
مهورية الجزائر الديمقراطية الشعبية
République Algérienne démocratique et populaire

وزارة التعليم العالي والبحث العلمي
Ministère de l'enseignement supérieur et de la recherche scientifique

جامعة سعد دحلبان
Université SAAD DAHLAB de BLIE

كلية التكنولوجيا
Faculté de Technologie

قسم الإلكترونيك
Département d'Électronique



Mémoire de Master

Filière : Électronique

Spécialité : Electronique des systèmes Embarqué

Présenté par

Eddaikra Wafik

&

Bounib Mouaadh

Etude d'un émetteur et récepteur chaotique

Proposé par : Mr. Ferdjouni Abdelaziz

Année universitaire 2020-2021

INTRODUCTION GÉNÉRALE

Depuis l'antiquité, l'homme n'a pas cessé de chercher les différents moyens pour transmettre un message à son correspondant et pouvoir ainsi communiquer avec lui en toute sécurité. Il a fourni à travers des époques successives, des efforts autant physiques qu'intellectuels pour pouvoir trouver une technique de communication efficace et appropriée.

En effet, les modes de télécommunications sont en évolution continue avec la recherche permanente de meilleurs débits, de facilité d'utilisation, de mobilité améliorée et surtout d'une confidentialité élevée.

Depuis des siècles, la cryptographie a été une histoire de conflit qui oppose deux camps, un qui cherche à cacher une information et l'autre qui essaie de trouver ce qu'on lui cache. Ainsi à chaque fois que le premier trouve un moyen de chiffrer ses messages le second essaie et avec le temps et les moyens dont il dispose, réussit à trouver la méthode ou l'astuce pour le décrypter. La cryptographie ancienne utilisait différents outils pour dissimuler une information ou un texte secret. Certains remplaçaient des mots par des nombres, d'autres mélangeaient, décalaient ou permutaient les lettres, comme dans la substitution alphabétique inverse, pour rendre la lecture du message difficile.

La cryptographie actuelle cherche à transformer de façon mathématique et algorithmique un message clair pour obtenir un autre chiffré et qui à première vue semble aléatoire. Plus l'inverse de la transformation est difficile, plus la sécurité est élevée et vice-versa. On cherche alors un phénomène d'apparence aléatoire mais qui est déterministe à l'origine pour le masquer l'information.

Il existe plusieurs systèmes présentant ce comportement, ils sont dits chaotiques, ils sont régis par des lois déterministes, dépendent d'un ou de plusieurs paramètres et leur évolution dans le temps est imprévisible. L'étude de tels systèmes est liée à la théorie du chaos qui a connu un grand essor à partir de 1960 grâce aux travaux de plusieurs chercheurs notamment ceux de Lorenz.

La cryptographie chaotique est ainsi née par inclusion du chaos dans les télécommunications et systèmes de transmission. L'idée consiste à noyer un message dans un signal chaotique pour faire face aux éventuelles tentatives de piratage.

La transmission chaotique est un mode de communication à clé secrète. La connaissance de cette clé est nécessaire du côté de l'émetteur du message ainsi que du récepteur pour le chiffrement et le déchiffrement du message. On doit alors disposer au

niveau

du récepteur, d'un signal chaotique identique à la porteuse pour pouvoir récupérer le message masqué.

Ce travail de mémoire consiste à réaliser un système de transmission sécurisée à base de chaos. Il repose d'une part sur la synchronisation chaotique et d'autre part sur le masquage de l'information secrète. Ces systèmes se composent de deux oscillateurs chaotiques liés par un canal de transmission publique. Un message sera crypté puis envoyé à partir de l'oscillateur émetteur. L'objectif est de récupérer ce signal utile en utilisant une synchronisation chaotique de l'oscillateur récepteur.

Pour cela, nous avons organisé notre mémoire de la manière suivante:

- Le premier chapitre représente un rappel sur les systèmes dynamiques en général et chaotiques en particulier. Il énoncera quelques concepts sur la théorie du chaos.
- Le second chapitre mettra en évidence d'une part, les différents types de la synchronisation et d'autre part la méthode que nous avons choisie pour récupérer notre signal crypté.
- Dans le troisième chapitre, consiste à étudier le cryptage et le décryptage d'image et le système de Chen qui l'émetteur et du circuit d'insertion du message à crypter.
- Le quatrième chapitre représente l'émetteur et le récepteur chaotique et la synchronisation des deux systèmes émetteur et récepteur. A la fin nous voyons l'insertion du message par modulation paramétrique puis la récupération du message et le plan de phase.

✚ Avant tout nous tenons à remercier Dieu qui nous incité à acquérir le savoir.

✚ A travers ce modeste travail , nous tenons à remercier vivement notre promoteur Dr Abdelaziz Ferjouni pour l'intéressantedocumentation qu'il sont mise a note disposition ,pour ces conseils précieux et pour tous les commodités et aisance qu'il nous apportées durant notre étude et réalisation de ce projet.

✚ Nous exprimons également notre gratitude à tout les professeurs et enseignants qui ont collaboré a notre formation depuis notre premiercycle d'étude jusqu'à la fin de notre cycle universitaire.

✚ Sans omettre bien sur ce de remercier profondément tous ceux qui ont contribué de près ou de loin à réalisation du présent travail.

Dedicas

✚ Au terme de ce travail , nous voudrons adresser nos vifs remerciements à nos chers parents pour leurs sacrifices , aides, soutiens et encouragements durant notre cursus d'étude.

✚ Nous dédions ce modestes travail :

A nos frères et nos sœur ainsi que tous les membres des familles

✚ A tous nos amis de la promo.

