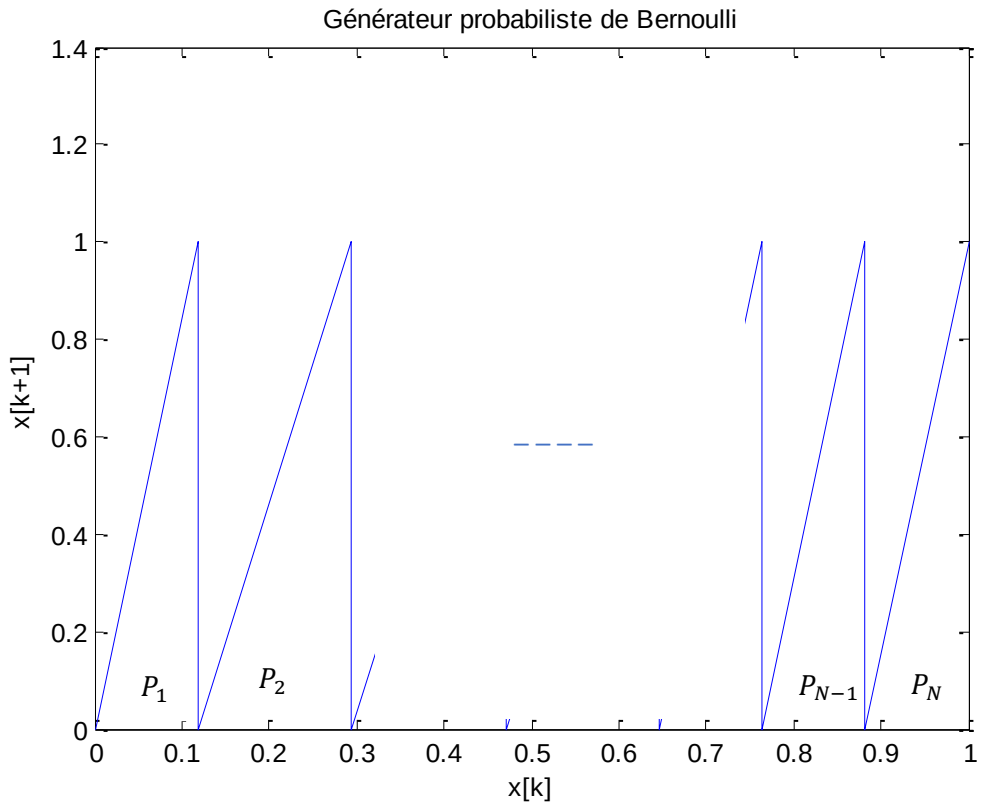

Figure 3.2 : Fonction caractéristique d'un générateur de Bernoulli

L'étude des propriétés de la fonction caractéristiques présentée dans l'équation (3.6) nous permet d'observé qu'elle respecte les conditions nécessaire pour appliquer la dynamique symbolique inverse, a part que la partie définie par $f_P^{(n)}: I_{\{n\}} \to I$ est bijective sur son intervalle de définition, et en conséquence inversible.

On peut donc affirmer que la fonction $f_p^{-1(n)}: I \to I_{\{n\}}$ existe pour tous $n = 1 \dots N$, et prend la forme d'expression suivante:

$$\begin{cases} \boldsymbol{f_P^{-1(1)}(x) = P_1 x} \\ \boldsymbol{f_P^{-1(n)}(x) = P_n x + \sum_{i=1}^{n-1} P_i} \end{cases} \quad \textbf{(3.7)}$$

Cette expression sera la base de l'algorithme de compression présenté prochainement. Nous verrons aussi que la dynamique symbolique inverse appliquée conduire à des performances très intéressantes du point de vue du taux de compression et du coût de calcul.

III.4 Un algorithme de compression chaotique

III.4.1 Performances de l'algorithme proposé

Pour atteindre un certain niveau de compression, il faut associer à l'algorithme de compression certaine des propriétés statistiques du signal informationnel à compresser, le but étant de réduire la redondance et ainsi ne laisser que le contenu informatif.

Généralement les informations d'un code source s_i est défini par $-\log_2(P(s_i))$, et par conséquent on définit la moyenne contenu d'information sur l'alphabet source comme l'entropie de cet alphabet:

$$\boldsymbol{H = -\sum_{n=1}^{N} P_n \, log_2(P_n)} \quad \textbf{(3.8)}$$

L'optimalité du code est considérée au sens de la redondance minimale, qui est défini par la différence entre la longueur moyenne du mot de code et l'entropie du alphabet, et donc un code est considéré asymptotiquement optimal si pour une probabilité donnée distribution, le rapport entre la longueur moyenne du mot de code et l'entropie se rapproche de 1 lorsque l'entropie tends vers l'infini.

