République **A**lgérienne **D**émocratique et **P**opulaire
Ministère de L'**E**nseignement **S**upérieur et de la **R**echerche **S**cientifique

UNIVERSITE **M**OULOUD **M**AMMERI DE **T**IZI-**O**UZOU

FACULTE DE GENIE ELECTRIQUE ET D'INFORMATIQUE
DEPARTEMENT D'ELECTRONIQUE

Mémoire de Fin d'Etude

EN MASTER PROFESSIONNEL

Filière : Génie électrique
Spécialité : Electronique Industrielle

Présenté par :

M. Omar AIT ALI
M. Farid AMIR

Mémoire dirigé par : **M. Hamid HAMICHE**

Co-dirigé par : **M^{elle} Sarah KASSIM**

Thème

Conception et étude d'un nouveau système de transmission d'image sécurisée par le chaos

Mémoire soutenu publiquement le 27 Septembre 2016 devant le jury composé de :

M Mourad LEHDIR	Président
M Youcef ATTAF	Examinateur
M Boussaad IJDRI	Examinateur

Promotion : 2016

Remerciements

On exprime nos remerciements les plus sincères à notre encadreur Mr Hamid HAMICHE, maitre de conférences a l'université Mouloud Mammeri, sous la direction duquel on a eu le plaisir de travailler. Ses conseils, ses critiques, et sa rigueur scientifique nous ont permis de réaliser ce travail.

Nous tenons particulièrement à exprimer notre profonde gratitude à M^{lle} Sarah KASSIM, Doctorante à l'université Mouloud Mammeri, qui a suivi l'évolution de notre travail avec une disponibilité permanente.

On ne manquera pas de remercier tous les membres du jury de nous avoir honorés par leur présence et d'avoir accepté d'évaluer notre travail.

Dédicaces

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

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

Sommaire

Sommaire

Liste des figures

Liste des figures

Liste des tableaux

Introduction générale

En 1963 Edward Lorenz expérimentait une méthode lui permettant de prévoir les phénomènes météorologiques [1]. C'est par pur hasard qu'il observa qu'une modification minime des données initiales pouvait changer de manière considérable ses résultats. Lorenz venait de découvrir le phénomène de sensibilité aux conditions initiales. Les systèmes répondant à cette propriété seront à partir de 1975 dénommés : systèmes chaotiques. C'est donc au cours des années soixante dix que la théorie du chaos a pris son essor. Cependant, les travaux de certains scientifiques menés bien avant cette découverte vont être très utiles à la compréhension de la dynamique chaotique. En effet, vers la fin du XIXe siècle le mathématicien, physicien et philosophe français Henri Poincaré avait déjà mis en évidence le phénomène de sensibilité aux conditions initiales lors de l'étude astronomique du problème des trois corps. [2]

L'emploi du chaos pour la transmission sécurisée de l'information a été considéré dans les dernières années comme une solution très prometteuse pour augmenter les performances des systèmes de transmission actuels. Ainsi, on trouve dans la littérature une multitude d'applications et d'études réalisées concernant plusieurs aspects de la transmission [3], [4], [5]. Grâce à ses caractéristiques quasi stochastiques le chaos offre une solution possible pour les systèmes à probabilités réduites de détection et d'interception ainsi que des applications dans l'accès multiple. En contradiction avec ces aspects positifs qui font du chaos une solution très attirante, il faut préciser qu'a priori la synchronisation entre deux systèmes dynamiques chaotiques, nécessaire à la récupération de l'information transmise, est difficile à réaliser [6].

Cacher des informations particulières à certaines personnes a toujours été un des intérêts principaux de l'Homme. On a ainsi cherché à établir des techniques dites de « cryptage » afin de rendre ces informations incompréhensibles à ceux qui n'ont pas accès à une « clé » secrète. Ces techniques intéressent des personnes de divers domaines que ce soit le militaire, le commercial ou tout simplement personnel [7].

Dans ce mémoire, nous allons concevoir et étudier un système de transmission sécurisé d'une image numérique à base du chaos.
Le mémoire est structuré comme suit :
Dans le premier chapitre, nous allons donner des rappels sur les différents systèmes, et principalement sur les systèmes dynamiques chaotiques, définir le chaos, ses classes et ses caractéristiques, par la suite on donnera deux exemples de systèmes chaotiques discret que l'on va simuler sous Matlab.

Dans le chapitre suivant, nous allons essayer de définir la synchronisation, concept et classes ainsi les différentes méthodes. Par la suite, on s'intéressera à la cryptographie chaotique, dont on aura à citer quelques techniques de chiffrement à base du chaos.

Dans le chapitre trois, nous allons concevoir un schéma de transmission de données numériques qui est une image dans notre cas à base de la synchronisation chaotique. On choisit le système émetteur, et le système récepteur, par la suite nous allons exposer les résultats de simulation sous Matlab.
On termine par une conclusion générale et quelques perspectives.

Chapitre I :
Généralités sur les systèmes chaotiques

I.1.Introduction :

Depuis longtemps, le chaos était synonyme de désordre et de confusion. Il s'opposait à l'ordre et devait être évité. La science était caractérisée par le déterminisme, la prévisibilité et la réversibilité. Poincaré fut l'un des premiers à entrevoir la théorie du chaos. Il a découvert la notion de sensibilité aux conditions initiales à travers le problème de l'interaction de trois corps célestes [8].

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 d'horizons 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, nous nous intéresserons principalement dans ce chapitre aux systèmes dynamiques chaotiques où nous attarderons sur les espaces de phases, les attracteurs étranges et les scénarios de transition vers le chaos (appelé aussi bifurcations), qui nous permettront de mieux comprendre la nature du chaos.

I.2. Généralités sur les systèmes chaotiques :

I.2.1. Système Dynamique :

Un système dynamique est un système physique qui évolue dans le temps, ou par rapport à une autre variable suivant l'espace de phase considéré. Ce dernier est réparti sur plusieurs états et structuré selon certaines propriétés; il est le plus souvent régi par un ensemble d'équations différentielles décrivant le mouvement des composants (leur dynamique).
Un système dynamique évolue au cours du temps de façon à la fois, causale, c'est-à-dire que son avenir ne dépend que de phénomènes du passé ou du présent ; et déterministe, c'est-à-dire qu'à une « condition initiale » donnée à l'instant « présent » va correspondre à chaque instant ultérieur un seul état « futur » possible.
Un système dynamique, présente deux types de variables: dynamiques et statiques. Les variables dynamiques sont les quantités fondamentales qui changent avec le temps. Les variables statiques, encore appelées paramètres du système, sont fixes. Il existe deux types de systèmes dynamique, linéaire, et non linéaire.

a)- Système dynamique linéaire :

Un système est dit linéaire (continu ou discret) si on distingue une relation entre les grandeurs d'entrée et de sortie, qui peut être définie par des équations différentielles linéaires (à coefficients constants).
Ces dernières vérifient alors les principes de proportionnalité des effets aux causes, et de superposition. Les solutions d'une équation linéaire forment un espace vectoriel, ce qui permet l'utilisation de l'algèbre linéaire et simplifie considérablement l'analyse.
Exemple 1:
Considérons le système linéaire continu suivant :

$$x_{t+1} = 3x_t \tag{I.1}$$

Dans ce cas, le membre de droite de l'équation est une fonction dépendant linéairement de *x*.
La somme de deux solutions d'un système linéaire est également solution (« principe de superposition »).

b)- Système dynamique non linéaire :

Un système non linéaire (continu ou discret) est un système qui ne peut pas être décrit par des équations différentielles linéaires à coefficients constants.
Cela explique la complexité de ce type de systèmes, dont on ne dispose pas de théorie générale pour l'étude de ces derniers.
Par ailleurs, plusieurs méthodes sont adaptées à certaines classes de systèmes non linéaires.

Prenons comme exemple le système non linéaire continu de Lorenz régit par les équations différentielles suivantes :
Exemple 2:

$$\begin{cases} \dot{x} = a(y - x) \\ \dot{y} = x(b - z) - y \\ \dot{z} = xy - cz \end{cases} \tag{I.2}$$

Le plan de phase de ce système est illustré par la figure suivante:

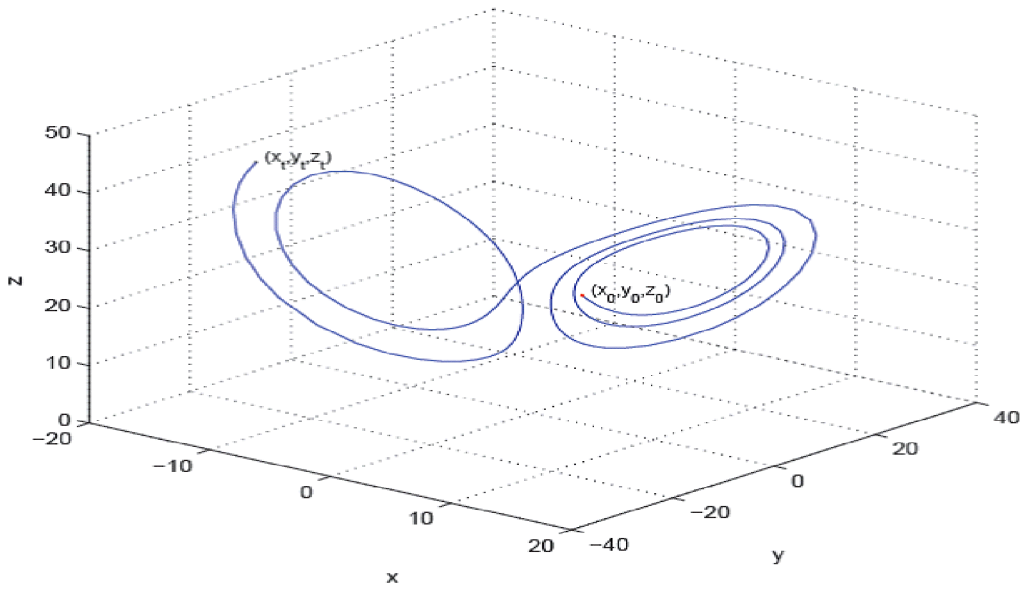


Fig. 1 : Exemple de trajectoire pour le système Lorenz

I.2.2. Système dynamique chaotique :

Le chaos se rattache principalement à une notion d'imprévisibilité.
Il présente un phénomène fondamental d'instabilité appelé « sensibilité aux conditions initiales », ce qui les rend non prédictible en pratique, ainsi l'impossibilité de prévoir une évolution à long terme du fait que l'état final dépend de manière si sensible de l'état initial.
Le chaos est défini généralement comme un comportement semblant aléatoire (imprévisible) d'un système dynamique défini par des équations différentielles déterministes.
Un système chaotique est un système dynamique non linéaire. Un système linéaire ne peut pas être chaotique.
On appelle donc un système dynamique chaotique, un système qui dépend de plusieurs paramètres. Il n'est pas déterminé ou modélisé par des systèmes d'équations linéaires ni par les lois de la mécanique classique.
Un système chaotique a des règles fondamentales déterministes et non probabilistes.
Il est généralement régi par des équations différentielles non linéaires qui sont connues, donc par des lois rigoureuses et parfaitement déterministes.
Certains phénomènes dynamiques non linéaires sont si sensibles aux conditions initiales, que même s'ils sont régis par des lois rigoureuses et parfaitement déterministes, les prédictions exactes sont impossibles.
Une autre propriété des phénomènes chaotiques est qu'ils sont très sensibles aux perturbations.

I.3. Théorie du Chaos :

La théorie du chaos est une des rares, une des très rares, théories mathématiques qui a connu un vrai succès médiatique. C'est même devenu une théorie à la mode qu'il est de bon ton de pouvoir citer si l'on veut passer pour quelqu'un de cultiver.
Il n'est pas rare d'entendre quelqu'un qualifier une situation de chaotique. Cette qualification porte par nature l'idée que cette situation relève du désordre ou de la plus grande confusion. Les phénomènes dans lesquels on ne pouvait déceler à priori aucune logique ont progressivement été regroupés sous le terme de "chaos".
Il n'existe pas de définition rigoureuse du chaos, il faut admettre la notion de "phénomène imprévisible et erratique".
Cependant, depuis une vingtaine d'années, on attribue le terme chaos à des" comportements erratiques qui sont liés à des systèmes simples pouvant être régis par un petit nombre de variables entre lesquelles les relations décrivant leur évolution peuvent être écrites. Ces systèmes sont donc déterministes bien qu'imprévisibles.
La théorie du chaos, déjà entrevue par Jacques Hadamard et Henri Poincaré au début du XXe siècle, a été définie à partir des années 1960 par de nombreux scientifiques.
On appelle chaotique des phénomènes complexes, dépendant de plusieurs paramètres et caractérisés par une extrême sensibilité aux conditions initiales: par exemple, les volutes décrites par la fumée d'une cigarette, ou la trajectoire d'un ballon qui se dégonfle.
Ces courbes ne sont pas déterminées, modélisées par des systèmes d'équations linéaires ni par les lois de la mécanique classique; pourtant, elles ne sont pas nécessairement aléatoires, relevant du seul calcul des probabilités : elles sont liées au chaos dit déterministe.
L'imprédictibilité est présente dans de tels systèmes, qui n'en sont pas moins munis d'un ordre sous-jacent.
Les signaux chaotiques peuvent être obtenus à partir de circuits non linéaires où interviennent des paramètres.
Géométriquement, ces phénomènes dynamiques sont représentés dans un espace dont la dimension, qui peut être supérieure à celle de l'espace à trois dimensions, dépend du nombre de paramètres choisis pour les décrire. À chaque instant, l'état du phénomène est représenté par un point dans cet espace appelé espace des phases. L'évolution du système est décrite par la trajectoire de ce point. Pour les phénomènes les plus simples, ce point est attiré vers un point d'équilibre ou une courbe limite, près duquel il repasse périodiquement. Les mathématiciens appellent ces courbes limites des attracteurs étranges.

I.3.1. Classe des systèmes chaotiques :

Il existe plusieurs systèmes chaotiques utilisés pour générer les signaux chaotiques. On présente dans ce qui suit deux classes : les systèmes chaotiques à temps continus, et les systèmes chaotiques à temps discrets.

a)- Système chaotique a temps continu :

Un système chaotique à temps continu est régi par un système d'équations différentielles de la forme :

$$\dot{x} = f(t, x, u) \; ; \; \dot{y} = h(t, x, u) \tag{I.3}$$

Si ce système ne dépend pas de l'entrée alors on aura :

$$\dot{x} = f(t, x) \tag{I.4}$$

Il existe plusieurs systèmes chaotiques à temps continus, parmi eux on peut citer :
Le système de Lorenz, Rossler, le circuit de Chua…etc.

- Système de Lorenz :

Il est représenté par le système d'équations suivant :

$$\begin{cases} \dot{x} = a(y - x) \\ \dot{y} = x(b - z) - y \\ \dot{z} = xy - cz \end{cases} \tag{I.5}$$

Les variables x, y, z représentent l'état du système à chaque instant, ainsi a, b, c représentent les paramètres du système.
Le système de Lorenz présente un comportement chaotique pour les valeurs :$a = 10$, b = 28, c = $\frac{8}{3}$.
L'attracteur de Lorenz présente un phénomène dit l'effet papillon.

b)- Système chaotique à temps discret :

Un système chaotique à temps discret est régi par un système d'équations différentielles de la forme :

$$x(k + 1) = G(x(k)u(k)y(k)) = (h(k), u(k)) \tag{I.6}$$

On note parmi les systèmes chaotiques à temps discrets les systèmes de Hénon, Hénon modifié, la fonction logistique…etc.
L'exemple suivant illustre la fonction logistique, elle est représentée par l'équation suivante :

$$x_n \rightarrow fr(x_n) = x_{n+1} = r\, x_n (1 - x_n) \tag{I.7}$$

La fonction logistique a un comportement chaotique pour r=4.
Le diagramme de bifurcation nous permet de connaitre le comportement de la suite logistique en fonction du paramètre r.
Pour r=3 on observe un doublement de période (bifurcation) et pour r=4 on bascule vers le chaos.

I.3.2. Caractéristique des systèmes chaotiques :

Le chaos ne dispose pas de définition mathématique universellement accepté par conséquent, pour qu'un système soit classifié autant que chaotique il doit comporter les propriétés suivantes :

a)- Aspect Aléatoire :

Les systèmes chaotiques en tendance à se comporter de manière qui semble aléatoire, cela vient du fait que l'on est incapable de donner une description mathématique du mouvement sur le long terme, mais il est décrit par des équations non linéaires parfaitement déterministes.

b)- Sensibilité aux conditions initiales :

Cette propriété a été observée pour la première fois par E. Lorenz sur son modèle Météorologique [1]. Elle est connue sous le nom populaire d'effet papillon.
Vers la fin du 19ème siècle, Poincaré montrait que les trois orbites de 3 corps en mouvement sous une force centrale due à la gravité changent radicalement avec une petite modification des conditions initiales. Pour un système chaotique, une très petite erreur sur la connaissance de l'état initial X0 dans l'espace des phases va se trouver (presque toujours) rapidement amplifiée.

C)- Attracteur étrange :

Il est contenu dans un espace fini. Son volume est nul. Sa dimension est fractale et non entière, sa trajectoire est complexe, presque toutes les trajectoires sur l'attracteur ont la propriété de ne jamais passer deux fois par le même point. En d'autres termes, chaque trajectoire est apériodique ; deux trajectoires proches à un instant " t " voient localement leur distance augmentée à une vitesse exponentielle. Ce phénomène traduit la sensibilité aux conditions initiales ; toute condition initiale appartenant au bassin d'attraction, c'est-à-dire à la région de l'espace des phases dans laquelle tout phénomène dynamique sera "'attiré " vers l'attracteur, produit une trajectoire qui tend à parcourir de façon spécifique et unique cet attracteur.

d)- Exposants de Lyapunov : [8]

Il est difficile d'appréhender l'évolution chaotique, cela à cause de la divergence des trajectoires sur l'attracteur.
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 (voir figure ci-dessous).