المخلص :

يتكون هذا العمل من استخدام إشارة فوضوية لتشفير وفك تشفير صورة واستعادة إشارة فوضوية. لهذا ، أولاً وقبل كل شيء ، درسنا أساسيات النظام الفوضوي (التشعب ، أس الليابونوف) ثم المرسل الفوضوي مع إدخال الرسالة. ثم تمت مزامنة نظامي الإرسال والاستقبال باستخدام طريقة المزامنة التكيفية. أكملنا عملنا بمحاكاة نظام Chen وتشفير صورة التعديل المعياري باستخدام برنامج (MATLAB (Simulink) ، الكلمات الرئيسية: إشارة Chaotic ؛ تشعب. أس ليابونوف. التزامن التكيفي نظام تشن تعديل حدودي

Résumé:

Cetravailconsisteàutiliserunsignalchaotiquepourcrypter et décrypter uneimageet récupérer un signal chaotique . Pourcela, dansunpremiertemps, on a étudié les bases systèmes chaotique (bifurcation, exposant de lyapunov) ensuite l'émetteurchaotique avec l'insertion du message. Ensuite on a synchronisé les deux systèmes émetteur -récepteurgrâceàlaméthodedesynchronisationadaptative.

Nous avons achevé notre travail par une simulation du système de Chen et cryptage d'image par modulation paramétrique à l'aide dulongicielMATLAB(Simulink),Motsclés:Signalchaotique ;bifurcation ;exposantdeLyapunov ;synchronisation adaptative ;système deChen ; modulation paramétrique

Abstract:

This work consists of using a chaotic signal to encrypt and decrypt an image and recover a chaotic signal. For this, first of all, we studied the essentials of the chaotic system (bifurcation, Lyapunov exponent) then the chaotic transmitter with the insertion of the message. Then the two transceiver systems were synchronized using the adaptive synchronization method.

We completed our work with a simulation of the Chen system and parametric modulation image encryption using MATLAB software (Simulink), Keywords: Chaotic signal; bifurcation; exponent of Lyapunov; adaptive synchronization; Chen system; parametric modulation

Chapitre 1

:GENERALITESURLESSYSTEMESDYNAMIQUESCHAOTIQUES

1-Introduction	7
2-Système dynamique.....	8
3-Systèmes autonomes et non autonomes.....	8
4-Le chaos.....	9
4.1-L'étude du chaos (concept et définitions).....	9
4.2-Définition d'un système chaotique.....	9
4.3-Caractéristique du chaos.....	10
4.4-Historique sur le chaos.....	12
4.5-Principales applications de l'étude du chaos.....	13
5-Points fixes, système de Lorenz.....	14
5.1-Les différents types de points fixes.....	15
6-Attracteur.....	16
6.1-Les différents types d'attracteurs.....	16
7-Section de Poincaré.....	18
8-Exposants de Lyapunov.....	19
9-Bifurcation et routes vers le chaos.....	20
9.1-Le doublement de période.....	21
9.2-L'intermittence.....	21
9.3-quasi-périodicité.....	21
10-Exemples de système chaotique.....	23
10-1-L'attracteur de Lorenz.....	23
Conclusion.....	24

Chapitre 2 : Synchronisation des systèmes chaotiques

1-introduction.....	25
2-Définition de la synchronisation.....	26
3-Méthodes de synchronisation.....	26
3-1-Synchronisation par répartition système.....	26
3-2-Synchronisation généralisé.....	29
3-3 synchronisations retardées.....	30
3-4 synchronisations projectives.....	30
3-5 synchronisations par boucle fermé.....	30
4-technique de cryptage par le chaos.....	32
4-1-insertion de message par addition.....	32
4-2insertion de message par modulation paramétrique.....	33
4-3insertion de message par inclusion.....	35
4-4insertion de message mixte.....	35
Conclusion.....	36

Chapitre 3: cryptage et décryptage d'image par le système chaotique

3-1 introduction.....	37
3-2 notion de base sur l'image.....	37
3-2-1 type d'image numérique.....	39
3-2-2. les diferrent format d'image.....	39
3-3. cryptage d'image.....	40
3-3-1. introduction a la cryptographie.....	40
3-3-2. cryptographie par le chaos.....	40
3-3-3 .méthode proposée : cryptage par matlab simulink.....	40
Conclusion.....	41

Chapitre 4: insertion et récupération de message du système chaotique avec modulation paramétrique et synchronisation

4-1. étude de l'émetteur.....	45
4-1-1Présentation des équations de système de Chen.....	45
4-1-2Définition des paramètres.....	45
4-1-3simulation du système.....	46
4-2. étude de l'émetteur complet en fonction de système de Chen.....	47
4-2-1. méthode utilisé.....	47
4-2-2. étude et réalisation.....	47
4-2-3. calcul du paramètre b modulé.....	48
4-3. réalisation du système émetteur sous MatlabSimulink.....	48
4-3-1. explication détaillée de chaque bloc.....	48
4-4. étude du récepteur.....	53
4-4-1.introduction.....	53
4-4-2. méthode utilisé : synchronisation adaptative.....	53
4-4-3. les étapes de la synchronisation adaptative.....	53
4-4-3-1. les étapes à suivre pour la réalisation du récepteur.....	53
Conclusion général.....	60

Liste des figures

Figure 1.1. Evolution dans le temps d'un système chaotique, comparé à une sinusoïde.....	10
Figure 1.2. Sensibilité aux conditions initiales du système de Lorenz.....	11
Figure 1.3. L'attracteur de Lorenz.....	12
Figure 1.5. Attracteur étrange de Lorenz.....	16
Figure 1.6 Les exemples d'attracteurs.....	17
Figure 1.7. Représentation de la section de Poincaré pour le système de Lorenz	
Figure 1.8. Les exposants de lyapunov du système de Lorenz.....	22
Figure 1.9. Représentation du système chaotique de Lorenz dans l'espace des phases.....	23
Figure 1.10. Représentation du système chaotique de Lorenz dans l'espace des phases.....	24
Figure2.1synchronisation maitre esclave.....	28
Figure2.2synchronisation par boucle fermée.....	31
Figure2.3cryptage par addition.....	32
Figure2.4insertion de message par modulation paramétrique.....	34
Figure2.5insertion de message mixte.....	35
Figure 3-1. Cryptage d'image sous matlab simulink avec le bloc Chen.....	41
Figure3-2. Image cryptée.....	42
Figure3-3. Image en cour de décryptage.....	42
Figure3-4.image démontre le processus et l'opération de décryptage.....	43
Figure3-5. Image décryptée.....	43
Figure4-1.schéma bloc du système de Chen.....	46
Figure4-2.les signaux du système de Chen en fonction du temps.....	46
Figure4-3.réalisation du système émetteur.....	49
Figure4-4. Image reconstituée.....	50
Figure4-5.graphe de variation du paramètre b modulé.....	51
Figure4-6.signal amplitude des pixels d'image.....	51
Figure4-7—4-10 traçage de l'émetteur en fonction du temps.....	57
Figure4-11—4-14 traçage d'émetteur en fonction d'erreur.....	60
Figure 4—15—4-18 traçage du plan de phase.....	63