Le but de l'introduction de la dynamique symbolique précédemment était de prouver qu'en utilisant un générateur particulier par morceaux, nous pouvons «coder», en utilisant une famille bijective récursive de fonctions, une séquence de symboles à un intervalle de conditions initiales obtenu de manière déterministe. Nous prouverons qu'en utilisant cette méthode et le générateur probabiliste de Bernoulli introduites dans la section III.3 d'atteindre la limite d'entropie pour le code obtenu.

La compression est obtenue en trouvant la meilleure condition initiale, codée au format binaire, l'utilisation de la forme particulière du générateur exprimée en (3.6) peut obtenir avec l'approche symbolique dynamique donne la séquence initiale. Maintenant, si nous voulons trouver les performances de cette méthode nous devons nous référer à la séquence binaire minimale nécessaire pour coder une condition initiale dans un intervalle particulier. On sait que pour représenter une valeur dans l'intervalle $I \subset [0,1)$ de dimension *d* nous avons besoin de $-\log_2 d$ nombre de bits, donc si nous pouvons développer une méthode pour calculer la taille de l'intervalle particulier que la condition initiale doit respecter, nous pouvons fournir une performance de compression de l'algorithme.

On considère la suite $s = \{s_i, i = 1 \dots M \mid s_i \in S\}$ où S est l'alphabet des symboles disponibles, $S_{\{n\}} \in \mathrm{S}, \mathrm{n} = 1 \dots \mathrm{N}$, avec la probabilité d'apparition du symbole donné par:

$$\boldsymbol{P_n = \frac{1}{M} card\{s_i | s_i = S_{\{n\}}\}} \quad \textbf{(3.9)}$$

Pour cette distribution probabiliste discrète on associe le générateur probabiliste de Bernoulli donnée dans (3.6) avec la propriété partielle des fonctions par la forme donnée en équation (3.7) et la disjonctive contiguë des intervalles de définition I_n.

Si nous considérons la méthode de propagation inverse, on peut fournir la même forme récurrente pour l'intervalle $I^{(i)}$ des valeurs possibles des conditions initiales, tel qu'il est donné en équation (3.3). Le symbole codé était $s_i = S_{\{n\}}$:

$$\boldsymbol{I^{(i)} = f_p^{-1(n)}(I^{(i+1)})} \quad \textbf{(3.10)}$$

En utilisant la relation au-dessus et la forme linéaire de $f_p^{-1}(.)$ On peut fournir une expression récurrente pour la taille de l'intervalle $I^{(n)}$:

$$\boldsymbol{size(I^{(i)}) = P_n size(I^{(i+1)})} \quad \textbf{(3.11)}$$

Grace à cette relation et celle donnée en (3.9), on obtient une relation qui nous permet de calculer directement la largeur d'intervalle de condition initiale pour toute la séquence informationnelle:

$$\boldsymbol{size\left(I^{(1)}\right) = \prod_{i=1}^{M} P(s_i \in S) = \prod_{n=1}^{N} (P_n)^{P_n M}} \quad \textbf{(3.12)}$$

Maintenant nous pouvons obtenir le nombre nécessaire de bits pour coder la condition initial:

$$\boldsymbol{-log_2\left(size\left(I^{(1)}\right)\right) = \sum_{n=1}^{N} P_n M\, log_2(P_n) = M.H} \quad \textbf{(3.13)}$$

La démonstration de l'optimalité est donnée par l'expression exprimée en (3.13). Un algorithme similaire classique a été introduit durant les années 60 par un certain nombre de chercheurs, et a reçu le nom d'algorithme arithmétique. Il utilise également un intervalle initial [0,1] mais avec la technique de projection vers l'avant et les implémentations directes de cet algorithme étaient interdites en exigent un effort de calcul élevé, Quelques travaux récents proposent des versions allégées de cet algorithme au niveau de la charge de calcul tout en gardant les mêmes performances [26].

L'algorithme de décompression dans notre cas est très simple, utilisant la condition initiale déterminée ainsi que le générateur probabiliste de Bernoulli définie par ($P_{\{n\}}$), nous pouvons

générer une séquence chaotique et juste faire une séparation de phases d'états conforme aux intervalles ($I_{\{n\}}$) .

Le problème de cet algorithme comme pour la méthode de compression arithmétique est que l'on ne sait quand s'arrêter, donc il faut ajouter à l'espace des symboles un caractère spécifique de *fin de séquence* qui affectera l'optimalité du processus de compression dans son ensemble, mais pour le cas de séquence informationnelle infiniment longue l'optimalité au sens de l'entropie est toujours garantie [27].

