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

N° Série : .....

Mémoire de fin d'étude

Présenté pour l'obtention du diplôme de Master

Filière : Télécommunications
Spécialité : Systèmes des Télécommunications

THEME

Cryptage chaotique d'une image en utilisant l'oscillateur de sprott.

Réalisé par : *-Reghis Rania.*
- Ramdani Nour Elhouda.

Devant Le Jury :

Président	*Dr. Bouras Moustafa*	***Université Abbes Laghrour- Khenchela***
Encadreur	*Dr. Maamri Fouzia*	***Université Abbes Laghrour- Khenchela***
Examinateur	*Dr. Friha Souad*	***Université Abbes Laghrour- Khenchela***

Promotion 2022/2023.

Dédicace

Tous les mots ne sauraient exprimer la gratitude, l'amour, le respect, la reconnaissance, c'est tout simplement que

Je dédie ce travail a

Nos chers parents Pour leur patience, leur soutien et leurs encouragements.

A nos frères et sœurs qui n'ont cessé de nous conseiller, de nous encourager et de soutenir tout au long de notre étude.

Que Dieu les protège et leur offre la chance et le bonheur.

A nos proches, nos familles, a tous ceux qui nous ont aidés de près ou de loin.

NOUR ELHOUDA ET RANIA

Remerciements

*Nous remercions avant tout **DIEU Allah** tout puissant pour la volonté, le courage et la patience qu'il nous a donnée afin de réaliser ce modeste travail.*

*Nous exprimons notre plus grande reconnaissance et notre respect à notre encadreur **Mme MAAMRI FOUZIA**, pour avoir accepté de diriger ce travail et nous guider tout au long de son développement, de nous avoir guidé et soutenu avec patience, pour ces lectures enrichissantes de notre mémoire et pour les précieux conseils.*

Nous tiendrons également à remercier tous les membres du jury, de l'honneur qu'ils nous ont fait en acceptant d'être membres du jury de ce modeste travail .

Enfin, Je remercie tous les professeurs du Faculté génie industriel : systèmes des télécommunication, Université Abbes Laghrour-Khenchela.

Résumé

Les besoins pour sécuriser les informations reste toujours en croissance. Pour cette raison, plusieurs systèmes cryptographiques ont été développés pour satisfaire ces besoins.

Dans ce mémoire on s'intéresse à la sécurisation de l'information par le chaos dû aux caractéristiques de ces systèmes tels que la sensibilité aux conditions initiales et leurs trajectoires qui sont considérés comme un bruit pseudo aléatoire.

Ce travail implique l'utilisation de signaux chaotiques de Sprott pour crypter les images. Ce signal doit être mélangé par le signal à transmettre pour le crypter et protéger ce dernier en utilisation l'algorithme Runge kutta.

Les résultats de simulation à l'aide du logiciel Matlab, nous montrent la robustesse de cryptage et de décryptage chaotique.

Mots clés

Cryptage, Décryptage, Runge kutta. Chaos, Sprott.

Abstract

Information security needs are constantly growing. For this reason, several cryptographic systems have been developed to satisfy these needs.

In this work we are interested in the security of information by the chaos due to the characteristics of these systems such as the sensitivity to the initial conditions and their trajectories, which are considered as a pseudo rando noise.

This work involves the use of chaotic Sprott signals to encrypt images. This signal must be mixed with the signal to be transmitted to encrypt it and protect it using the Runge kutta algorithm.

Simulation results in Matlab show us the robustness of chaotic encryption and decryption.

Key words

Encryption, Decryption, Runge kutta, Chaos, Sprott.

ملخص

احتياجات امن المعلومات تتزايد باستمرار. لهذا السبب، تم تطوير العديد من أنظمة التشفير لتلبية هذه الاحتياجات.

الهدف من هذا العمل في إطار الأطروحة هو أننا نهتم بأمن المعلومات من خلال الفوضى بسبب خصائص هذه الأنظمة مثل الحساسية للظروف الأولية ومساراتها التي تعتبر ضجيجًا عشوائيًا زائفًا.

يتضمن هذا العمل استخدام إشارات Sprott الفوضوية لتشفير الصور ويجب مزج هذه الإشارة مع الإشارة المراد إرسالها لتشفيرها وحمايتها باستخدام برنامج Matlab باستخدام خوارزمية Runge kutta.

تظهر لنا نتائج المحاكاة متانة التشفير وفك التشفير.

الكلمات المفتاحية

التشفير، فك التشفير، Runge Kutta، الفوضى، Sprott.

Sommaire

Sommaire

Chapitre II : *Etude du cryptage.*

Chapitre III : *Cryptage par chaos*

Liste des figures

Liste des tableaux

Symboles mathématique

$\mathbf{x_0, y_0, z_0}$ **:** *Conditions Initiales D'un Système d'équations différentielles*

$\mathbf{x, y, z}$ **:** *Les variables d'états d'un système d'équations différentielles*

$\mathbf{a, b, c}$ **:** *Paramètres du système de Hénon, Lorenz, Rössler*

Somme algébrique

$\mathbf{R^n}$ **:** *Espace vectorielles de dimension n.*

$\mathbf{R^p}$ **:** *Espace vectorielles de dimension P.*

$\mathbf{R^+}$ **:** *Ensembles des nombres réels positifs.*

$\mathbf{Z^+}$ **:** *Ensembles des nombres entiers positifs.*

R : *Ensemble des nombres réels.*

$\boldsymbol{x_0}$ **:** *L'état initial.*

$\boldsymbol{x_k}$ **:** *L'état x au temps t=k.*

$\dot{\boldsymbol{x}} = \frac{\boldsymbol{dx}}{\boldsymbol{dt}}$ **:** *Dérivée de la variable x par rapport au temps.*

$\boldsymbol{\tau}$**:** *Temp le retard positif.*

$\mathbf{x(t)}$ *et* $\mathbf{x'(t)}$ **:** *l'état de système émetteur et récepteur .*

Lim: *Limite.*

$\mathbf{u(t)}$ **:** *L'entrée inconnues.*

$\boldsymbol{Q_1}$ **à** $\boldsymbol{Q_7}$ **:** *Paramètre du système de sprott.*

$\boldsymbol{f_1}$ **et** $\boldsymbol{f_2}$ **:** *des fonctions non linéaires.*

$\boldsymbol{S_1}$ **et** $\boldsymbol{S_2}$ **:** *de système chaotiques.*

$\dot{\boldsymbol{x}}$ **(t) :** *L'état du système maître (S1).*

$\hat{x}$ **(t) :** *L'état du système esclave (S2).*

V **:** *vecteur du paramètre.*

v_{cc} **:** *est la tension de polarisation utilisée.*

Liste des abréviations

AOP : *Amplificateur opérationnel.*

BMP : *C'est une abréviation du mot bitmap.*

CSK: *Chaos shift Keying.*

CGM: *Computer Graphics Metafile.*

JPEG: *Joint Photographic Experts Group.*

GIF: *Graphics Interchange Format.*

TIFF : *Tag Image File Format.*

XOR: *Exclusive OR.*

WMF: *Windows Metafile Format.*

m(t): *message informatif.*

y(t): *signal porteuse chaotique plus message.*

s(t): *le signal de transmission.*

c(t): *Le signal chaotique.*

Introduction générale

Introduction générale

Le développement de la technologie a conduit à l'apparition d'une révolution dans les systèmes de communication dont les utilisateurs exigent une authentification et une protection de leurs données confidentielles et sensibles. Tout système de communication efficace nécessite un système de sécurité pour le protéger. Pour cela, de nouvelles méthodes de cryptage ont été développées. Le chiffrement des informations assure la sécurisation, la confidentialité des systèmes de transmission de données, en masquant le contenu du message transmis de manière à le rendre illisible et imperceptible aux personnes non autorisées à en connaître ce contenu.

Les méthodes de cryptage reposées sur des algorithmes de calcule qui admette une certaine efficacité et rapidité pour chiffrer ou déchiffrer l'information, devenue aujourd'hui avec le développement des techniques de cryptanalyse et la montée des calculateurs, faible en prenant un temps de calcule long. Ce qui a poussé les chercheurs à élaborer de techniques de cryptage efficace : la cryptographie chaotique.

Les systèmes dynamiques chaotiques sont des systèmes déterministes non linéaires, non périodiques et éventuellement finis. Les signaux qui évoluent dans ces systèmes sont généralement à large bande, leur sortie est pseudo aléatoire et est très sensible aux conditions initiales. En raison de ces propriétés et de la fragilité des systèmes de codage classiques, il est probable que les signaux chaotiques fourniront une classe importante de signaux qui peuvent être utilisés pour masquer des informations dans une transmission sécurisée, il suffit donc de les mélanger de manière appropriée avec l'information.

Le cryptage chaotique noyer un message dans un signal chaotique pour faire face à d'éventuelles tentatives de piratage en insérant le chaos dans les systèmes de communication. Cette technique de communication est faite avec une clé secrète, la connaissance de cette clé est nécessaire de la part de l'expéditeur du message ainsi que de la part du destinataire pour chiffrer et déchiffrer le message. Il faut alors agir au niveau du récepteur.

Ce mémoire est organisé en trois chapitres répartis comme suit :

Introduction Générale

Dans le premier chapitre, nous présenterons quelques concepts importants de la théorie des systèmes chaotiques, nous allons définir les systèmes dynamiques qu'ils soient en temps continu ou en temps discret Où nous apporterons quelques notions de base, tel que l'illustration des caractéristiques des systèmes chaotiques.

Dans le deuxième chapitre, nous aborderons le principe de la cryptographie et ses objectifs ainsi que ses deux types à savoir cryptographies symétrique et asymétrique. Nous allons présenter également la synchronisation et leurs déférentes méthodes.

Dans le dernier chapitre nous allons achever notre travail par une simulation du système de sprott à l'aide du logiciel Matlab en utilisation l'algorithme Runge kutta, ensuite nous utiliserons ces signaux chaotiques pour chiffrer les images.

Nous terminerons notre travail par une conclusion générale.

Chapitre I:

Etude des systèmes non linéaires chaotiques

I.1.Introduction

Le terme chaos définit un état particulier d'un système dont le comportement ne se répète jamais qui est très sensible aux conditions initiales, et imprédictible à long terme. Des chercheurs divers ont alors commencé à s'intéresser à ce comportement. Le chaos a ainsi trouvé de nombreuses applications dans les domaines tant physiques que biologique, chimique ou économique ainsi qu'électronique.

Dans ce chapitre, nous nous intéresserons principalement aux systèmes dynamiques chaotiques en espaces de phases, en fonction de t, les attracteurs étranges et les scénarios de transition vers le chaos où bifurcations pour mieux comprendre le phénomène chaotique.

I .2. Système dynamique

Un système dynamique est un système physique dont l'état (ensemble des grandeurs suffisant à qualifier le système) évolue en fonction du temps. L'étude de l'évolution d'un système dynamique nécessite donc la connaissance :

- De son état initial : valeurs de ses grandeurs caractéristiques à l'instant initial de l'étude.
- De sa loi d'évolution : équations différentielles reliant ses grandeurs caractéristiques.

Ses grandeurs caractéristiques sont donc des grandeurs physiques fonctions du temps.

Un système dynamique peut être vu comme un processus transformant un signal d'entrée en un signal de sortie **[1]**.

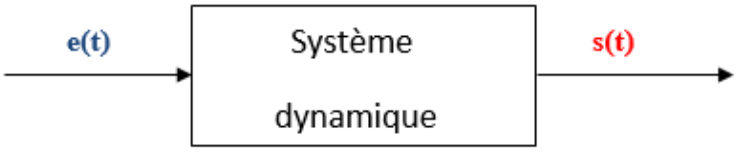


Figure I.1 : Système dynamique **[1].**

Du point de vue mathématique, les systèmes dynamiques sont classés en deux catégories :

• Systèmes dynamiques continus.

• Systèmes dynamiques discrets.

I.2.1. Systèmes dynamiques continus

Dans le cas continu un système dynamique est présenté par un système d'équations différentielles de la forme :

$$\frac{dx}{dt} = \dot{x} = f(x, t, v) \qquad \text{(I .1)}$$

Où $\mathbf{x} \in \mathbf{R^n}$ et $v \in \mathbf{R^p}$ où $\mathbf{f} : \mathbf{R^n} \times \mathbf{R^+} \rightarrow \mathbf{R^n}$ désigne la dynamique du système **[15]**.

I.2.2. Systèmes dynamiques discrets

Un système dynamique dans le cas discret, est représenté par des équations aux différences, appelées également « équations de récurrences » **[5].**

$$x(k+1) = g(k, x(k), x(k_0)) = x_0 \qquad \text{(I .2)}$$

Où K est l'instant discret, k_0 est l'instant discret initial, x_0 est le vecteur des états initiaux et $\mathbf{g} : \mathbf{R^n} \times Z^+ \rightarrow R^n$ indique la dynamique du système en temps discret.

I.2.3. Systèmes autonomes ou non autonome

Si le champ de vecteurs ne dépend pas explicitement du temps, le système dynamique est autonome. Sinon il est non autonome. Un système dynamique non autonome de dimension n peut être transformé en un système dynamique autonome de dimension n+1 [**8].**

I.2.4. Notions sur les systèmes dynamiques

- **Système autonome** : un système est dit autonome lorsqu'il ne dépend pas explicitement du temps **[5]**.
- **Causalité :** un système est dit « causal », lorsque son entrée ne précède jamais sa sortie.
- **Trajectoire temporelle** : représente une grandeur décrite en fonction du temps qui peut être par exemple une variable d'état ou une sortie.
- **Trajectoire de phase** : est une trajectoire représentée sur une plane phase et qui décrit l'évolution du système au cours du temps pour des conditions initiales données.

- **Espace de phase :** est un espace mathématique, souvent multidimensionnel, dont chaque axe de coordonnées correspond une variable d'état du système dynamique étudié.

- **Portrait de phase :** est constitué par l'ensemble des trajectoires de phase possibles d'un système dynamique.
- **Point d'équilibre (ou point fixe)** : on appelle point d'équilibre d'un système le point x∗ pour laquelle on obtient f (x ∗) = 0 dans le cas continu, g(x ∗) = x ∗ dans le cas discret.
- **Cycle limite** : est un phénomène non linéaire, qui peut être siège d'oscillations, auto soutenues, Caractérisées par leur amplitude et leur période fixes, indépendante de la condition initiale x0 et sans excitation extérieure.
- **Tore :** est un cas particulier du cycle limite qui représente les mouvements résultants de deux ou plusieurs oscillations dépendantes que l'on appelle aussi « mouvements quasi-périodiques », la trajectoire de phase ne se referme pas sur elle même.
- **Attracteur :** est une forme géométrique de l'espace de phase vers lequel tendent les trajectoires de phase.

I.3. Système non linéaire

La plupart des systèmes physiques ne sont pas linéaire. En Effet de nombreuses caractéristiques conduisent à des non linéarités. Un système est dit non linéaire s'il ne respecte pas le principe de superposition et si la relation entre les grandeurs d'entrée et de sortie est une équation différentielle avec des coefficients non constants généralement. Il peut être représenté par un système de la forme suivante **[11].**

Equation d'état : $\dot{\boldsymbol{x}}(\boldsymbol{t}) = (\boldsymbol{x}(\boldsymbol{t}), \boldsymbol{u}(\boldsymbol{t}))$ (I.3)

Equation de sortie : $\boldsymbol{y}(\boldsymbol{t}) = \boldsymbol{h}(\boldsymbol{x}(\boldsymbol{t}), \boldsymbol{u}(\boldsymbol{t}))$ (I.4)

I.4.Etude de système de chaos

I.4.1. La théorie du chaos

La théorie du chaos s'applique à de nombreux modèles développés pour expliquer des situations rencontrées dans presque tous les domaines de la connaissance scientifique. L'étude du chaos touche donc de larges champs de recherche, allant de la physique à la psychologie, en passant par l'économie et la biologie. Elle donne un cadre mathématique permettant une étude quantitative (chiffrée) de phénomènes auparavant étudiés de manière qualitative. Comprendre les systèmes chaotiques permet notamment de connaître les limites des modèles utilisés Mathématiquement **[2]**.

Le chaos Décrit le comportement des systèmes apériodiques sensibles aux conditions initiales. Dans ces systèmes, un petit changement dans les conditions initiales a d'importantes conséquences sur le comportement à moyen terme **[2]**.

I.4 .2. Définition du chaos

Le chaos est une propriété qui émerge lors de l'étude des systèmes dynamiques. Il apparaît dans des systèmes non linéaires discrets (comme la suite logistique) ou continus à plus de 3 degrés de liberté (comme le système de Lorenz).

La représentation graphique des solutions de ces systèmes conduit souvent à des structures caractéristiques appelées « attracteurs étranges », comme le papillon de Lorenz représenté ci- contre :

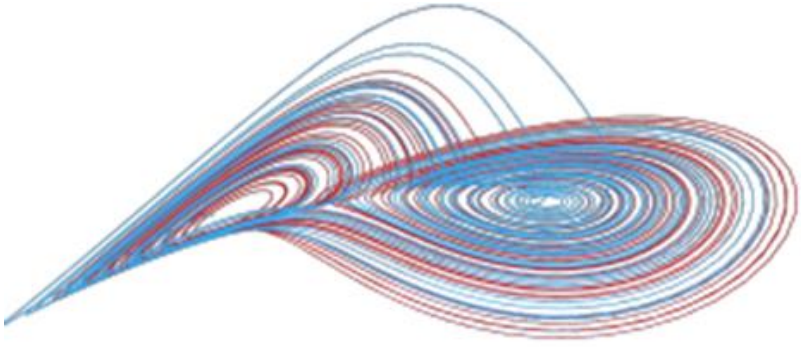


Figure I.2 : papillon de Lorenz.