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 :
$|Z2| \approx \exp(\lambda.\Delta t)\,|Z1|$

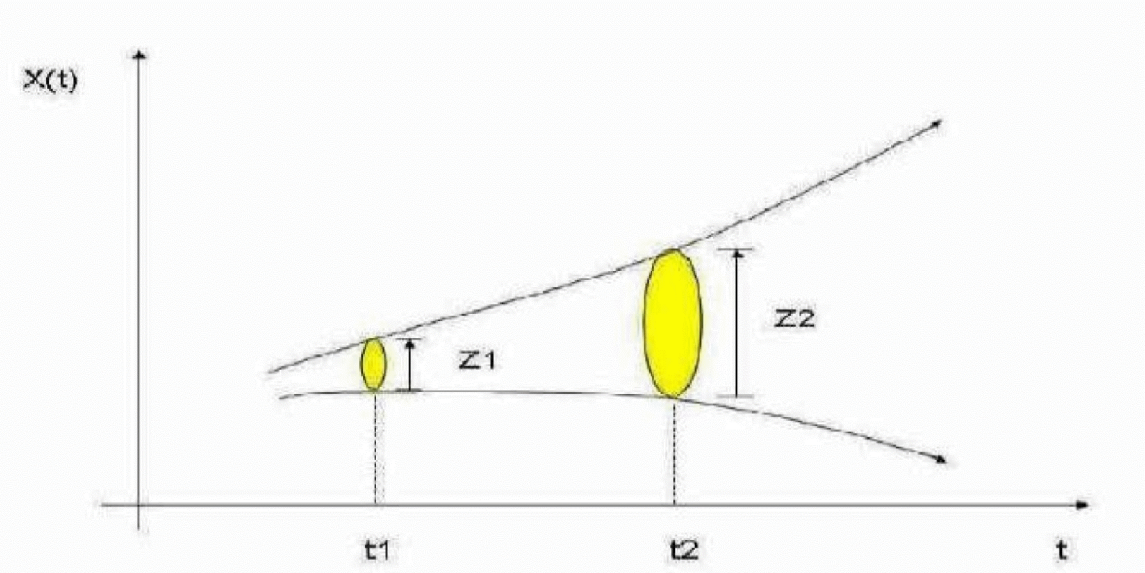


Fig. 2 : Divergence de deux trajectoires dans le plan de phase

Considérons un système dynamique dont l'espace des phases est de dimension n et prenons à t=0 une hyper sphère infiniment centré en X appartenant à l'attracteur ($X \in Rn$) avec un rayon ε_0.
Au temps $t >> 0$, cette hyper sphère se transforme en une hyper-ellipsoïde de n demi-axes

$$\varepsilon_i(t) \approx \varepsilon_0 \exp(\lambda_i t) \qquad i= 1, 2, \ldots n$$

Les exposants de Lyapunov sont tels que :

$$\lambda_i = \lim_{t\to\infty} \lim_{\varepsilon_0\to 0} \frac{1}{t} \log\frac{\varepsilon_i}{\varepsilon_0} \qquad (I.8)$$

Ils caractérisent de façon assez précise la dynamique du système.
Pour un attracteur non chaotique, les exposants de Lyapunov sont tous inférieurs ou égaux à zéro et leur somme est négative. Dans le cas continu, un attracteur étrange d'un système sans entrée possèdera toujours au moins trois exposants de Lyapunov, dont un au moins doit être positif. Dans le cas discret, le système peut avoir un seul état dont l'exposant de Lyapunov est positif. Plus de détails sont présentés au tableau suivant.

Etat	Attracteur	Dimension	Exposants de Lyapunov
Point d'équilibre	Point	0	$\lambda_n \leq \cdots \leq \lambda_1 \leq 0$
Périodique	Cercle	1	$\lambda_1 = 0$ $\lambda_n \leq \cdots \leq \lambda_2 \leq 0$
Période d'ordre 2	Tore	2	$\lambda_1 = \lambda_2 = 0$ $\lambda_n \leq \cdots \leq \lambda_3 \leq 0$
Période d'ordre K	K-Tore	K	$\lambda_1 = \cdots = \lambda_k = 0$ $\lambda_n \leq .. \leq \lambda_{1k+1} \leq 0$
Chaotique		Non entier	$\lambda_1 > 0$ $\sum_{i=1}^{n} \lambda_i < 0$
Hyper chaotique		Non entier	$\lambda_1 > 0 \ \ \lambda_2 > 0$ $\sum_{i=1}^{n} \lambda_i < 0$

Tableau (I.1) : Exposants de Lyapunov et Dimensions

e)- Fonction d'auto corrélation et spectre de puissance :

Le spectre de puissance (densité spectrale d'énergie d'un signal f(t)

$$v \longrightarrow \text{TF } [\text{f}(v)]^2$$

Corrélation : c'est la mesure de ressemblance du signal f avec lui-même dans le temps d'une valeur de t_0.

f)- Les sections de Poincaré : [10]

Henri Poincaré a apporté une contribution très utile pour l'étude des systèmes chaotiques. Parmi ces contributions on trouve les sections de Poincaré.
Faire une section de Poincaré revient à couper la trajectoire dans l'espace des phases, afin d'étudier les intersections de cette trajectoire avec, par exemple en dimension trois, un plan. On passe alors d'un système dynamique à temps continu à un système dynamique à temps discret. Les mathématiciens ont bien sûr démontré que les propriétés du système sont conservées après la réalisation d'une section de Poincaré judicieusement choisie.

g)- Bifurcation : [11]

Un autre ensemble de concepts utiles à l'analyse des systèmes dynamiques est la théorie de la "bifurcation". Ce concept renvoie à l'étude des changements de comportement d'un système lorsque les paramètres de ce dernier changent. La bifurcation signifie un changement qualitatif de la dynamique du système, qui résulte du changement d'un des paramètres du système. Par exemple, déstabilisation d'un équilibre stable, apparition ou disparition d'un cycle ou d'un attracteur, ...etc. La valeur pour laquelle la bifurcation se produit est nommée le point de bifurcation.

I.4. Exemples : Dans ce qui suit, nous allons tester quelques caractéristiques des systèmes chaotiques sur deux systèmes chaotiques l'un continu et l'autre discret.

I.4.1. Cas continu :

Considérons le système de Lorenz donné par (I.4) avec les mêmes paramètres.

a)- Aspect Aléatoire :

L'aspect aléatoire des états du système de Lorenz est donné par la figure suivante:

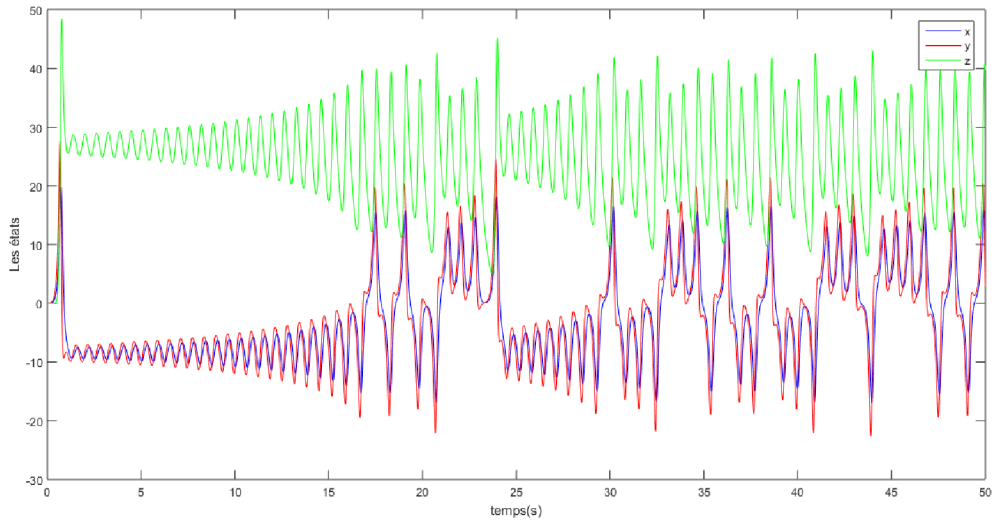


Fig. 3 : Aspect aléatoire des états du système de Lorenz

b)- Sensibilité aux conditions initiales :

La sensibilité aux conditions initiales est donnée par la figure ci-dessous:

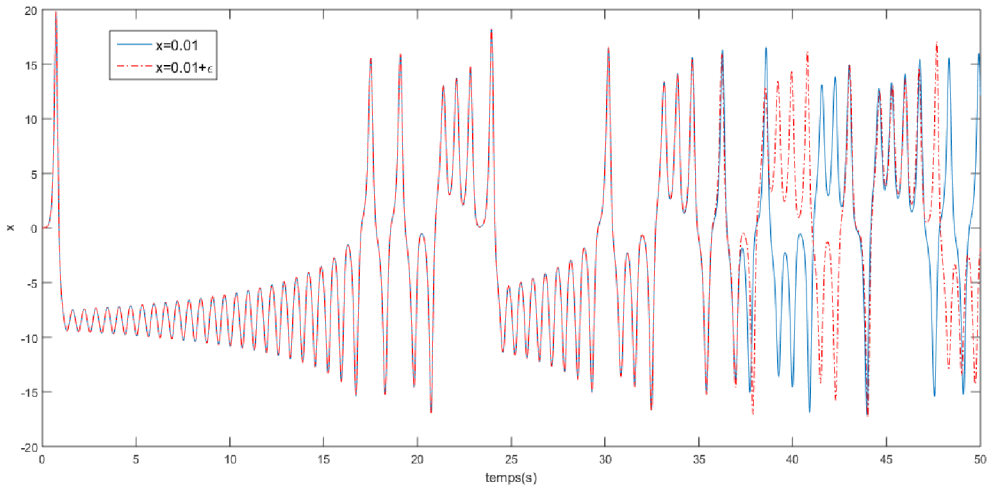


Fig. 4 : Sensibilité aux conditions initiales

C)- Attracteur de Lorenz :

L'attracteur étrange du système de Lorenz est donné par la figure ci-dessous :

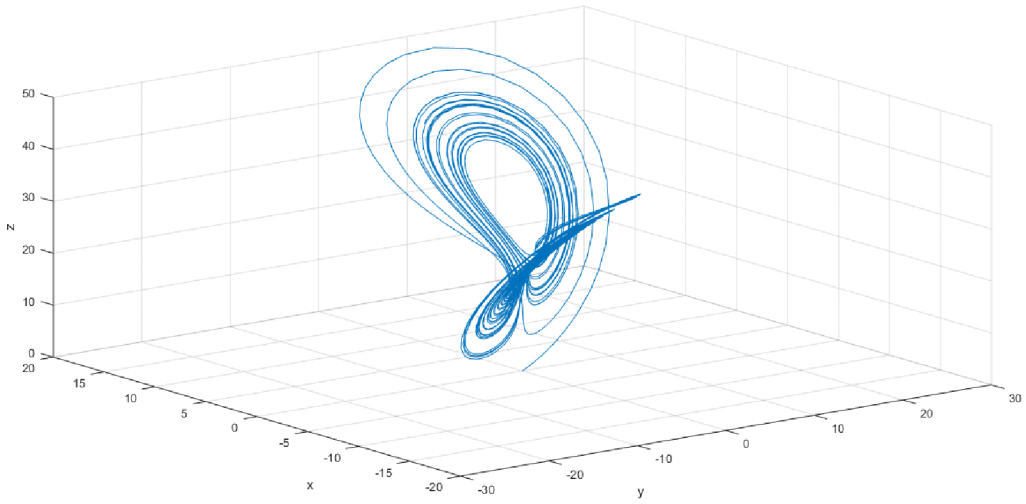


Fig. 5 : Attracteur de Lorenz

La sensibilité aux conditions initiales de deux attracteurs de Lorenz est donnée par la figure ci-dessous:

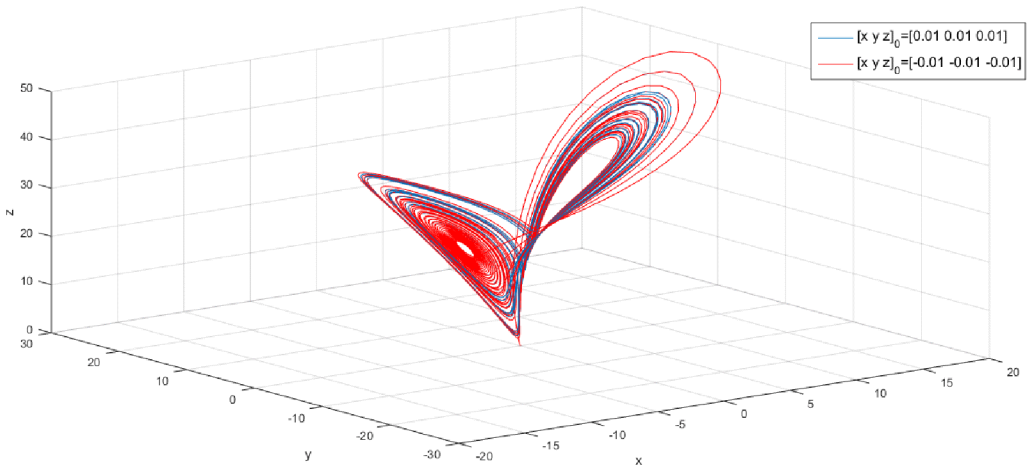


Fig. 6 : Sensibilité aux conditions initiales deux attracteurs

d)- Exposants de Lyapunov :

La figure suivante illustre le calcul des exposants de Lyapunov

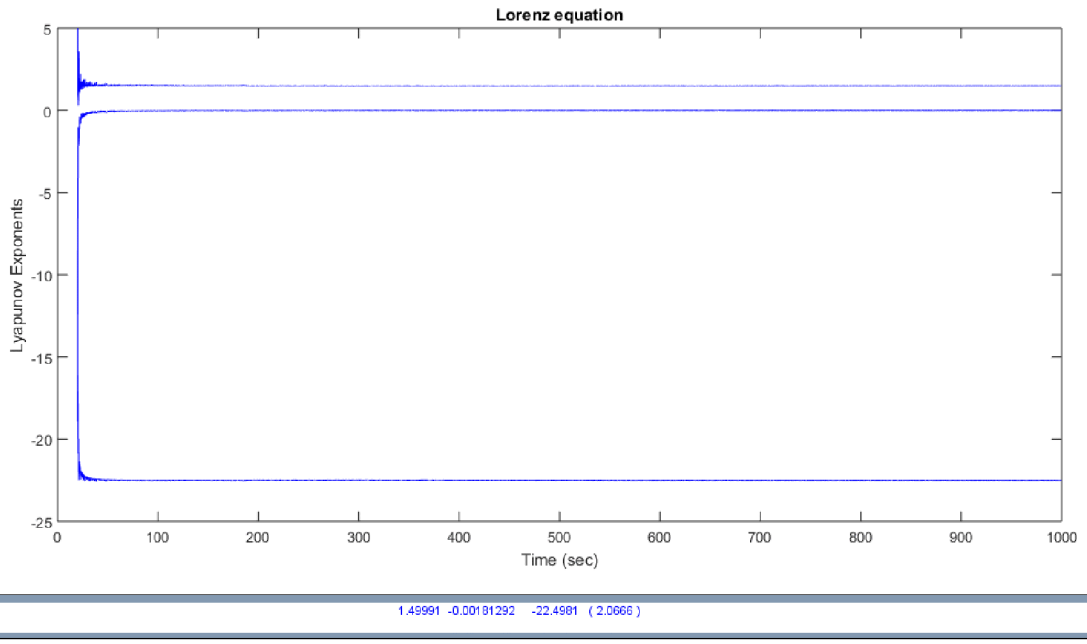


Fig. 7 : Exposants de Lyapunov du système continu de Lorenz

A travers les résultats obtenus en bas de la figure, nous constatons bien qu'il y a une valeur de la constante de Lyapunov positive (λ=1.49991). Ceci confirme bien que le système considéré est chaotique.

I.4.2. Cas discret :

Pour le cas de système chaotique discret, on considère la fonction logistique donnée par (I.7).

a)- Aspect Aléatoire :

L'aspect aléatoire de la fonction logistique est donné par la figure ci-dessous :

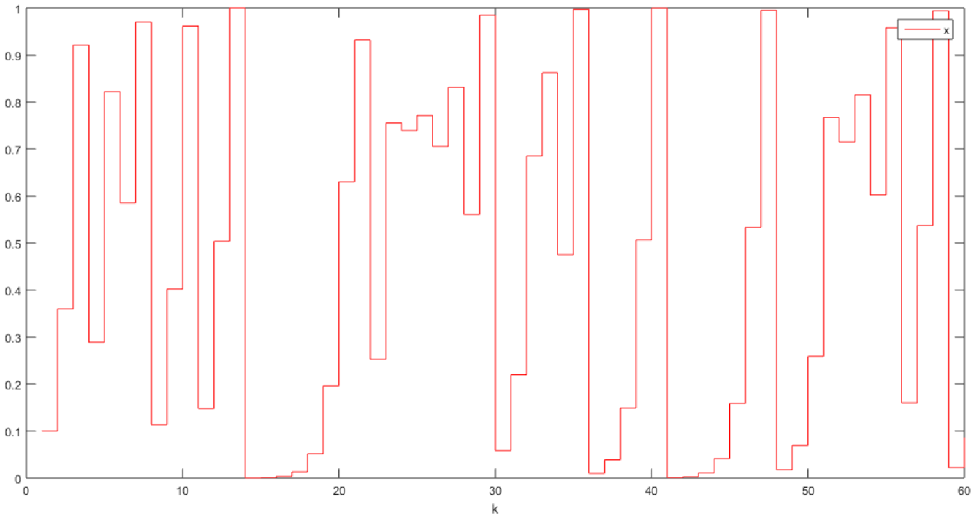


Fig. 8 : Aspect aléatoire de la fonction Logistique

b)- Sensibilité aux conditions initiales :

La sensibilité aux conditions initiales est donnée par la figure ci-dessous:

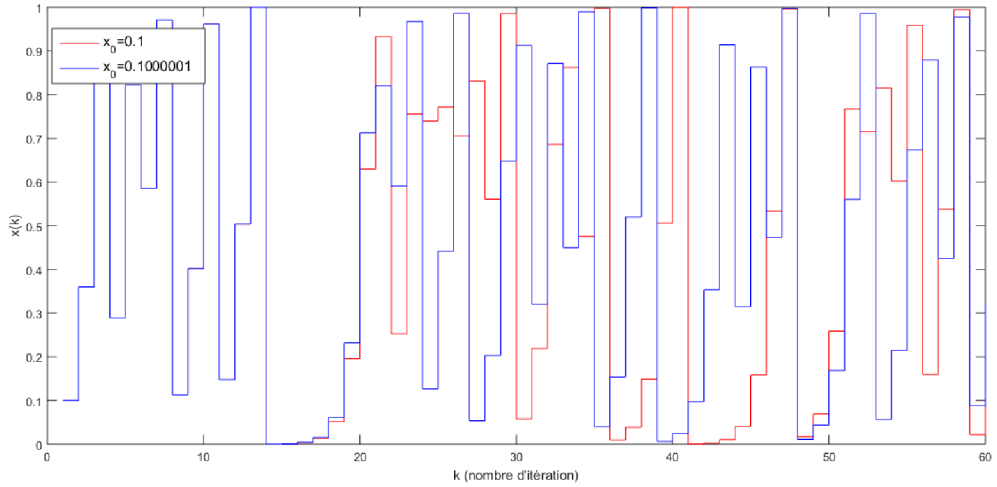


Figure 9 : Sensibilité aux conditions initiales de la fonction Logistique

Le même constat que pour le cas continu, nous remarquons bien que pour deux valeurs très voisine de la condition initiale, les états de la fonction logistique se distinguent.