CHAPITRE 1

GENERALITES SUR LES SYSTEMES DYNAMIQUES CHAOTIQUES

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 alors caractérisée par le déterminisme, la prévisibilité et la réversibilité. Poincaré fut l'un des premiers à entrevoir la théorie du chaos [1].

Il découvrit la notion de sensibilité aux conditions initiales à travers le problème de l'interaction de trois corps célestes.

Le terme "chaos" définit un état particulier d'un système dont le comportement ne se répète jamais et 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. Ils ont cherché à répondre à des questions telles que : les arythmies cardiaque ou les variations d'une population animale obéissent-elles à des règles ? Les mouvements commerciaux ou les marchés financiers peuvent-ils s'expliquer ?

Le chaos a ainsi trouvé de nombreuses applications dans les domaines tant physiques que biologiques, chimiques ou économiques [2]. Ainsi, ce chapitre est organisé de la manière suivante. On commence par une définition des systèmes dynamiques. Ensuite, on passe à la présentation des systèmes chaotiques et à la caractérisation de leur comportement.

On termine le chapitre par la description de système chaotique à savoir le système de Lorenz.

2-Système dynamique

Un système dynamique est une structure qui évolue au cours du temps de façon à la fois :

Causale, où son avenir ne dépend que de phénomènes du passé ou du présent déterministe, c'est-à-dire qu'à partir d'une condition initiale donnée à l'instant présent va correspondre à chaque instant ultérieur un et un seul état futur possible. L'évolution déterministe du système dynamique peut alors se modéliser de deux façons distinctes

Une évolution continue dans le temps, représentée par une équation différentielle ord

Une évolution discrète dans le temps. L'étude théorique de ces modèles discrets est fondamentale, car elle permet de mettre en évidence des résultats importants, qui se généralisent souvent aux évolutions dynamiques continues. Elle est représentée par le modèle général des équations aux différences finies [2].

3- Systèmes autonomes et non autonomes

Soit le système dynamique suivant :

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

Lorsque le champ de vecteur f ne dépend pas explicitement du temps, on dit que le système dynamique est autonome. Dans le cas contraire il est non autonome.

Dans un système autonome, la trajectoire ne dépend pas du temps initial t , alors que dans un système non autonome, elle dépend de t [3].

4- Le chaos

Actuellement il n'y a pas de définition précise du terme Chaos. En fonction de ce contexte, on dit qu'un état est chaotique quand il est non périodique, très irrégulier sur une période.

4-1 L'étude du chaos (concept et définitions) :

Déterminisme et prévisibilité [4]

L'essence de la science est la science est la prévisibilité. La plupart des lois fondamentales de la nature sont déterministes ; elles permettent de savoir exactement ce qui va se produire, à partir de la connaissance des conditions actuelles (ou passées). Il est maintenant largement admis que déterminisme et prévisibilité ne sont pas synonymes. Comme il est impossible de connaître les conditions initiales avec une précision parfaite, la prévision à long terme l'est également, même lorsque les lois physiques sont déterministes et exactement connues.

Le comportement imprévisible de systèmes déterministes est appelé chaos.

Le chaos définit un état particulier d'un système caractérisé par une dépendance sensible aux conditions initiales (des différences extrêmement faibles dans les valeurs du système peuvent aboutir à des résultats largement divergents) [5].

4-2 Définition d'un système chaotique :

C'est un système dont les variables évoluent de manière continue. On peut alors déterminer les valeurs de différentes coordonnées à tout moment et cela en fonction des autres valeurs. Pour les systèmes chaotiques à temps continu, on peut citer comme exemple : le système de Lorenz.

4-3 Caractéristique du chaos :

La non-linéarité

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

La notion de système dynamique est relative à tous les systèmes dont l'évolution dépend du temps.

En général, pour prévoir des phénomènes réels générés par ces systèmes, la démarche consiste à construire un modèle mathématique qui établit une relation entre un ensemble de

causes et un ensemble d'effets.

Si cette relation est une opération de proportionnalité, le phénomène est linéaire.

Dans le cas d'un phénomène non linéaire, l'effet n'est pas proportionnel à la cause [6].

Le déterminisme

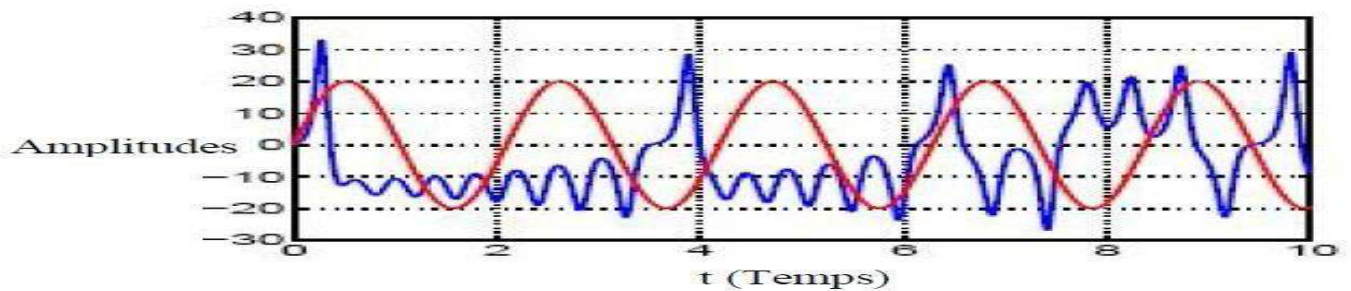
Un système chaotique a des règles fondamentales déterministes et non probabilistes. Il est généralement régi par des équations différentielles non linéaires qui sont connues, donc par des lois rigoureuses et parfaitement déterministes [6].