I.4.3. Historique de chaos

1890	Le Roi Oscar II de Suède octroie un prix au premier chercheur qui pourrait déterminer et résoudre le problème des n-corps des orbites des corps célestes et ainsi prouver la stabilité du système solaire.
1890	Henri Poincaré gagne le premier prix du Roi Oscar II. Etant le plus comportement instable et imprévisible. Ainsi, le chaos est naît.
1963	Edward Lorenz découvre le premier système chaotique dans la météo ou encore appelé affracteur étrange.
1975	Tien Yien et James A. York ont présenté pour la première fois le terme ‘’chaos’ dans un article intitulé ‘’Période Three implies chaos’’.
1978	Mitchell Feigenbaum introduit un nombre universel associé au chaos.
1990	Edward Ott, Celso Grebogi et James A. York. Introduisent la notion de Contrôle du chaos.
1990	Lou Pecora. Synchronisation des systèmes chaotiques

Tableau I. 2: Historique du chaos**[4].**

I.4.4. Système chaotique

Un système dit chaotique est un système déterministe mais dont la sortie semble aléatoire et qui est très sensible aux conditions initiales. Pour être chaotique, le système doit être au minimum d’ordre 3 (3 états) et la sommation des valeurs propres sur toute la trajectoire du système doit conduire à deux valeurs propres négatives et une valeur propre positive.

L'évolution de la trajectoire passe donc par un état d'expansion puis de rétraction. De par une non linéarité active, tout se passe comme si le système revenant vers un état stable, reçoit une quantité d'énergie avant d'être de nouveau dissipatif **[3]**.

I .4.4.1. Les types du système dynamique chaotique

Après la découverte de l'attracteur de Lorenz en 1963, les chercheurs et les experts ont attiré par le domaine du chaos, donc plusieurs sortes de système chaotique et hyper chaotique ont été présentés par la suite **[9]**.

a) Les systèmes chaotiques continus

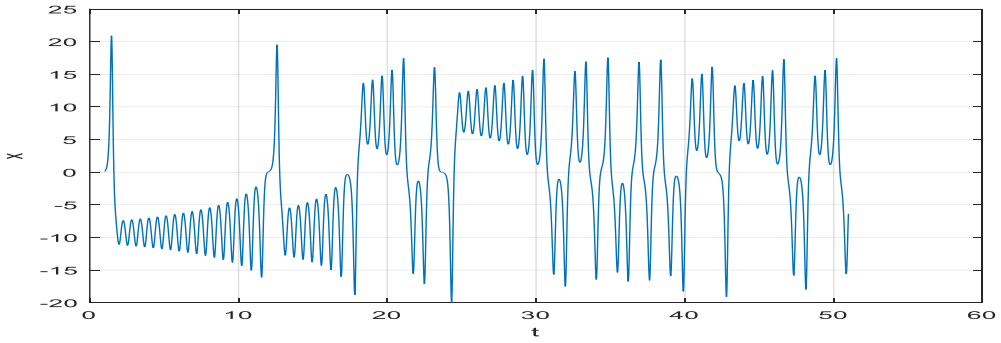
En 1963 Lorenz découvre que l'on peut obtenir un comportement chaotique avec seulement trois variables, soit un système non linéaire à trois degrés de liberté.

Il montre donc qu'une dynamique très complexe peut apparaître dans un système formellement très simple, ç'est le système de Lorenz. On peut considérer : le système de Lorenz, le système de Rössler et l'oscillateur de Chua.

- On obtient le système de Lorenz et Rössler comme exemple des systèmes chaotiques continus qui définit par **[9]**:

$$\begin{cases} \dot{x} = \sigma(y - x) \\ \dot{y} = x(\rho - z) \\ \dot{z} = xy - bz \end{cases} \tag{I.5}$$

Les figures suivantes représentent le comportement chaotique de système de Lorenz, La figure (I.2) représente la variation des états x, y et z d'une façon erratique :



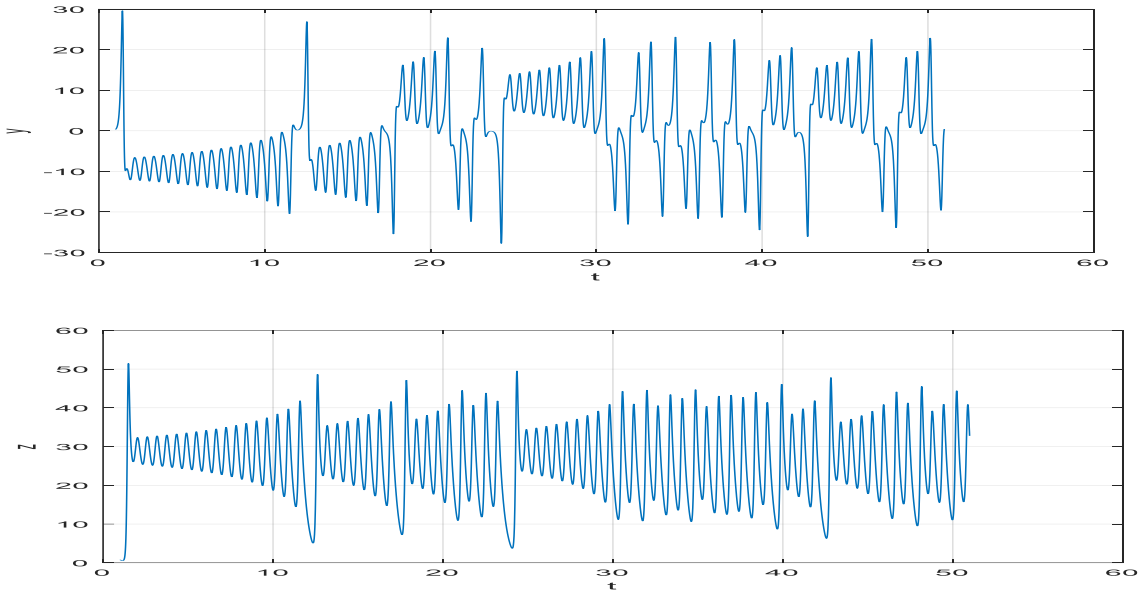


Figure I.3 : L'évolution des états x, y et z du système de Lorenz au cours du temps.

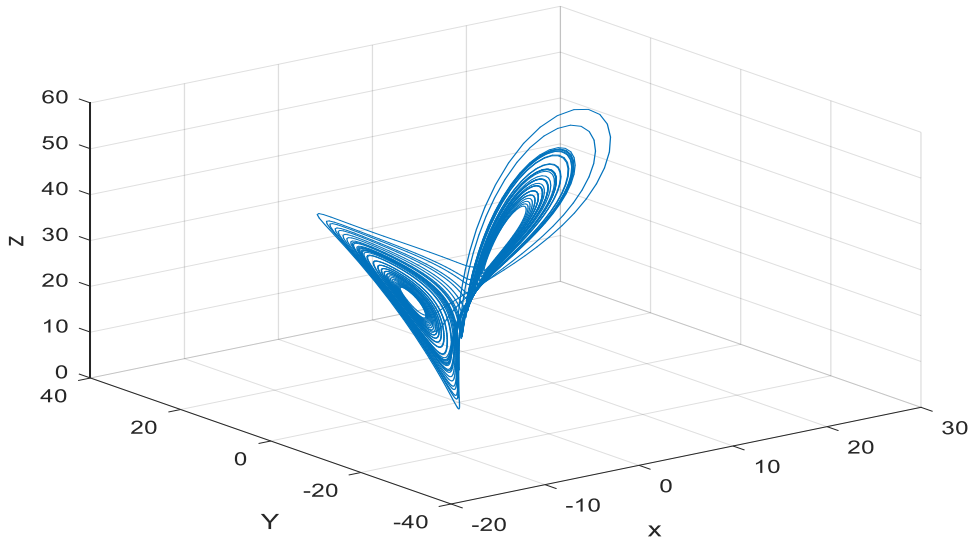


Figure I.4 : L'attracteur étrange de Lorenz.

❖ **Système de Rössler**

Le système de Rössler est donné par l'équation suivant travaux en cinétique chimique :

$$\begin{cases} \dot{x} = -y + z \\ \dot{y} = x + Ay \\ \dot{z} = Bx + xz - cz \end{cases} \quad \text{(I.6)}$$

x, y, et z sont les variables d'états du système .a, b, c sont les paramètres réels. Les paramètres et les conditions initiales de cette équation ont été choisis de la manière suivante : **A=0.2, B=0 ,3, c=6, (x0, y0, z0) = (0. 3, 0.8, 0.4).**

L'ensemble des trajectoires de ce système définissent un attracteur étrange aux propriétés fractales sur le long terme :

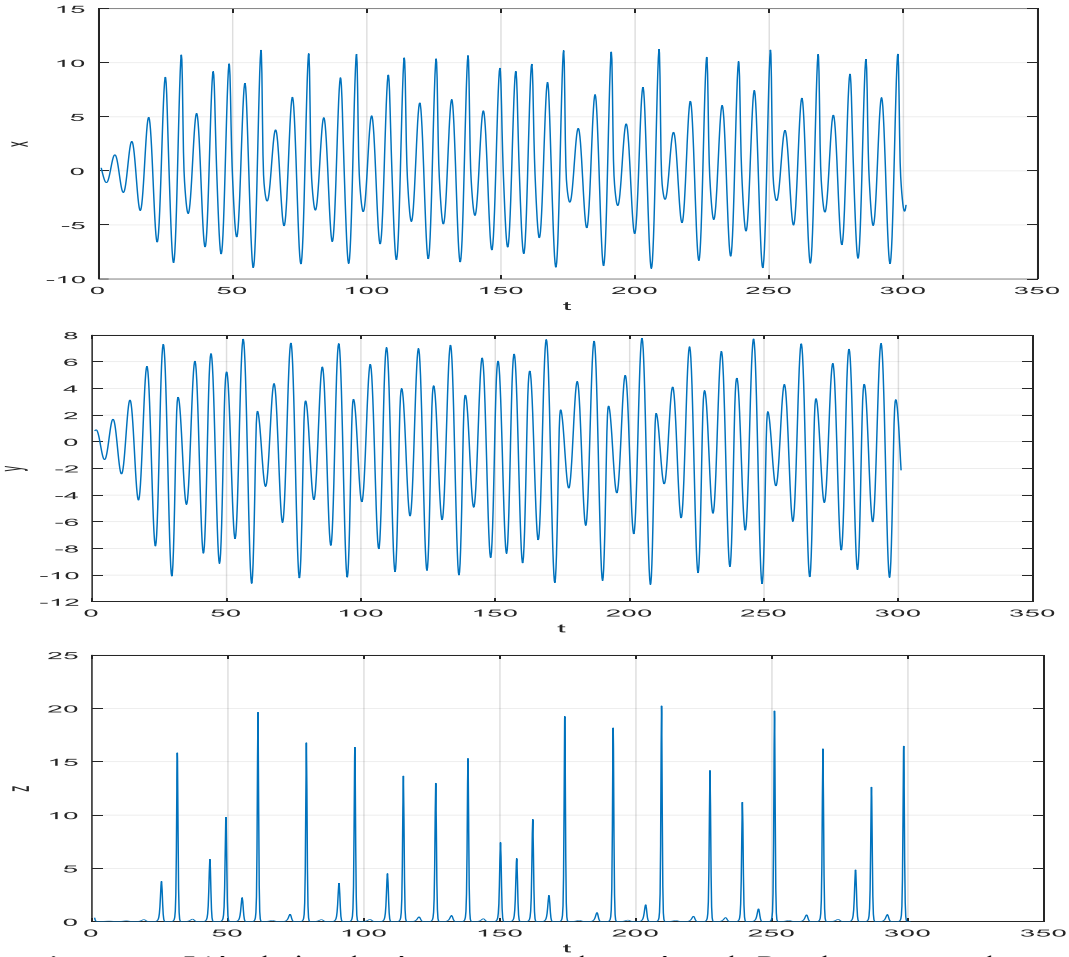


Figure I.5: L'évolution des états x, y et z du système de Rössler au cours du temps.

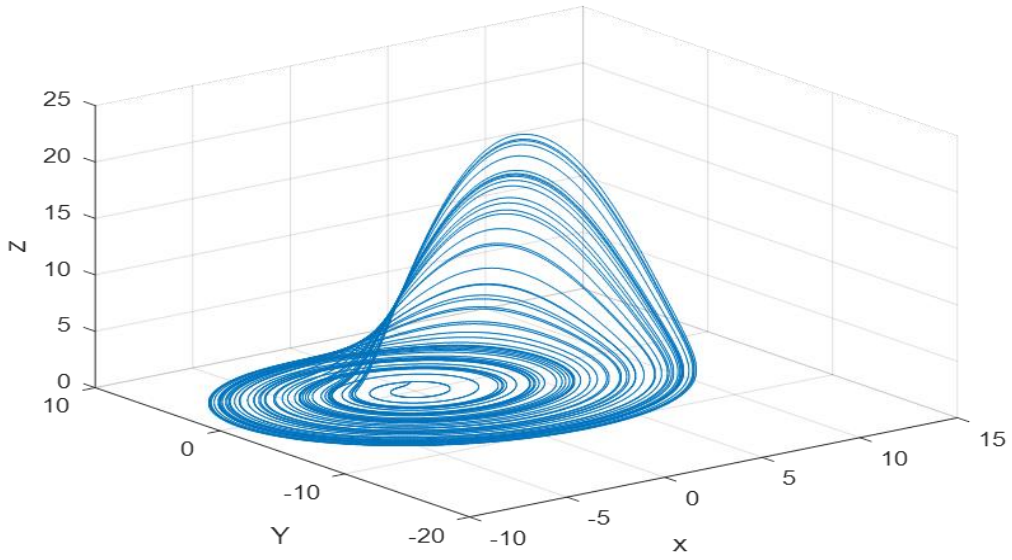


Figure I.6 : l'attracteur étrange de Rössler.

b) Les systèmes chaotiques discrets

Le système chaotique discret veut dire que les variables n'évoluent pas d'une manière continue. La fonction logistique est parmi les systèmes chaotiques discrets les plus connus, elle est une des systèmes de Tchebychev, il existe d'autres systèmes comme la fonction Tent, la fonction Gaussienne discrète et le système de Henon.

On obtient le système de Henon comme exemple

$$\boldsymbol{x_{(n+1)=(y_{(n)+1})-(a*x_{(n)})}} \qquad \text{(I.7)}$$

$$\boldsymbol{y_{(n+1)} = b \times x_{(n)}} \qquad \text{(I.8)}$$

Puis on prend les valeurs suivantes pour la réalisation de système : **a = 1.4, b = 0.3**, avec l'initialisation par : **x (1) = y (1) = 0.1.** Les figures qui convient représentent le comportement chaotique du système de Henon pour les paramètres précédents.

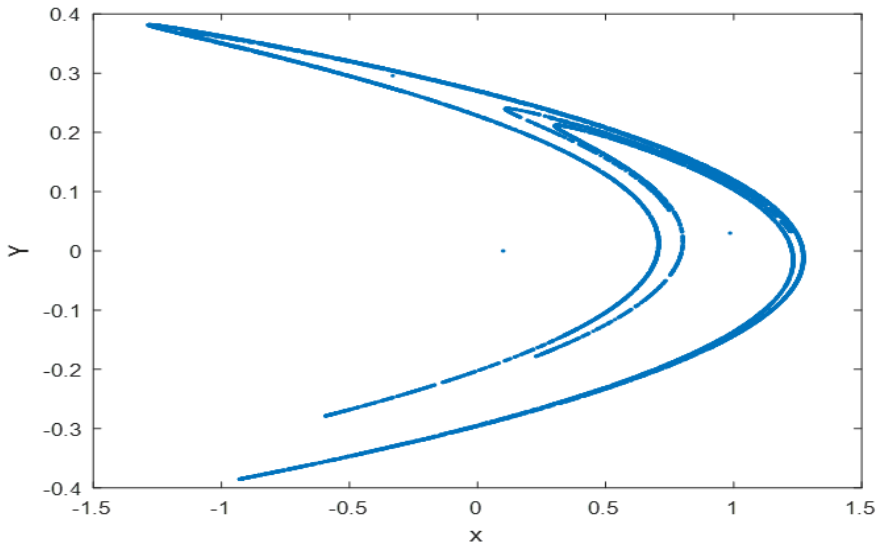


Figure I.7 : l'attracteur étrange de Henon.

I.4.5. Caractéristiques principales du comportement chaotique [4].

a) Non linéaire

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

b) Déterministe

Un système déterministe est un système dont l'état présent est complétement déterminé par les conditions initiales, en contradiction avec un système stochastique pour lequel l'état présent reflètes conditions initiales avec en plus d'une réalisation particulière d'un paramètre aléatoire.

c) Aspect aléatoire

Tous les états d'un système chaotique présentent des aspects aléatoires. La figure suivante illustre l'aspect aléatoire du système de Rössler.

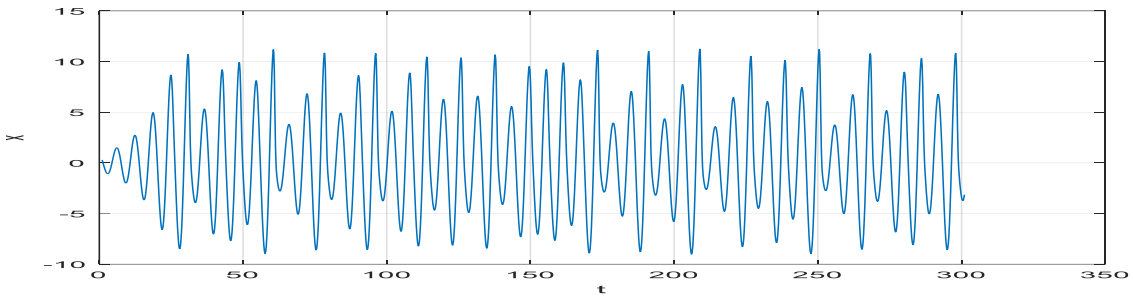


Figure I.8: Aspect aléatoire.

d) Sensibilité aux conditions initiales

Sensibilité aux conditions initiales signifie que chaque point dans un système chaotique est arbitrairement prés approchée par d'autres des points avec sensiblement différentes voies d'avenir, ou trajectoires. Ainsi, un petit changement arbitraire, ou perturbation, de la trajectoire actuelle peut conduire à un comportement futur significativement différente.

e) L'imprévisible

À cause de la sensibilité aux conditions initiales, le système chaotique évolue d'une manière qui semble aléatoire.