c)- Attracteur de la fonction logistique :

L'attracteur étrange donné par la figure ci-dessous :

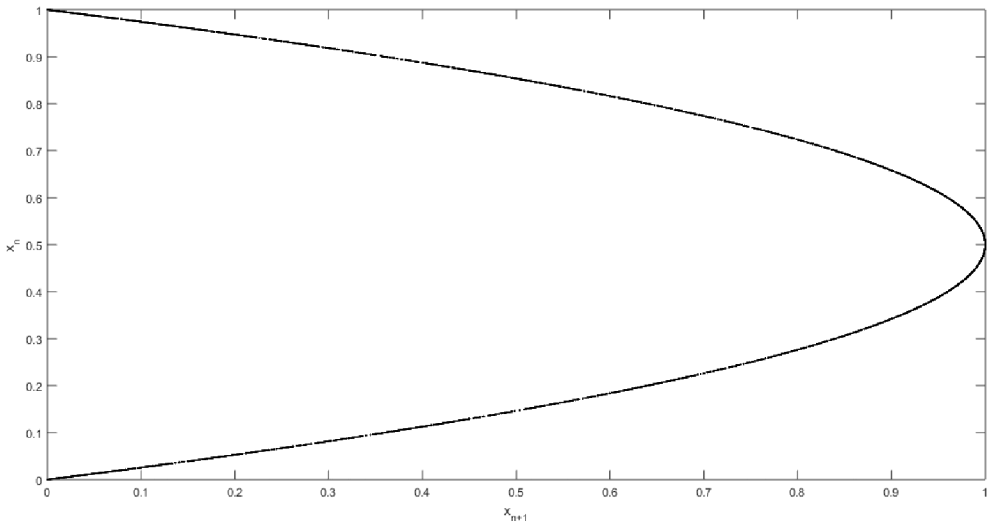


Fig. 10: Attracteur de la fonction Logistique

d)-Diagramme de bifurcation fonction Logistique:
La figure suivante illustre le diagramme de bifurcation de la fonction Logistique :

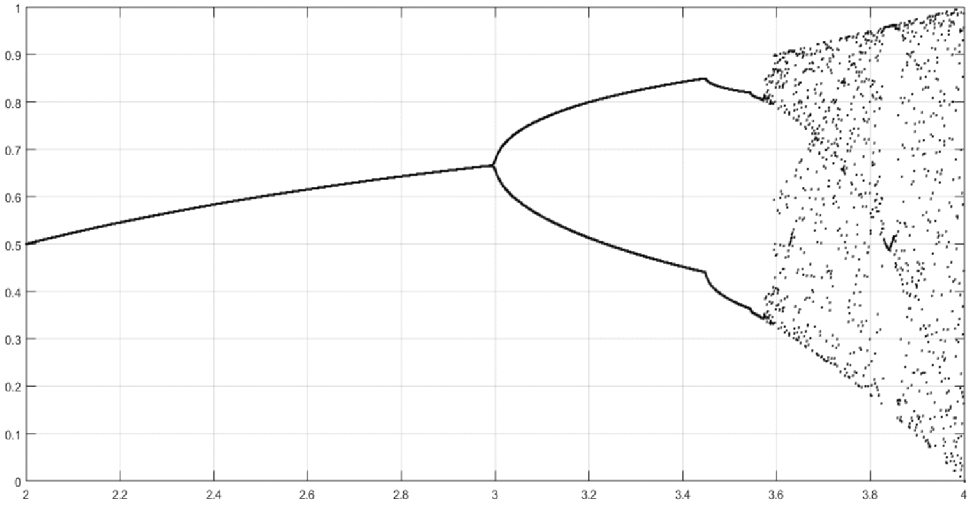


Fig. 11 : Diagramme de bifurcation de la fonction Logistique

On remarque que chaque point se dédouble et on obtient un cycle attracteur de période 4. On dit qu'il ya doublement de période.

I.5. Routes vers le chaos : [11]

On ne sait pas à l'heure actuelle dans quelles conditions un système va devenir chaotique. Cependant il existe plusieurs types d'évolution possible d'un système dynamique régulier vers le chaos. Supposons que la dynamique étudiée dépende d'un paramètre de contrôle. Lorsqu'on varie ce paramètre, le système peut passer d'un état stationnaire à un état périodique, puis au-delà d'un certain seuil, suivre un scénario de transition et devenir chaotique. Il existe plusieurs scénarios qui décrivent le passage du point fixe au chaos.
D'une manière générale, l'évolution du point fixe vers le chaos n'est pas progressive mais marquée par des changements discontinus appelée bifurcations. Une bifurcation marque le passage soudain d'un régime dynamique à un autre, qualitativement différent. Tous ces scénarios ont été prédits par la théorie et observés dans de nombreuses expériences.
En physique, c'est notamment la convection thermique de Rayleigh-Bénard, dans laquelle une couche de fluide situé entre deux plaques horizontales est soumise à un gradient de température vertical, qui a servi à l'origine de système-modèle pour l'étude du chaos. Depuis,

le chaos a été mis en évidence dans bien d'autres domaines. Nous allons en exposer brièvement trois types d'évolution possibles.

I.5.1. Par doublement de période :

Ce scénario de transition vers le chaos est sans doute le plus connu. Par augmentation du paramètre de contrôle de l'expérience, la fréquence du régime périodique double, puis est multipliée par 4, par 8, par 16 < etc. Les doublements étant de plus en plus rapprochés, on tend vers un point d'accumulation auquel on obtiendrait hypothétiquement une fréquence infinie. C'est à ce moment que le système devient chaotique. Il a été étudié en particulier en dynamique de populations par R.May sur l'application logistique, $x_{n+1} = r.x_n(1-x_n)$. Selon la valeur du paramètre (a), la suite converge soit vers un point fixe nul ou pas. Dès que (a) est plus grand que 3 le système bifurque, c'est à dire qu'il oscille entre 2 valeurs autour du point fixe. On parle de cycle attracteur de période 2. En continuant à augmenter a, ces 2 attracteurs s'écartent du point fixe jusqu'à ce qu'une nouvelle bifurcation ait lieu. Chaque point se dédouble et on obtient un cycle attracteur de période 4. On dit qu'il ya doublement de période. C'est à partir de cet exemple que Feigenbaum pressentit l'existence d'une forme d'universalité dans cette transition vers le chaos sous forme de cascade de doublement de période.

I.5.2. Par Intermittences :

Ce scénario via les intermittences se caractérise par l'apparition erratique de bouffées chaotiques dans un système qui oscille de manière régulière. Le système conserve pendant un certain laps de temps un régime périodique ou pratiquement périodique, c'est à dire une certaine "régularité", et il se déstabilise, brutalement, pour donner lieu à une sorte d'explosion chaotique. Il se stabilise de nouveau ensuite, pour donner lieu à une nouvelle "bouffée" plus tard. On a constaté que la fréquence et la durée des phases chaotiques avaient tendance à s'accroître plus on s'éloignait de la valeur critique de la contrainte ayant conduit à leur apparition. L'intermittence suppose en particulier que le cycle limite (correspondant à l'état périodique d'où est issu ce phénomène de transition) bifurque de façon sous-critique et qu'il n'y ait pas d'attracteur à proximité. C'est ce que l'on observe dans le système de Rössler.

I.5.3. Quasi-périodicité :

Le scénario via la quasi-périodicité a été mis en évidence par les travaux théoriques de Ruelle et Takens (1971) illustré par exemple sur le modèle de Lorenz (1963). Ce scénario a été confirmé par de nombreuses expériences dont les plus célèbres se trouvent en thermo hydrodynamique convection de Rayleigh-Bénard dans une petite boîte et en chimie réaction de Bélousov-Zabotinsky entre autres. Cette route vers le chaos résulte de la "concurrence" de

différentes fréquences dans le système dynamique. Dans un système à comportement périodique à une seule fréquence, si nous changeons un paramètre alors il apparaît une deuxième fréquence. Si le rapport entre les deux fréquences est rationnelle comportement est périodique. Mais, si le rapport est irrationnel, le comportement est quasi périodique Dans ce cas, les trajectoires couvrent la superficie d'un tore. Alors, on change de nouveau le paramètre et il apparaît une troisième fréquence, et ainsi de suite jusqu'au chaos. Il existe aussi des systèmes qui passent directement de deux fréquences au chaos.

I.6. Conclusion :

Nous avons donc vu au cours de ce chapitre les définitions et les principales caractéristiques de ce qu'on appelle "chaos". On a ainsi mis en avant que ce phénomène se caractérisait par une extrême sensibilité aux conditions initiales qui tendent à amplifier même la plus minime des variations.

Nous avons mis en œuvre ses classes et ses propriétés, par la suite on à donné des exemples de simulation de systèmes chaotiques sous Matlab.

Chapitre II : Synchronisation des systèmes chaotiques

II.1.Introduction

La synchronisation existe depuis le 16^{ième} siècle, elle caractérise l'évolution de deux systèmes qui se comportent de la même façon, en même temps.
Grace à l'expérience réalisée par Huygens (1629-1695), qui a fait l'étude de deux horloges de fréquence, dont la différence est très petite a constaté, par la suite il a relié les deux horloges avec un morceau de bois, ce qui a donné un mouvement complètement identique dit synchronisation.

Les domaines d'utilisation de la synchronisation sont vastes, elle existe en technologique et en diverses sciences, et principalement en télécommunication, dont elle est une clé importante pour une transmission réussie. Dans le domaine de la transmission sécurisée à base du chaos, la synchronisation chaotique au niveau du récepteur cherche à dupliquer le signal chaotique envoyé de l'émetteur malgré l'hypersensibilité aux conditions initiales. Cela veut dire que deux signaux chaotiques sont dits synchronisés, seulement s'ils sont asymptotiquement identiques quand le temps tend vers l'infini [6].

Dans ce chapitre nous allons présenter la synchronisation, introduire le concept et les classes de synchronisation (unidirectionnelle, bidirectionnelle). Ensuite, nous proposons quelques méthodes de synchronisation (identique, généralisée, retardée, impulsive, de phase, et par boucle fermée). Enfin, on termine avec quelques techniques de cryptage à base du chaos.

II.2. Communications sécurisées par chaos : [8]

Protéger les informations sensibles de l'interception indésirable a toujours attiré l'attention dans les réseaux de communication. Traditionnellement, la confidentialité et l'authentification de l'information sont réalisées grâce à des algorithmes mathématiques. Plus récemment, d'autres techniques de cryptage ont été introduits, tels que des clés quantiques la distribution et de la communication par chaos.
Comme il a été déjà mentionné dans le premier chapitre, le chaos déterministe peut générer des comportements dynamiques d'apparences aléatoires. Il serait donc intéressant d'utiliser ces derniers comme porteuses d'informations en télécommunication.
Le diagramme principal de la communication sécurisée par le chaos est montré sur la figure (12). Le principe est de masquer une information par des signaux chaotiques et de l'envoyer vers le récepteur sur un canal public. L'information cryptée est récupérée au niveau du récepteur.

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

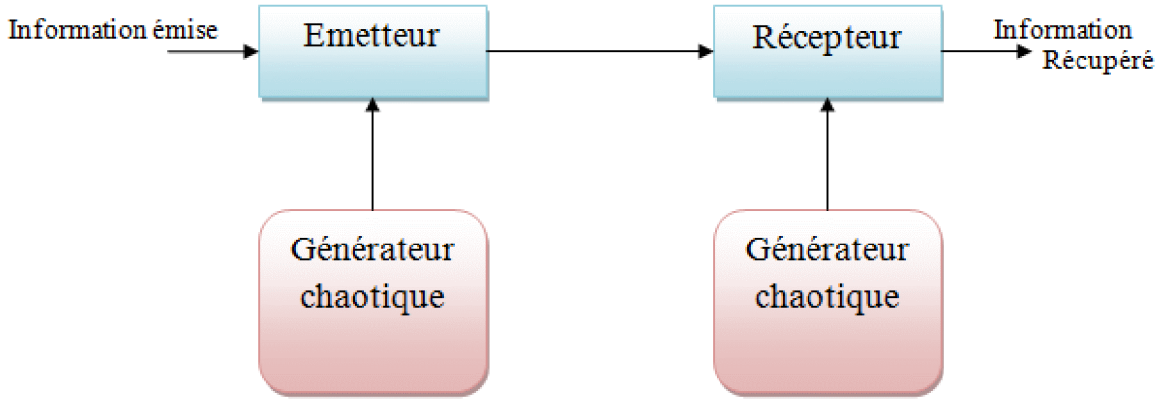


Fig. 12 : Principe d'une communication sécurisée par le chaos

Le chiffrement d'un message par le chaos s'effectue donc en superposant à l'information initiale un signal chaotique. On envoie par la suite le message noyé dans le chaos à un récepteur qui lui connaît les caractéristiques du générateur de chaos. Il ne reste alors plus au destinataire qu'à soustraire le chaos de son message pour retrouver l'information. Si la génération du chaos et le cryptage du message ne présentent pas de problème majeur, on va voir par la suite que du fait de la nature même du chaos, le décryptage va quant à lui présenter des étapes critiques notamment pour recréer la composante chaotique du message (synchronisation) et la soustraire.

II.3. Concept et classes de synchronisation : [12]

Les méthodes de synchronisation sont en général basées sur l'utilisation des circuits identiques.

Supposant deux systèmes chaotiques identiques oscillant de façon totalement indépendante. Si par un moyen, on leur permet d'échanger de l'énergie, action que l'on nomme « couplage » les deux systèmes finiront par céder la place à un comportement commun : ils se synchronisent. Il est possible de coupler les systèmes chaotiques dans un sens (couplage unidirectionnel) ou dans les deux sens (couplage bidirectionnel). Dans le cas d'un couplage unidirectionnel, l'énergie est transférée d'un système à l'autre, à l'aide d'un élément de couplage fonctionnant dans un seul sens comme par exemple un suiveur. Par contre, dans le couplage bidirectionnel, l'élément de couplage permet l'échange d'énergie dans les deux sens. Ceci peut être par exemple une simple résistance.

En plus de couplage simple (par résistance ou suiveur), d'autres méthodes ont été proposées pour la synchronisation des systèmes chaotiques. Ainsi pour la synchronisation des systèmes

unidirectionnelle, on peut citer la méthode par décomposition du système, la synchronisation impulsive, la synchronisation par des méthodes itératives ou la synchronisation par la boucle fermée.

Dans la majorité des cas, les deux systèmes doivent avoir des structures identiques, ce qui n'est pas tout à fait réalisable en pratique. Un petit écart entre les valeurs des composants peut entrainer un écart considérable entre le comportement des deux circuits et détruire le phénomène synchronisation. On note deux classes de synchronisation unidirectionnelle, et bidirectionnelle.

a) Synchronisation par couplage unidirectionnel : [13]

Dans la synchronisation par couplage unidirectionnel, l'énergie est transférée d'un système à l'autre entre deux systèmes identiques notés a et b à laide d'un élément de couplage fonctionnant dans un seul sens, comme par exemple un suiveur. Ceci est illustré par la figure ci-dessous :

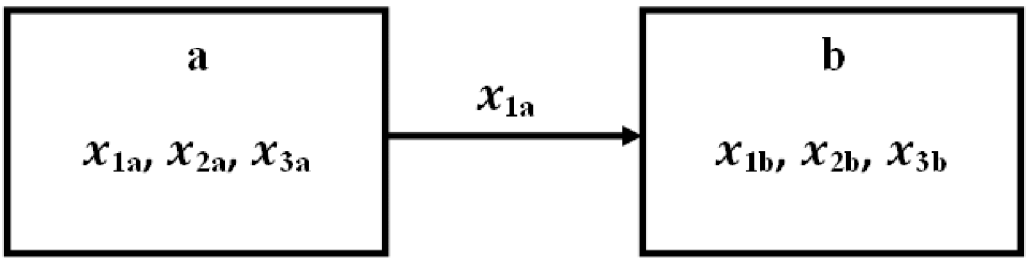


Fig. 13 : schéma de coulage unidirectionnel

b) Synchronisation par couplage bidirectionnel : [13]

Lors d'une synchronisation par couplage bidirectionnel, l'élément de couplage permet l'échange de l'énergie dans les deux sens, ceci peut être par exemple une simple résistance (voir figure ci-dessous)

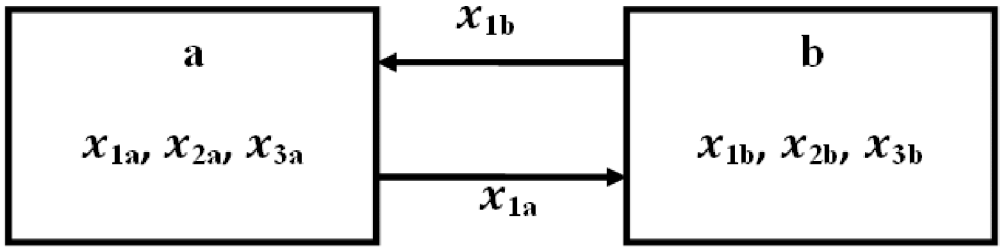


Fig. 14 : schéma de coulage bidirectionnel

II.4. Méthodes de synchronisation :

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

a) Synchronisation identique : [14] [15] [16]

Parmi les méthodes de synchronisation par couplage entre deux systèmes chaotiques, la synchronisation identique proposée par Pecora et Carroll [6], cette dernière a l'avantage de représenter une solution simple et perforante de synchronisation.
L'objectif de la méthode et que le système l'esclave (récepteur) reproduit le plus fidèlement possible l'état du système maître (émetteur), après un régime transitoire.
Considérons un système dynamique autonome, en temps continu, de dimension n, représenté par la relation :

$$\dot{x}(t) = F(x(t)) \qquad \text{(II.1)}$$

Où $x = [x_1, ..., x_n]^T$
Ensuite, on devise le système initial en deux sous systèmes {S1, S2} :

$$\begin{cases} S_1 : \dot{x}^{\{1\}} = F^{\{1\}}(x^{\{1\}}, x^{\{2\}}) \\ S_2 : \dot{x}^{\{2\}} = F^{\{2\}}(x^{\{1\}}, x^{\{2\}}) \end{cases} \qquad \text{(II.2)}$$

Avec les états et les dynamiques définis conformément aux relations suivantes :

$$x = [\, x^{\{1\}}, x^{\{2\}}]^T \tag{II.3}$$

Avec

$$x^{\{1\}} = [\, x_1, \ldots, x_m]^T \tag{II.4}$$

$$x^{\{2\}} = [\, x_{m+1}, \ldots, x_n]^T \tag{II.5}$$

Donc, on peut écrire

$$F(x) = [\, F^{\{1\}}(x), F^{\{2\}}(x)] \tag{II.6}$$

Cette opération peut être réalisée de manière arbitraire avec une réorganisation des variables d'états dans un ordre quelconque.
Soit un système S'_2 = caractérisé par une dynamique identique $F^{\{1\}}$, et un vecteur d'état $\dot{x}^{\{1\}}$:

$$S'_2 : \dot{\hat{x}}^{\{2\}} = F^{\{2\}}\,(x^{\{1\}}, \hat{x}^{\{2\}}\,) \tag{II.7}$$

On peut dire que le sous système réplique S'_2 est un candidat susceptible de se synchroniser avec la dynamique complète initiale. La condition nécessaire pour que cette proposition soit vraie, et que le sous système S'_2 soit stable, hypothèse qui est équivalente avec la condition que l'ensemble des coefficients Lyapunov de sous-système S'_2 soit négatifs.

$$\lim_{t\to\infty} \| \hat{x}^{\{2\}}\,(t) - x^{\{2\}}(t) \| = 0 \tag{II.8}$$

La figure suivante représente le processus de composition en sous systèmes, avec la notion $y = x^{\{1\}} + n$ de la variable d'état qui commande le système S'_2, ou n'est un éventuel bruit additif associé au canal de communication.