L'aspect aléatoire

En effet, un système chaotique évolue d'une manière qui semble aléatoire.

Figure ci-dessous montre l'aspect aléatoire

Figure 1.1. Evolution dans le temps d'un système chaotique, comparé à une sinusoïde.



Sensibilité aux conditions initiales

La sensibilité des trajectoires chaotiques aux conditions initiales est une autre caractéristique permettant de reconnaître un comportement chaotique. Quelle que soit la proximité de deux états initiaux, les trajectoires qui en sont issues divergent rapidement l'une de l'autre. Elles restent cependant liées au même attracteur donc confinées dans un espace borné. Cela a pour conséquences :

Le bruit le plus infime altère complètement la connaissance des états futurs du système. En effet, la divergence des trajectoires dans un espace borné signifie qu'elles sont très rapidement décorrélées. Par conséquent, bien que le système soit déterministe, aucune prévision à long terme n'est possible.

La moindre perturbation du système peut à terme conduire à des états extrêmement différents. Un événement insignifiant n'a donc pas toujours des conséquences insignifiantes. Cette propriété a été observée pour la première fois par E. Lorenz sur son modèle météorologique. Elle est connue sous le nom populaire d'effet papillon

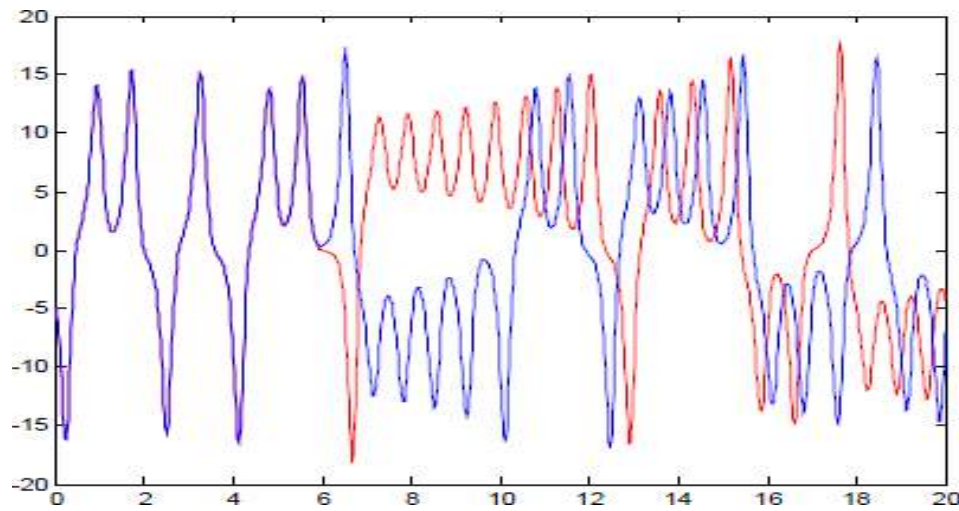


Figure 1.2. Sensibilité aux conditions initiales du système de Lorenz

4-4-Historique sur le chaos :

Edward Norton Lorenz (1917 – 2008) est un scientifique américain largement considéré comme le père de la théorie du chaos.

Lorenz s'intéressait à la météorologie, qui n'était pas encore vraiment considérée comme une ressource pour tenter d'établir des prévisions météorologiques très loin d'être précises.

Avec un modèle informatique basé sur trois variables seulement (simplifié jusqu'à le rendre presque ridicule par rapport à ceux développés par des instituts privés), Lorenz étudia la prévision du temps et obtint bientôt des résultats inédits. Il démontre que les mouvements atmosphériques ne sont pas périodiques, et que des changements minimes dans les paramètres initiaux peuvent aboutir à des résultats totalement différents. C'est la sensibilité aux conditions initiales ou « effet papillon ».

science par un grand nombre de personnes. A cette époque, on dépensait en effet beaucoup de

Le terme « effet papillon » correspond à une image quelque peu poétique : le battement d'ailes d'un papillon peut provoquer une tornade à l'autre bout du monde. Mais l'origine première de ce terme vient en réalité de la forme de l'attracteur de Lorenz, qui peut être assimilée aux ailes d'un papillon [figure 1.3].

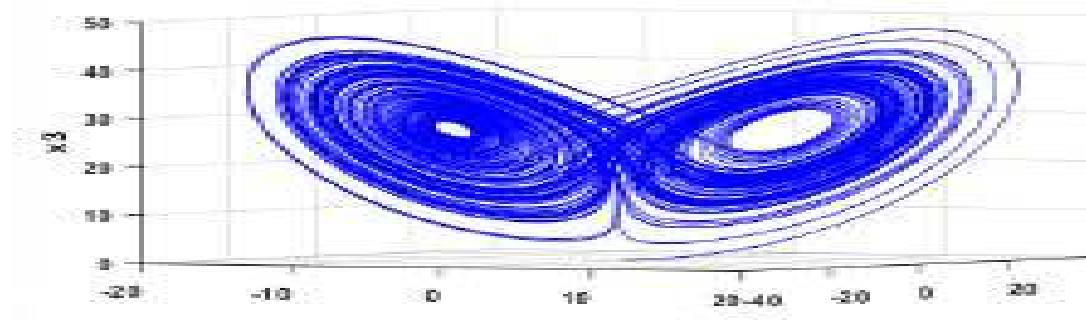


Figure 1-

3L'attracteur de Lorenz.