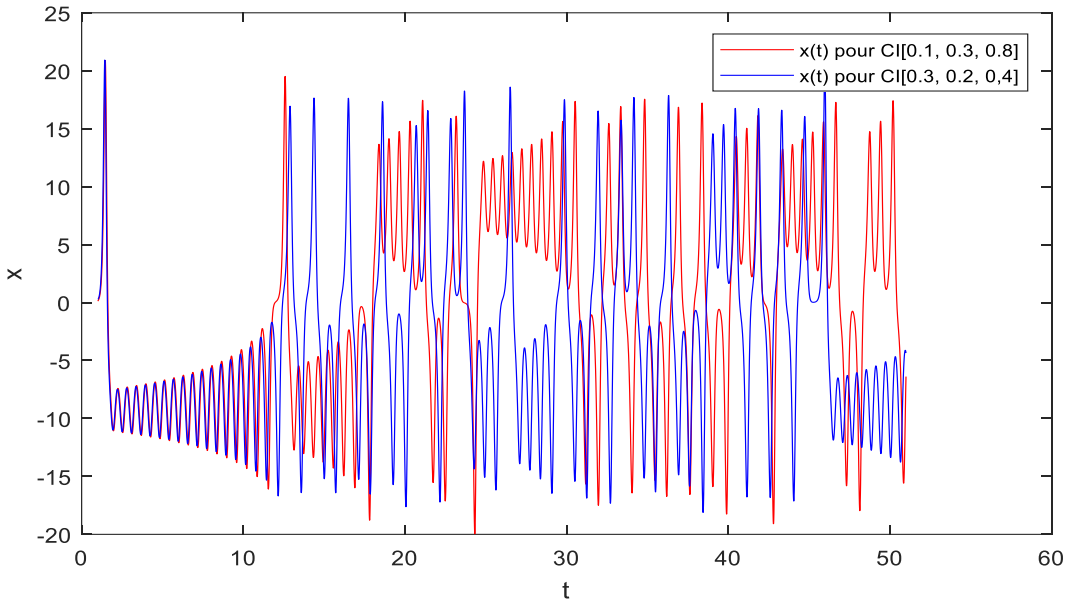


Figure I.9: Illustration de la propriété de sensibilité aux condition initial sur l'état x1.

I.5. L'espace de phase

Dans un système dynamique de dimension **n**, l'espace **x1, x2,** …….. , **xn** est appelé espace de phases ou espace d'états .l'évolution par rapport au temps de système se traduit alors par un déplacement du point représentatif dans l'espace de phase, traçant ainsi une trajectoire de phase et **x1,x2**, ….. , **xn** sont les états du système .Par un point de l'espace de phase ne passe qu'une seul trajectoire .Par conséquent ,deux trajectoires avec deux condition initiales différent ne coïncident jamais au cours du temps **[10]**.

I.6. Les attracteurs

Définition : Un attracteur est un objet géométrique vers lequel tend toute les trajectoires des points de l'espace des phases, c'est à dire une situation (ou un ensemble de situations) vers laquelle évolue un système, quelles que soient ses conditions initiales **[12].**

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

I.6.1. Attracteurs réguliers

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

• **Le point fixe** : est l'attracteur le plus simple (a).

• **Un cycle limite** : qui n'existe que pour les systèmes dynamiques à temps continue, on appelle cycle limite sur un plan ou une variété bidimensionnelle, telle qu'au moins une autre trajectoire spirale à l'intérieur lorsque le temps tend vers $\pm\infty$ (b).

• **Un tore :** Il est caractérisé par un régime quasi−périodique ayant n fréquences de base indépendantes(c).

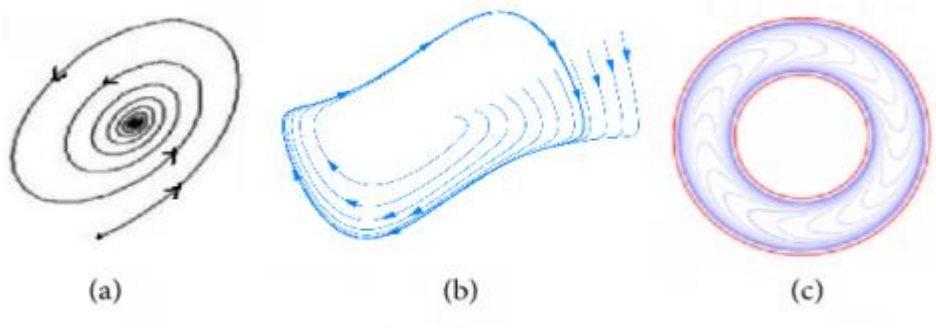


Figure I.10 : Attracteurs réguliers **[12].**

I.6.2. Attracteurs étranges

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

L'attracteur étrange se caractérise par

1. Sensibilité aux conditions initiales (deux trajectoires de l'attracteur initialement voisines finissent toujours par s'éloigner l'une de l'autre, ceci traduit un comportement chaotique) ;

2. La dimension d de l'attracteur est fractals avec $2 < d < n$ (ce qui justifie l'adjectif étrange)

3. L'attracteur est de volume nulle dans l'espace des phases.

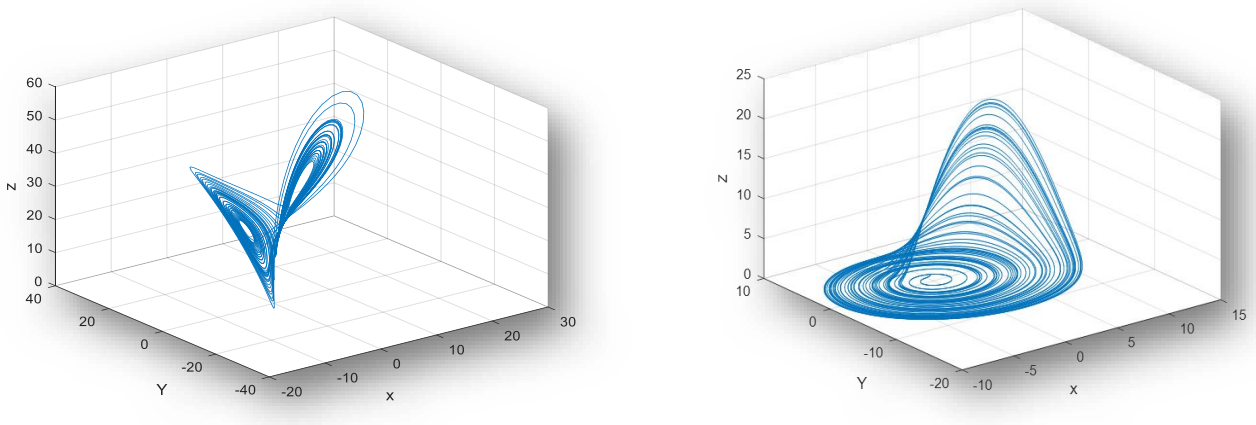


Figure I.11 : Attracteur étrange de Rössler et Lorenz.

I.7. Dimension d'Hausdorff

Un attracteur occupe un volume nul dans l'espace des phases, sa dimension est donc inférieure à celle de l'espace en question, et elle est fractale plus précisément. Pour déterminer cette valeur une méthode simple consiste à recouvrir l'attracteur avec des hyper cubés d'arrête (ε) et examiner le nombre minimum N(ε) de cubes nécessaires à cette opération. La dimension fractale de l'attracteur est donné par la dimension de Hausdorff Besicovutch.

$$\mathbf{D} = \lim_{\varepsilon \to 0} \frac{\ln N(\varepsilon)}{\ln(\frac{1}{\varepsilon})} \tag{I.9}$$

I.7.1. Quelques exemples

• Pour un point, N (ε)=1 et D =0

• Pour un segment S, N(ε) = $\frac{S}{\varepsilon^2}$ et D= 2

Cette détermination permet de caractériser l'aspect d'autocorrélation spatiale ou topologique de l'attracteur, qui ne donne aucun renseignement sur la façon dont une trajectoire va peupler les différentes parties de l'attracteur. Pour mettre en évidence la dynamique du peuplement, on introduit la dimension d'information **[8]**.

I.8. Les exposants de Lyapunov

L'évolution chaotique est difficile à appréhender car la divergence des trajectoires sur l'attracteur est rapide. Pour cette raison on essaye si c'est possible de mesurer sinon d'estimer la vitesse de divergence ou de convergence. Cette vitesse est donnée par l'exposant de Lyapunov qui caractérise le taux de séparation de deux trajectoires très proches.

Donc deux trajectoires dans le plan de phase initialement séparées par un taux $Z1$ Divergent après un temps $\Delta t = t2 - t1$ vers $Z2$ tel que :

$$|Z_2| \approx e^{\lambda.\Delta t} |Z_1| \tag{I.10}$$

En passant à la limite on obtient l'exposant de Lyapunov qui représente le logarithme moyen de l'accroissement **[8]** :

$$\boldsymbol{\lambda \approx \lim_{\Delta t \to \infty} \frac{1}{\Delta t} \ln \frac{|Z_1|}{|Z_2|}} \qquad \text{(I.11)}$$

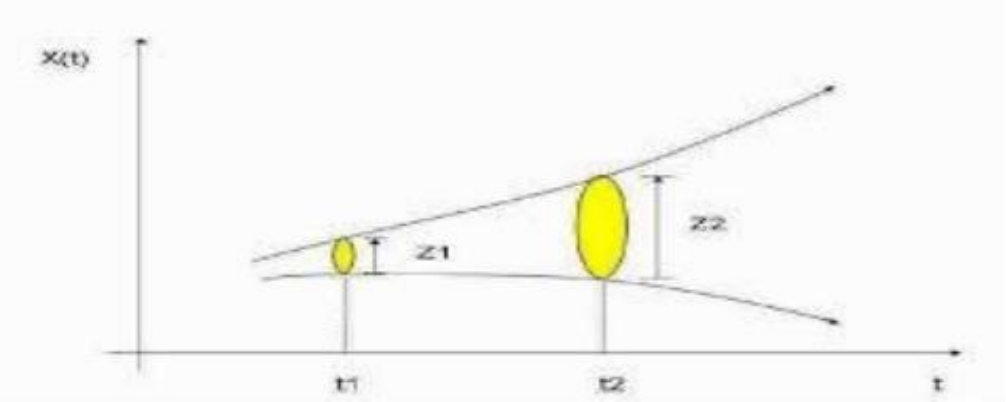


Figure I.12 : Divergence de deux trajectoires dans le plan de phase **[8].**

La classification des comportements des systèmes dynamiques selon les exposants de Lyapunov est représentée sur le tableau suivant **[9]** :

Régime permanent	Attracteur	Exposants de Lyapunov
Point d'équilibre	Point	$\lambda_n \leq \lambda_{n-1} \leq \cdots \leq \lambda_1 < 0$
Périodique	Courbe fermée (Cycle limite)	$\lambda_n \leq \lambda_{n-1} \leq \cdots \leq \lambda_2 < \lambda_1 < 0$
Quasi-périodique	Toer	$\lambda_1 = \cdots = \lambda_i = 0$ $\lambda_n \leq \lambda_{n-1} \leq \cdots \leq \lambda_{i+1} < 0$
Chaotique	Attracteur chaotique	$\lambda_1 > 0$ $\lambda_n \leq \lambda_{n-1} \leq \cdots \leq \lambda_2 \leq 0$
Hyper chaotique	Attracteur chaotique	$\boldsymbol{\lambda_1 > 0 \; et \; \lambda_2 > 0}$ $\lambda_n \leq \lambda_{n-1} \leq \cdots \leq \lambda_3 \leq 0$

Tableau I.2: Comportement des systèmes dynamiques en fonction des Exposants de Lyapunov.

I.9.Bifurcation

Définition1

Soit le système dynamique non-linéaire suivant :

$$\boldsymbol{x(k+1) = F(x(k), \alpha)} \qquad \text{(I.12)}$$

D'où : $\boldsymbol{x(k) \in R^n, \alpha \in R^m, k \in N \text{ et } F : R^n \times R^m \times N \rightarrow R^n}$

Définition2

Une **bifurcation** est un **changement qualitatif** de la solution x du système (1.5) lorsqu'on modifie le **paramètre de contrôle** α, c'est à dire la disparition ou le changement de stabilité et l'apparition de nouvelles solutions.

Définition3

Un diagramme de bifurcation est une portion de l'espace des paramètres sur laquelle sont représentés tous les points de bifurcation **[6]**.

I.9.1. Types de Bifurcations

Il existe plusieurs types de bifurcations selon les propriétés des secondes dérivées de la famille des fonctions $\boldsymbol{F(x(k), \alpha)}$. Chacune de ces bifurcations est caractérisée par une forme normale, qui est l'équation générale typique de ce type de bifurcation **[a, b, c].** Parmi les différents types de bifurcations, pour les systèmes dynamiques discrets, on trouve **[d]** :

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

Cette bifurcation se produit lorsque l'une des deux valeurs propres de $\boldsymbol{DF(x(k), \alpha)}$ est égale **à +1**. Sur le diagramme des bifurcations on observe, dans ce cas, une courbe de points fixes continue tangente à la ligne droite verticale. Deux points d'équilibres existent (un stable et un instable) avant la bifurcation. Après la bifurcation, plus aucun équilibre n'existe.

b. Bifurcation Transcritique :

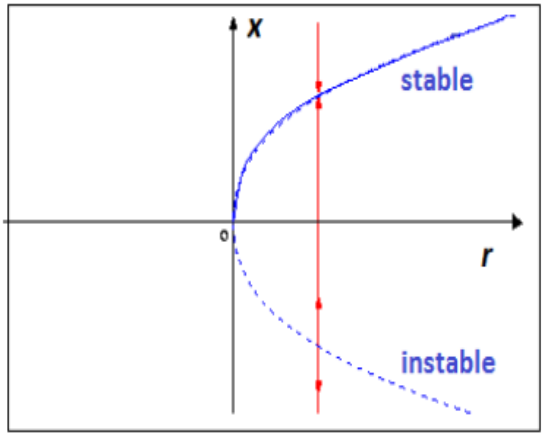
Sur le diagramme de bifurcations cela se traduit par deux branches différentes de points fixes qui se croisent en un point et par le changement de stabilité des deux branches au passage par le point d'intersection.

c. Bifurcation de doublement de période (ou flip) :

Cette bifurcation a lieu lorsque l'une des deux valeurs propres de **DF(x(k), α)** est égales à −1. Un point fixe stable d'ordre 1, devient instable en même temps que l'apparition d'un cycle d'ordre 2 stable.

d. Bifurcation de Neimark-Sacker :

Cette bifurcation se produit lorsque DF(x(k), α) possède deux valeurs propres complexe égale à e ±iθ **[7]**.



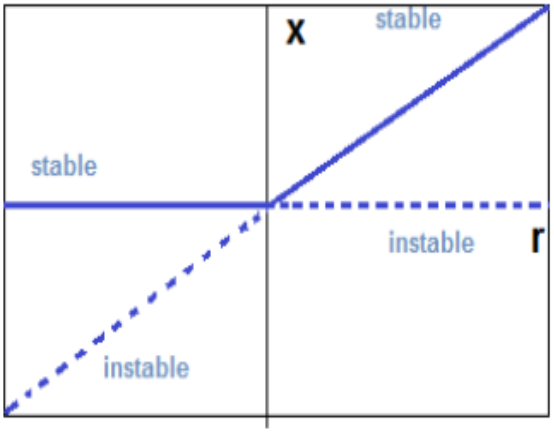


Figure I.13 : Diagramme de bifurcation nœud-col **[16]. Figure I.14 :** Diagramme de bifurcation transcritique **[16]**

I.10. Route vers le chaos

Un système dynamique possède en général un ou plusieurs paramètres dit " paramètre de contrôle", qui agissent sur les caractéristiques de la fonction de transition.

Selon la valeur du paramètre de contrôle, les mêmes conditions initiales mènent à des trajectoires correspondant à des régimes dynamiques qualitativement différents.

La modification continue du paramètre de contrôle conduit dans bien des cas à une complexification progressive du régime dynamique développé par le système **[7]**.

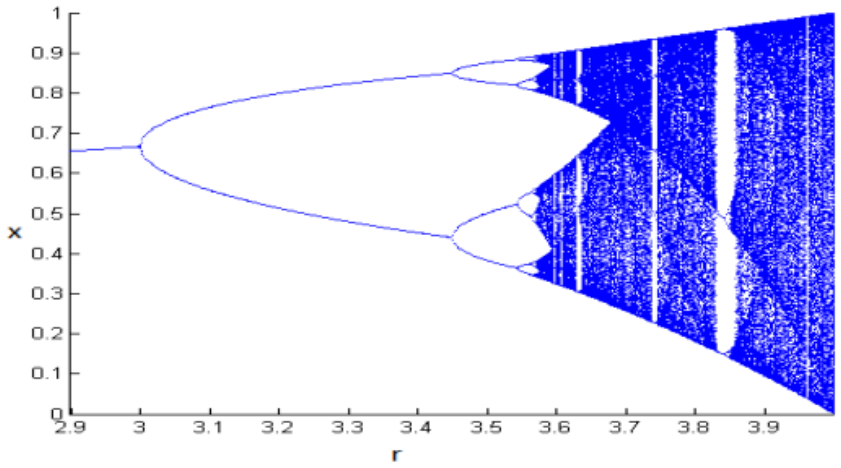


Figure I.15 : Diagramme de bifurcation pour la fonction logistique **[7].**

❖ **En général les trois scénarios de transition vers le chaos sont les suivants :**

I.10.1. Intermittence

L'intermittence vers le chaos se caractérise par un mouvement périodique entrecoupé par des bouffées chaotiques, puis le régime redevient périodique et ainsi de suite.

La survenance des bouffées apparaissent de manière irrégulière dans le temps. L'augmentation d'un paramètre réalise l'augmentation de la fréquence des perturbations, puis les bouffées sont rares et espacées et finalement le chaos domine le comportement du système.

I.10.2. Doublement de période

Par l'augmentation progressive de la valeur de bifurcation, la période d'un système forcé est multipliée par deux, puis par quatre, par huit, etc.… ces doublements de période étant de plus en plus rapprochés, lorsque la période est infinie, le système devient chaotique.