III.4.2 Implémentation en pratique

La transformation des opérations sous forme binaire est obligatoire pour l'implémentation en pratique de l'algorithme proposé. Pour cela on propose deux solutions. La première et la moins couteuse est d'utiliser un format binaire pour toutes les opérations de multiplication et d'additions à réaliser. Malgré la grande performance de cette méthode, mais d'autre part elle suppose le développement d'une bibliothèque de fonction de calcul arithmétique particulière. Alors nous avons choisi la seconde approche reposant sur les opérations en virgule flottante et codage de la condition initiale en binaire.

Quelle que soit la méthode choisie on propose l'expression d'une valeur quelconque $x \in [0,1[$, sous forme de somme infinie de puissance négative de deux:

$$\boldsymbol{x_{CI} = \sum_{k=1}^{\infty} b_k 2^{-k}} \qquad \textbf{(3.14)}$$

Ou b_K= {0,1}, k=1... ∞.

Si on considère que l'intervalle $I^{(1)}$, obtenu par la propagation inverse de toute la séquence informationnelle est défini sous la forme $I^{(1)} = [l_{inf}, l_{sup}]$ avec $l_{inf}, l_{sup} \in [0,1[$, on peut démontrer la proposition suivante sur le calcul d'une condition initiale dans l'intervalle déterminé.

Proposition: Etant donnée un intervalle $[l_{inf}, l_{sup}] \subset [0,1[$, on va demontrer qu'avec l'expression de ses limites en fonction d'une somme infinie de puissance négative de deux $l_{inf} = \sum_{k=1}^{\infty} b_k^{\{i\}} 2^{-k}$, $l_{sup} = \sum_{k=1}^{\infty} b_k^{\{s\}} 2^{-k}$, il existe $M < \infty$ toujours tel que $b_k^{\{i\}} = b_k^{\{s\}}$ $\forall\, k \leq M$, avec $b_{M+1}^{\{i\}} \neq b_{M+1}^{\{s\}}$. Aussi la valeur $x_{CI} = \sum_{k=1}^{M+1} b_k^{\{s\}} 2^{-k}$ appartient à l'intervalle $[l_{inf}, l_{sup}]$.

- *Démonstration:* pour prouver l'existence de M, deux cas seront considérés
  - Cas ou $0{,}5 \in]l_{inf}, l_{sup}[$

Dans ce cas l'expression des limites de l'intervalle sous la forme (3.14), implique $b_1^{\{i\}} = 0$ et $b_1^{\{s\}} = 1$. Nous considérons alors que $M = 0$ et aussi $x_{CI} = 2^{-1} \in [l_{inf}, l_{sup}]$.qui convient pour répondre au problème.

- Cas ou $0{,}5 \notin]l_{inf}, l_{sup}[$

Dans ce cas nous allons utiliser la propriété suivante:

$$\sum_{k=M}^{\infty} \mathbf{2^{-k}} = \mathbf{2^{-M}} \lim_{k\to\infty} \frac{1-2^{-k-1}}{1-2^{-1}} = \mathbf{2^{-M+1}} \qquad \textbf{(3.15)}$$

Pour montrer l'existence de *M*, on va écrire les inégalités suivantes pour une valeur quelconque $l \in [0{,}1[$:

$$\begin{aligned} \boldsymbol{l} &= \sum_{k=1}^{\infty} \boldsymbol{b_k 2^{-k}} \\ &= \boldsymbol{b_1 2^{-1}} + \sum_{k=2}^{\infty} \boldsymbol{b_k 2^{-k}} \\ &\geq \boldsymbol{b_1 2^{-1}} \end{aligned} \qquad \textbf{(3.16)}$$

$$\begin{aligned} \boldsymbol{l} &= \sum_{k=1}^{\infty} \boldsymbol{b_k 2^{-k}} \\ &= \boldsymbol{b_1 2^{-1}} + \sum_{k=2}^{\infty} \boldsymbol{b_k 2^{-k}} \\ &< \boldsymbol{b_1 2^{-1}} + \sum_{k=2}^{\infty} \boldsymbol{2^{-k}} \\ &< \boldsymbol{b_1 2^{-1}} + \boldsymbol{2^{-1}} \end{aligned} \qquad \textbf{(3.17)}$$

Avec les expressions (3.16) et (3.17) nous allons montrer l'égalité des symboles binaires $b_k^{\{i\}}$ et $b_k^{\{s\}}$ pour $k \leq M$

La supposition $b_1^{\{i\}} = 1$ et $b_1^{\{s\}} = 0$ nous conduirais à $l_{min} \geq 0{,}5$, $l_{max} < 0{,}5$ ce qui est en contradiction avec l'hypothèse de départ $l_{min} < l_{max}$.