L'attracteur de Lorenz est défini comme l'ensemble à long terme des trajectoires dans l'espace des phases du modèle créé par Lorenz. Il conclut de sa découverte qu'il est impossible de réaliser une prévision météorologique précise à long terme. En effet, des incertitudes inévitables dans les données fournies aux modèles et de la quantité de

paramètres à prendre en compte comme le vent, la température, le degré d'humidité rendent cela impossible [8].

De plus, il réalise qu'il suffit ici de trois variables seulement pour provoquer un comportement chaotique : l'introduction d'un nombre très limité de données peut induire une dynamique à la fois complexe et imprévisible.

Il met en évidence que la complexité peut être le propre d'un système. On pensait jusque-là qu'elle résultait d'apports accidentels dus à une multitude de causes.

En 1964, Lorenz formalise sa théorie du chaos. Il décrit comment, en jouant seulement sur quelques variables, un comportement chaotique peut être engendré dans un système en théorie très simple.

4-5-Principales applications de l'étude du chaos :

Les principales applications du chaos sont :

-Médecine : cœur, Détection du cancer du sein, Schizophrénie, cardiologie analyse du rythme de cœur (ECG) , prédiction et contrôle d'activité irrégulière du

-Biologie : Évolution d'une population, Consommation de CO2 d'une forêt.

-Communication électronique

-Méta matériaux et invisibilités Effets spéciaux

-Communications : compression et stockage d'image, conception et management des réseaux d'ordinateurs.

Management et finance : prévisions économiques, analyse financière, et prévision du marché.

5-points fixe du système de Lorenz :

Nous allons tout d'abord préciser, sans détailler les calculs, l'origine physique de ce système

$$\begin{aligned} \dot{x}_1 &= f_1(x) \\ \text{d'équations. On a : } \dot{x}_2 &= f_2(x) \\ \dot{x}_3 &= f_3(x) \end{aligned}$$

Le système de Lorenz s'écrit alors:

$$\begin{cases} \dot{x}_1 = \sigma(x_2 - x_1) \\ \dot{x}_2 = \rho x_1 - x_2 - x_1 x_3 \\ \dot{x}_3 = -\beta x_3 + x_1 x_2 \end{cases}$$

$$J = \begin{bmatrix} \frac{df_1}{dx_1} & \frac{df_1}{dx_2} & \frac{df_1}{dx_3} \\ \frac{df_2}{dx_1} & \frac{df_2}{dx_2} & \frac{df_2}{dx_3} \\ \frac{df_3}{dx_1} & \frac{df_3}{dx_2} & \frac{df_3}{dx_3} \end{bmatrix}$$

Analyse du système par la matrice jacobienne

$$\begin{pmatrix} -\sigma & \sigma & 0 \\ \rho - x_3 & -1 & -x_1 \\ x_2 & x_1 & -\beta \end{pmatrix}$$

L'espace des phases est tridimensionnel (x,y,z). L'espace de contrôle est tridimensionnel (β, ρ, σ).

Détermination des points fixes: on a : $\dot{x}_1 = \dot{x}_2 = \dot{x}_3 = 0$

un point fixe évident: (0,0,0)

on : $x_1 = x_2$

$$x_3 = \frac{x_1^2}{\beta}$$

$$\rho x_1 - x_1 - \frac{x_1^3}{\beta} = 0$$

deux autres points fixes, $|\lambda_i - j| = 0 \implies \lambda_i = \begin{pmatrix} \lambda & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda \end{pmatrix} = \begin{bmatrix} \lambda + \sigma, -\sigma & 0 \\ -\rho + x_3, \lambda + 1 + x_1 \\ -x_2 - x_1, \lambda + \beta \end{bmatrix}$

détermines par les racines du polynôme:, c'est-à-dire

$$(\lambda + \beta)((\lambda + \sigma)(\lambda + 1) - \rho\sigma) = 0$$

$$\lambda + \beta = 0, \quad \lambda = -\beta$$

$$\lambda^2 + \lambda(\sigma + 1) + \sigma - \rho\sigma = 0$$

$$\lambda^2 + \lambda(\sigma + 1) + \sigma(1 - \rho) = 0$$

Calcule :

$$\Delta = (\sigma - 1)^2 - 4(\sigma(1 - \rho))$$

$$\Delta = \sigma^2 + 1 + 2\sigma - 4\sigma + 4\sigma\rho$$

$$\Delta = \sigma^2 - 2\sigma + 4\sigma\rho + 1$$

$$\Delta = \sigma^2 - 2\sigma + 1 - 4\rho$$

$$\Delta = (\sigma + 1)^2 - 4\rho$$

$$\Delta = (\sigma + 1)^2 - 2(2\sqrt{\rho})^2$$

$$\Delta = (\sigma + 1) + (2\sqrt{\rho}) * ((\sigma + 1) + (2\sqrt{\rho}))$$

Donc les racines polynômes sont :

$$(\pm\sqrt{\beta(\rho - 1)}, (\pm\sqrt{-\beta(\rho - 1)}, \rho - 1$$

Stabilité des points fixes:

Pour $\rho < 1$, l'origine est stable et devient instable l'orsque $\rho = 1$

6-Attracteur :

Un attracteur est un objet géométrique vers lequel tendent toutes les trajectoires des points de l'espace des phases, c'est à dire une situation (ou un ensemble d'états) vers lesquels évolue un système, quelles que soient ses conditions initiales [10].