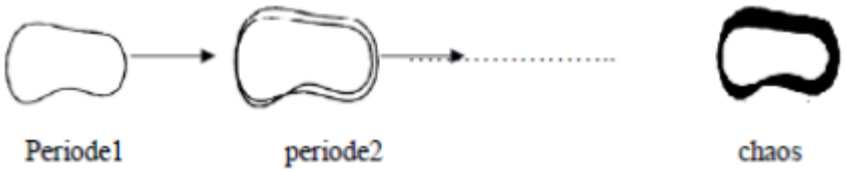
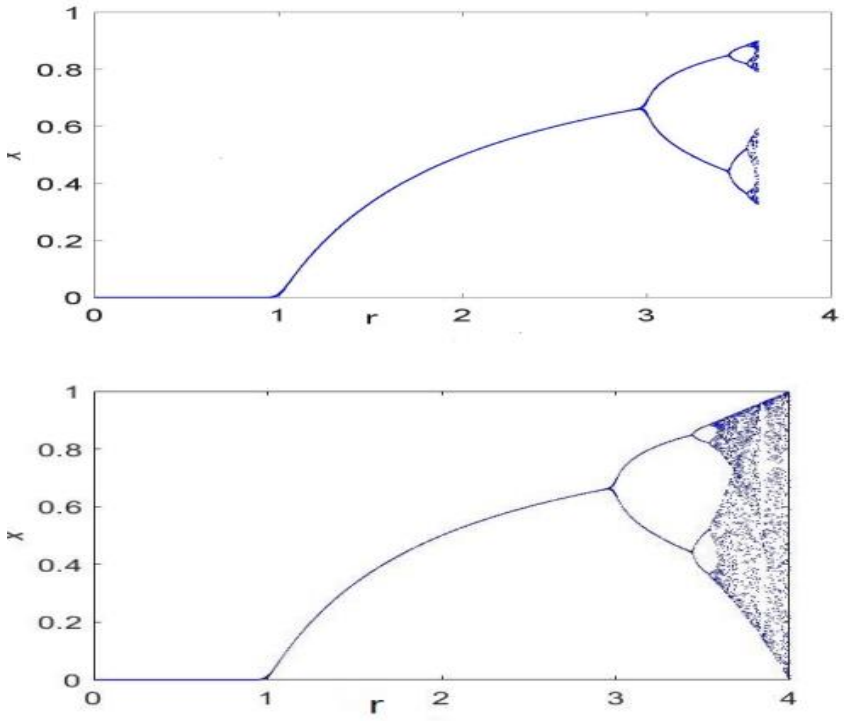


Figure I.16 : Principe d'une cascade a doublement de période.

I.10.3. Quasi périodicité

Le troisième scénario de transition vers le chaos est la quasi périodicité, qui intervient quand un deuxième système perturbe un système initialement périodique. Si le rapport des périodes des deux systèmes en présence n'est pas rationnel, alors le système est dit quasi périodique. Ce régime peut, à son tour, perdre la stabilité et devenir alors soit directement chaotique, soit par la survenance d'une troisième fréquence **[7].**



I .11. Utilisation des systèmes chaotiques

La théorie du chaos est utilisée dans divers domaines tels que :

- La biologie, elle permet d'expliquer les variations des populations animales, les oscillations du cerveau, ainsi que les arythmies cardiaques et bien d'autres.

- En économie, les mouvements commerciaux et les marchés financiers, ainsi que les cycles économiques, peuvent être expliqués en partie par cette théorie.

- Dans le domaine de l'art, depuis les années 1980, la beauté des fractales est exploitée et appréciée, et on voit des expositions se multiplier avec pour thème des images fascinantes **[11].**

I.12. Avantages et inconvénients du chaos

- L'avantage de la théorie chaotique, c'est un champ d'application plus vaste que le déterminisme classique, la biologie, les sciences de la terre, les sciences humaines... Une capacité à décrire le complexe.
- L'inconvénient majeur d'un système chaotique (quand on parle de système chaotique c'est que l'on a choisi de le décrire à l'aide d'un modèle chaotique déterministe) est le renoncement à la prédiction stricte de son évolution.
- Si la prédiction stricte est impossible, des renseignements sont quand même disponibles.
- La sensibilité aux conditions initiales fait des systèmes chaotiques ou presque chaotiques des champions de la rapidité de réaction.

Le fait de savoir quand un système est chaotique va permettre d'appliquer encore mieux le déterministe classique. Un modèle scientifique n'est réellement intéressant que lorsque l'on sait précisément quand il est possible de l'appliquer **[13]**.

I.13. Conclusion :

Dans ce chapitre nous avons présenté quelques notions et définitions sur les systèmes chaotiques, ainsi que leurs caractéristiques. On a vu que ces systèmes sont utilisés dans divers domaines dont la cryptographie.

Chapitre II:

Etude du cryptage

II.1. Introduction

Le nombre des besoins pour sécuriser la vie quotidienne restent toujours en croissance. Pour cette raison, plusieurs systèmes cryptographiques ont été développés pour satisfaire ces besoins.

Le cryptage des images a plusieurs applications dans divers domaines, tel que la communication mobile. Internet, l'imagerie médicale...etc. La cryptographie est utilisée pour atteindre sécurisation des données qui sont des nécessités dans les systèmes d'aujourd'hui. Dans ce chapitre nous allons présenter les notions de base liés à la cryptographie de l'image.

II.2. Définition et Vocabulaire de base

Chiffrement : Transformation à l'aide d'une clé de chiffrement d'un message intelligible appelé texte clair ou libellé en un message incompréhensible ou inintelligible appelé texte chiffré ou cryptogramme si on ne dispose pas d'une clé de déchiffrement (en anglais encryptions) ; En cryptographie, le chiffrement, parfois appelé à tort cryptage.

Déchiffrement: C'est la méthode ou l'algorithme utilisé pour transformer un texte chiffré en texte en clair. Chiffre : utilisation de la substitution au niveau des lettres ; anciennement code secret, par extension l'algorithme utilisé pour le chiffrement

Code : Utilisation de la substitution au niveau des mots ou phrases pour coder

Coder : Utilisation d'un code sur un texte

Cryptogramme : Message chiffré ; Le destinataire légitime doit pouvoir déchiffrer le cryptogramme et obtenir le texte clair.

Cryptosystème : Un ensemble composé d'algorithmes cryptographiques et de tous les textes en clairs, textes chiffrés et clés possibles.

Décrypter : Retrouver le message clair correspondant à un message chiffré sans posséder la clé de déchiffrement (terme que ne possèdent pas les anglophones, qui eux « cassent » des codes secrets), ceci est effectué par un espion (cryptanaliseur, décrypteur ou oreille indiscrète).

Cryptographie : étymologiquement « écriture secrète », devenue par extension l'étude de cet art (donc aujourd'hui la science visant à créer des cryptogrammes, c'est-à-dire à **chiffrer).**

Cryptanalyse : Science analysant les cryptogrammes en vue de les décrypter.

Cryptologie : Science regroupant la cryptographie et la cryptanalyse. Le fait de coder un message de telle façon à le rendre secret s'appelle chiffrement. La méthode inverse, consistant à retrouver le message original, est appelée déchiffrement.

Clef : Il s'agit du paramètre impliqué et autorisant des opérations de chiffrement et/ou déchiffrement. Dans le cas d'un algorithme symétrique, la clef est identique lors des deux opérations. Dans le cas d'algorithmes asymétriques, elle diffère pour les deux **[17].**

Figure II.1 : Chiffrement et déchiffrement **[17].**

II. 3. Domaines de cryptologie

La cryptographie comprend deux domaines d'études complémentaires : la cryptanalyse. La cryptographie générale ou à clé secrète symétrique et à clé publique asymétrique est illustrée dans la figure ci-dessous **[21]**.

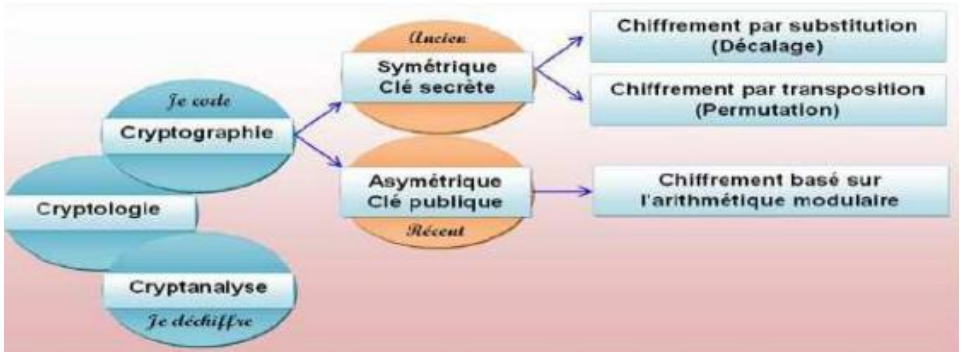


Figure.II.2: Schéma général de la cryptologie **[21].**

II. 4. Système de cryptage par chaos

Un système de cryptage chaotique se compose de deux parties : un brouilleur et un décrypteur. Celles-ci sont strictement identiques pour assurer au mieux le respect des conditions initiales. La synchronisation des dispositifs s'établit dans le système récepteur, qui initie le chaos en injectant toutes les informations à transmettre dans sa boucle à retard, superposées à la dynamique chaotique. Ce composant constitue un système de chiffrement symétrique à clé. L'émetteur et le récepteur ont la même clé. La synchronisation représentera une phase critique de l'opération de déchiffrement. En raison de la complexité du comportement du signal interférant, la moindre déviation dans le processus de décodage peut conduire à des pics d'information, connus sous le nom de **"bruit de décryptage"**. Une mauvaise synchronisation peut rendre les informations illisibles.

L'idée de base nécessite que l'expéditeur génère un signal chaotique pour masquer le message à transmettre, également connu sous le nom de "texte en clair". À l'extrémité de réception, un deuxième système chaotique est introduit pour se synchroniser avec le signal d'entrée masqué, également connu sous le nom de texte chiffré. Ensuite, une simple opération de soustraction affichera le message (en clair) **[19]**.

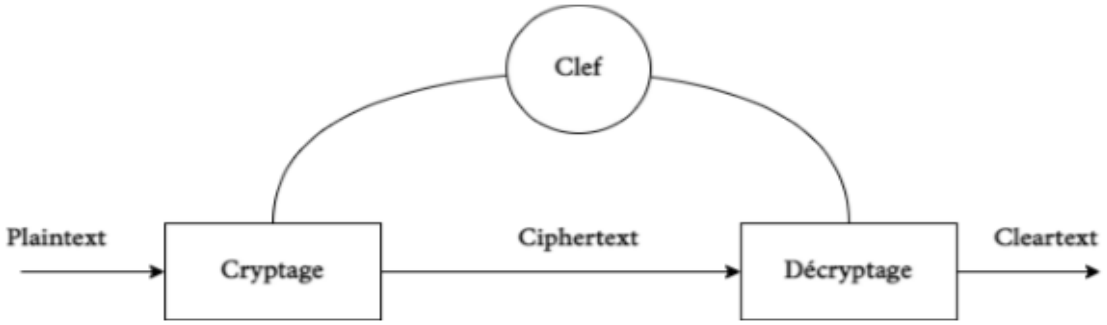


Figure II.3: Système de cryptage symétrique **[12]**.

II.5. Définition de la cryptographie

La cryptographie est un ensemble de techniques permettant de chiffrer des messages (textes ou images), même s'ils sont difficiles à comprendre. Encoder un message de manière à ce qu'il reste privé s'appelle le cryptage. La méthode inverse consiste à trouver le message d'origine, connu sous le nom de déchiffrement. Le chiffrement est généralement effectué avec une clé de chiffrement et le déchiffrement nécessite une clé de déchiffrement **[20]**.

- ***On distingue généralement deux types de clefs***

II.5.1. Les clés symétriques

Ce sont les clés utilisées pour le chiffrement et le déchiffrement. C'est ce qu'on appelle le cryptage symétrique ou le cryptage à clé **[20]**.

II.5.1.1. Principe

• Le chiffrement symétrique consiste à utiliser une clé privée pour appliquer une opération (algorithme) aux données à chiffrer, les rendant incompréhensibles.

• Nous donnons le message à quelqu'un et lui donnons la clé privée afin qu'il puisse déchiffrer le message **[21]**.

Figure II.4 : Principe de cryptage symétrique **[22].**

II.5.2. Les clés asymétriques

Ce sont les clés utilisées dans le cas du chiffrement asymétrique (également appelé chiffrement à clé publique). Dans ce cas, différentes clés sont utilisées pour le chiffrement et le déchiffrement **[21]**.

II.5.2.1. Principe

• L'utilisateur choisit une clé aléatoire connue de lui seul (il s'agit de la clé privée).

• Ils dérivent chacun automatiquement un algorithme (il s'agit de la clé publique).

• Les utilisateurs échangent cette clé publique sur un canal non sécurisé.

• Lorsqu'un utilisateur souhaite envoyer un message à un autre utilisateur, il lui suffit de chiffrer le message à envoyer avec la clé publique du destinataire.

• Ce dernier pourra déchiffrer le message grâce à sa clé privée (connue de lui seul) **[22]**.

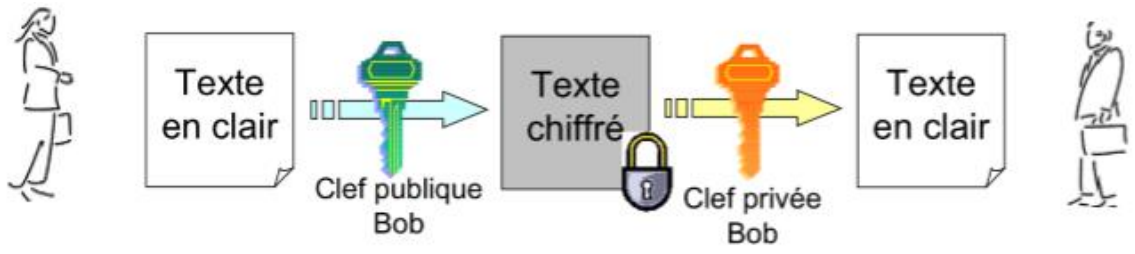


Figure II.5: Principe de cryptage asymétrique **[22].**

II.6. Les avantages et les inconvénients de cryptographies symétriques et asymétriques

Cryptographie	Avantages	Inconvénients
Symétrique	-Système rapide de chiffrement/déchiffrement. -Clés relativement courtes (128 ou 256 bits). -Primitive de mécanismes cryptographiques, et Bonne performances et sécurité bien étudié. -Assure la confidentialité des données.	-Gestion des clés difficiles (nombreux clés). -Point faible : l'échange de la clé secrète. -Dans un réseau de N entités susceptibles de communiquer secrètement il faut distribuer N ∗(N-1) /2 clés.
Asymétrique	-Pas de secrèt à transmettre. -Nombre clés à distribuer est réduit par rapport aux clés symétriques. -Très utile pour échanger des messages facilement. -La distribution est simplifiée : La clé privée n'est jamais révélée ou transmise et la clé publique est disponible à tous les utilisateurs.	-Les algorithmes à clé publique nécessitent une capacité de traitement importante, ce qui n'est pas raisonnable pour les systèmes à ressources limitées. -La relation clés publique/clés privée impose : -La taille de clés et relativement longue (généralement entre 512 et 2048 bits). -Gestion de certificats de clés publiques. -Lenteur de calcul. -Pas d'authentification de la source.

Table.II.1: Les avantages et les inconvénients symétriques/asymétriques **[21].**

II.7. La différence entre Cryptage symétrique et cryptage asymétrique

Cryptage symétrique	Cryptage asymétrique
- Gestion des clés difficiles (nombreuses clés)	- La transmission n'est pas confidentielle.
-Point faible dans l'échange de la clé secrète	- Très utile pour échanger les clés
- Clés relativement courtes (128 ou 256 bits)	- Des clés plus longues (1024 à 4096 bits).
-Système rapide du chiffrement/déchiffrement.	-Lenteur de calcul.
-Facile.	-Difficile.

Table.II.2: Comparaison entre cryptographie asymétrique et symétrique **[20]**.

II.8. Objectif de cryptographie

Les principaux objectifs à garantir par l'application de la cryptographie sont:

- **Confidentialité :** Mécanisme de transmission des données de manière à ce que seuls les destinataires autorisés puissent les lire**.**
- **Intégrité des données :** Un mécanisme pour s'assurer que les données reçues n'ont pas été frauduleusement ou accidentellement modifiées pendant la transmission**.**
- **Authentification :** Un mécanisme qui permet aux utilisateurs de s'authentifier afin de limiter l'accès aux données, serveurs et ressources aux seules personnes autorisées (via le nom de connexion ou le mot de passe d'un certificat numérique).
- **Non-répudiation :** Mécanisme d'enregistrement d'un acte ou d'une promesse par une personne ou une entité afin qu'elle ne puisse pas nier que l'acte a été accompli ou que la promesse a été faite **[20].**

II. 9. Principe du cryptage par chaos

Le chiffrement chaotique est réalisé en superposant des signaux chaotiques aux informations initiales. Nous envoyons par la suite le message noyé dans le chaos à un récepteur qui connaît les caractéristiques du générateur de chaos. Le destinataire n'a plus qu'à soustraire l'encombrement de son message pour trouver l'information **[19]**.

II.10. Technique de cryptage par chaos

Le véritable cryptage, ou comment mélanger et séparer des données et des signaux chaotiques, est la dernière étape de la construction d'un système de communication chaotique. Les signaux chaotiques porteurs d'informations représentent une généralisation des systèmes de modulation conventionnels. Par conséquent, les messages source de faible amplitude sont masqués par des signaux chaotiques plus importants.

Cependant, contrairement aux porteuses sinusoïdales classiques, et en raison du manque de notion précise d'amplitude, de phase et de fréquence, les signaux chaotiques se mélangent au message source d'une manière différente**.**

Il existe plusieurs techniques de cryptages, nous décrivons ici quelques-uns **[4]** :

II.10.1.Cryptage par addition (additive chaos masking scheme)

La première méthode de chiffrement, et la plus simple, illustrée à la Figure (II.6), a été mise au point en 1993. Il se compose de deux systèmes chaotiques identiques, l'émetteur et le récepteur. Le signal chaotique $c(t)$ est l'une des variables d'état du système dans l'émetteur. Le message d'information (signaux utiles qui doivent être cryptés) m(t), qui est typiquement très faible devant c(t), est ajouté au signal c(t) et donne le signal transmis s(t). Comme c(t) est très complexe et m(t) est beaucoup plus petit que c(t), alors il est difficile de séparer m(t) du signal s(t) sans connaître c(t).