De la même façon, si nous supposons que $b_1^{\{i\}} = 0$ et $b_1^{\{s\}} = 1$ on a $l_{min} < 0{,}5$, $l_{max} \geq 0{,}5$ qui par contre ne respecte pas l'hypothèse initiale que $0{,}5 \notin]l_{inf}, l_{sup}[$. Nous pouvons en conclure qu'il existe bien $M \geq 1$ tel que $b_k^{\{i\}} = b_k^{\{s\}}$, $\forall\, k \leq M$.

L'existence de M étant prouvée, en supposant de façon similaire les différentes combinaisons possibles des valeurs de $b_{M+1}^{\{i\}}$ et $b_{M+1}^{\{s\}}$, nous obtenons comme seule solution admissible $b_{M+1}^{\{i\}} = 0$ et $b_{M+1}^{\{s\}} = 1$.

On va choisir alors la variable $x_{CI} = \sum_{k=1}^{M+1} b_k^{\{s\}} 2^{-k}$ qui respecte les inégalités suivante:

$$\begin{aligned} \boldsymbol{l_{inf}} &= \sum_{\boldsymbol{k=1}}^{\infty} \boldsymbol{b_k^{\{i\}} 2^{-k}} \\ &= \sum_{\boldsymbol{k=1}}^{\boldsymbol{M}} \boldsymbol{b_k^{\{i\}} 2^{-k}} + \sum_{\boldsymbol{k=M+2}}^{\infty} \boldsymbol{b_k^{\{i\}} 2^{-k}} \\ &< \sum_{\boldsymbol{k=1}}^{\boldsymbol{M}} \boldsymbol{b_k^{\{i\}} 2^{-k}} + \boldsymbol{2^{-M-1}} \\ &< \sum_{\boldsymbol{k=1}}^{\boldsymbol{M+1}} \boldsymbol{b_k^{\{s\}} 2^{-k}} \\ &< \boldsymbol{x_{CI}} \end{aligned} \qquad \textbf{(3.18)}$$

$$\begin{aligned} \boldsymbol{l_{sup}} &= \sum_{\boldsymbol{k=1}}^{\infty} \boldsymbol{b_k^{\{s\}} 2^{-k}} \\ &= \sum_{\boldsymbol{k=1}}^{\boldsymbol{M+1}} \boldsymbol{b_k^{\{s\}} 2^{-k}} + \sum_{\boldsymbol{k=M+2}}^{\infty} \boldsymbol{b_k^{\{s\}} 2^{-k}} \\ &\geq \sum_{\boldsymbol{k=1}}^{\boldsymbol{M+1}} \boldsymbol{b_k^{\{s\}} 2^{-k}} \\ &\geq \boldsymbol{x_{CI}} \end{aligned} \qquad \textbf{(3.19)}$$

Ainsi $x_{CI} = \sum_{k=1}^{M+1} b_k^{\{s\}} 2^{-k}$ appartient bien à l'intervalle $\left[l_{inf}, l_{sup}\right]$.

La notion x_{CI} a été choisie pour désigner la condition initiale finalement sélectionnée comme la représentation binaire de la séquence informationnelle compressée [4].

III.4.3 Exemple d'application de l'algorithme proposé

Pour illustrer le fonctionnement de l'algorithme on a choisi deux séquences qui l'on la même longueur et les probabilités d'apparition des symboles. Ce choix va nous permettre d'observer l'influence d'ordre des symboles sur la trajectoire générée et sur la condition initial déterminée.

Séquence 1#:

'ABACACABCACACBAACAC#', De longueur : M= 20

Le tableau suivant présente la probabilité d'apparition et l'intervalle de chaque symbole :

Tableau 3.1: Probabilité d'apparition des symboles

Caractère	Probabilité	Intervalle
A	0.450	[0, 0.45]
B	0.150	[0.45, 0.60]
C	0.350	[0.60, 0.95]
#	0.050	[0.95, 1]