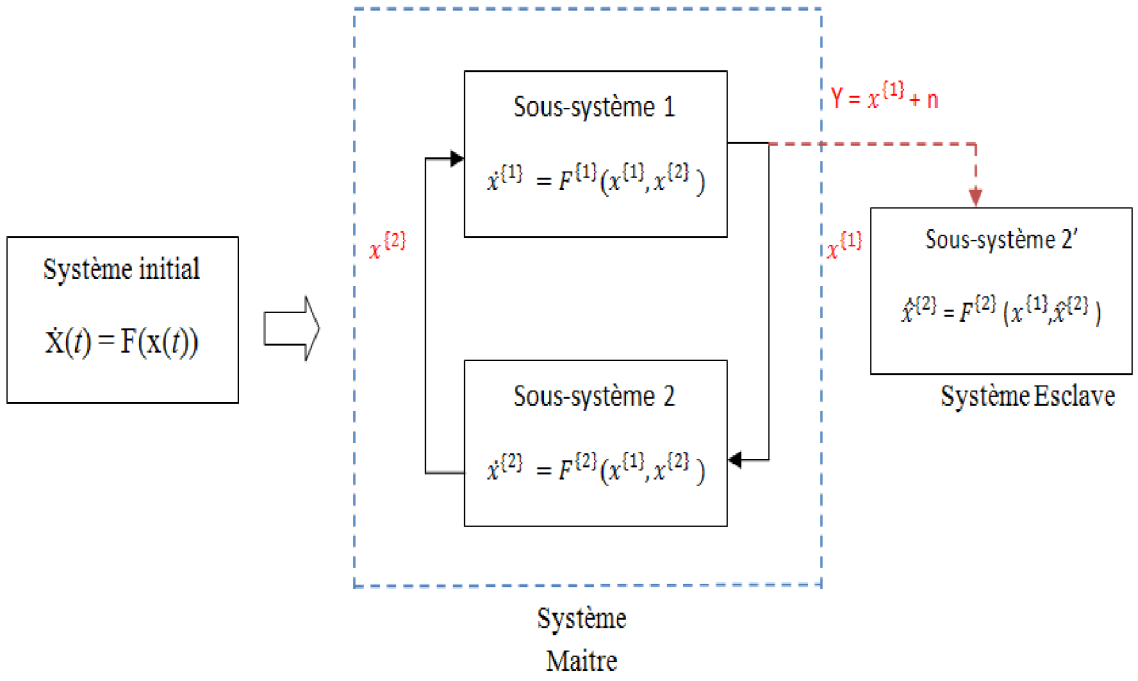


Fig. 15 : Synchronisation Maitre-Esclave en utilisant la décomposition en sous-systèmes

Parfois l'équation (II.8) qui traduit la convergence asymptotiquement ne reste plus valable. Pour y remédier, on doit utiliser une autre approche qu'est la synchronisation généralisée.

b) Synchronisation généralisée : [17] [18]

La synchronisation généralisée est considérée comme une généralisation de la synchronisation complète.
Pour synchroniser des systèmes chaotiques de modèle différent, elle se manifeste par une relation fonctionnelle entre deux systèmes chaotiques couplés, s'il existe une transformation M telle que :

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

Ou x(t) et l'état du système émetteur, et x'(t) est l'état du système récepteur, sans tenir en compte les conditions initiales dans ce cas.

Si M est invisible, alors $M^{-1}(x')$ fourni une estimation de l'état x, mais on trouve des soucis majeurs qui présente des inconvénients dans les techniques de communication en utilisant l'état de l'émetteur pour décrypter le message transmis.

c) Synchronisation retardée :

Dans la synchronisation retardée, le système esclave converge vers l'état décalé dans le temps du système maître, et cela revient à des oscillateurs non identiques qui sont faiblement couplés.
On applique la synchronisation retardée dans le cas des oscillateurs chaotiques non identiques (faible couplage), ou les phases sont verrouillées ainsi les amplitudes ne corrèlent pas au moment où le couplage devient important. Le processus de synchronisation retardée apparaît comme une coïncidence des états décalés dans le temps de deux systèmes. Donc, la condition de synchronisation est résumée par l'expression suivante:

$$\lim_{t\to\infty} \| x'(t) - x(t-\tau) \| = 0 \qquad \text{(II.10)}$$

Ou x(t) est l'état du système émetteur, x'(t) est l'état du système récepteur et τ est un retard positif.

d) Synchronisation impulsive : [19]

Dans un schéma de transmission usuelle, un des états du système dynamique transmis afin de réaliser la synchronisation par le récepteur. On propose la synchronisation impulsive, dans le but de réduire la redondance du signal transmis.
Le contrôle impulsif d'un système signifie qu'à des moments choisis, les états du système changent soudainement.
Dans ce schéma de synchronisation, on considère un système maître de forme générale :

$$\hat{x} = (f(x)) \qquad \text{(II.11)}$$

On définit un signal impulsif qui consiste en une suite d'instants discrets auxquels un signal Y(t) = Cx(t) est envoyé par le système esclave, dont les variables d'état subissent un saut et changement d'état.

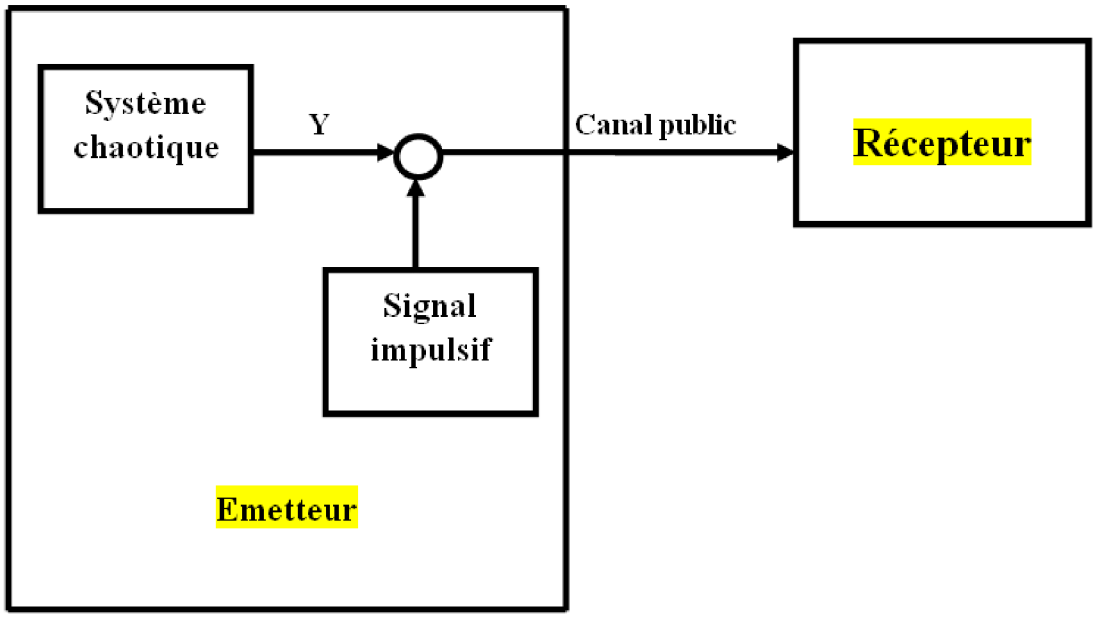


Fig. 16 : Synchronisation impulsive

e) Synchronisation de phase :

La synchronisation de phase est une méthode qui est totalement différente des autres présentées précédemment.
Ce phénomène se produit malgré les oscillateurs chaotiques couplés, qui conserve la différence de phase, ainsi leurs amplitudes restent non corrélées.
Lorsque la synchronisation chaotique est obtenue, les exposants de Lyapunov du système esclave deviennent non chaotiques, avec une sortie chaotique.
Si $\varphi 1(t)$ et $\varphi A(t)$ désignent les phases de deux oscillateurs couplés.
La synchronisation de phase est donnée par la relation :

$$n\,\varphi 1(t) = m\,\varphi A(t) \qquad (II.12)$$

Avec m et n des nombres entiers.

f) Synchronisation par boucle fermée : [19]

La synchronisation des systèmes chaotiques par les méthodes en boucle ouverte implique une sensibilité aux variations paramétriques. Par la suite de nouvelles techniques basées sur un bouclage par contre réaction ont été proposées.
L'idée est d'appliquer une correction au système en fonction de l'erreur entre le signal transmis par le premier système, et le signal régénéré par l'autre.
Cette erreur est ainsi injectée en contre-réaction d'où l'appellation de l'approche.

Cette technique permet également la synchronisation entre des paires différentes de systèmes chaotiques. Le principe de cette méthode est illustré par la figure ci-dessous :

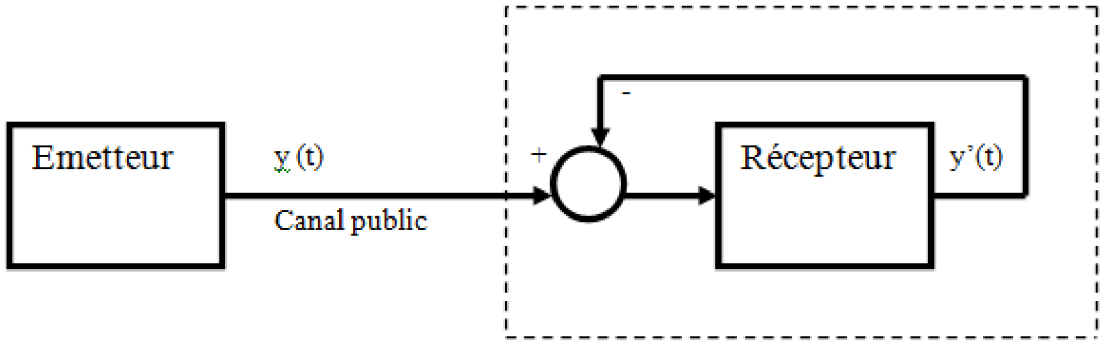


Fig. 17 : Synchronisation en boucle fermée

II.5. Techniques de cryptage par le chaos :

Les résultats obtenus par la synchronisation des systèmes chaotiques, on permit la possibilité d'employer des signaux chaotiques continus comme porteurs d'information.
A partir d'un message contenant l'information, l'émetteur génère un signal qui est transmis au récepteur par l'intermédiaire du canal. Alors, le message est décodé et extrait du signal chaotique par le récepteur. Dans ce qui suit, on propose des méthodes de transmission chaotique.

a)-Cryptage par addition : [20]

Le masquage chaotique par addition est la technique de transmission la plus simple, et la plus élémentaire. L'idée de base consiste à additionner le message (analogique ou numérique) m(t) ou M(k) à transmettre à un signal chaotique x(t) en bande de base, la figure (II.7) illustre le principe de base de cette technique.
Au niveau du récepteur, un système chaotique identique à celui de l'émetteur essaie de se synchroniser avec le signal chaotique reçu y(t). Ce point de vue de la synchronisation des deux systèmes chaotiques, le message m(t) est pris comme un élément perturbateur du signal x(t).
En considérant un canal de propagation idéal non bruité et sans trajets multiples, le signal chaotique reçu s'écrit :

$$Y(t) = m(t) + x(t) \qquad \text{(II.13)}$$

En utilisant par exemple le principe de Pecora et Carroll pour réaliser la synchronisation et on suppose que les deux systèmes chaotiques soient de configuration favorable (problème de sensibilité aux conditions initiales), l'erreur de synchronisation ne dépend que de m(t).
Donc si l'amplitude du message m(t) est suffisamment faible par rapport au signal chaotique x(t), le signal contenant l'information ne modifie que modérément y(t) et la synchronisation s'effectue correctement, ensuite pour démoduler le message, il suffit de soustraire le signal à l'entrée du système chaotique y(t) avec celui en sortie de ce même dispositif y'(t).

$$m' = y(t) - y'(t) \qquad \text{(II.14)}$$

Si la synchronisation est parfaite alors $y'(t) = x(t)$ et $m'(t) = m(t)$

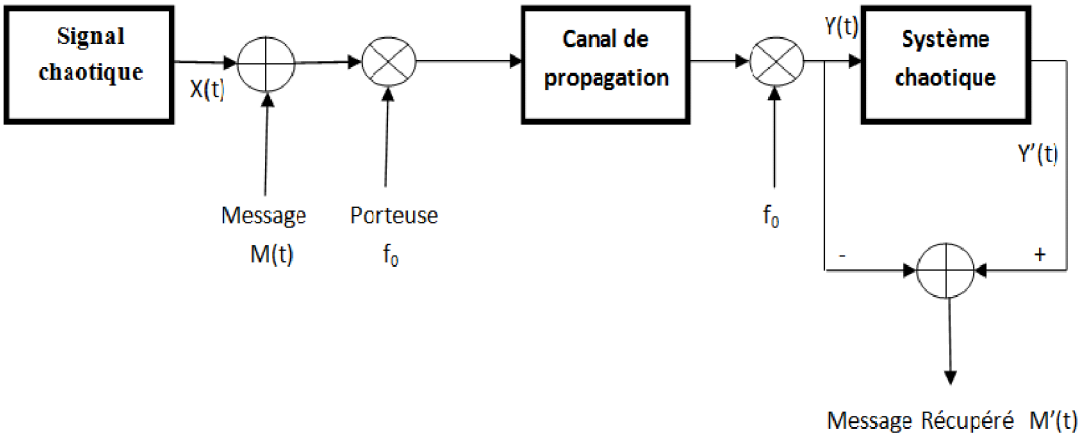


Fig. 18 : Architecture d'un système utilisant le masquage chaotique par addition

En considérant un canal de propagation réel qui prend en compte la non linéarité de l'amplificateur de puissance, les trajets multiples…etc., cette méthode ne se révèle pas très efficace car elle est sensible au bruit.
Au cours de la démodulation le bruit additif ne se distingue pas du message, il est nécessaire de pouvoir l'éliminer surtout si le niveau du bruit n'est pas suffisamment faible par rapport à celui du message.
Il existe bien évidemment d'autres méthodes plus efficaces pour crypter que de faire une simple somme de signaux. Elles sont résumées ci-dessous.

b) Cryptage par commutation : [20]

Le cryptage par communication chaotique est une technique proposée dans le cadre des communications numériques pour la transmission des messages binaires. L'émetteur est composé de deux systèmes chaotiques A(t) et B(t), et pour chaque niveau de message M(t) (**0** ou **1**) l'un des systèmes envoie sa sortie sur la ligne de transmission, le message binaire M(t) est utilisé pour commuter entre A(t) en codant le bit 1 et B(t) en codant le bit 0. Le récepteur est composé de deux systèmes esclaves, dont le premier système esclave synchronise exclusivement avec le premier oscillateur A(t) de telles façons que le bit 1 est détecté par la convergence d'une erreur de synchronisation vers zéro et par conséquent le signal d'information peut être enfin restauré à la fin de processus de détection. Le principe de cette méthode est illustré par la figure ci-dessous :

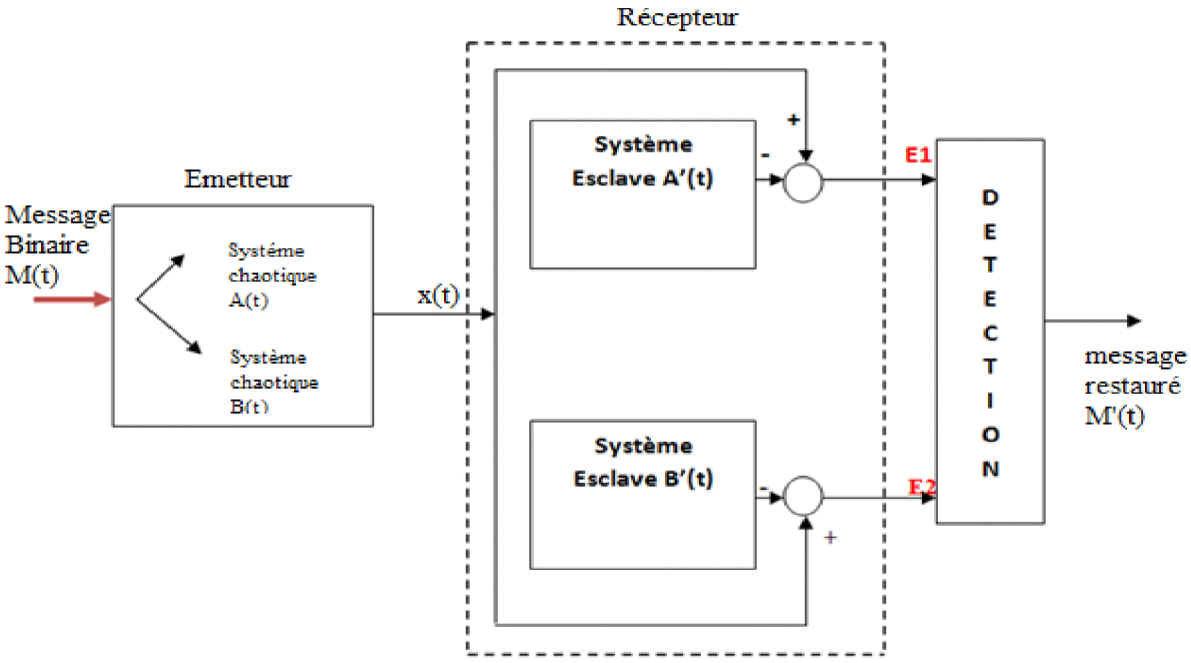


Fig. 19 : Architecture d'un système utilisant la méthode de transmission par commutation

c) Cryptage par injection (inclusion) : [20]

Le schéma de principe de cette technique est représenté dans la figure ci-dessous. Il s'agit d'injecter le signal d'information dans la dynamique de l'émetteur chaotique. Le récepteur a pour but de se synchroniser avec l'émetteur et de reconstruire le signal d'information.