L'émetteur et le récepteur utilisent le même système, la différence est que le récepteur est contrôlé par le signal d'émission pour obtenir la synchronisation. Au niveau du récepteur, après avoir été synchronisé grâce au signal reçu, le message d'origine est récupéré par simple soustraction. Par conséquent, les intrus ne soupçonneront pas qu'un message est en

cours de transmission, même s'ils interceptent le signal $y(t)$ (porteuse chaotique plus message), ils ne chercheront donc pas à appliquer des techniques de décryptage **[4]**.

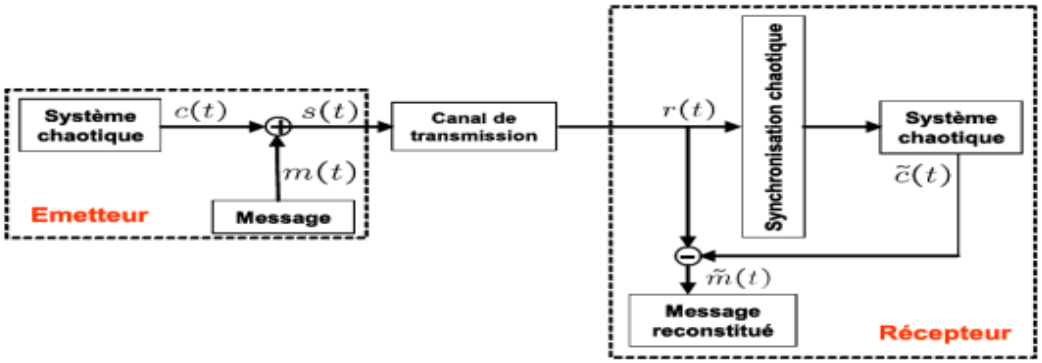


Figure II.6: Cryptage par addition **[4].**

II.10.2. Cryptage par commutation (Chaotic Shift Keying, CSK)

Aussi connu sous le nom de cryptage par décalage, il s'agit d'une technique réservée aux messages numériques. Dans le schéma de communication illustré à la Figure (II.7), le message d'information est utilisé pour commuter le signal de transmission entre deux attracteurs chaotiques statistiquement similaires, qui sont utilisés respectivement pour coder le bit 0 et le bit 1 du message d'information numérique. Ces deux attracteurs sont générés par deux systèmes chaotiques de même structure et de paramètres différents. A ka réception, le signal reçu est utilisé pour produire un système chaotique identique à ceux de l'émetteur. Le message d'information est restitué par application d'un filtre passe-bas et ensuite un seuillage de l'erreur de synchronisation $e(t)$ **[4]**.

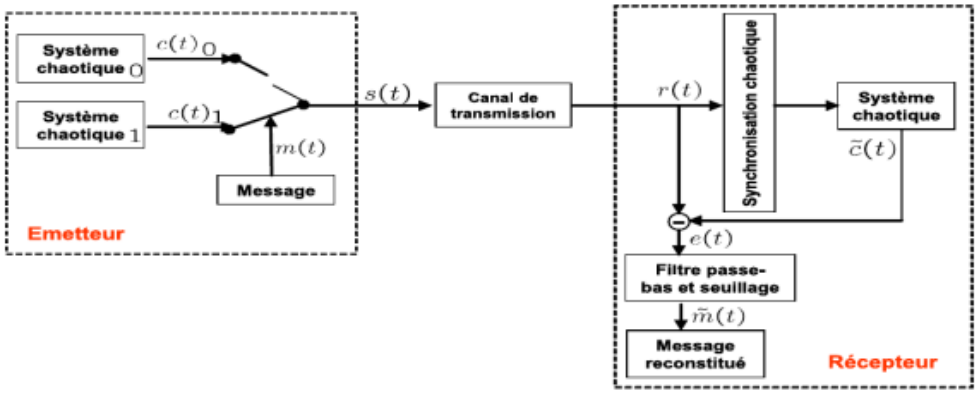


Figure.II.7: Cryptage CSK **[4].**

II.10.3. Cryptage Par Modulation

La technique utilise des messages contenant des informations pour moduler les paramètres d'un émetteur chaotique. Un contrôleur adaptatif est responsable du maintien de la synchronisation au niveau du récepteur tout en suivant les modifications des paramètres de modulation. Le schéma de principe correspondant est représenté sur la Figure (II.8). Au niveau de l'émetteur, le fait de moduler un (ou plusieurs) paramètre oblige la trajectoire à changer constamment d'attracteur, et ainsi, le signal émis est plus complexe qu'un signal chaotique normal. Cependant, la façon dont les messages sont injectés et la fonction de modulation des paramètres ne peuvent pas supprimer le caractère chaotique du signal envoyé au récepteur. Il convient de souligner que cette technique tire pleinement parti des propriétés des systèmes chaotiques.

Il n'a pas d'équivalent dans les systèmes de communication traditionnels. Cependant, le chiffrement par modulation s'est avéré vulnérable à certaines attaques **[27]**.

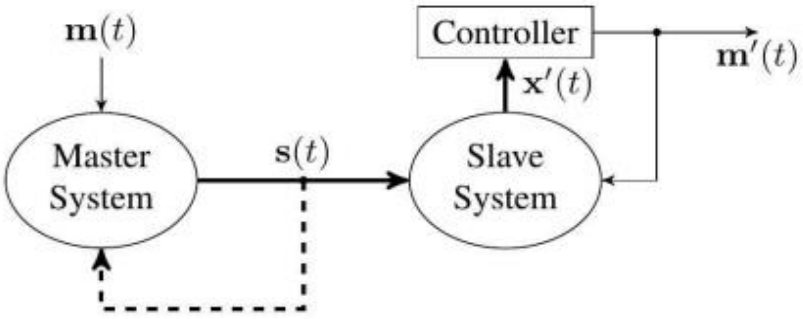


Figure.II.8: Cryptage par modulation **[27].**

❖ ***Il existe deux types de cryptage par modulation***

- Modulation de paramètres, où le signal $m(t)$ module la valeur d'un ou plusieurs paramètres de contrôle.

- Modulation directe, où le signal $m(t)$ est injecté dans une ou plusieurs variables du système principal sans changer aucune valeur du paramètre de contrôle.

Par rapport au chiffrement additif, la modulation chaotique permet de restituer très fidèlement les messages transmis si certaines conditions sont remplies. Étant donné que le cryptage CSK n'est utilisé que pour les signaux numériques, la modulation a de meilleures performances que CSK. S'il est correctement conçu, le cryptage de modulation peut transmettre plusieurs messages. Il est nécessaire de moduler n paramètres de contrôle du système principal avec n signaux de message.

Un avantage important du cryptage de modulation est que le contrôleur dépend de la structure du système maître-esclave, ce qui signifie que différents contrôleurs doivent être conçus pour différents systèmes maîtres, et parce que certains systèmes peuvent ne pas avoir de contrôleur. Panne du système maître/esclave **[27]**.

II.10.4. Cryptage par inclusion

Cette technique de chiffrement consiste en un système dynamique qui injecte des messages dans l'émetteur, mais n'effectue pas de modulation des paramètres. La récupération des informations se fait principalement par deux techniques, soit en s'appuyant sur un observateur à entrée inconnue, soit en s'appuyant sur l'inversion du système émetteur **[25]**.

II.10.4.1. Observateurs à entrées inconnues

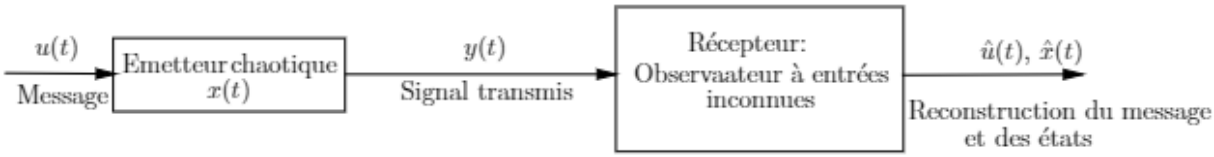


Figure.II.9 : observateurs à entrées inconnues **[25].**

Le schéma de la figure (II.9) illustre un problème classique d'estimation d'état non linéaire avec des entrées inconnues : il est nécessaire de reconstruire l'état x(t) du système de transmission avec l'entrée inconnue u(t). Différentes techniques de synthèse d'observateurs avec des entrées inconnues sont utilisées dans la littérature et peuvent être utilisées à des fins de décryptage. Dans un article qui utilise ces types d'observateurs pour décrypter l'information, on peut citer **[23]**.

II.10.4.2. Décryptage par inversion

Cette figure illustre le processus de déchiffrement par inversion, c'est-à-dire que le récepteur est conçu en inversant le modèle de l'émetteur. La figure (II.10) montre le principe général de cette approche. Passons en revue quelques concepts sur les systèmes hybrides. **[23]**.

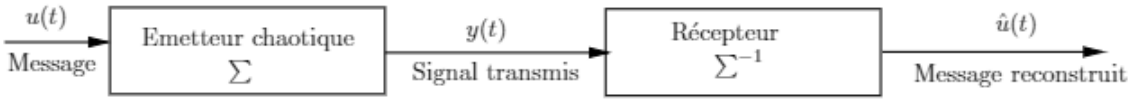


Figure.II.10: Principe du cryptage par inverse **[23].**

II.10.5. Cryptage mixte

Afin de résoudre le problème de sécurité des procédés antérieurs, une nouvelle technique combinant des principes de cryptographie standard et des principes de synchronisation chaotique est proposée. Un message u(t) contenant des informations est chiffré à l'aide d'une clé c(t) générée par l'expéditeur chaotique.

Les messages chiffrés sont alors injectés dans la dynamique du système chaotique, le rendant encore plus complexe. Ensuite, un signal y(t) qui dépend des variables d'état de l'émetteur est transmis au récepteur, qui établit une synchronisation avec l'émetteur. La clé est ensuite reconstituée par le destinataire, qui peut éventuellement décoder le message. Le principe général de la méthode est représenté sur la Figure (II.11) **[26]**.

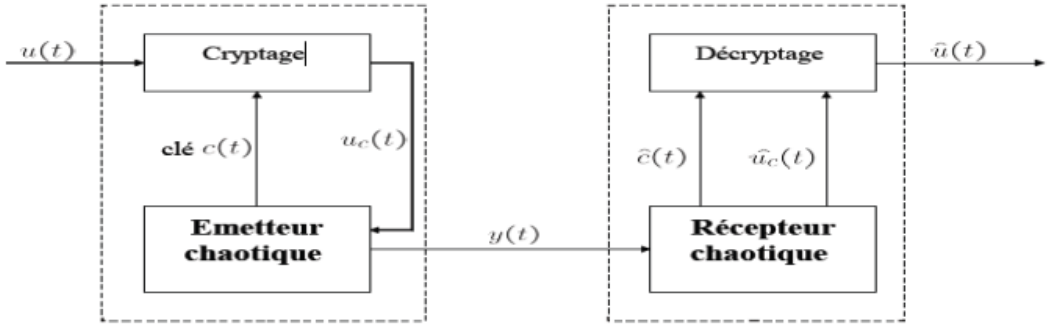


Figure. II.11: Cryptage mixte **[26].**

II.10.6. Transmission par deux voies

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

- Le premier signal y est une fonction à valeurs réelles de l'état x du système émetteur chaotique et son seul but est de permettre la synchronisation du récepteur.

- Le deuxième signal $y2$ envoyé sur un autre canal est un signal chaotique contenant l'information à transmettre **[26]**.

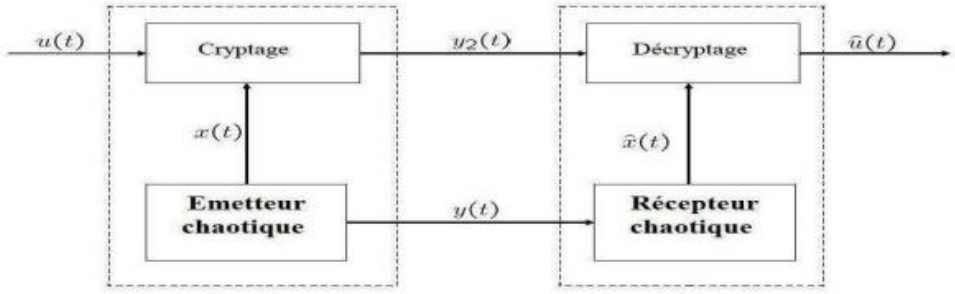


Figure.II.22: Transmission par deux voies **[26].**

❖ **Cette méthode présente plusieurs avantagent**

• Le signal y ne contient aucune information, la synchronisation peut donc être établie de manière optimale.

• L'information contenue dans le deuxième signal $y2$ peut être chiffrée par une fonction non linéaire de l'état x, ou simplement masquée par un signal chaotique généré par l'émetteur en tant que porteuse.

• Les deux étapes de synchronisation et de cryptage étant totalement indépendantes, le décryptage n'est pas nécessairement effectué, au niveau du récepteur, en même temps que la synchronisation **[26]**.

II.11. La cryptanalyse

II.11.1. Définition

La cryptanalyse est un peu l'opposé de la cryptographie en ce qu'elle est l'étude des faiblesses des systèmes cryptographiques, généralement effectuée par des intrus qui mettent en œuvre des méthodes pour extraire des informations (chiffres, chiffrements, algorithmes) de ce qui est considéré comme public, la cryptanalyse est l'un des sujets d'étude. En cryptanalyse, les humains sont supposés être faibles et facilement soudoyés, de sorte que la force du système doit dépendre de la force des principes utilisés.

Si le but de la cryptographie est d'élaborer des méthodes de protection, le but de la cryptanalyse est au contraire de casser ces protections. Une tentative de cryptanalyse d'un système est appelé une attaque, et elle peut conduire à différents résultats :

- ***Cassage complet :*** La cryptanalyse trouve la clé de déchiffrement.
- ***Obtention globale :*** La cryptanalyse trouve un algorithme équivalent à l'algorithme de déchiffrement, mais sans connaître la clé de déchiffrement.
- ***Obtention locale :*** La cryptanalyse trouve le message en clair correspondant au message chiffré.
- ***Obtention d'information :*** la cryptanalyse obtient une indication du message ou de la clé en clair (certains bits de la clé, des informations sur la forme du message en clair).

En général, on suppose toujours que la cryptanalyse connaît les détails de l'algorithme, de la fonction mathématique ou du protocole utilisé. Même si ce n'est pas toujours le cas en pratique, s'appuyer sur le secret des mécanismes utilisés pour sécuriser le système est risqué, d'autant plus que l'utilisation croissante des ordinateurs a facilité la reconstruction d'algorithmes à partir de programmes **[24].**

II.12. Synchronisation des systèmes chaotiques

II.12.1. Définition

La synchronisation de deux systèmes dynamiques signifie que chaque système évolue au fur et à mesure que l'autre système se comporte. Ce concept est basé sur le fait qu'un système chaotique est déterministe et a un ou plusieurs exposants de Lyapunov positifs et qu'il est instable. En supposant que deux systèmes chaotiques identiques oscillent de manière totalement indépendante, si par certains moyens ils sont autorisés à échanger de l'énergie, une action appelée "couplage", les deux systèmes finiront par céder la place à un comportement commun et ils finiront par se synchroniser.

La synchronisation de deux systèmes $S1$ et $S2$ peut être définie comme suit :

Avec $\dot{\boldsymbol{x}}(\boldsymbol{t}), \hat{\boldsymbol{x}}(\boldsymbol{t}) \in \boldsymbol{R^n}, \boldsymbol{f_1}\ \boldsymbol{et}\ \boldsymbol{f_2}$ des fonctions non linéaires définies de $\boldsymbol{R^n} \rightarrow \boldsymbol{R}$ Les deux systèmes sont synchronisés si :

$$\lim_{t\to\infty} \mathbf{e}(\boldsymbol{t}) = \lim_{t\to\infty} |\, \dot{\boldsymbol{x}}\,(\mathbf{t}) - \hat{\boldsymbol{x}}(\mathbf{t})\,| = \mathbf{0} \qquad \text{(II.1)}$$

Avec : $\dot{x}(t)$: L'état du système maître ($S1$).

$\hat{x}(t)$: L'état du système esclave ($S2$) **[26]**.

II.12.2. Principe de synchronisation des systèmes chaotiques

La synchronisation chaotique du signal a été découverte en 1996 par Thomas Carol et Louis Peccora.

La synchronisation est un phénomène qui se produit lorsque deux systèmes dynamiques identiques évoluent dans le temps. Elle consiste à synchroniser et rapprocher les trajectoires des deux systèmes jusqu'à les confondre. La synchronisation suit la configuration de

synchronisation la plus répandue, ou cette dernière consiste à forcer un système dynamique appelé esclave à se synchroniser (suivre la même trajectoire) avec un second système dynamique appelé maître **[8]**.

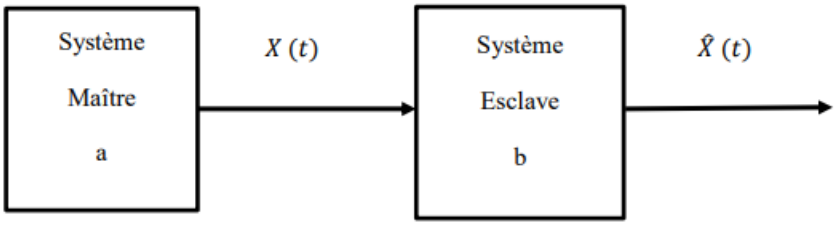


Figure II.13: Système maître-esclave pour réaliser la synchronisation **[4]**.

II.12.3. Type de synchronisation des systèmes chaotiques

Suite à cette découverte de Pecora et Caroll, plusieurs types de synchronisation ont été introduits, souvent basés sur les mêmes principes utilisant les mêmes circuits. Supposons que deux systèmes chaotiques identiques oscillent de manière complètement indépendante. S'ils sont autorisés à échanger de l'énergie de quelque manière que ce soit, un effet connu sous le nom de "couplage", les deux systèmes finiront par céder la place à un comportement commun appelé synchronisation.

Selon le sens d'échange d'énergie entre deux systèmes chaotiques, la synchronisation est de deux types :

Synchronisation de couplage unidirectionnelle et synchronisation de couplage bidirectionnelle.