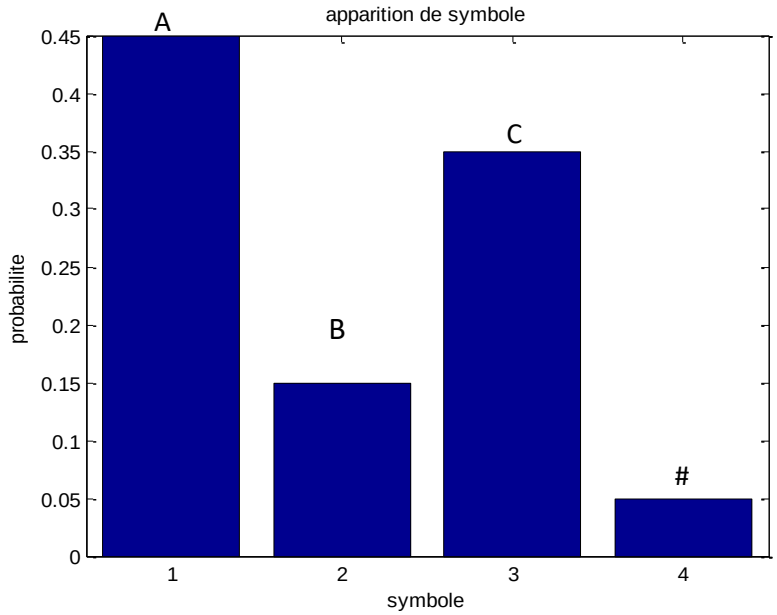

Figure 3.3: Histogramme de la distribution de probabilité discrète

La figure suivante exprime la fonction caractéristique de la séquence choisie :

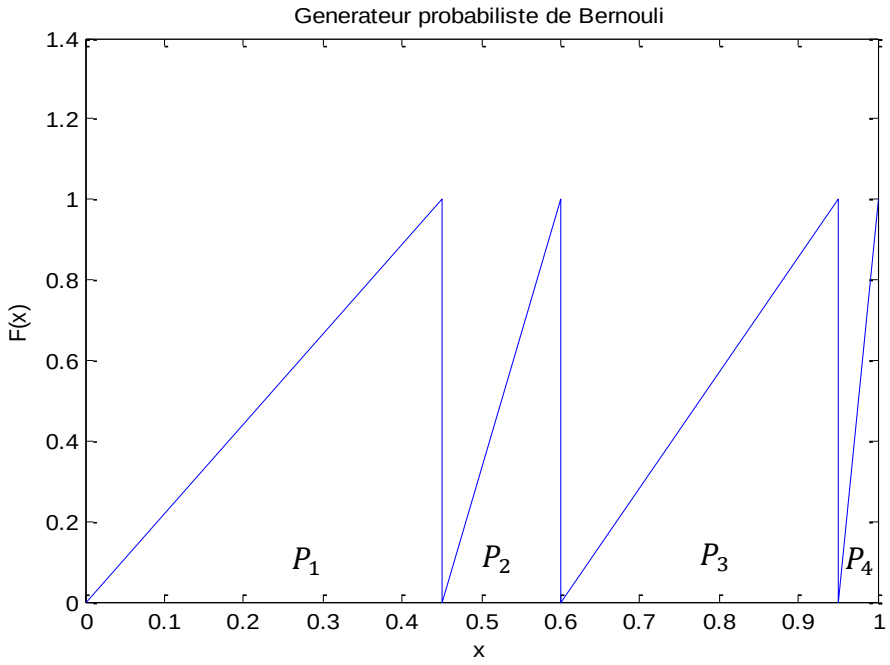

Figure 3.4: Générateur probabiliste de Bernoulli

Entropie $H = 2.8584$; codage normal pour la CI : $M.H = 33.5028$.

CI codée: [0 0 1 1 1 0 0 1 0 1 0 1 1 0 0 1 0 0 1 1 0 0 0 1 0 0 0 0 1 0 0 0 1], longueur de 33 bits.

La valeur réelle de la condition initiale est $x_0 = 0.224017204869385$.

Séquence 2# : AABCACABCACACBAACAC#'

CI codée: [0 0 0 0 1 1 1 0 0 1 1 0 1 0 1 1 0 0 0 0 1 1 1 1 0 1 0 0 1 1 0 1 0], longueur de 33 bits.

La valeur réelle de la condition initiale est $x_0 = 0.112642204869385$.

L'explication de la figure (3.5) est que la propriété de bijectivité des fonctions $f_p^{(n)}(x)$ nous assure que la trajectoire régénérée à partir de l'état initial x_0 sera toujours connue dans les intervalles $I^{(i)}$ obtenus par propagation inverse. La génération de la trajectoire s'arrête en détectant le symbole *fin de séquence.* Une autre manière différente de l'emploi de symbole de *fin de séquence*, peut être considérer pour réaliser la compression, avec la longueur fixe de la séquence informationnelle à compresser.

Une observation s'impose au niveau des possibilités de reconstruction de la séquence des symboles dans le cas où une erreur sera commise au niveau de la condition initiale (représentée sous forme binaire).