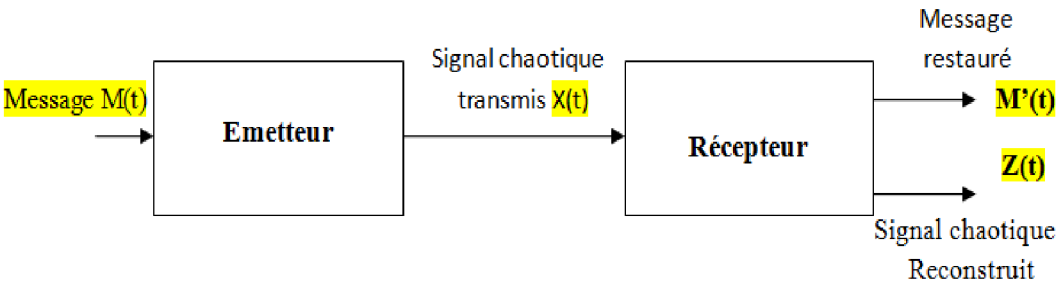


Fig. 20 : Schéma représentatif de la technique de cryptage par injection

Cette technique est valable pour transmettre un message de nature binaire ou analogique, mais la puissance de ce dernier doit être suffisamment petite pour ne pas détériorer le comportement chaotique du système maître et que le signal chaotique disponible dans le canal public ne porte pas l'information d'une manière directe comme dans le cas de la technique de masquage chaotique.

d)- Transmission à deux voix : [21]

L'idée de base consiste à séparer les tâches de synchronisation et de cryptage en utilisant deux voies de communication. L'émetteur chaotique génère un signal chaotique y(t) transmit dans un premier canal de communication (canal 1) vers le récepteur qui doit se synchroniser avec le système maître. L'émetteur génère également un autre signal chaotique x(t) utilisé par une fonction de cryptage qui produit le signal du texte chiffré $y_2(t)$ transmis dans un deuxième canal de transmission (canal2).

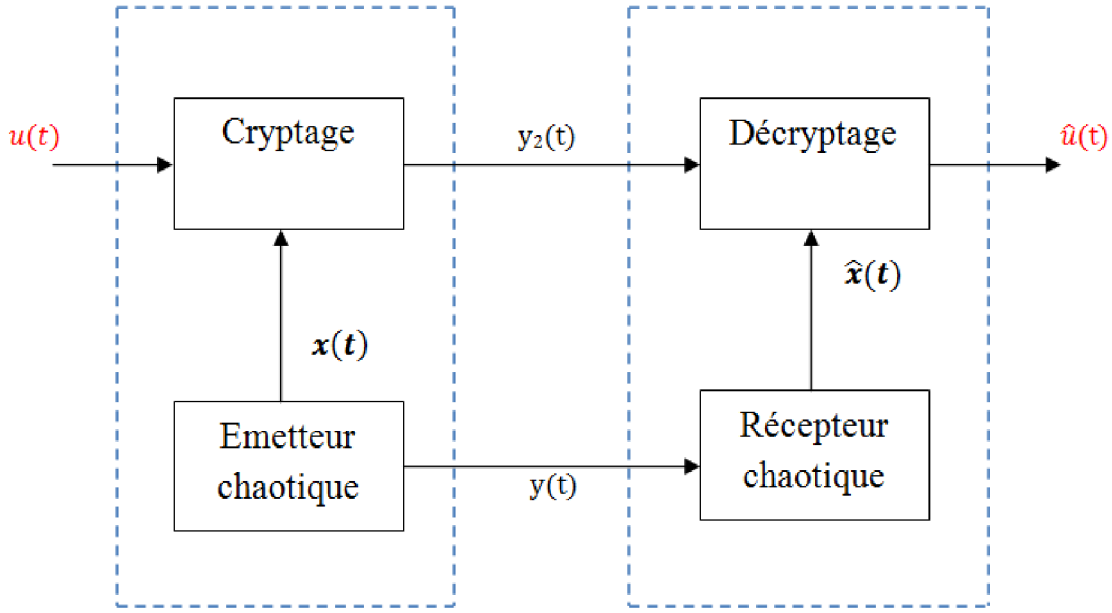


Fig. 21 : Schéma de principe d'une transmission à deux voies

Grace à cette indépendance entre les taches de synchronisation et de cryptage, il n'y a pas de contrainte à imposer sur l'amplitude du signal d'information puisque dans ce cas, ce dernier n'agit ni sur la dynamique de l'émetteur chaotique ni sur le signal transmis y(t) contrairement aux autres techniques. De plus, le signal d'information n'a aucune influence sur l'opération de synchronisation qui s'établit d'une façon idéale, ce qui permet de garantir une meilleure qualité de l'information récupérée au niveau du récepteur.

D'un autre coté, cette méthode garantit un meilleur niveau de sécurité par rapport aux autres techniques puisque la séparation entre les opérations de cryptage et de synchronisation permet de concevoir une fonction de cryptage de plus en plus complexe sans se soucier de détériorer l'aspect chaotique de l'émetteur ou de perdre la synchronisation entre le système maître et esclave. Cependant, cette technique présente des mauvaises performances en présence du bruit de transmission puisque l'effet du bruit est doublé en agissant à la fois sur le signal transmis y(t) dans la première voie du texte chiffré y2(t) présents dans la deuxième voie de transmission.

Cette méthode présente plusieurs avantages :

- Le signal y ne contient aucune information, par conséquent la synchronisation peut s'établir de façon optimale.
- Le second signal y_2 contient l'information qui peut être soit cryptée par une fonction non linéaire des l'état x, soit simplement masqué par un signal chaotique généré par l'émetteur, qui sert de porteuse.

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

e)-Chiffrement par modulation : [12]

Cette technique utilise le message contenant l'information pour moduler un paramètre de l'émetteur chaotique.
Un contrôleur adaptatif est chargé de maintenir la synchronisation au niveau du récepteur, tout en suivant les changements du paramètre modulé. Le schéma correspondant est présenté par la figure suivante :

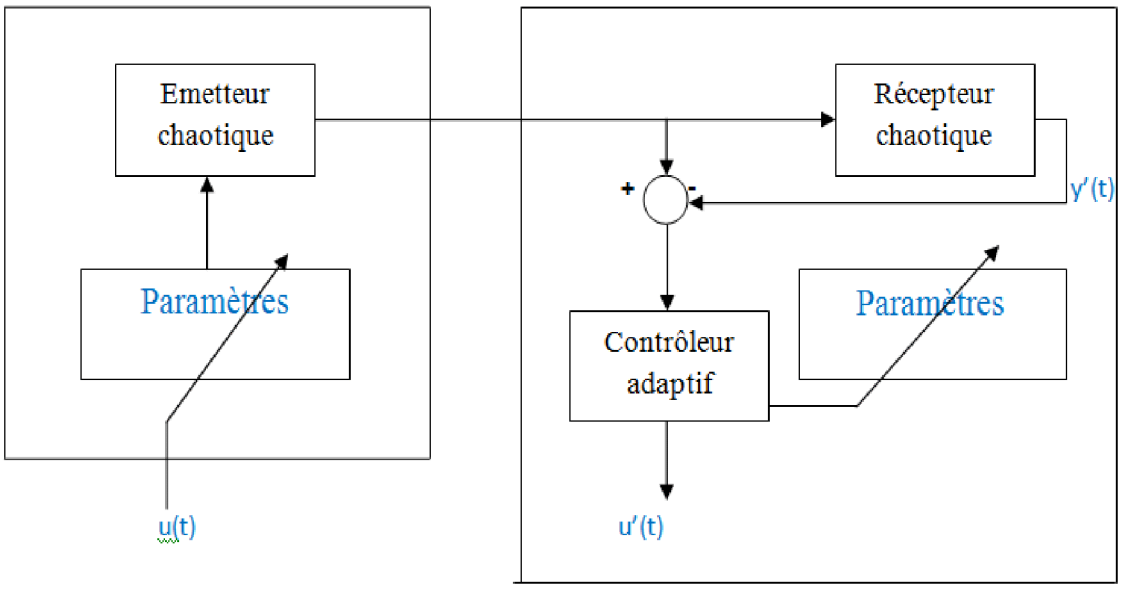


Fig. 22 : Schéma de cryptage par modulation

Au niveau de l'émetteur, le fait de moduler un ou plusieurs paramètre(s) impose à la trajectoire de changer continûment d'attracteur, et de ce fait, le signal transmis est plus complexe qu'un signal chaotique normal.
Cependant la façon d'injecter le message et donc la fonction de modulation des paramètres ne doivent pas supprimer le caractère chaotique du signal envoyé au récepteur.
Il est important de souligner que cette technique exploite pleinement les qualités des systèmes chaotiques. Elle n'a pas d'équivalent parmi les systèmes de communication classiques. Cependant, le cryptage par modulation s'est avéré sensible à certaines attaques.

II.6. Conclusion

Dans ce chapitre, nous avons présenté et expliqué le concept de synchronisation des systèmes chaotiques, ainsi quelques méthodes de synchronisation. Nous avons aussi donné des techniques de chiffrement par le chaos. On a déduit que la cryptographie chaotique peut s'effectuer sous divers schémas, ce qui importe c'est la façon d'introduire le message dans l'émetteur.

Dans le chapitre qui suit nous allons concevoir et étudier un schéma de transmission sécurisée d'une image à base de système chaotique.

Chapitre III : Conception et étude d'un schéma de transmission d'images sécurisées

III.1. Introduction :

La théorie du chaos a été appliquée pour l'étude et la compréhension, la manipulation et l'analyse du comportement des systèmes dans divers domaines, dont l'astronomie, la météorologie, la physique et principalement dans la télécommunication, dans la transmission sécurisée de l'information par la résolution de plusieurs problèmes relatifs à la synchronisation de systèmes chaotiques.

Avant la plupart des travaux de synchronisation des systèmes chaotiques (continus ou discret) se sont consacrée aux systèmes dynamiques à temps continu, mais après l'apparition des phénomènes hyper chaotiques et leurs émergences, beaucoup de scientifique ont adressé leurs études sur la synchronisation des systèmes chaotiques à temps discret, pour leurs divers avantages principalement dans la télécommunication privée, aussi la possibilité de reconstituer les clés d'un cryptosystème chaotique. Par conséquent, la clé d'un cryptosystème doit être conçue de façon à ce qu'elle ne soit pas identifiable, car même si on procède l'algorithme de cryptage, on ne peut récupérer l'information que si on a la clé exacte.

Dans ce chapitre, nous allons concevoir un schéma de transmission d'images sécurisées basée sur la synchronisation en utilisant un observateur du système chaotique discret. Notre travail commence d'abord par la présentation du principe de la méthode proposée, on choisit le système émetteur, et le système récepteur de cette transmission. Par la suite, on expose les résultats de simulation.

III.2. Description de la chaine de transmission Privée :

Cette partie est consacrée à la mise en œuvre du système de communication basé sur un système dynamique chaotique à temps discret.
Le schéma proposé est constitué d'un émetteur et d'un récepteur. L'émetteur est construit autour d'un système dynamique chaotique à temps discrets dit de Hénon modifié. Le récepteur est composé d'un observateur à temps discret dit observateur retardé étape par étape. Le message à envoyer sera introduit par la méthode d'injection, dans une des dynamiques de l'émetteur. Le rôle du récepteur est de reconstruire tous les états du système émetteur, ainsi que le message information.

La figure (23) représente le schéma général du système proposé pour établir une communication sécurisée.

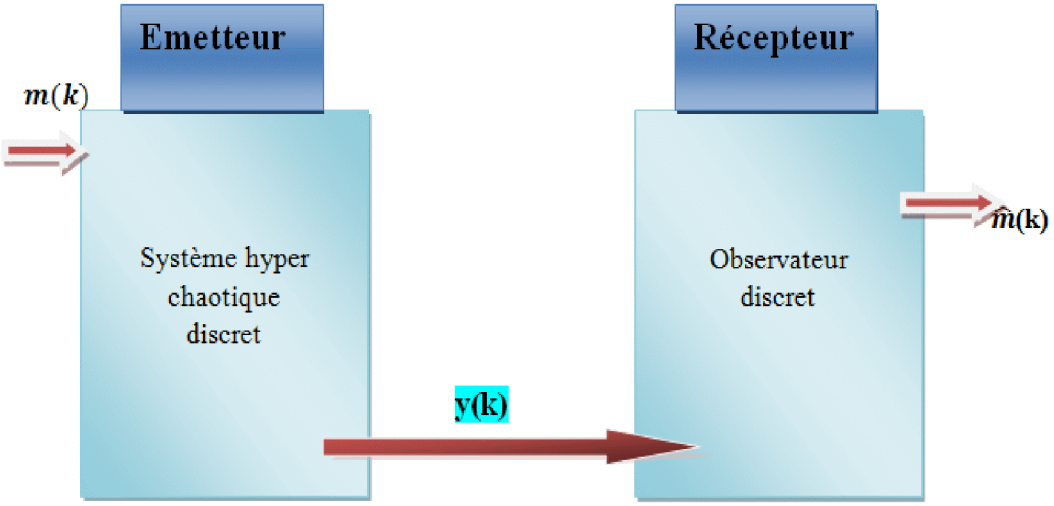


Fig. 23 : Schéma général du système de transmission

III.3. Principe de la méthode :

Notre plan de travail est donné comme suit :

- présentation de l'émetteur
- présentation du récepteur

III.3.1. Présentation de l'émetteur :

Le système chaotique en temps discret utilisé dans notre travail, et dit système de Hénon modifié.

Ce système a été largement étudié dans la littérature. On peut citer par exemple les travaux de Vesely [22]. Il est donné par les équations suivantes :

$$\begin{cases} x(k+1) = a - y^2(k) - b\,z(k) \\ y(k+1) = x(k) \\ z(k+1) = y(k) \\ s(k) = y(k) \end{cases} \qquad \text{(III.1)}$$

Pour avoir le comportement chaotique, les paramètres du système (III.1) sont donnés comme suit :

a= 1.7, b= 0.1 avec les conditions initiales du système x(1) = 0.2, y(1) = 0.5, z(1)=0.1 qui sont choisies à l intérieur du bassin d'attracteur étrange et s(k) = y(k) est la sortie du système.

La figure ci-dessous illustre la représentation de l'attracteur du Henon modifié.

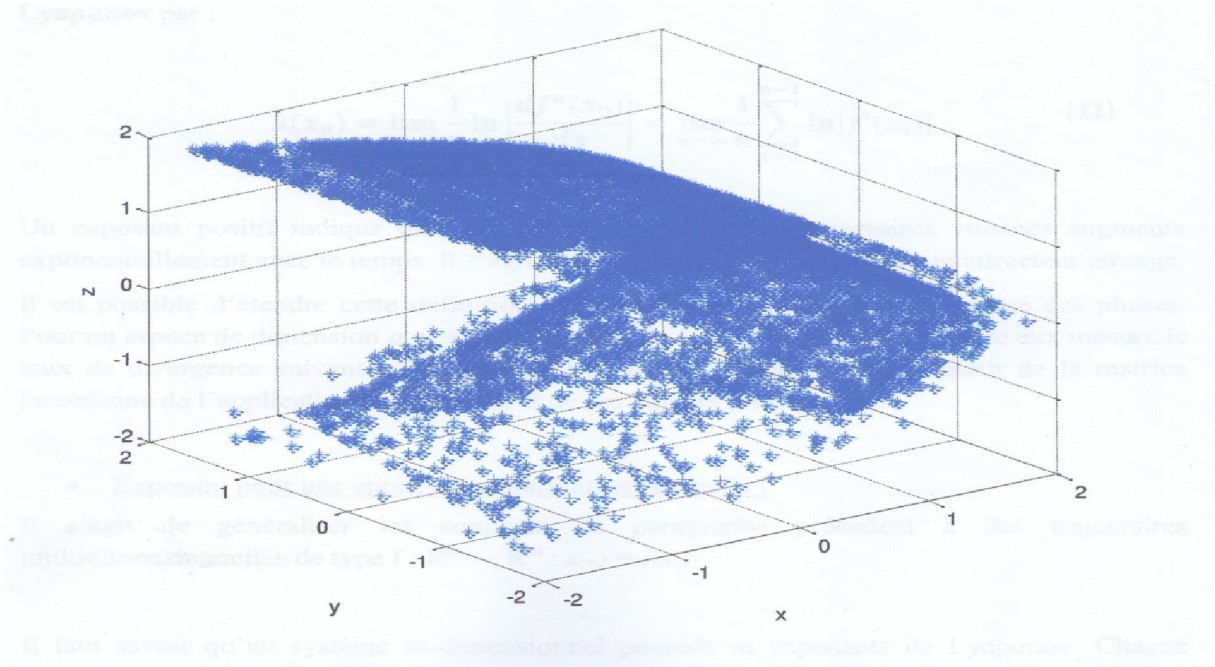


Fig. 24 : Attracteur du Henon modifié

L'exploitation des phénomènes chaotiques, nous est très utile, dans la communication privée. Cela nous a permis d'augmenter la sécurité des systèmes de transmission.
Au niveau de l'émetteur notre objectif et de rendre la structure du système plus complexe.
Notre travail consiste à inclure un message (m) dans la troisième dynamique du système (III.1) par la méthode de chiffrement par injection.
Le message est ajouté dans l'itéré de z(k) du système, ainsi l'état z(k) est modulé en fonction du message (m), donc il représente l'état modulé, par ailleurs le signal transmis au récepteur c'est l'état y. Ce qui implique que l'on ne transmet pas directement l'état modulé au récepteur.
Après avoir introduit le message dans la dynamique de z(k) du système de Henon modifié on obtient le système d'équation suivant :

$$\begin{cases} x\,(k+1) = a - y2(k) - b\,z(k) \\ y\,(k+1) = x(k) \\ z\,(k+1) = y(k) + m(k) \\ s\,(k) = y(k) \end{cases} \qquad \text{(III.2)}$$