Ci-dessous nous allons définir et donner deux principes de synchronisation **[8].**

II.12.3.1. Synchronisation unidirectionnelle

Dans le cas d'une synchronisation unidirectionnelle, le couplage entre deux systèmes identiques a et b est réalisé à l'aide d'éléments fonctionnant dans un seul sens, par exemple à l'aide d'un circuit électrique suiveur **[25].**

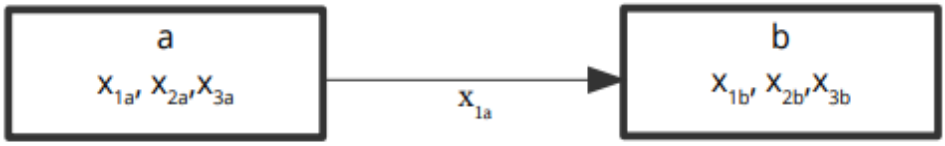


Figure II.14: Couplage unidirenctionnel **[27]**.

II.12.3.2. Synchronisation Bidirectionnelle

Dans le cas d'une synchronisation bidirectionnelle, le couplage entre deux systèmes identiques a et b est réalisé à l'aide d'éléments permettant un échange d'énergie bidirectionnel, par exemple à l'aide de simples résistances **[25].**

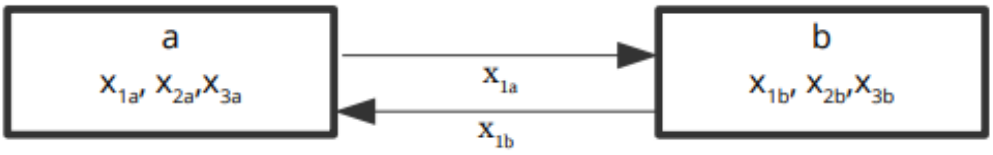


Figure II.15: Couplage bidirenctionnel **[27].**

II.13. Méthodes de synchronisation

Plusieurs méthodes de synchronisation ont été proposées dans la littérature. Dans ce qui suit nous citons quelque approche en expliquant leurs principes.

II.13.1. Synchronisation identique

Ou la synchronisation complète, la synchronisation la plus ancienne et la plus simple des systèmes chaotiquement couplés, donne une **solution** simple mais puissante. Son principe est de reproduire l'état du système maître à partir du système. Considérons deux systèmes dynamiques: **[25]**

$$\dot{\boldsymbol{x}}(\boldsymbol{t}) = \boldsymbol{f}\big(\boldsymbol{xm}(\boldsymbol{t})\big) \qquad \text{(II.2)}$$

Et $$\dot{\boldsymbol{xs}}(\boldsymbol{t}) = \boldsymbol{f}\big(\boldsymbol{xs}(\boldsymbol{t})\big) \qquad \text{(II.3)}$$

Où $\boldsymbol{xm}(\boldsymbol{t}), \boldsymbol{xs}(\boldsymbol{t}) \in \boldsymbol{R}^{\boldsymbol{n}}$ sont des vecteurs d'état de dimension n.

C Alors (II.2) et (II.3) sont identiquement synchronisés si, quelles que soient leurs conditions initiales :

$$\lim_{t\to\infty}|xs(t) - xm(t)| = 0 \qquad \text{(II.4)}$$

II.13.2. Synchronisation par boucle fermée

Synchroniser un système chaotique par une approche en boucle ouverte implique une sensibilité aux variations de paramètres. Pour résoudre ce problème, de nouvelles techniques basées sur des boucles de rétroaction ont été proposées. L'idée est de corriger le système en fonction de l'erreur entre le signal émis par le premier système et le signal régénéré par l'autre système. Ainsi, cette erreur est injectée en retour, d'où le nom de la méthode.

La technique permet également la synchronisation entre différentes paires de systèmes chaotiques **[27]**.

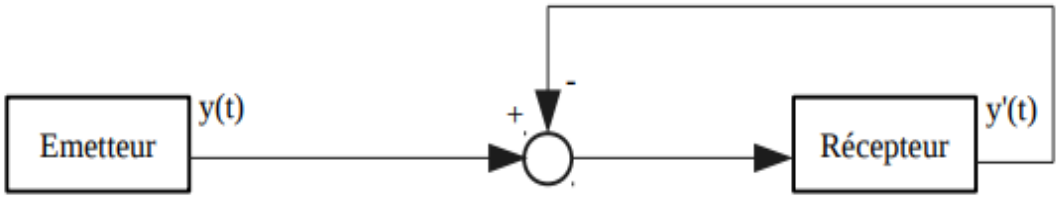


Figure II.16: Synchronisation par boucle fermée **[27].**

II.13.3. Synchronisation projective

Dans cette approche, l'état du système récepteur est synchronisé avec un multiple de l'état du système émetteur, il existe donc $\boldsymbol{a}$ et $\boldsymbol{\tau}$ tels que :

$$\lim_{t\to\infty} \|x'(t) - ax(t-\tau)\| = 0 \qquad \text{(II.9)}$$

Où **a** est le facteur d'échelle $\boldsymbol{x}$ $(\boldsymbol{t})$ est l'état du système émetteur, $\boldsymbol{x}'(\boldsymbol{t})$ est l'état du système récepteur et $\boldsymbol{\tau}$ est le retard positif.

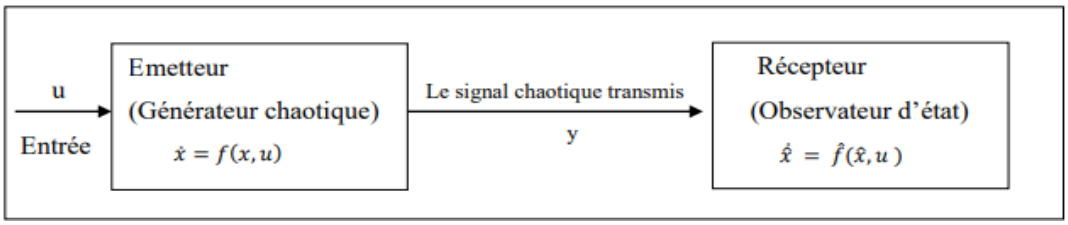
Cette approche est utilisée pour les systèmes partiellement linéaires et permet la synchronisation avec des facteurs d'état non synchronisables **[26].**

II.13.4. Synchronisation à l'aide d'observateur

La synchronisation peut également être effectuée à l'aide d'observateurs. Un observateur est un système dynamique qui estime des états inconnus du système qui ne peuvent pas être mesurés directement (pour des raisons techniques ou économiques). Un système dynamique est dit observable si toutes ses quantités peuvent être récupérées (statiquement ou dynamiquement) par des combinaisons de mesures de ses sorties et de leurs dérivées.

La synthèse d'observateurs de systèmes linéaires a fait l'objet de nombreux travaux, en fait les premiers travaux sur les observateurs publiés par Kalman et Luenberger vers les années 60, les premiers s'intéressant aux systèmes linéaires variant dans le temps, les seconds aux systèmes d'intérêt linéaires invariants dans le temp.

Dans la synchronisation d'observateur, le système maître est un système chaotique arbitraire et le système esclave est un observateur de l'état correspondant. La figure (II.19) illustre ce principe de synchronisation.



.

Figure II.17: Principe de synchronisation à l'aide d'observateur **[8].**

L'émetteur et le récepteur se synchronisent si les systèmes $\dot{\hat{x}} = \hat{f}(\hat{x}, u)$ (défini au niveau du récepteur) est un observateur convergent pour le système $\dot{x} = f(x, u)$ (défini au niveau de l'émetteur). Autrement dit, le problème de synchronisation revient à déterminer une fonction $\hat{f}$ telle que :

$$\lim_{t\to\infty} \|x(t) - \hat{x}(t)\| = 0 \qquad \text{(II.11)}$$

Des différents types d'observateur (en temps continue et en temps discret) dans différent buts ont été proposés :

- Observateur de Kalman étendu.
- Observateur à gain élevé.
- Les observateurs à modes glissants sont basés sur la théorie des systèmes à structures variables.
- Observateurs adaptatifs pour évaluer les états et les paramètres des systèmes dynamiques.
- L'observateur dead-beat pour les systèmes en temps discret **[8]**.

II.13.5. Synchronisation généraliste

Cette méthode est une généralisation du concept de synchronisation identique. S'il existe une transformation M telle que les deux systèmes soient synchronisés au sens large

$$\lim_{t\to\infty} \|x'(t) - M(x(t))\| = 0 \qquad \text{(II.12)}$$

Où $x(t)$ **:** est l'état du système émetteur.

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

Les conditions initiales ne sont pas prises en compte dans ce cas. Si M est inversible, alors $M^{-1}(x')$ fournit une estimation de l'état x ; sinon il est impossible de fournir une estimation de l'état x.

Ceci est un inconvénient majeur pour les techniques de communication qui utilisent l'état de l'expéditeur pour déchiffrer les messages transmis **[26]**.

II.14. Propriétés des systèmes de communication a base chaos

Dans cette partie, des propriétés des systèmes de communication chaotiques seront étudiées et comparées aux propriétés des systèmes classiques **[26]**.

II.14.1. Spectre à large bande

Les systèmes chaotiques en particulier ont un spectre large bande. Cette propriété est avantageuse pour les applications nécessitant une immunité élevée au bruit et une faible probabilité de détection.

Le premier système de transmission à utiliser un large spectre de fréquences et une modulation par sauts de fréquence a tenu compte de ces problèmes. Cependant, malgré ces méthodes, la synchronisation entre émetteur et récepteur reste une tâche pas toujours triviale. En pratique, un schéma de transmission par saut de fréquence nécessite une nouvelle synchronisation à chaque changement de fréquence porteuse. Ainsi, l'utilisation de systèmes chaotiques permet la transmission de signaux large bande et donc une synchronisation plus simple entre émetteur et récepteur.

II.14.2. Signal non périodique

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

II.14.3. Implémentation analogique simple

La périodicité des communications sécurisées peut générer des pics spectraux indésirables. D'autre part, les signaux chaotiques sont apériodiques et ne peuvent prédire leur évolution sur de longs intervalles de temps. Il n'y a donc pas de pics spectraux. De plus, développer des modèles prédictifs de dynamique non périodique est plus difficile.

II.15. La cryptographie visuelle

La cryptographie visuelle est le domaine de la cryptographie qui utilise ou transmet des images dans le but de pouvoir crypter des images en images cryptées, chacune sans ressemblance ni corrélation avec l'original **[20]**.

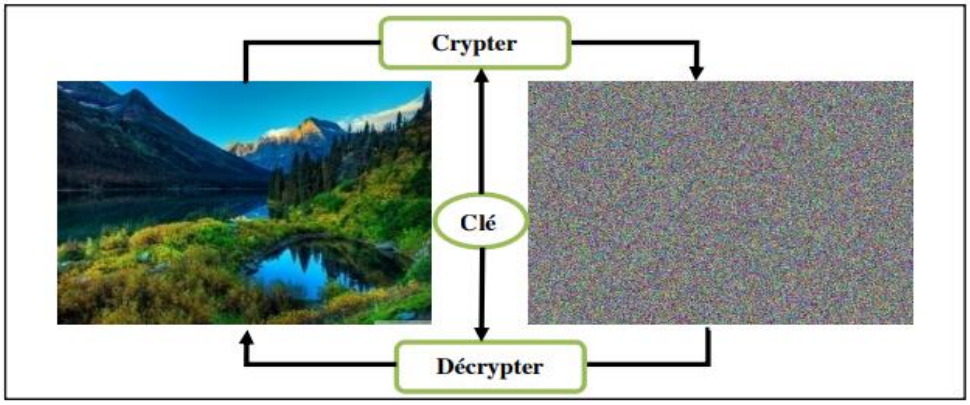


Figure II.18: Cryptage d'image**.**

II.15.1. Définition d'image numérique

- C'est une matrice de X×Y pixels (Picture élément ou pixel), correspondant à l'échantillonnage et à la quantification du signal acquis avec la caméra.
- Chaque pixel est associé à n niveaux de gris ou N niveaux de composantes de couleur codées en bits.
- Chaque pixel est localisé par ses coordonnées x et y dans l'image.
- La représentation des images numériques en codes binaires (zéros et uns) est caractérisée par les paramètres suivants :
  - ✓ **Le pixel :** Le plus petit composant d'une image numérique. Tous ces pixels sont contenus dans le tableau à deux dimensions qui compose l'image.
  - ✓ **Définition :** On appelle la définition du nombre de points (pixels) qui composent une image, c'est-à-dire le nombre de colonnes de l'image multiplié par le nombre de lignes de l'image **[20]**.

II.15.2. Types d'image numérique

Il existe deux types d'images numériques, le premier est basé sur les pixels et l'autres sur des formules mathématiques :

II.15.2.1. Les images matricielles

Une image raster (ou bitmap) est une image composée d'un ensemble de points : les pixels. Chaque point porte des informations de position et de couleur. Formats d'image bitmap :

BMP, PCX, GIF, JPEG, TIFF. Les photographies numériques et les images numérisées entrent dans cette catégorie **[17]**.

II.15.2.2. Les images vectorielles

Les images vectorielles sont constituées de formes géométriques qui peuvent être décrites mathématiquement. Par exemple, une ligne sera définie par 2 points et un cercle sera défini par le centre et le rayon. Le processeur se charge de "traduire" ces formes en informations que la carte graphique peut interpréter (images Word, Publisher, CorelDraw - formats WMF, CGM, etc.)

Les avantages des images vectorielles : les fichiers qui les composent sont petits, et peuvent être redimensionné facilement sans dégradation de la qualité.

Les inconvénients : les graphiques vectoriels ne peuvent représenter que des formes simples. Par conséquent, il ne peut pas être utilisé pour la photographie, en particulier le photoréalisme **[17]**.

II.15.3. Cryptage d'image

Pour chiffrer une image, nous devons à nouveau utiliser des bits. Chaque pixel a une couleur : celle-ci est définie par un entier, qui est ensuite converti en binaire.

Le principe de cryptage est simple : par exemple, il s'agit d'additionner" deux images, une image-clé et l'image qu'on veut crypter, grâce à l'opérateur bit à bit XOR **[17]**.

Exemple :

(1) 1er pixel de l'image à crypter	01110011
(2)1er pixel de l'image clé	10100101
(1) XOR (2) -->1er pixel de l'image cryptée	11010110

II.15.4. Les techniques de cryptage d'image

Les techniques de base des systèmes de chiffrement d'images peuvent être divisées en deux catégories : la confusion et la diffusion.

- **La diffusion**

-C'est la transformation des valeurs des pixels dans l'image.

- **Chaos**

-C'est la permutation des positions des pixels dans l'image sans changer leurs valeurs **[17]**.

II.16. Conclusion

Dans ce chapitre, nous avons présenté les connaissances générales de la cryptographie et quelques avantages et inconvénients de chaque type de chiffrement.

Nous avons vu les principes de synchronisation dans les systèmes chaotiques et les différentes méthodes utilisées pour la synchronisation.

Chapitre III:

Cryptage par chaos

III.1. Introduction

Nous introduisons dans ce chapitre une méthode de cryptage chaotique d'images qui se base sur l'utilisation d'oscillateur sprott. Nous avons testé par simulation sur Matlab 2017 et nous avons utilisé la méthode d'intégration Runge-Kutta de quatrième ordre pour résoudre les systèmes d'équation différentielle.

III.2. Transmission basée sur la synchronisation des systèmes chaotique

Dans cette partie, nous nous intéressons à la technologie de transmission de sécurité de l'information basée sur le principe de synchronisation chaotique. La plupart des techniques développées dans la littérature est l'utilisation de la configuration maître-esclave, où il y a un émetteur chaotique (système maître) qui génère un signal qui transporte des messages transmis dans un canal de communication vers un système récepteur (système esclave).

Les signaux chaotiques peuvent être utilisés pour sécuriser la transmission d'informations. Le premier objectif est de protéger les informations transmises et le second objectif est d'utiliser tous les avantages de la technologie à spectre étalé pour diffuser le signal d'information.

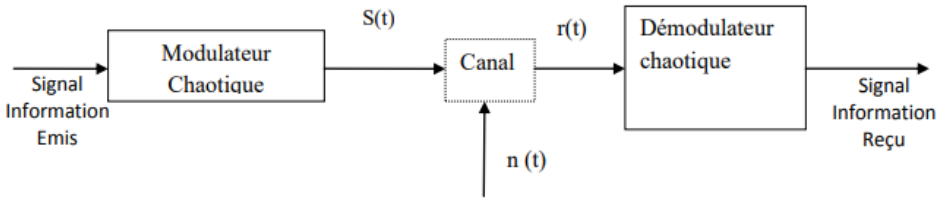


Figure III.1: Modulation directe du signal informationnel par porteuse chaotique haute fréquence **[28].**

L'avantage de cette solution est qu'elle est très simple à mettre en œuvre, mais en revanche elle nécessite un système chaotique avec de fortes contraintes sur ses paramètres.

La deuxième solution est de moduler le signal d'information par un signal chaotique puis d'appliquer une transformation haute fréquence par une porteuse sinusoïdale.

Le schéma est illustré à la figure (III.2).

Son principal avantage est la simplification significative du modulateur chaotique.