En fonction de la position de cette erreur dans la séquence binaire il se peut que les premiers symboles informationnels soient correctement régénérés, mais dans le cas où un symbole de *fin de séquence* est utilisé, nous allons commettre aussi une erreur sur la longueur de la séquence régénérée. L'usage d'une séquence de longueur fixe se place de ce point de vue, comme avantage.

L'usage d'une stratégie pour l'étape de décompression dépend fortement de la nature de l'information manipulée.

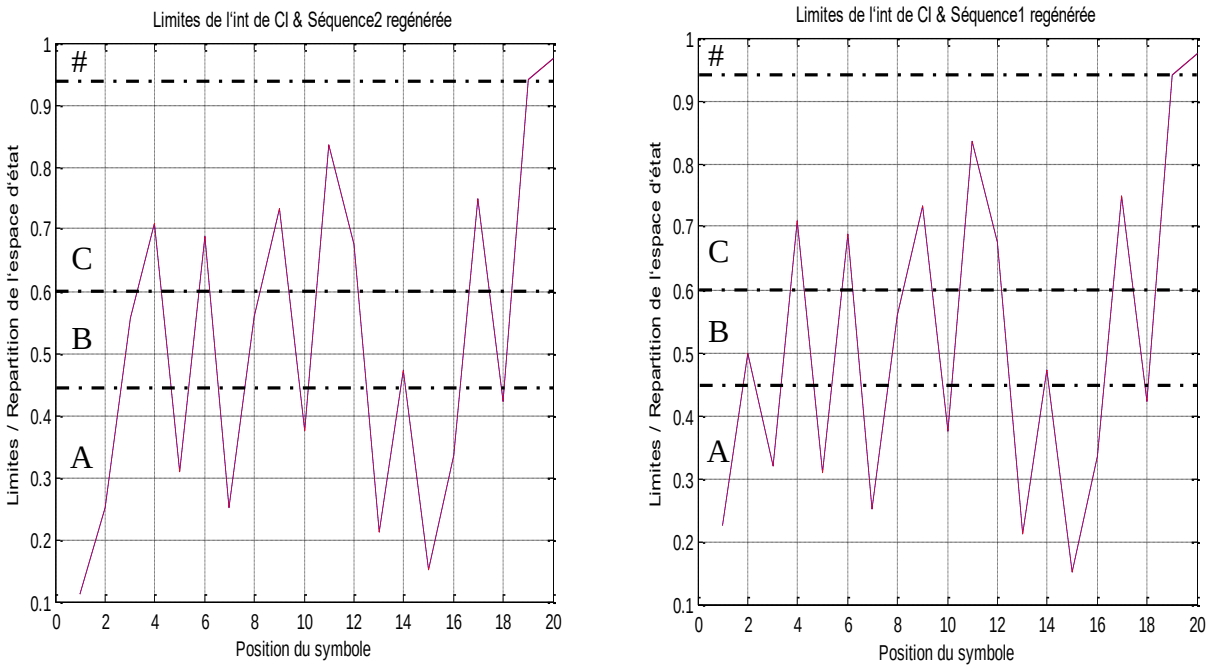

Figure 3.5: Limites des trajectoires qui déterminent l'intervalle récurrent des CI et la trajectoire régénérée

III.5 Conclusion

Un algorithme de compression sans perte de critères d'entropie optimale a été introduit comme une nouvelle application des signaux chaotique a la procédure de codage. L'utilisation de la dynamique chaotique et d'un type spécial de générateur chaotique s'appelé générateur probabiliste de Bernoulli, a été considérer pour transformer une séquence informationnelle quelconque en une trajectoire comprise dans l'intervalle [0,1].

Seul l'algorithme statique de compression est considéré dans ce chapitre, une forme adaptative peut être envisagée, pour améliorer les performances. L'emploi d'une fonction

linéaire par partie permet la reconstruction rapide de la séquence initiale, rendant la méthode très intéressante pour des implémentations en temps réel.

Conclusion générale

Dans ce mémoire on a présentés plusieurs aspects sur les communications numériques à l'aide de systèmes dynamiques chaotiques.

Dans le premier chapitre de ce mémoire, nous avons évoqué d'abord quelques notions sur les systèmes dynamiques qu'ils soient en temps continu ou en temps discret. Par la suite, nous nous sommes intéressés à une classe particulière de systèmes non linéaires qui sont dits chaotiques.