Ou m(k) est une image numérique de dimension 128*128. Elle est illustrée par la figure ci-dessous :

Fig. 25 : L'image originale

A)- Représentation des états du système de Henon modifié et du message (Emetteur) :
Dans ce qui suit, nous allons représenter les états $x(k)$ $y(k)$ $z(k)$ de notre système Henon modifié ainsi que le message $m(k)$ à envoyer. Ceci est illustré par les figures ci-dessous :

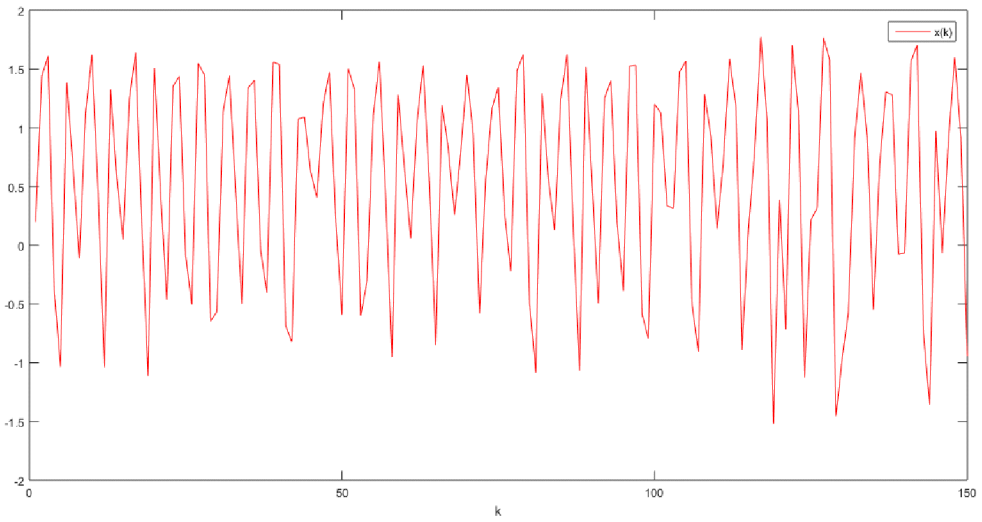


Fig. 26 : Etat $x(k)$ du système émetteur du Hénon modifié

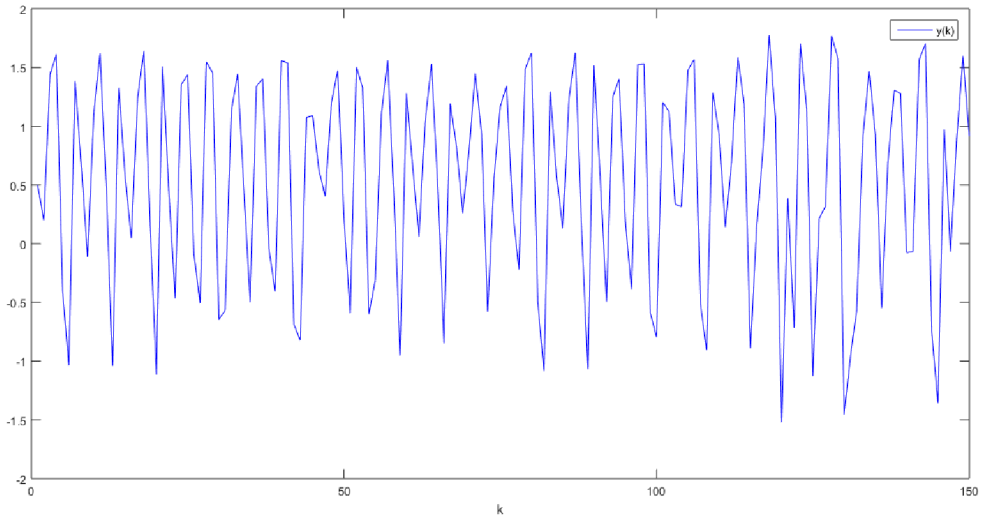


Fig. 27 : Etat y(k) du système émetteur du Hénon modifié

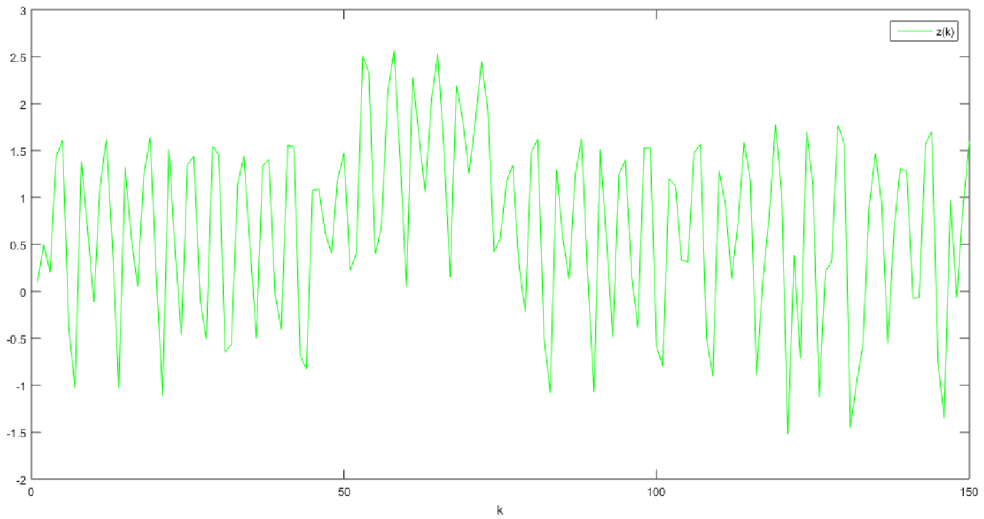


Fig. 28 : Etat z(k) du système émetteur du Hénon modifié

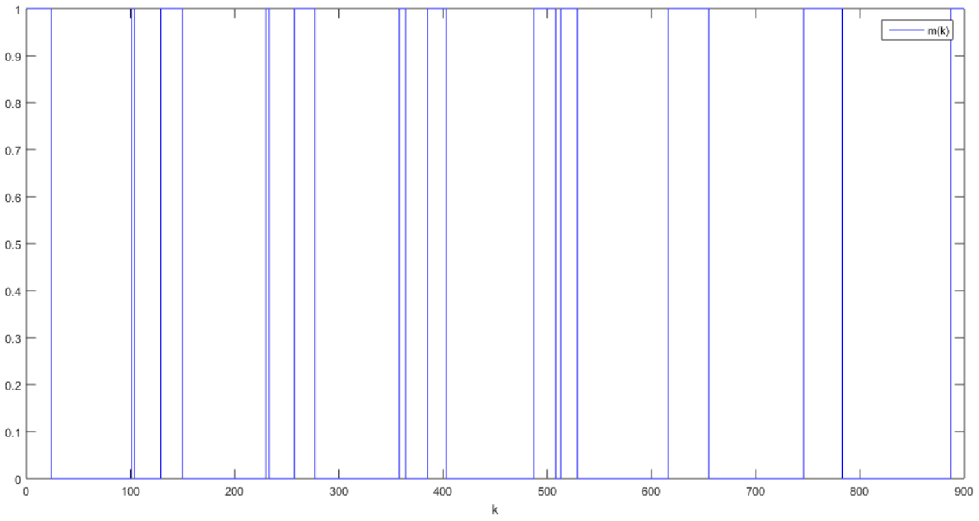


Fig. 29 : Message m(k) de l'image de Lena

III.3.2. Présentation du récepteur :

Dans cette partie, nous considérons le système donné par (III.2) avec la sortie s(k) = y(k).
Pour la réception, nous allons concevoir un observateur en temps discret, retardé fonctionnant à la période T, qui représente la période d'échantillonnage.
L'observateur est choisi dans le but de récupérer les états, ainsi le message (m) du système (III.2) du Henon modifié.
Les choix de la sortie s(k) = y(k) ainsi que l'envoie du message sur la troisième dynamique du système (III.2) respectivement est assuré par la condition d'observabilité, ainsi que la propriété d'inversion à gauche.

a)- Condition d'observabilité et propriété d'inversion à gauche :

On considère le système non linéaire discret suivant :

$$\begin{cases} x(k+1) = f\,(x(k) + p\big(x(k)\big)w(k) \\ s(k) = h(x(k)) \end{cases} \qquad \text{(III.3)}$$

Ou w(k) représente un entrée inconnue, qui peut être une perturbation, une erreur ou dans notre cas, un message.

Les champs des vecteurs f, p : f, p : $\mathbb{R}^n \rightarrow \mathbb{R}$ et h : $U \in \mathbb{R}^n \rightarrow \mathbb{R}$ sont supposés réels.

Le message doit être discret, la sortie du système (III.3) est transmise au récepteur, ce qui devrait générer un vecteur de sortie qui converge asymptotiquement vers le vecteur d'entrée de l'émetteur. Ceci constitue le problème de l'inversion à gauche. Il est possible de concevoir

un observateur discret retardé pour le système (III.3). Pour cela, il est nécessaire de vérifier certaines conditions qui sont [23] :

1) Les états ainsi que les perturbations sont bornés
2) L'espace vectoriel span $\{dh(f \circ h), ..., d(f^{n-1} \circ h)\}$ est de rang n.
3) $O * p = ((dh)^T, (d(f \circ h)^T, ..., (d(f^{n-1} \circ h))^T)^T * p = (0, ..., \theta)^T$

C'est une fonction differante de zero presque partout dans $U \in \mathbb{R}^n \rightarrow \mathbb{R}$

La condition 3 est appelée condition d'observabilité, elle garantit la proprieté d'inversion à gauche est la possibilité de recuperer tous les états, et le message w(k) à partir de s(k) et ses iterations[23].

Pour garantir l'observabilité du système c'est à nous d'etudier le choix de signal de sortie et ensuite nous expliquons que la methode d'inclusion du message dans une des dynamique du système verifier l'inversion à gauche de ce dernier.

B)- Vérification des conditions d'observabilité de notre système :

On pose notre système (III.2) que l'on veut réécrire sous la forme (III.3), dans le but de vérifié les trois hypothèses nécessaire afin de concevoir un bon observateur discret pour notre système.

a)- Vérification de la première condition :

On a tout les états ainsi le message (m) du système (III.2) bornées, ce qui nous assure la vérification de l'hypothèse 1.

b)- Vérification de la seconde condition :

On a : h = [0 y 0] et sa dérivée dh = [0 1 0], on étudie la faible observabilité locale du système (III.2).

On calcule la matrice d'observabilité (O) dans le voisinage du point d'équilibre (0, 0, 0) du système (III.2).

$$O = \begin{pmatrix} dh \\ d(f \circ h) \\ d(f^2 \circ h) \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & -2x2 & -b \end{pmatrix}$$

On trouve alors avec ses valeurs que le rang n = 3.

Donc notre système (3.2) faiblement observable, ainsi l'hypothèse 2 est vérifiée.

c)- Vérification de la troisième condition :

Nous avons dans notre cas :

$$p = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

On calcule donc O * p :

$$O*p = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & -2x2 & -b \end{pmatrix} * \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \theta = -b \end{pmatrix}$$

θ est différent de zero .
Ainsi l'hypothèse 3 qui represente la condition d'observabilité est vérifiée.
Après avoir vérifié les conditions d'observabilité de notre système (III.2), on peut dire que notre observateur donné permet de reconstruire le message de notre système emetteur.
Nous allons concevoir un observateur discret retardé étape par étape, qui fonctionne avec un pas d'échantillonnage de période T.
La reconstruction des états du message (m) set faite étape par étape.
Dans la première étape on aplique un pas de retard (n-1) sur la sortie et ainsi reconstruire le premier état du message.
La seconde étape on applique deux pas de retard (n-2) sur la sortie, et un pas de retard sur le premier état trouvé avant, dans le but de reconsrtuire le second état du message.
L'application de retard est faite ainsi sur tous les états jusqu'à la dérnière information qui contient l'entrée du système de départ.
A noter que chaque état reconstuit à l'itération n contribue à la reconstruction du prochain état à l'itération n-1. [23] [24]

- **Reconstruction des états et du message :**
- **Reconstruction des états :**

La conception de l'observateur se fait à travers les étapes suivantes :

a)- Etape de reconstruction de l'état $\hat{x}$(k) :
A partir de la deuxième équation du système (III.2), on a :

$$\hat{y}(k+1) = \hat{x}(k)$$

En appliquant un retard d'un pas sur la sortie, on déduit l'état $\hat{x}$(k) comme suit :

$$\hat{x}(k-1) = s(k) = x_0(k-1) \qquad \text{(III.4)}$$

b)- Etape de reconstruction de l'état ẑ(k) :
A partir de la première équation du système (III.2), on a :

$$\hat{z}(k) = \frac{a - \hat{x}(k+1) - y^2(k)}{b}$$

En appliquant cette fois-ci deux pas de retards sur la sortie, ainsi que l'équation (III.4), on déduit l'état ẑ(k) comme suit :

$$\hat{z}\,(k-2) = \frac{a - s(k) - s^2(k-2)}{b} = z_0\,(k-2) \qquad \text{(III.5)}$$

- **Etape de reconstruction du message $\hat{m}$(k) :**

A partir de la troisième dynamique du système (III.2), on a :

$$\hat{m}(k) = \hat{z}\,(k+1) - \hat{y}\,(k)$$

En appliquant trois pas de retards cette fois, et en utilisant les équations (III.4) (III.5), on obtient :

$$\hat{m}(k-3) = \frac{a - s(k) - s^2(k-2)}{b} - s(k-3) = m_0(k-3) \qquad \text{(III.6)}$$

On aura donc les équations de notre observateur qui sont données par les équations (III.4) (III.5) (III.6), obtenue dans les étapes précédentes :

$$\begin{cases} \hat{x}\,(k-1) = s(k) \\ \hat{z}\,(k-2) = \dfrac{a - s(k) - s^2(k-2)}{b} \\ \hat{m}\,(k-3) = \dfrac{a - s(k) - s^2(k-2)}{b} - s(k-3) \end{cases}$$

III.4. Représentation des résultats de simulation :

- **Représentation des états et du message de l'observateur obtenu :**

Dans cette partie, nous allons représenter les états reconstruits par notre observateur, et le message synchronisé. On note que dans les figures(30) (31) (32) les états $\hat{x}(k)$ $\hat{z}(k)$, et le message $\hat{m}(k)$ sont appelé respectivement par xs(k) zs(k) et ms(k). Ceci est illustré par les figures ci-dessous :

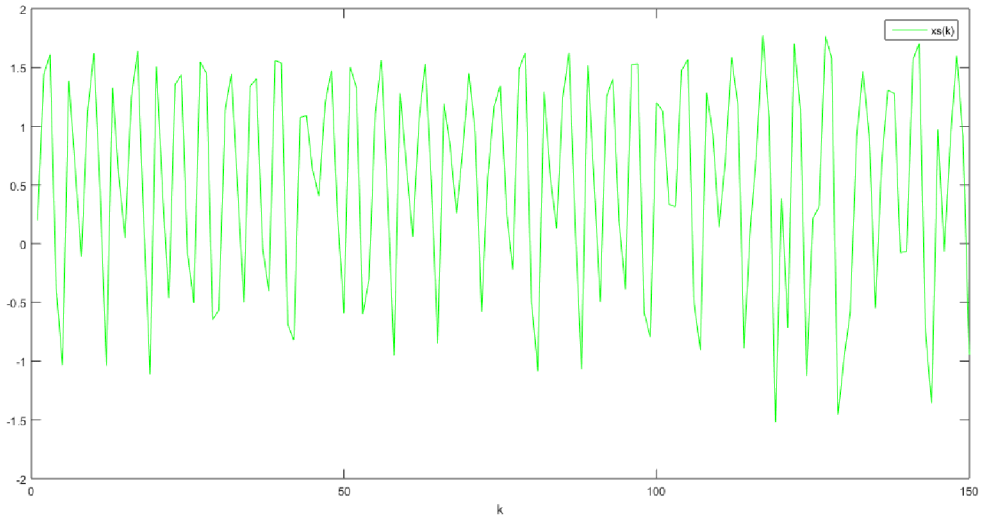


Fig. 30 : Etat $\hat{x}$(k) de l'observateur

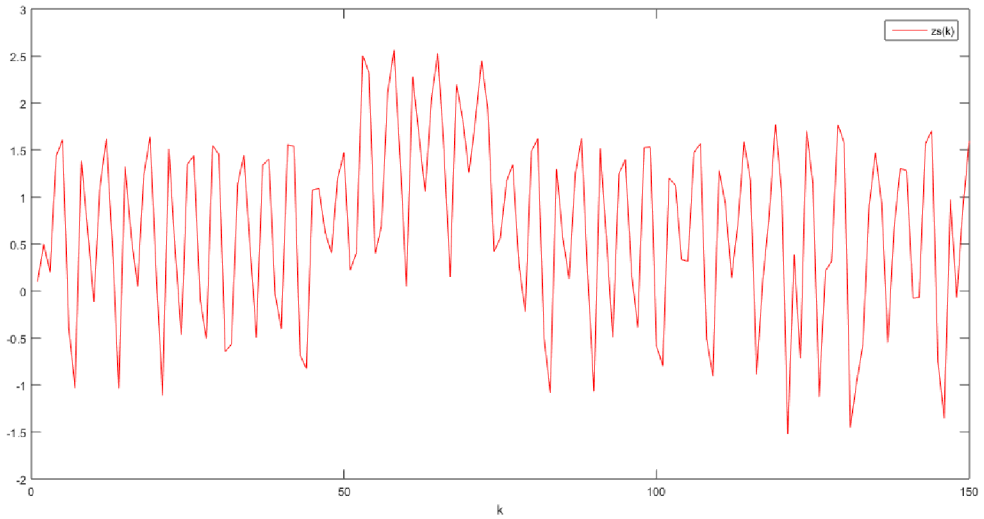


Fig. 31 : Etat $\hat{z}$(k) de l'observateur

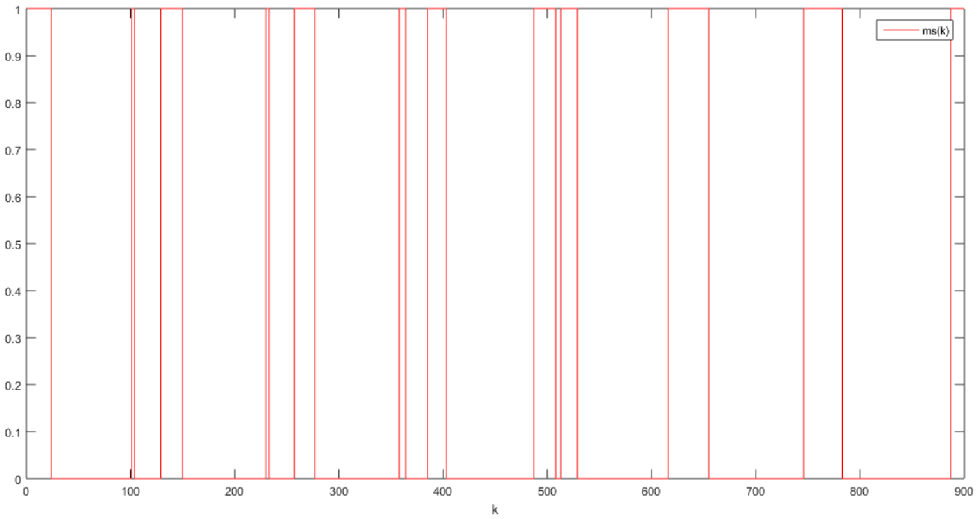


Fig. 32 : Le message $\widehat{m}$(k) de l'observateur

III.5. Transmission d'image :

Dans cette partie, nous donnons les mêmes paramètres de simulation que ceux donnée dans la partie précédente, notre exemple est une image de 128*128 pixels.