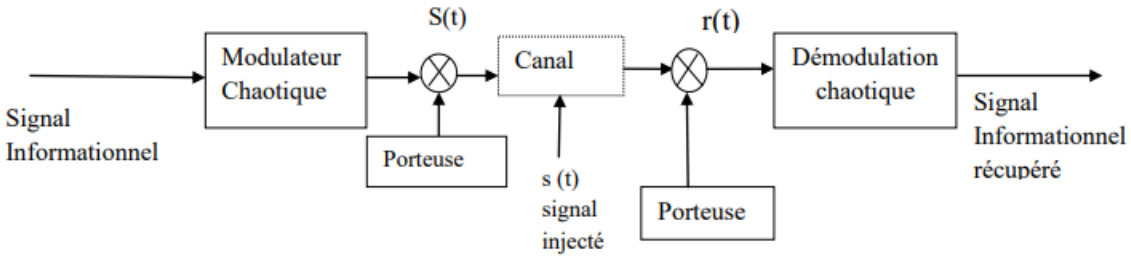


Figure III.2 : Modulation en bande du signal informationnel par le signal chaotique, combinée avec une mise sur porteuse classique **[28].**

Les techniques de communication traditionnelles basées sur le chaos comprennent le masquage du chaos, la modulation paramétrique, la commutation du chaos, le cryptage par injection (intégré), la transmission bidirectionnelle et le cryptage combiné, etc. **[28].**

III.3. Oscillateur chaotique de Sprott

III.3.1. Etude du montage

L'oscillateur chaotique de Sprott est représenté par la figure (III.3)

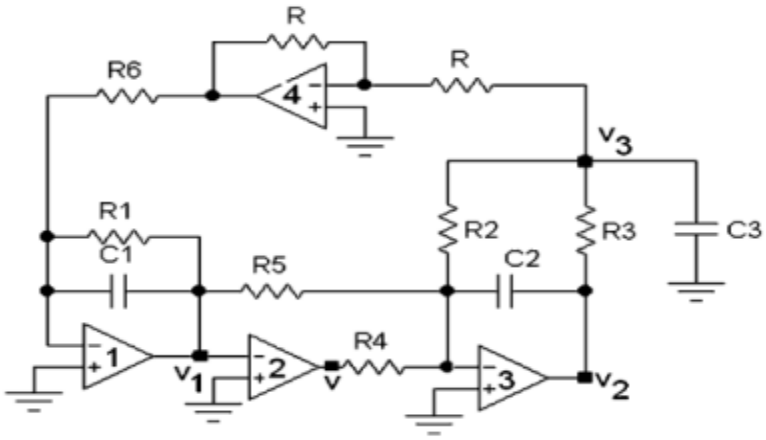


Figure III.3: Oscillateur de Sprott.

III.3.2. Équations de l'oscillateur

La figure (III.3) représente l'oscillateur de Sprott qui comporte des résistances, condensateurs et des amplificateurs opérationnels. Seul le deuxième AOP agit comme un amplificateur non linéaire et sa tension de sortie $\boldsymbol{v}$ est donnée par l'équation suivante:

$$\boldsymbol{v = -v_{cc}\ singn(c1)} \qquad \text{(III.1)}$$

Où $\boldsymbol{v_{cc}}$ est la tension de polarisation utilisée.

L'oscillateur est un système dynamique du troisième ordre. La dynamique de l'oscillateur est donnée par les trois équations différentielles suivantes:

$$\frac{dv1}{dt'} = -\frac{1}{R_1C_1}V_1 + \frac{1}{R_6C_1}V_3$$

$$\frac{dv_2}{dt'} = -\frac{1}{R_5C_2}v_1 - \frac{1}{R_2C_2}V_3 + \frac{1}{R_4C_2}V_{CC}sign(V_1) \qquad \text{(III. 2)}$$

$$\frac{dv_3}{dt'} = \frac{1}{R_5C_3}V_2 - (\frac{1}{RC_3} + \frac{1}{R_2C_3} + \frac{1}{R_3C_3})V_3$$

La fonction signe est définie par:

$$\text{sign}(X) = \begin{cases} = -1 \sin < 0 \\ = 0 \sin = 0 \\ = 1 \sin > 0 \end{cases} \qquad \text{(III.3)}$$

On précède ensuite les changements de variable suivants:

$$x = \frac{v_1}{V_{CC}}, y = \frac{v_2}{V_{CC}}, z = \frac{v_3}{V_{CC}}, t = w_0t$$

$$Q_1 = \frac{1}{R_1C_1w_0}, Q_2 = \frac{1}{R_6C_1w_0}, Q_3 = \frac{1}{R_5C_2w_0} \qquad \text{(III. 4)}$$

$$Q_4 = \frac{1}{R_2C_2w_0}, Q_5 = \frac{1}{R_4C_2w_0}, Q_6 = \frac{1}{R_3C_3w_0}$$

$$Q_7 = \left(\frac{1}{R_3C_3w_0} + \frac{1}{R_2C_3w_0} + \frac{1}{RC_3w_0}\right), w_0 = \frac{1}{\sqrt{R_2R_3C_2C_3}}$$

Le changement de variable sert à rendre les grandeurs adimensionnelles. On obtient le système d'équations différentielles suivant **[29]** :

$$\dot{x} = -Q_1 + Q_2 z$$

$$\dot{y} = Q_3 x - Q_4 z + Q_5(x) \qquad \text{(III .5)}$$

$$\dot{z} = Q_6 y - Q_7 z$$

III.4. Simulation en Matlab

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

Les techniques de Runge-Kutta sont des schémas numériques à un pas qui permettent de résoudre les équations différentielles ordinaires. Elles font parties des méthodes les plus populaires de parleur facilité de mise en œuvre et leur précision.

C'est Carle Runge et Martin Kutta qui, au début du XXe siècle, ont inventé ces méthodes.

Nous décrivons ici algorithme assez utilisés : celles de Runge-Kutta d'ordre 4 **[30].**

1. Initialisation du pas h, de la durée T.
2. Initialisation des conditions initiales : $t = 0 \ \ et \ y = y(0)$
3. Définition de la fonction $f(t, y)$.
4. Tant que $t \leq T$ faire :
5. Calcul de $K_1 = h.f\ (t_n, y_n)$
6. Calcul de $K_2 = h.f(t_n + h_2, y_n + k_{12})$
7. Calcul de $K_3 = h.f(t_n + h_2, y_n + K_{22})$
8. Calcul $de \ \ K_4 = h.f(t_n + h, y_n + k_3\ )$
9. $e.y = y + \frac{h}{6}(k_1 + 2K_2 + 2K_3 + K_4); t = t + h.$
10. Enregistrement des données.

III.5. Résultats des simulations

La figure (III.4) présente un état chaotique dans l'espace de phase par l'utilisation de l'algorithme Runge kutta sous MATLAB et la figure (III.5) présente l'évolution des trois variable (x, y, z) du système non linéaire de chaos en fonction du temps dont les paramètres du circuit sont (Q1=1.5, Q2=2.5, Q3=0.85, Q4=-1, Q5=3, Q6=3,Q7=10 ; x0= 0. 3, y0= 0.6, z0=0.4).

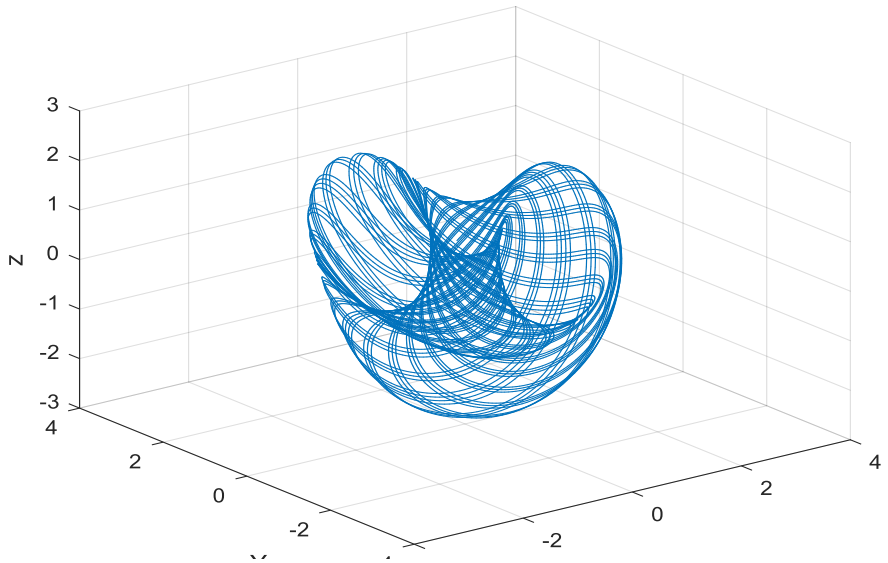
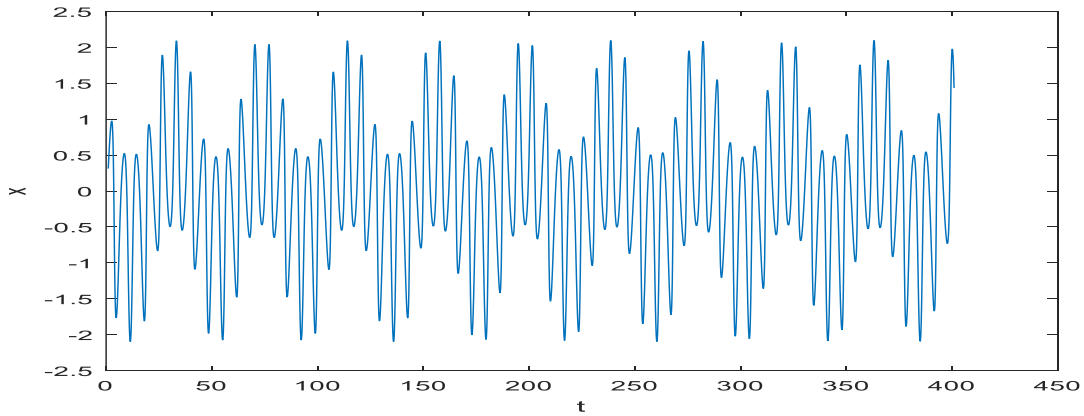


Figure III.4 : Espace de phase de système de l'oscillateur de Sprott **(x0= 0. 3, y0= 0.6, z0=0.4).**

La figure III.5 présente le comportement chaotique dans le domaine temporel.



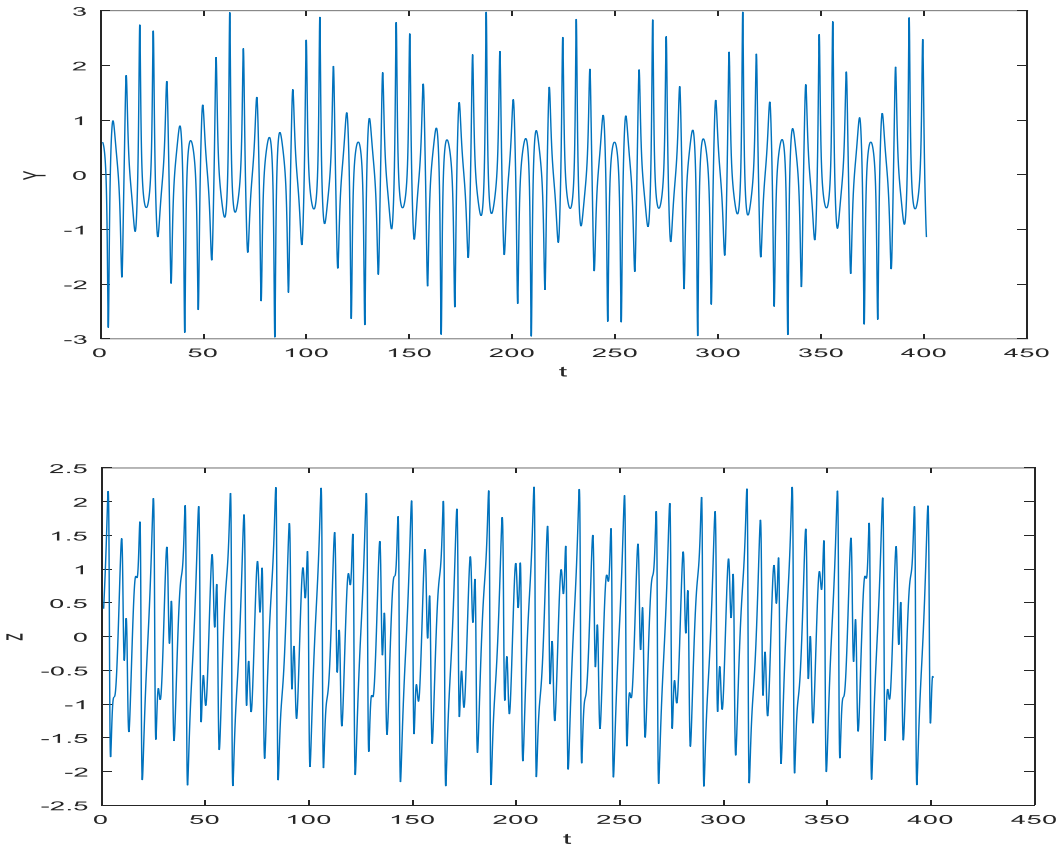


Figure III.5 : signal chaotique x(t), y(t) et z(t).

Dans le cas d'un système chaotique,la modification des condition initiales permet de modifier la trajectoire pour l'évolution d'un attracteur a un autre. La trajectoire est ainsi déterminée par le comportement non linéaire du système et commandée par la modification des condition initiales du système. Un autre exemple pour d'autres contions initiales du systém est présenté dans les figures (**Figure III.6** et **Figure III.7**).

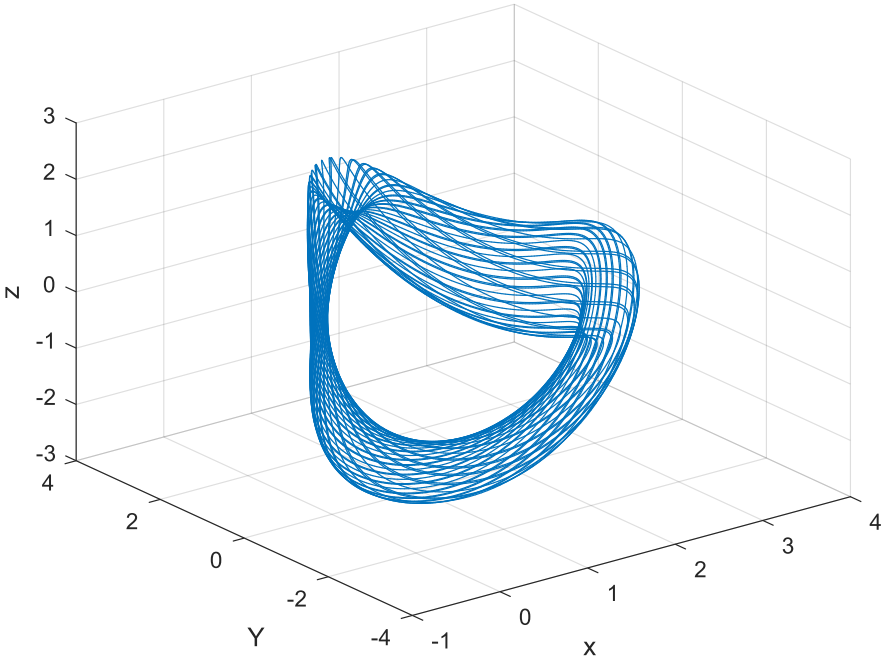
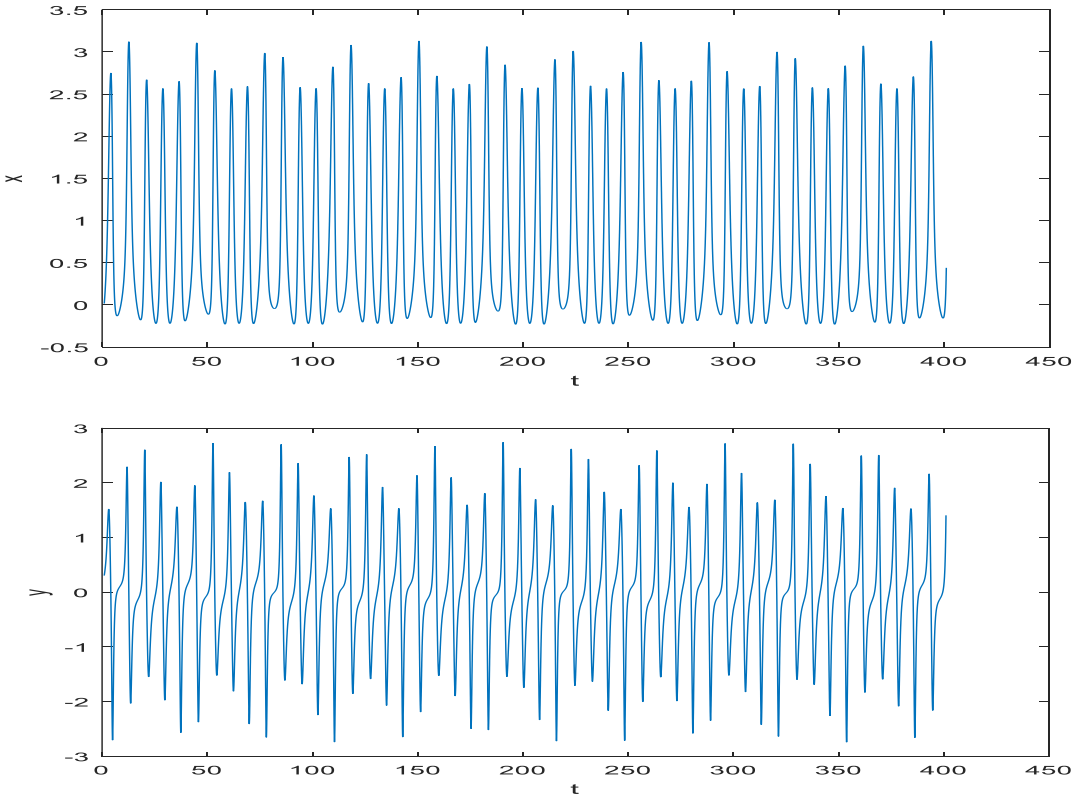


Figure III.6 : Espace de phase de système de ’oscillateur de Sprott **(x0= 0. 1, y0= 0.3, z0=0.8).**



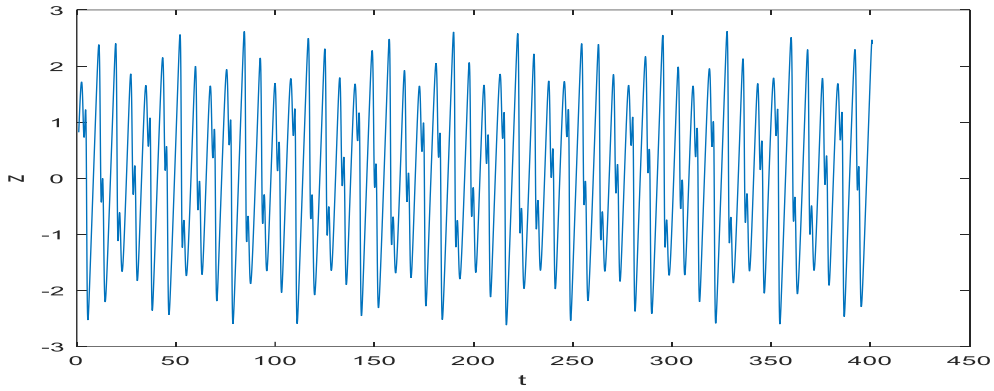


Figure III.7 : signal chaotique x(t), y(t) et z(t), Sprott **(x0= 0. 1, y0= 0.3, z0=0.8).**

III.6. Chiffrement d'une image

Nous avons utilisé l'algorithme Runge kutta pour simuler le model de l'oscillateur de Sprott.