Ces systèmes présentent plusieurs caractéristiques dont l'exploitation serait intéressante pour la transmission de données. Parmi ces caractéristiques que nous avons développées avec plus de détails, nous pouvons citer le déterminisme qui signifie que ces systèmes sont régis par des règles fondamentales non probabilistes. Il est alors possible de reproduire le comportement chaotique. Une autre propriété intéressante de ces systèmes, est la sensibilité aux conditions initiales. En effet, un moindre écart ou imprécision dans les conditions initiales engendre des évolutions totalement différentes. Ceci implique l'impossibilité de prédiction à long terme du comportement du système chaotique. Nous avons également cité les différentes classes des systèmes chaotiques, et pour chaque catégorie nous avons donné des exemples de systèmes chaotiques utilisés par la communauté scientifique.

Dans le deuxième chapitre nous avons exposé les principales méthodes des transmissions sécurisées basé sur le chaos que ce soit analogique ou numérique ; ainsi leurs avantages et inconvénients .de là nous avons conclu qu'aucun standard de transmission par chaos n'a émergé jusqu'à présent, car les études de faisabilité et de robustesse des algorithmes développés remettent en cause leur niveau de sécurité qui est souvent indéterminé.

Le dernier chapitre de ce mémoire est dédié à la présentation d'une méthode de compression originale qui utilise la dynamique symbolique chaotique pour réaliser le codage d'une séquence informationnelle sous la forme d'un intervalle de conditions initiales. On démontre que l'emploi d'un générateur particulier, dénommé générateur probabiliste de Bernoulli, construit en fonction de la probabilité d'apparition de chaque symbole, va générer la séquence informationnelle initiale à partir d'une condition initiale située dans un intervalle donné (la détermination de celui-ci est issue de l'étape de compression). Théoriquement on a démontré,

que la performance de compression atteint la limite entropique, ainsi on a obtient le résultat très important que la méthode développée soit optimale.

Rappelons que cet algorithme suit les mêmes étapes que la compression arithmétique, mais avec une formulation plus générale grâce aux systèmes dynamiques chaotique, ce qui en fait l'originalité. En perspective, en utilisant cette approche, on pourra développer un algorithme de compression qui sera associé à la probabilité conditionnée d'apparition des symboles à un ordre supérieur.

Références bibliographiques

[1] M. SAIDI, *Etude dynamique d'une application discrete du plan,* Mémoire de Magister , Université de M'sila, 2012.

[2] H. HAMICHE, *Inversion à Gauche des Systèmes Dynamiques Hybrides Chaotiques.Application à la Transmission Sécurisée de Données,* Thèse doctorat ,Tizi ouzou :Université Mouloud Mammeri, 2011.

[3] O. MEGHERBI, *Etude et réalisation d'un système sécurisé à base de systèmes chaotiques,* Mémoire de Magister , Tizi-Ouzou:Uuniversité Mouloud Mammeri,2013.

[4] B. L. MIHAI, *Apports du chaos et des estimateurs d'états pour la Transmission sécurisée de l'information,*Thèse doctorat, Université de Bretagne Occidentale, 2003.

[5] E. N. LORENZ, «*Deterministic Nonperiodic Flow*,» journal of the atmospheric sciences, vol. 20, pp. 130-141, 1963.

[6] M. A. DJENOURI et M. A. CHIKHI, *communication securisee par chaos: Etude et implementation sur la carte FPGA,* Mémoire de Master,Blida:Université Saad Dahleb, 2014.

[7] N. KHODOR, *Application des fonctions génératrices de chaos à la réalisation de codeurs du canal,*Thèse doctorat,Limoges, 2010.

[8] M.-a. JAMEEL, *The numerical solution of fractional differential chaotic system,* Université de Mutah,2009.

[9] H. A. M.AIT, *Etude et realisation d'un systeme chaotique base sur le circuit de Chua,* Mémoire de Master ,Tizi-Ouzou:Université Mouloud Mammeri, 2014.

[10] A. BOUKABOU, *Méthodes de contrôle des systèmes chaotiques d'ordre élevé et leur application pour la syncronisation:Contribution à l'élaboration de nouvelles approches,*Thèse doctorat, Université de Constantine, 2006.

[11] M. CHERIF, *Capacité d'un memoireassociative a fonction de sortie chaotique,*Mémoire de Master, Université du Quebec à Montreal, 2010.

[12] H. ELHACHI, *Sécurisation de la couche physique OFDM dans un réseau de capteurs: application sur les images médicales,* Mémoire de Master ,Guelma: Université 8 mai 1945, 2019.

[13] C. BENHABIB, *Etude d'un système chaotique pour la sécurisation des communications optiques ,* Thèse doctorat,Tlemcen, 2014.

[14] A. R. KIHAL, *Systèmes chaotiques pour la transmission sécurisée de données,*Mémoire de Magister ,Biskra:Université Mohamed Khider, 2013.