On donne ici les résultats de simulation sur la synchronisation des états x(k) $\hat{x}$(k), z(k) $\hat{z}$(k) et des messages m(k) $\widehat{m}$(k).
La représentation des états x(k) et $\hat{x}$(k) synchronisés est donnée par la figure ci-dessous:

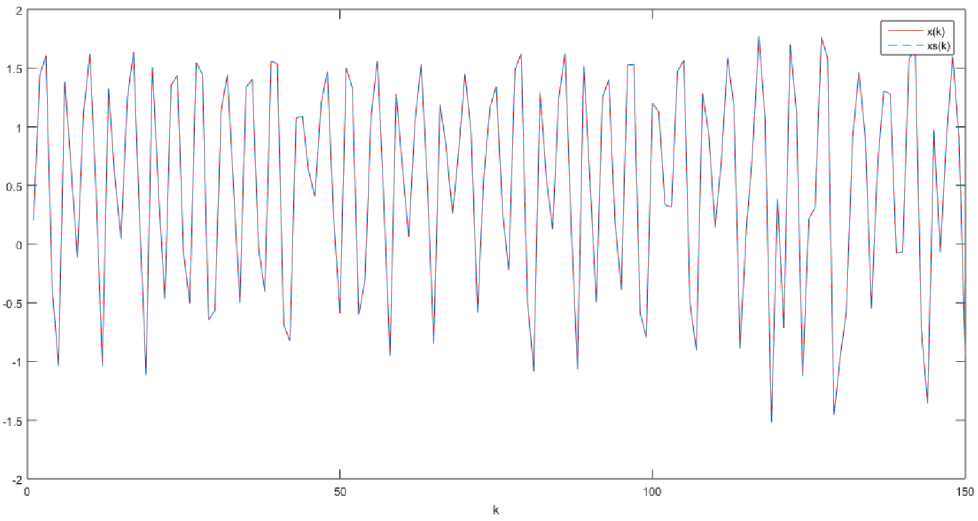


Fig. 33 : Résultat de simulation sur la synchronisation des états x(k) et $\hat{x}$(k)

La représentation des états z(k) et $\hat{z}$(k) synchronisés est donnée par la figure ci-dessous:

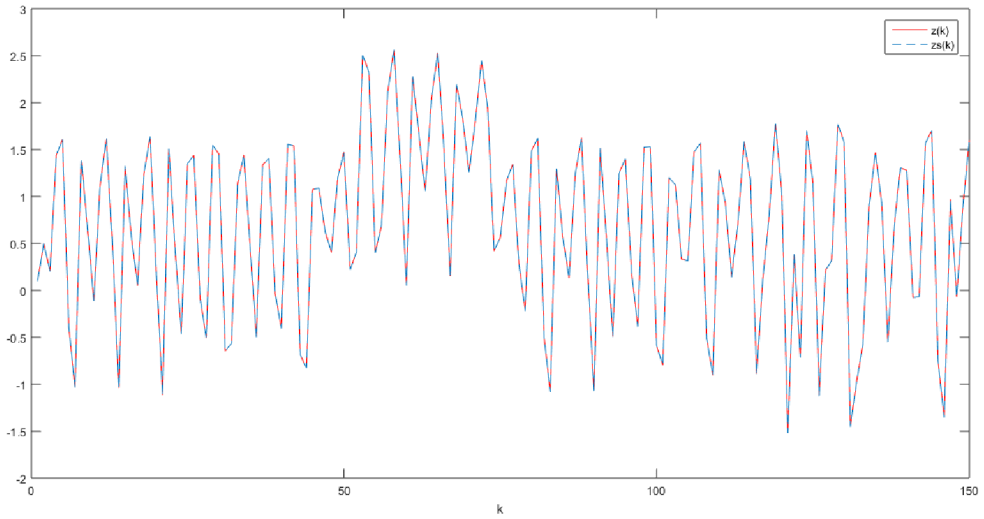


Fig. 34 : Résultat de simulation sur la synchronisation des états z(k) et $\hat{z}$(k)

La représentation des messages m(k) et $\widehat{m}$(k) synchronisés est donnée par la figure ci-dessous:

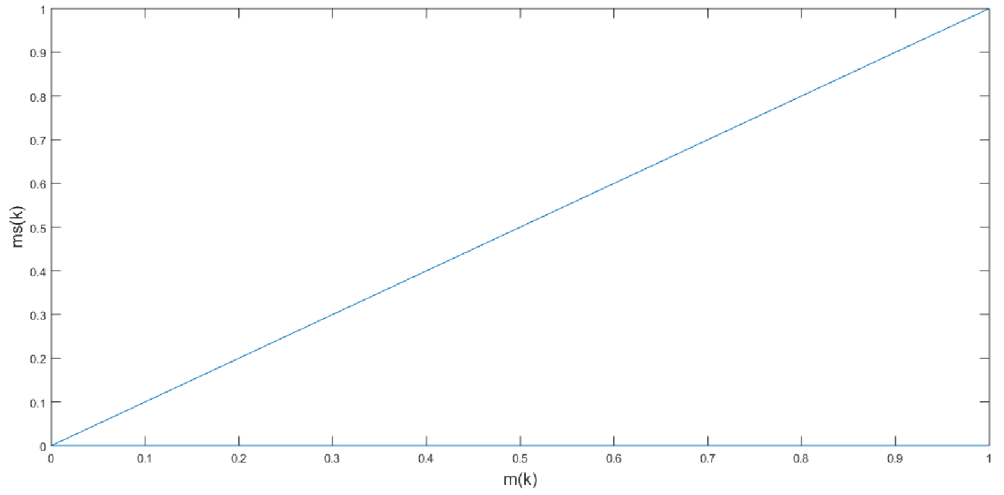


Fig. 35 : Résultat de simulation sur la synchronisation des messages m(k) et $\widehat{m}$(k)

La représentation des images suivant l'ordre :(image originale, image cryptée, image décryptée), est illustrée par les figures ci-dessous :

Fig. 36 : L'image originale

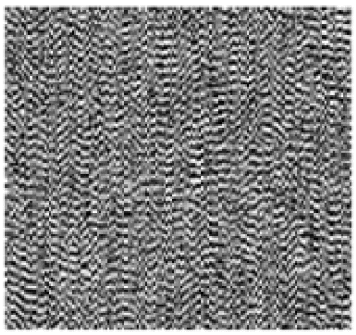


Fig. 37 : L'image cryptée

Fig. 38: L'image décryptée

III.6. Analyse de la robustesse du système de transmission proposé :

Analyse statistique:

Dans cette partie, on propose une analyse statistique basée sur les histogrammes des images originale, cryptée, décryptée, qui sont représentées par les figures (39), (40), (41).

L'image originale avec son histogramme est donnée par la figure ci-dessous :

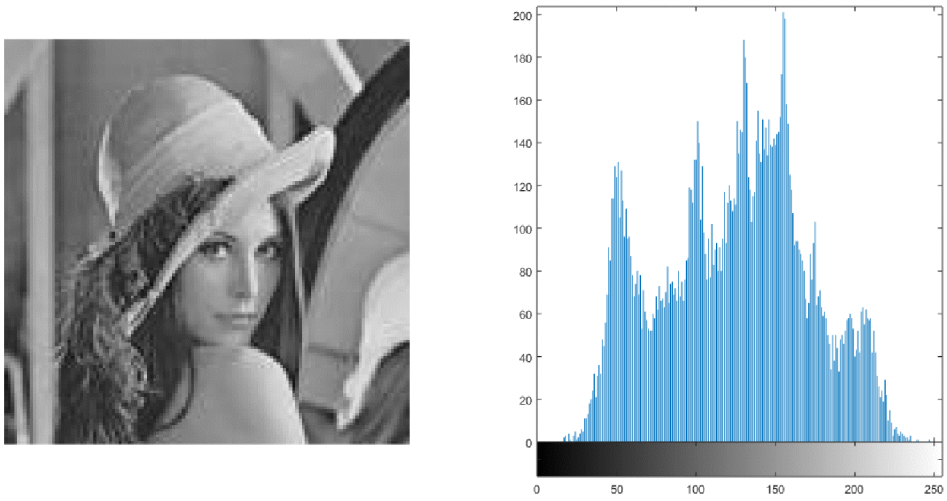


Fig. 39 : L'image originale avec son histogramme

L'image cryptée avec son histogramme est donnée par la figure ci-dessous :

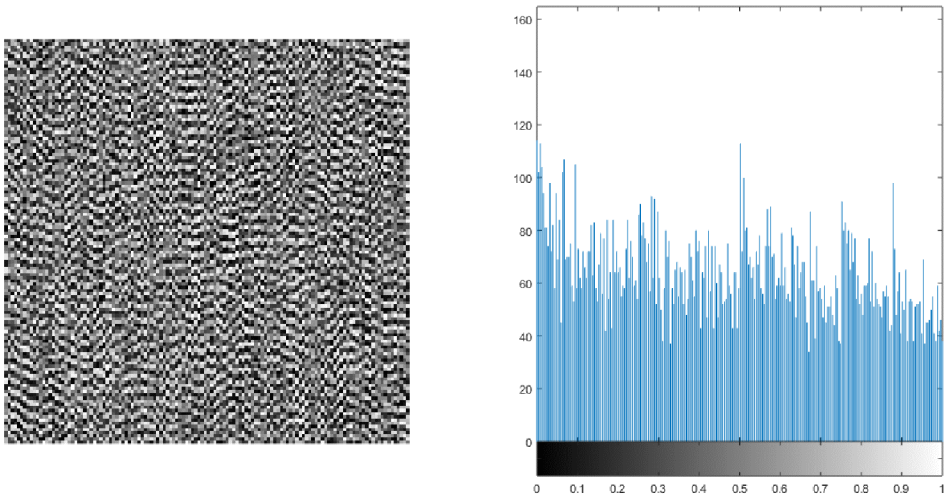


Fig. 40 : L'image cryptée avec son histogramme

L'image décryptée avec son histogramme est donnée par la figure ci-dessous :

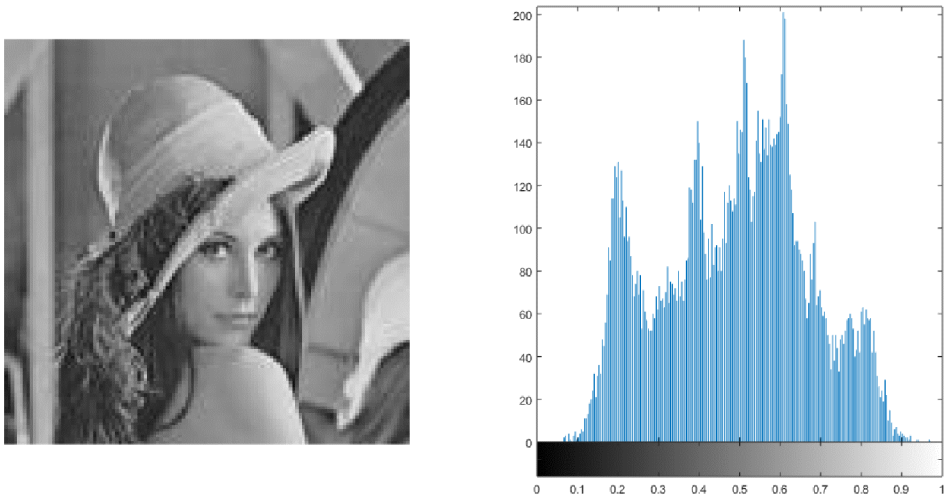


Fig. 41 : L'image décryptée avec son histogramme

Si on fait une comparaison des histogrammes des figures (39) et figure(41), on peut voir que l'histogramme de l'image déchiffrée, ne représente pas de différence de celui de l'image originale.

On propose aussi une autre méthode d'analyse statique basé sur la corrélation, représentée par les figures suivantes (42) (43) (44).

Présentation de la corrélation des pixels adjacents horizontalement de l'image originale et l'image cryptée donné par la figure ci-dessous :

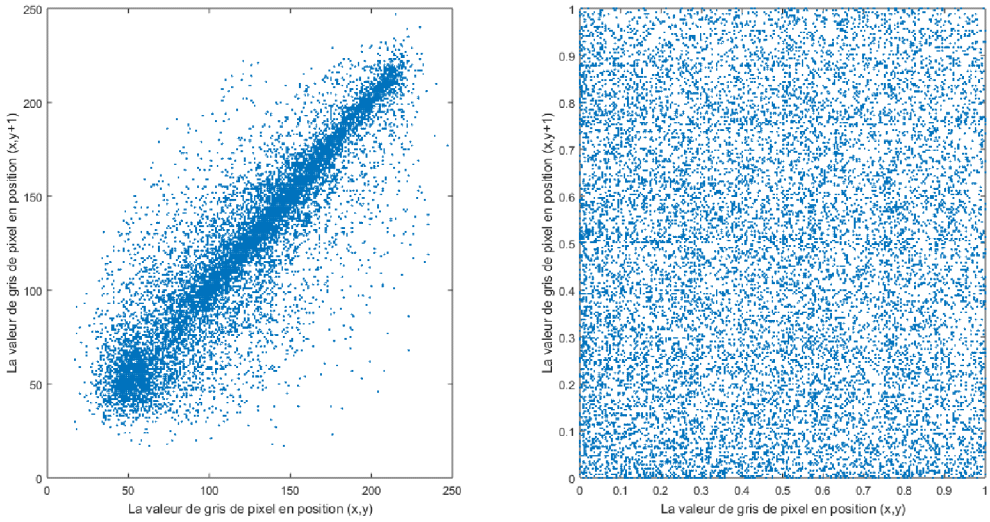


Fig. 42 : Corrélation des pixels adjacents horizontalement de l'image originale et l'image cryptée

Présentation de la corrélation des pixels adjacents verticalement de l'image originale et l'image cryptée donné par la figure ci-dessous :

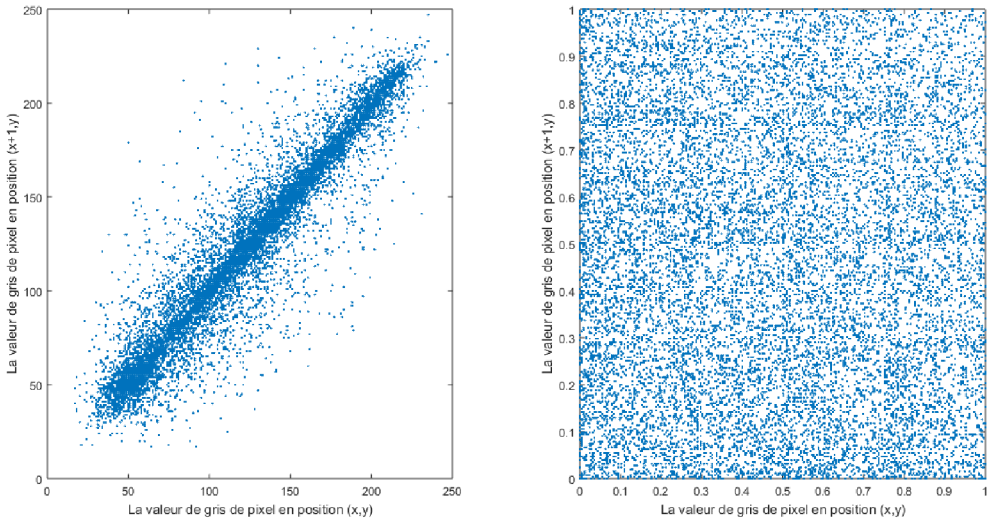


Fig. 43 : Corrélation des pixels adjacents verticalement de l'image originale et l'image cryptée

Présentation de la corrélation des pixels adjacents diagonalement de l'image originale et l'image cryptée donné par la figure ci-dessous :

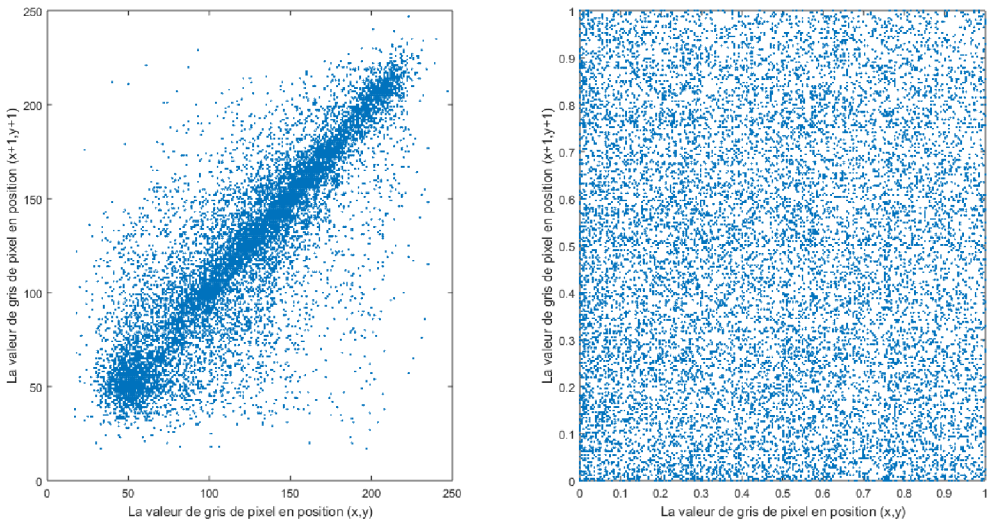


Fig. 44 : Corrélation des pixels adjacents diagonalement de l'image originale et l'image cryptée

Les figures (42) (43) (44), montrent la distribution de la corrélation des pixels adjacents horizontalement verticalement, et diagonalement, des images originale et cryptée.