Pour crypter une image on doit tout d'abord :

1. Convertir l'image en matrice des pixels, après cette étape
2. On choisit une clé de cryptage (symétrique) dont la clé utilisée est les conditions initiales de l'oscillateur chaotique.
3. On fait mélanger les valeurs de la matrice par le signal chaotique délivré par l'oscillateur de Sprott.
4. Et pour faire le décryptage de cette image, on soustrait le signal chaotique de l'image chiffrée pour obtenir l'image originale.

Les exemples de cryptage des images en niveau de gris sont illustrés par les figures suivantes:

➢ Résultats de tests

a. Exemple 1

Une image est une extension d'un signal de deux dimensions. Pour essayer cette méthode de cryptage en utilise l'image « **cameraman.tif** » de 256*256 pixels.

Image originale

Figure III.8 : L'image originale à crypter.

Le signal chaotique est mélangé par l'image originale à crypter, la figure (III.9) présente une image embrouillée où les positions et les valeurs des pixels sont complètement changées.

Image cryptée

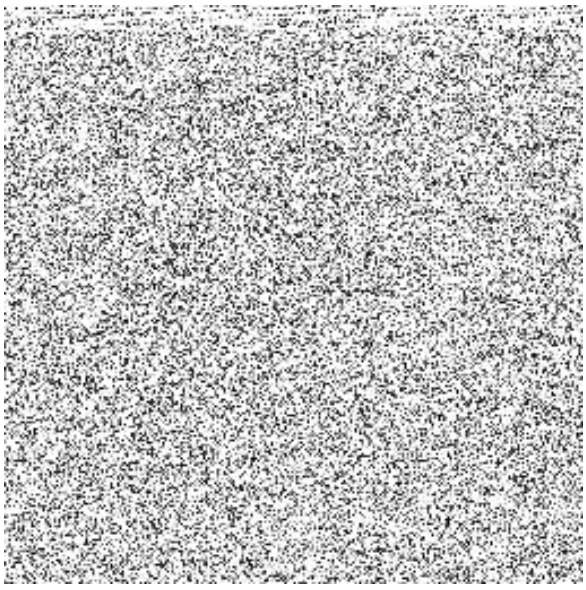


Figure III.9 : L'image cryptée.

Après addition du signal chaotique aux valeurs de pixels de l'image, nous obtenons l'image cryptée qui est la même image reçue à la réception Figure (III.10).

Image reçue

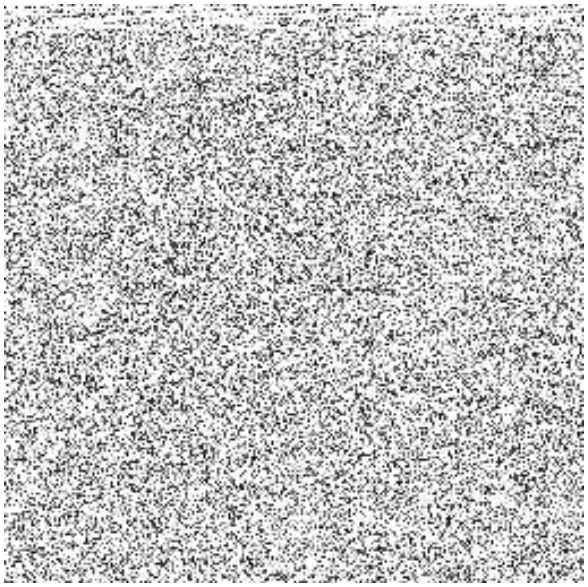


Figure III.10 : Image reçue avant décryptage.

Pour revenir à l'image originale Nous faisons décrypter l'image cryptée est l'inverse du processus de cryptage d'image.

Image décryptée

Figure III.11 : Image décryptée.

b. Exemple 2

Un autre exemple, c'est l'image onion.png en gris.

Image originale

Figure III.12 : L'image originale à crypter.

image cryptée

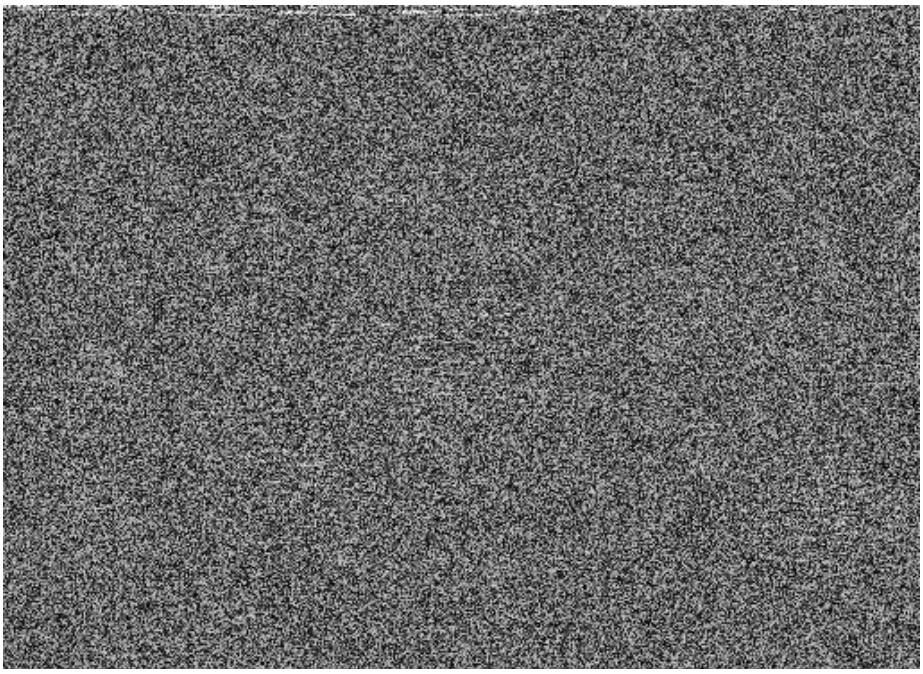


Figure III.13 : L'image cryptée.

image reçue

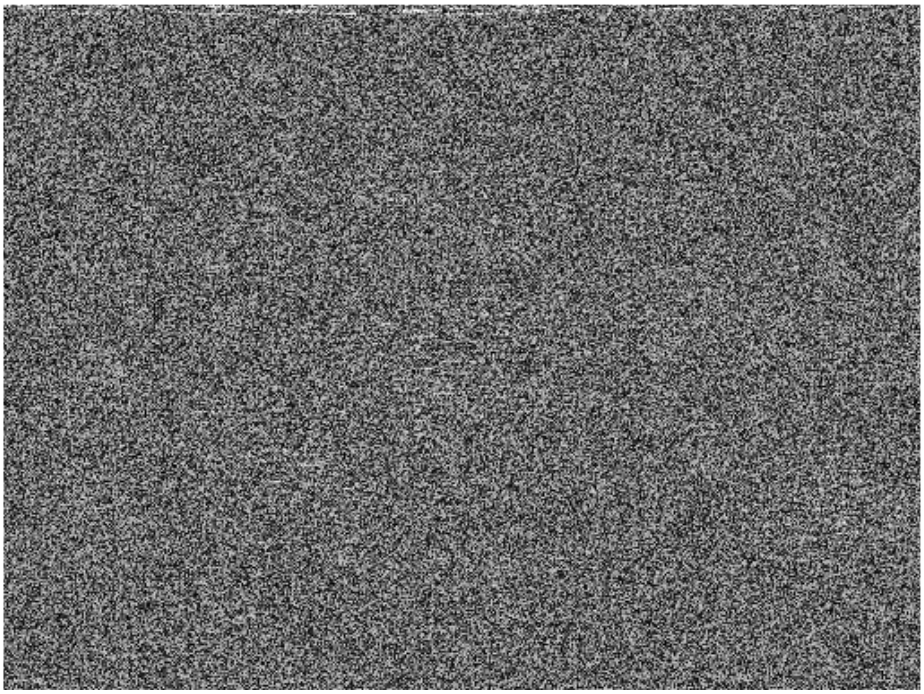


Figure III.14 : Image reçue avant décryptage.

Image décryptée

Figure III.15 : Image décryptée.

Le décryptage est le processus de conversion d'un message chiffré en un message clair pour le destinataire en utilisant la clé de cryptage. Le processus de décryptage utilise la technique inverse de cryptage. Le décryptage est donc très difficile sans la clé de chiffrement convenable.

III. 8. Conclusion

Dans ce chapitre nous avons étudié l'oscillateur de Sprott permettant de générer un signal chaotique non linéaire déterministe. Ce signal doit être mélangé par le signal à transmettre pour le crypter et protéger ce dernier. Les résultats de simulation nous montrent l'efficacité de l'utilisation du chaos pour crypter les images.

Conclusion générale

Conclusion générale

Un système chaotique est un système dynamique qui évolue dans un domaine borné avec des orbites apériodiques infiniment denses. Leurs caractéristiques à un comportement instable et non linéaire défini par une formule mathématique. Le comportement chaotique est causé par la haute sensibilité du système dans son état initial.

De nos jours, La sécurisation des informations contre les menaces et les piratages est un sujet très importants et essentiel dans les systèmes de télécommunication. La cryptographie est un outil de noyer l'information transmise pour assurer la sécurité. Pour cette raison nous avons étudié le cryptage des images et spécifiquement le cryptage chaotique.

Dans ce mémoire, Nous avons proposé d'utiliser la technique dite cryptographie symétrique a clé secrète pour le cryptage des images en gris en utilisant le signal délivré par l'oscillateur de Sprott.

Dans le premier chapitre de ce mémoire, nous avons donné quelques définitions générales des systèmes dynamiques chaotiques, tels que l'état continu et discret, nous avons présenté leurs caractéristiques telles que le déterminisme et la sensibilité aux conditions initiales. Ensuite, nous avons donné quelques exemples de systèmes chaotiques, tels que les systèmes de Lorenz, Rössler et Henon, ainsi que les points d'équilibre, leur stabilité, les méthodes de Lyapunov, les bifurcations et les domaines d'application des systèmes chaotiques.

Dans le deuxième chapitre, nous avons présenté les types de cryptage et les concepts de base des systèmes de cryptage. Nous avons expliqué le codage chaotique pour cacher des informations utiles qui seraient transmises par des signaux chaotiques. Nous explorons également différents principes de synchronisation de systèmes chaotiques en introduisant des méthodes et des types de synchronisation.

Dans le chapitre trois et après avoir étudié l'oscillateur non linéaire et chaotique de Sprott. Nous avons testé la méthode de cryptage en Matlab. Les résultats de simulation, nous montrent la robustesse de cryptage et de décryptage. Cela signifie l'efficacité de

l'utilisation du chaos pour la sécurisation des informations. En perspectif, nous envisageons de tester cette technique sur des images en couleur.

Bibliographie

Bibliographie

[1]: Site webe: https://si.blaisepascal.fr/1t-systemes-dynamiques/

[2]: Site webe: https://www.phys.ens.fr/IMG/pdf/fiche_chaos.pdf

[3]: Frédéric, L. "COURS MASTER-2 CommETUDE DES SYSTEMES NON LINEAIRES ande Robuste et Systèmes Non Linéaires".

[4]: M.HAMICHE.HAMID. "ÉTUDE ET RÉALISATION D'UN SYSTEME CHAOTIQUE BASÉ SUR LE CIRCUIT DE CHUA".Mémoire de Fin d'Etudede MASTER PROFESSIONNEL.UNIVERSITE MOULOUD MAMMERI DE TIZ-OUZOU,2014.

[5] :S.Khemidja, Guendouz, A., A.Badaoui. "Etude des suites chaotiques et leurs applications en cryptage d'images".Memoire Présenté pour obtenir LE DIPLOME DE LICENCE.Université de Mohamed El-Bachir El-Ibrahimi - Bordj Bou Arreridj.2021.

[6] : BENHABIB. Chouaib, "ETUDE D'UN SYSTEME CHAOTIQUE POUR LA SECURISATION DES COMMUNICATIONS OPTIQUES". MEMOIRE Pour l'obtention du diplôme de MASTER TELECOMMUNICATIONS. L'UNIVERSITE DE TLEMCEN.2014.

[7] : Chahrazed. B et Inass . Z. "Nouveau schéma de communication sécurisée à base du chaos" 'Mémoire préparé en vue de l'obtention du diplôme de Master Mathématiques, Centre universitaire Abd Elhafid Boussouf Mila,2020.

[8] : Rofia , HANK Amina .YOUNSI. "SYSTEMES CHAOTIQUES POUR LA TRANSMISSION SECURISEE DE DONNEES' 'Mémoire de fin d'études Pour L'Obtention du Diplôme Master en Télécommunication. Université Mohammed Seddik Benyahia-Jijel.2020.

[9]: HAMICHE, M. H. "Conception et étude d'un système de transmission sécurisée de données à base d'un système chaotique d'ordre fractionnaire, Mémoire de Fin d'Etudes de MASTER ACADEMIQUE Automatique. Université Mouloud Mammeri de Tizi-Ouzou ,2015.

[10] : AZIRA HIBA, K. M. "Analyse et implémentation du système chaotique de Qi' 'Mémoire de Master Mention électroniques. Université SAAD DAHLAB DE BLIDA,2016.

[11]: Amine K, Farid. "Conception et réalisation d'un système de transmission sécurisé de données basé sur le chaos en utilisant la carte". Mémoire de Fin d'Etudes de MASTER ACADEMIQUE.UNIVERSITE MOULOUD MAMMERI DE TIZI-OUZOU.2016.

[12] : FEKHR EL ISLAM KHELIL. "Les systèmes chaotiques pour le chiffrement" Mémoire de fin d'études Pour l'obtention du diplôme de Master. Université Larbi Ben M'hidi - Oum El Bouaghi,2021.

[13] Site web: http://guerillot.chez.com/physique/chaos/chaos4.htm

[14] : Dib, Sonya. "Etude des systèmes dynamiques à temps' 'Mémoire préparé En vue de l'obtention du diplôme de Master Mathématiques. Centre Universitaire Abd elhafid boussouf Mila.2022.

[15] : Chahra, LEMMOUCHI. "Utilisation d'une rotation 3D et des systèmes chaotiques pour le cryptage d'images' 'Pour l'obtention du diplôme de Master en informatique. Université d'Oum El Bouaghi,2013.

[16] : Saadi Alima. " Les système chaotiques et leur application dans la sécurité de communication ", Mémoire présenté en vue de l'obtention du diplôme de Master Mathématiques. Université MOHAMED KHIDER, BISKR, 2021.

[17]: I. BELKADI and N. AMIAR. "Cryptage d'image par considération des plans de bits des pixels séparément par ordre de leurs poids avec une clé publique de taille libre". Mémoire Pour l'obtention du diplôme de Master en informatique. UNIVERSITE LAEBI BEN M'HIDI OUM EL BOUAGHI,2018.

[18]: Site webe : file:///C:/Users/Win%2010/Downloads/Documents/chapitre1_2.pdf

"Généralité sur la cryptographie ".chapitre1_2.pdf,2012.

[19]:N.REBHI, M.A BEN FARAH, A. KACHOURI, M. SAMET. "Analyse De Sécurité d'une Nouvelle Méthode De Cryptage Chaotique". Laboratoire d'Electronique et des Technologies de l'Information (LETI). Ecole Nationale d'Ingénieurs de Sfax B.P.W. 3038 Sfax, Tunisie,2007.

[20]: C. Merdjal and A. Merakchi. "cryptage d'image par un signal unidimensionnel quelconque ". Mémoire pour l'obtention du diplôme de master en informatique. Université Larbi ben M'hidi Oum el Bouaghi, 2019.

[21]: M.A. BEN AMMARI and M. K. HADDOUCHE .

"amélioration de la génération des sous clés del'algorithme cryptographique DES ".mémoire de master pour obtenir le diplôme en systèmes électroniques complexes.universite akli mohand oulhadj bouira,algerie,2017.

[22]:Site webe:
file:///C:/Users/Win%2010/Downloads/Documents/Crypto_CM_chap1.pdf

[23]: HAMICHE, HAMID. "Inversion a Gauche des Systemes Dynamiques Hybrides Chaotiques. Application a la Transmission Sècurisèe de Donnèes". THÈSE DE DOCTORAT,2011.

[24]:Site webe : file:///C:/Users/Win%2010/Downloads/Documents/chapitre1.pdf

[25]: M. KOUIDRI and A. DAIFI. "ÉTUDE DE LA SYNCHRONISATION DE DEUX CIRCUITS IDENTIQUES GENERATEURS DE SIGNAUX CHAOTIQUES".Mémoire de fin d'Etude pour l'obtention du diplôme de Master en Electromécanique et Systèmes de Commandes(ESC) .Université de Bouira,2016.

[26]: M. MEGHERBI OUERDIA. "Etude et réalisation d'un système sécurisé à base de systèmes chaotiques".MEMOIRE DE MAGISTER.UNIVERSITE MOULOUD MAMMERI TIZI-OUZOU,2013.

[27]: Z.Zine and F. Bounar. "Application du chaos pour le cryptage des données".MEMOIRE DE FIN D'ETUDE.UNIVERSITE MOHAMED SEDDIK BENYAHIA JIJEL,2022.

[28] : A. BERKANE, "transmission sécurisée à base de la synchronisation impulsive de deux système chaotique discrets", Mémoire de master Professional. Université Mouloud Mammri de Tizi-Ouzo,2016.

[29]: M. A. DJENOURI and M.H. CHIKHI. "Communication sécurisée par chaos: Etude et implémentation sur carte FPGA"Mémoire de Projet de Fin d'ÉtudesPour l'obtention du diplôme de Master en Électronique.Université SAAD DAHLAB de BLIDA,2014.

[30]: Site webe: https://femto-physique.fr/analyse-numerique/runge-kutta.php