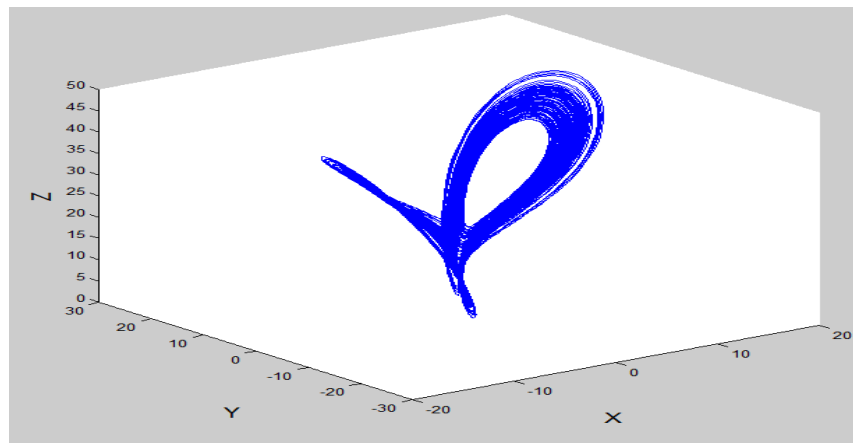


Figure 1.4. Attracteur étrange de Lorenz.

6-1 Les différents types d'attracteurs :

Il existe deux types d'attracteurs : les attracteurs réguliers et les attracteurs étranges ou chaotiques [11].

Attracteurs réguliers

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

Le point fixe : C'est le plus simple attracteur : le système évolue vers un état de repos (Point).

Le cycle limite périodique : Il peut arriver que la trajectoire de phase se referme sur elle-même. L'évolution temporelle est alors cyclique, le système présentant des oscillations permanentes. Dans un système physique dissipatif, cela exige la présence d'un terme de forçage dans les équations qui vient compenser en moyenne les pertes par dissipation.

Le cycle limite pseudopériodique : C'est presque un cas particulier du précédent. La trajectoire de phase ne se referme pas sur elle-même, mais s'enroule sur une variété de dimension.

Attracteurs étranges :

Il est contenu dans un espace fini. 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 augmenter 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 [12].

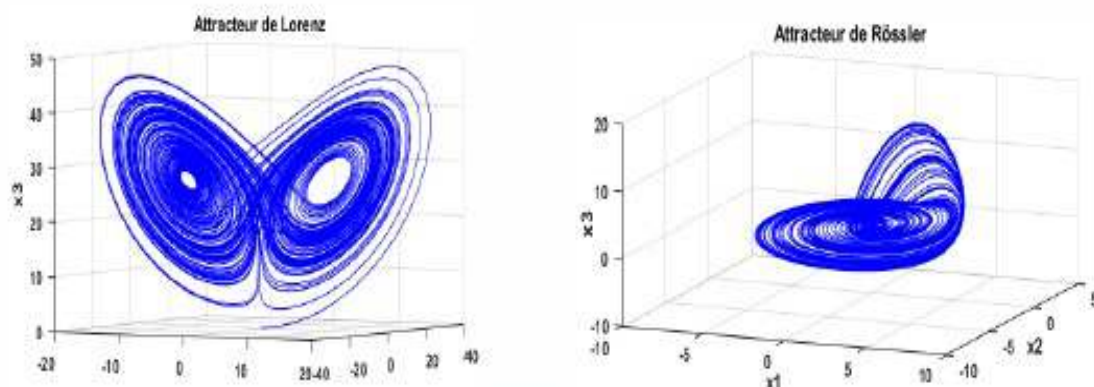


Figure 1.5 Les exemples d'attracteurs.

Attracteur chaotique ou étrange

Un sous-ensemble de l’espace des phases est un attracteur chaotique si et seulement si c’est un attracteur contenant une orbite dense, présentant une sensibilité aux conditions initiales et possédant une structure fractale.

7-Section de Poincaré :

La section de Poincaré est un outil mathématique permettant de transformer un système continu en un système dynamique discret[13]. Cette transformation s’opère via une réduction de l’ordre du système.

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,

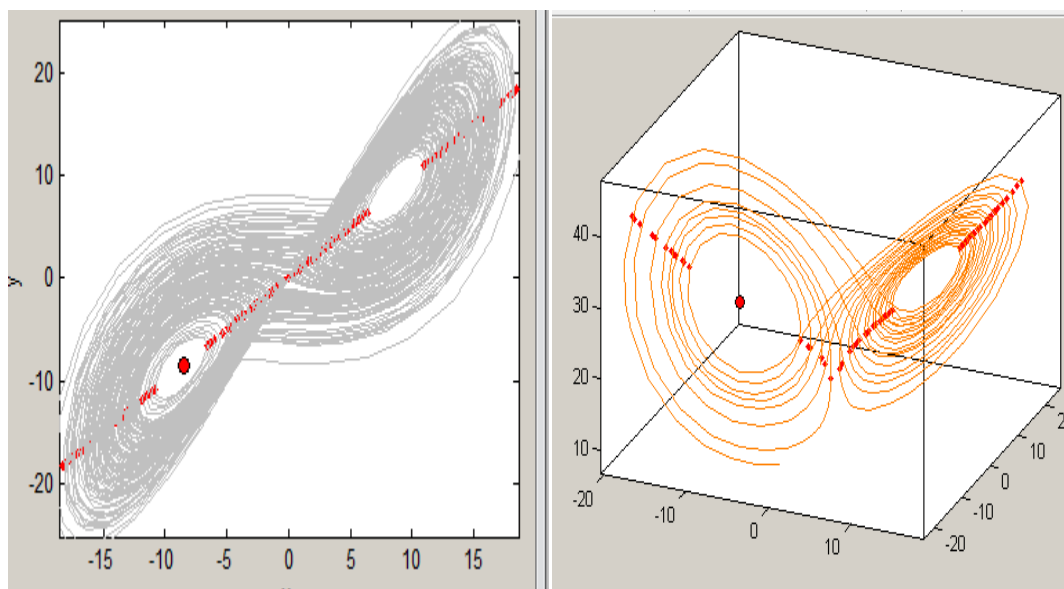


Figure 1.6. Représentation de la section de Poincaré pour le système de Lorenz. un plan illustre en bleu avec l’attracteur de Lorenz représenté en rouge sur la figure(1.7), sa section de Poincaré correspond au plan x-y.