III.7. Résultats de simulation :

Dans cette section, nous présentons les résultats de simulation à l'aide de logiciel Matlab pour la synchronisation de deux systèmes. Le système (III.2) qui représente l'émetteur va se synchroniser avec le récepteur, qui est dans notre cas un observateur.

Dans notre système de communication le message envoyé est une image numérique de dimension 128*128 pixels.

Les figures (30) (31) (32) montrent respectivement les états $\hat{x}$(k) et $\hat{z}$(k) et le message $\widehat{m}$(k) récupérés.

La reconstruction des états se fait à l'aide d'un observateur pas à pas. L'histogramme de l'image cryptée, présente une grande différence de ceux des images originale et décrypté, ce qui démontre la sécurité de notre crypto-système.

Les figures (39) (40) (41) représentent respectivement les images, originale, cryptée et décryptée, et leurs histogrammes, dont on remarque que l'histogramme de l'image originale est identique à celui de l'image décryptée.

La corrélation des pixels adjacents dans les positions horizontale, verticale, et diagonale est illustrée par les figures (42) (43) (44).

III.8. Conclusion :

Dans ce chapitre, nous avons proposé des simulations sous Matlab pour la transmission sécurisée d'une image à base d'un système dynamique hyper chaotique discret.

Dans la première partie, nous avons présenté l'émetteur qui est constitué principalement d'un système hyper chaotique à temps discret dit Hénon modifie, et le récepteur qui est un observateur discret retardé. Ensuite on a illustré les figures de la synchronisation des états et du message de notre système, ainsi que les images originale, cryptée, et décryptée.

En seconde partie, On a donné les résultats de simulation sur la synchronisation des états $x(k)$ $\hat{x}(k)$, $z(k)$ $\hat{z}(k)$ et des messages $m(k)$ $\widehat{m}(k)$.
L'analyse statistique de robustesse de notre système de transmission, nous donne de très bons résultats sur la performance de notre système de cryptage, qui est efficace contre les attaques statistiques, ainsi l'image originale est bien récupérée.

Conclusion générale

Ce mémoire a proposé une étude sur un domaine très complexe qui est le chaos. Nous avons étudié les différents types des systèmes chaotiques, ainsi leurs caractéristiques, ce qui nous a donné la possibilité de simuler un schéma de transmission d'une image sécurisée à base de chaos.

Le premier chapitre a proposé des généralités sur les systèmes dynamiques, dont nous avons étudié une classe particulière appartenant aux systèmes dynamiques non linéaires dit chaotique. Dans cette partie, nous avons abordé les caractéristiques les plus importantes des systèmes chaotiques, comme l'aspect aléatoire qui est défini par des équations non linéaires déterministes, la sensibilité aux conditions initiales où une très petite erreur sur la connaissance de l'état initial X0 dans l'espace des phases va se trouver (presque toujours) rapidement amplifiée. Pour finir, nous avons montré le chemin de transition vers le chaos par doublement de période, la quasi-périodicité, et par intermittence.

Dans le chapitre deux, nous avons cité les différentes méthodes de synchronisation des systèmes chaotiques, qui est une base indispensable pour réussir une transmission de données. Comme nous avons mentionné vers la fin du chapitre quelques techniques de chiffrement chaotiques.

Nous avons proposé dans le chapitre trois, la simulation sous Matlab d'un nouveau schéma de transmission sécurisée d'une image avec un système hyper chaotique dit Henon modifié. D'abord nous avons inclus un message information dans la dynamique du système émetteur, par la méthode de chiffrement par injection. Pour la réception, nous avons conçu un observateur discret dans le but de récupérer les états, ainsi le message original envoyé au niveau de l'émetteur. Dans la dernière section, nous avons proposé une analyse statistique de robustesse du système de transmission.

Les résultats de simulation obtenus ont bien illustré bien les performances de notre système de cryptage proposé. Ce dernier est efficace contre les attaques statistiques, ce qui nous a permis de bien protéger l'information. Cette dernière a été récupérée sans distorsion, une preuve de la fiabilité et la robustesse de notre système de chiffrement par le chaos.

En perspectives, nous envisageons de réaliser le système de transmission proposé en utilisant deux cartes Arduino Méga ou bien d'autres cartes plus sophistiqués comme les cartes Rasberry.

Bibliographie

Bibliographie

[1] E.N. Lorenz, Deterministic nonperiodicflow, Journal of the atmospheric sciences, vol 20, no.2, 1963.

[2] H. Poincaré, Problème des 3 corps, Acta Match, vol 13, pp. 1-270, 1890.

[3] A. Kiani-b, K.Fallahi, IN.Paris and H.Leung, « A chaotic secure communication scheme using fractional chaotic based on an extended fractional Kalman filter », Communication in nonlinear sciences and numerical simulations, vol.14, pp.863-879, 2009.

[4] H.Hamiche, S.Guermah, R.Saadaoui, K.Hannoun, M.Laghrouche, S.Djennoune, « Analysis and implementation of a novel robust transmission scheme for private digital communication using Arduino Uno board », Nonlinear dynamics, vol.81 (4), pp.1921-1932, 2015.

[5] H.T.Yan, Y.C.Pu, S.C.Li, « Application of chaotic synchronization system to secure-communication », Information technology and control, 2012.

[6] L.M.Pecora, T.L.Carroll « Synchronization in chaotic systems », Physical Review Letters, February, volume 64, (8), pp. 821-825, 1990.

[7] T.Hoet, B.Lorenzi, S.Sahin « La cryptographie chaotique», INSA Toulouse, France, 2012.

[8] C.Benhabib, « Etude d'un système chaotique pour la sécurisation des communications optiques », Mémoire de master en télécommunications, Faculté de technologie, Université de Tlemcen, Algérie, Juin 2014.

[9] G. Zabi, « Sécurisation par dynamiqueschaotiques des réseaux locaux sans fil au niveau de la couche MAC », Thèse de doctorat, Université de Toulouse, France, 2012.

[10] O.Jerèmy, « Le chaos dans les systèmes dynamiques », 5 juillet 2007.

[11] T. Hamaizia « Systèmes Dynamiques et chaos : application à l'optimisation à l'aide d'algorithme chaotique », Université de Constantine-1, Algérie 2013.

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

[13] S.Penaud, « Etude des potentialités du chao pour les systèmes de télécommunications, évaluation des performances de systèmes à accès multiples à répartition par les codes (CDMA) utilisant des séquences d'étalement chaotique », Thèse de doctorat de L'université de Limoges, France, 2001.

[14] G.R.Cooper, R.w.Nettleton « Spread spectrum technique for high capacity mobile communications », IEEE Trans.Veh.Tech, .Vol.VT-1978.

Bibliographie

[15] G.R .Cooper, R .W. Nettleton «Spectral efficiency in cellularand –mobile communications: a spread spectrum approach », Final Report, TR-EE 78-44, Purdue University, West Lafayette, Ind .1978.

[16] M.Abramowitz, I.S. Stegun « Handbook of mathematical function with Formulas, graphs and mathematical tables» Dover publications ,Inc ,New york,1965.

[17] S.Boccaletti, J.Kurth, G.Osipov, D.L.Valladares, V.S.Zhou, « The synchronization of chaotic systems », physics reports, 2002:1-101.

[18] E.Cherier, « Estimation de l'état et des entrées inconnues pour une classe de systèmes non linéaires », thèse de Doctorat, Nancy, France, 2006.

[19] O.Megherbi «Etude et réalisation d'un système sécurisé à base de systèmes chaotiques » Mémoire de magister, Université Mouloud Mammeri Tizi Ouzou, Algérie, 2013.

[20] H.Dimassi, « Synchronisation des systèmes chaotiques par observateurs et application à la transmission d'information», Thèse de doctorat de l'Université de Paris Sud 11, France, 2012.

[21] K.Hannoun, « Etude, simulation etimplémentation d'un émetteur hyper chaotique sur carte Arduino Uno », Mémoire de master académique en Electronique, Département d'Electronique, Université Mouloud Mammeri de Tizi-Ouzou, Algérie, 2013

[22] K.Vesely, J.Podolsky, « Chaos in a modified Hénon- Heiles system describing geodesics in gravitational waves » Technical physics letters A, vol, 271, pp.368-371,2000.

[23] M.Djemai, J.P. Barbot and I.Belmouhoub, « Discrete-time normal form for left invertibility problem», Universit´e de Valenciennes et du Hainaut-Cambresis, Le Mont Houy, 59313 Valenciennes Cedex 9, France.

[24] I.Bemouhoub, M.djemai and J.P.Babot, « Observability quadtatic normal form for discrete-time systems », IEEE Transactions on Automatic Control, vol.15, pp.194-204, 2009.

Annexe

Annexe

1. Déterminisme

La notion de déterminisme signifie la capacité de « prédire » le futur d'un phénomène à partir d'un événement passé ou présent.

Un système déterministe est un système dont l'état présent est complètement déterminé par les conditions initiales, en contradiction avec un système stochastique pour le quel l'état présent reflète les conditions initiales avec en plus d'une réalisation particulière d'un paramètre aléatoire (bruit et variable interne).

2. Cycle limite

Les cycles limites sont des phénomènes non linéaires, ce sont des trajectoires fermées isolées. Tout système non linéaire qui a un siège d'oscillations est dit cycle limite, ils sont caractérisés par leurs amplitudes et leurs fréquences indépendantes de la condition initiale, et par le fait d'être sans excitation extérieure.

3. Non Linéarité

La non-linéarité renvoie d'une manière générale à une rupture de la proportionnalité des causes et des conséquences.

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

4. Tore

Cas particulier du cycle limite, le système présente aux moins deux période simultanés dont le rapport est irrationnel (aléatoire), la trajectoire de phase ne s'annule pas sur elle-même.

5. Système autonome

Un système dynamique non linéaire est dit autonome lorsqu'il ne dépend pas explicitement du temps. Un système autonome est donné ci-dessous :

$$\begin{cases} \dot{x} = f(x,y) \\ \dot{y} = g(x,y) \end{cases}$$

Un système autonome est indépendant du temps initial, alors qu'un système non autonome ne l'est pas. Dans un système autonome, tout instant peut être considéré comme instant initial, et tout état $x(t)$ du système peut être considéré comme un état initial.

6. Bassin d'attraction

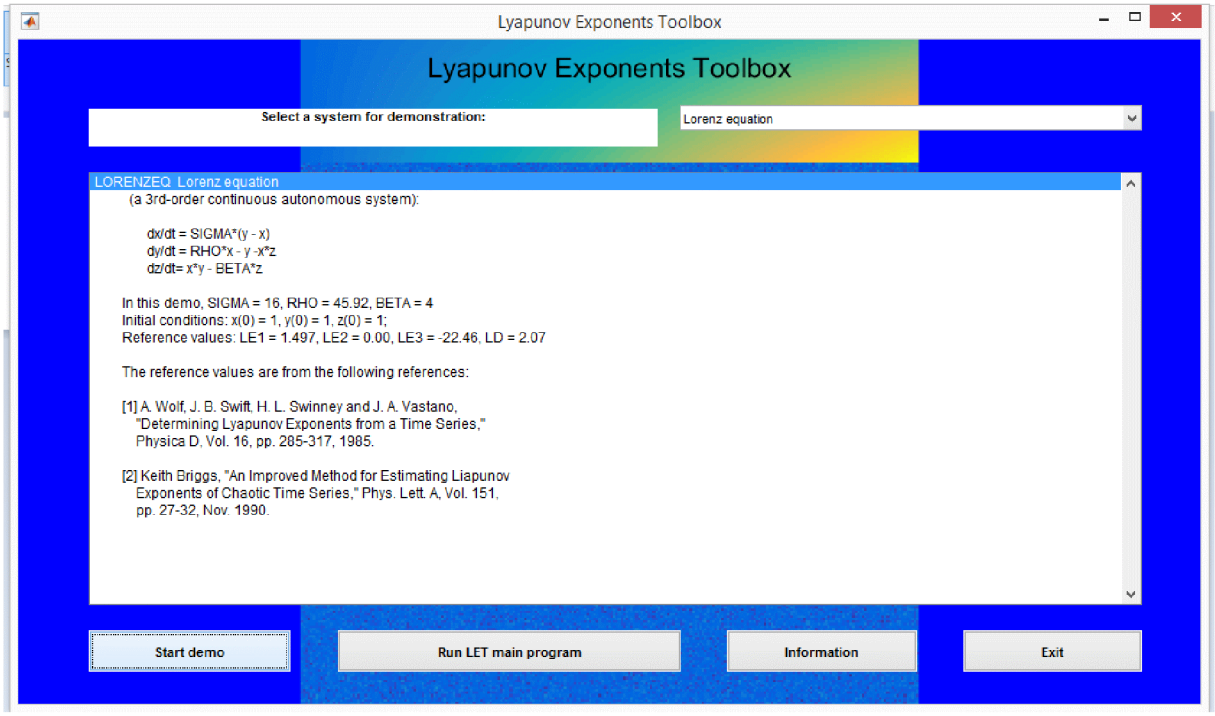
Le bassin d'attraction est l'ensemble des points de l'espace des phases qui sont sous l'effet de l'attracteur. C'est à dire que toutes les trajectoires qui commencent à ces points tendent vers l'attracteur après un temps fini.

7. LET (Lyapunov Exposant Toolbox)

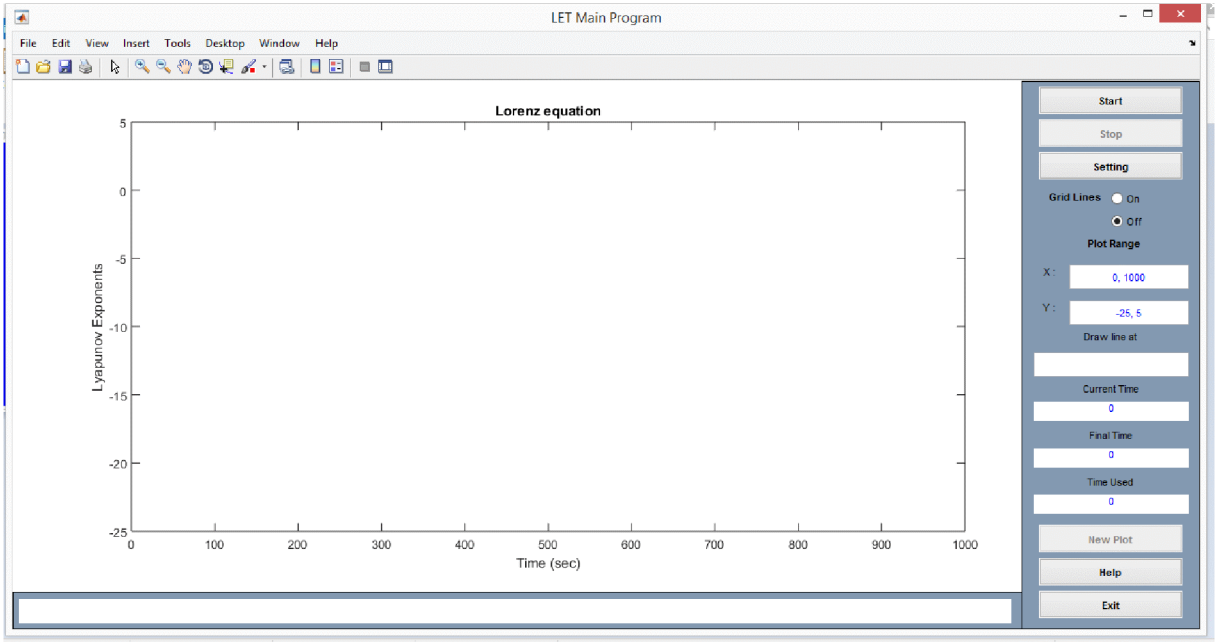
Lyapunov exposant toolbox(L.E.T) fournit une interface graphique utilisateur pour les utilisateurs afin de déterminer les ensembles complexes d'exposants de lyapunov et lyapunov et lyapunov dimension des systèmes chaotiques continus et discrets

Cette boite à outils ne peut fonctionner que sur MATLAB ou versions supérieures du matlab.il a été testé sous Windows et Unix et peut aussi fonctionner sur d'autre plate-forme.

La fenêtre sur la figure ci-dessous s'ouvre on a le choix entre plusieurs systèmes chaotiques.



Annexe



8. Comment utiliser le programme

Pour exécuté le programme entré, entrez « let » dans MATLAB fenêtre workspace. Afin d exécuter le programme correctement, tout les fichiers du cette boites doivent être dans le dossier du travail. Quand la fenêtre GUI apparait, les utilisateurs peuvent exécuter un programme de démonstration en appuyant sur le bouton Run LET main program. Let fournit certains systèmes chaotiques connus pour des demonstration.les utilisateurs peuvent choisir l'un deux dans le menu pop-up.

Pour calculer les exposants de lyapunov et la dimension d un système suivez les étapes ci-dessous.

1-écrire une fonction dans ODE qui décrit le système spécifié.

2-entré « let » dans MATLAB fenêtre de commande.

3-appuyez sur le « Run »dans la fenêtre de démarrage.

4-entré le paramètre souhaité dans la fenêtre de réglage.

5-Appuyez sur le bouton « démarrer »dans la fenêtre principale pour démarrer le calcul.

Résumé :

Ce mémoire a proposé une étude sur un domaine très complexe qui est le chaos. Il a exposé les différents types des systèmes chaotiques, ainsi leurs caractéristiques, ce qui nous a donné la possibilité de simuler un schéma de transmission d'une image sécurisée à base de chaos.

L'objectif préliminaire est de manipuler le logiciel MATLAB afin d'arriver à réaliser un programme capable de réussir la transmission sécurisée proposé.

Ce travail est efficace contre les attaques statistiques, ce qui nous a permis de bien protéger l'information. Cette dernière a été récupérée sans distorsion, une preuve de la fiabilité et la robustesse de notre système de chiffrement par le chaos.

Mots Clés :

Système chaotique, transmission sécurisée, simulation MATLAB, théorie du chaos, nouveau schéma de transmission.