[15] M. KRIM, *Implémentation des séquences chaotiques sur les systèmes de communication moderne :Etalement de spectre à séquence directe DS-SS.,* Thèse doctorat ,Oran:Université Mouhamed Boudyaf , 2019.

[16] OPPENHEIM,V.ALAN «*Signal processing in the context of chaotic signals.*,» Proc.IEEE ICASSP.vol.4,1992.

[17] Y. TAO, *A survey of chaotic secure communication systems*, vol. 2, n°12, pp. 81-130, 2004.

[18] L. PECORA et T, CARROLL, *Driving systems with chaotic signals*. Physical Review A, 1991, pp. 2374-2383.

[19] G. Kolumbân, M. Kennedy et L. Chua, *The role of synchronization in digital communications using chaos,—Part II: Chaotic modulation and chaotic synchronization.* IEEE Trans. Circuits Syst. I, Fundam. Theory Appl, 1998.
45(11): p. 1129-1140.

[20] S. ATWAL, *Un système de communication a faible probabilite d'interception base sur la modulation chaotique,* Mémoire professionnel ,Quebec:Ecole de technologie superieure 2010.

[21] H. N. BELLAHBIB et I. ABDELLI, *L'exploitation du chaos numerique dans les transmissions securisées,* Mémoire de master,Tlemcen: Université Abou-Bekr Belkaid ,2017.

[22] B. AKBIL, *Optimisation des performances des techniques d'accès multiple par l'utilisation des systèmes chaotiques et par regroupement des utilisateurs,* Thèse doctorat,Rabat:Université Mohamed-V,2016.

[23] N. W. ABDERAHIM, *Étude et conception d'un modèle chaotique dédié aux transmissions chiffrées,*Thèse doctorat, Tlemcen: Université Abou-Bekr Belkaid , 2015.

[24] C. SHANON, «Communication theory of secrecy systems*,» *The Bell system technical journal*, vol. 28, n° %14, pp. 656-715, 1949.

[25] «Comment Ça Marche - Communauté informatique,» 2007. [En ligne]. Available: https://web.maths.unsw.edu.au/~lafaye/CCM/video/compress.htm.

[26] u. patent, *Arthmetic coding and decoding methods and related systems,* 2003.

[27] L. Mihai Bogdan, S. Alexandru, A. Stéphane et B. Gilles, *A new compression method using a chaotic symbolic approach,* Bucharest, Romania,: IEEE communications, 2004.

[28] B.-L. Hao, Elementary symbolic dynamics and chaos in dissipative systems, world scientific, 1989.

[29] Y. Lau, *Technique in Secure Chaos Communication,* School of electrical and computer engineering science,RMIT university, 2006.

Compression de l'information à l'aide de systèmes chaotiques

Résumé

Dans ce modeste mémoire notre travail consiste à étudier une méthode de compression basée sur une approche symbolique qui permet d'associe à chaque séquence informationnelle une trajectoire dans l'espace d'états du générateur chaotique. On a introduit également un nouveau type de générateur chaotique adapte à la distribution de probabilité de la séquence informationnelle, et en utilisant le générateur décrit les performances de compression théorique atteignent la compression d'entropie optimale. Enfin, nous confirmons l'analyse théorique avec des tests de performance pour deux différentes séquences avec différentes probabilités symbolique.

Mot clés: chaos, dynamique symbolique, générateur probabiliste de Bernoulli.

Abstract

This work consists in studying a method of compression method based on a symbolic approach which allows to associate each information sequence with a trajectory in the state space of the chaotic generator. A new type of chaotic generator adapted to the probability distribution of the informational sequence is introduced, and prove to ourselves that by using the described generator the theoretical compression performances reach the optimal entropy compression. Finally, we confirm the theoretical analysis with performance tests for two different sequence with different symbolic probabilities.

Keywords: chaos , symbolic dynamics, probabilistic Bernoulli generator,

ملخص

يخص هذا العمل دراسة نموذج خاص بضغط المعلومة، لذلك تم استخدام نوع معين من التعديل الفوضوي.مع ادخال نوع من الترميز الذي يسمح بإرفاق مسار تسلسل المعلومات بحالات مولد الفوضى(chaos)، الذي يتكيف مع التوزيع الاحتمالي للتسلسل المعلوماتي، ولتقييم مدى حسن أداء هذا النموذج من الضغط النظري تم انجاز حسابات رياضية تضمن تحقق مبدأ الانتروبيا الأمثل. أخيرًا، نؤكد التحليل النظري باختبارات الأداء لتتابعين مختلفين باحتمالية رمزية مختلفة.

كلمات مفتاحية: الفوضى، ديناميات رمزية، مولد برنولي الاحتمالي.