8-Exposants de Lyapunov :

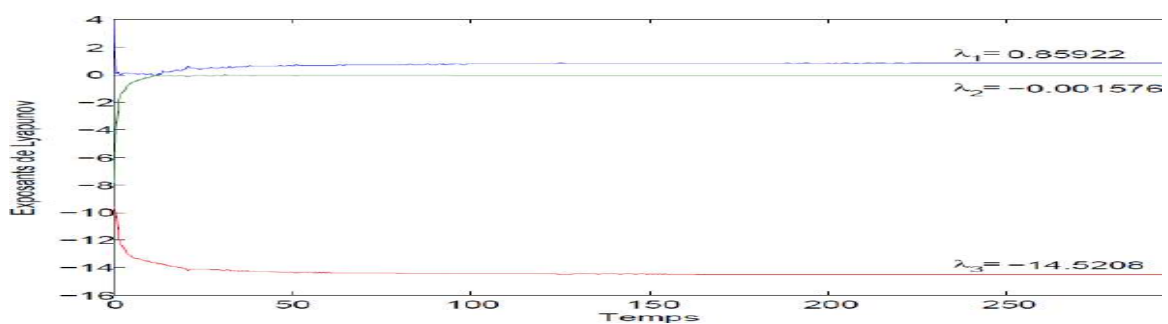
L'exposant de Lyapunov sert à mesurer le degré de stabilité d'un système. Un système sensible à très petites variations de la conditions initiale aura un exposant positif (système chaotique). En revanche, l'exposant est négatif si le système n'est pas sensible à des petites variations des conditions initiales, les trajectoires se rapprochent et on perd donc l'information sur les conditions initiales[10]. Un système de dimension n possède n exposants de Lyapunov qui mesurent le taux de divergence suivant un des axes de l'espaces de phase. L'apparition du chaos exige l'existence d'un exposant positif selon au moins un axe[14], tout en rendant compte que la somme des exposants est négative (respectivement nulle) pour les systèmes dissipatifs(respectivement conservatifs).

Un exposant de Lyapunov positif(respectivement négatif) selon une direction indique, qu'une divergence entre deux trajectoires voisines augmente (respectivement diminue) exponentiellement avec le temps [14].

Les différents types d'attracteurs d'un système tridimensionnel en fonction des signes des Exposants de Lyapunov sont représentés dans le tableau ci-dessous.

Type d'attracteur	Signe des Exposants de Lyapunov
Point fixe	- - -
Cycle limite	0 - -
Attracteur étrange	+ 0 -

Tableau 1. Caractérisation des attracteurs



La Figure(1.7) représente le tracé des valeurs des exposants de Lyapunov pour le système Lorenz en utilisant Matlab et MatdS.

9- Bifurcation et routes vers le chaos :

Une bifurcation est un changement qualitatif de la solution x_0 du système lorsqu'on modifie un paramètre μ et d'une manière plus précise la disparition ou le changement de stabilité et l'apparition de nouvelles solutions. La condition d'une bifurcation est la plus petite dimension de l'espace des paramètres telle que la bifurcation soit persistante.

La théorie de bifurcation est l'étude mathématique des changements qualitatifs ou topologiques de la structure d'un système dynamique [15].

Une bifurcation survient lorsqu'une variation quantitative d'un paramètre du système engendre un changement qualitatif des propriétés d'un système et que la stabilité, le nombre de points d'équilibre ou la nature des régimes permanents. Les valeurs des paramètres au moment du changement sont appelées valeurs de bifurcation.

Dans les systèmes dynamiques, un diagramme de bifurcation montre les comportements possibles d'un système, à long terme, en fonction des paramètres de bifurcation [13].

9-1 Le doublement de période :

L'augmentation d'un paramètre provoque, pour un système périodique, l'apparition d'un doublement de période, la période se multiplie ainsi en 4, 8, 16, ...

A partir d'une certaine valeur du paramètre, les doublements étant de plus en plus rapprochés, on tend vers un point auquel on obtiendrait hypothétiquement une fréquence infinie et c'est à ce moment que le chaos apparaît [figure 1.9].

9-2 L'intermittence :

Ce scénario est caractérisé par un mouvement périodique stable entrecoupé par des mouvements chaotiques qui apparaissent de manière irrégulière.

Le système conserve pendant un certain laps de temps un régime périodique ou pratiquement quasi-périodique, c'est-à-dire une certaine « régularité », et il se déstabilise, brutalement, pour donner lieu à un comportement chaotique. Il se stabilise de nouveau, pour donner lieu à une autre « explosion chaotique » plus tard.

La fréquence et la durée des phases chaotiques ont tendance à s'accroître plus on s'éloigne de la valeur critique de la contrainte ayant conduit à leur apparition.

9-3 quasi-périodicité :

Ce troisième scénario fait intervenir pour un système périodique l'apparition d'une autre période dont le rapport, avec la première, n'est pas rationnel. pratiquement quasi-périodique, c'est-à-dire une certaine « régularité », et il se déstabilise, brutalement, pour donner lieu à un comportement chaotique. Il se stabilise de nouveau, pour donner lieu à une autre « explosion chaotique » plus tard.

La fréquence et la durée des phases chaotiques ont tendance à s'accroître plus on s'éloigne de la valeur critique de la contrainte ayant conduit à leur apparition.

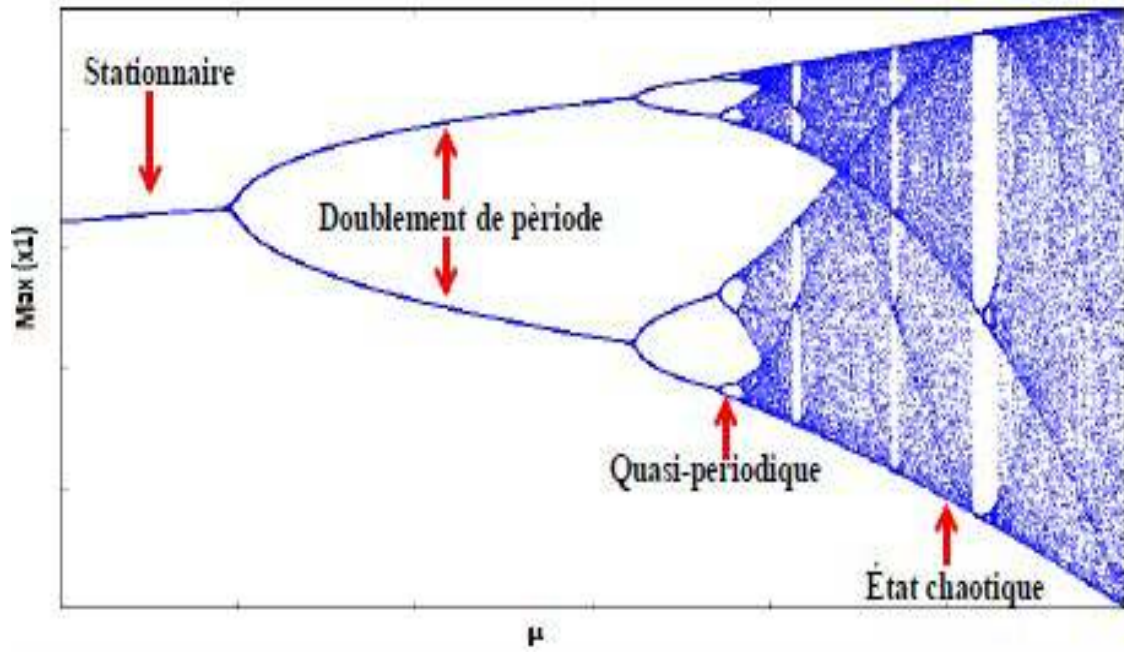


Figure 1.8. Bifurcation par doublement de période

10-Exemples de système chaotique :

10-1L'attracteur de Lorenz :

L'attracteur de Lorenz fut introduit par Edward Lorenz en 1963. Il s'agit d'un système dynamique non linéaire de dimension 3, obtenu à partir des équations de transfert de la chaleur dans un liquide. Le système de Lorenz est défini par :

$$\dot{x} = (y - x) \quad (1-3)$$

$$\dot{y} = (b - z) - y$$

$$\dot{z} = xy - cz$$

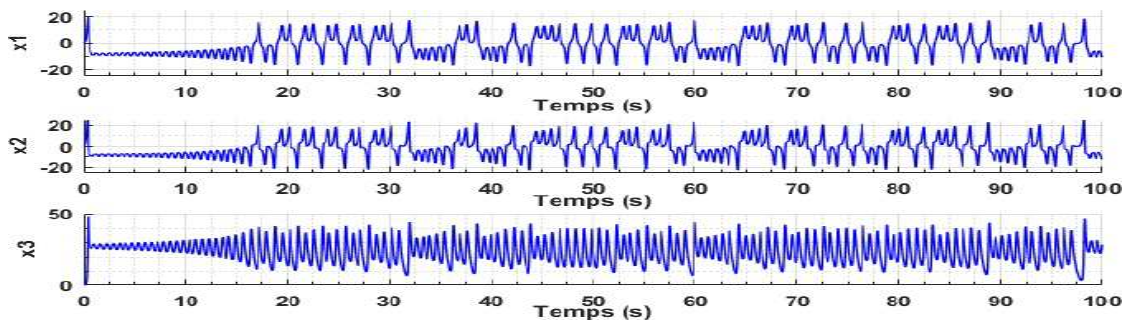


Figure 1.9 Réponse temporelle du système chaotique de Lorenz.

Le système de Lorenz montre un comportement chaotique et génère un attracteur étrange pour $\alpha = 10$, $\beta = 28$, $\rho = 8/3$. La dimension de Hausdorff de l'attracteur de Lorenz est estimée entre 2 et 3. La figure 1.10 montre l'attracteur de Lorenz en partant des conditions initiales $x_0 = y_0 = z_0 = 0,01$ et le pas de simulation choisi de 0,01. Si l'on regarde l'attracteur de plus près, nous constatons que la trajectoire mêle deux comportements différents : le premier est un comportement apparemment régulier, c'est à dire dans plusieurs régions de l'espace d'états, elle forme des boucles semblables à celles de trajectoires périodiques. Le deuxième comportement semble aléatoire, c'est à dire que le nombre de boucles décrites dans une région avant de rejoindre brusquement une autre région est imprévisible. Aussi, les instants auxquels ces changements de région apparaissent sont imprévisibles. Dans la figure (1.10) et (1.11) les signaux générés et les plans de phases par le système de Lorenz sont représentés.

Réponses temporelles

Plans des phases :

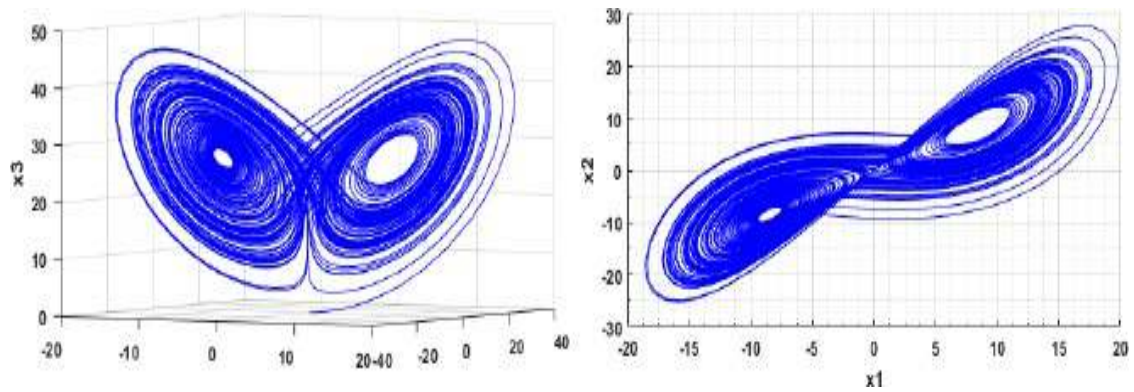
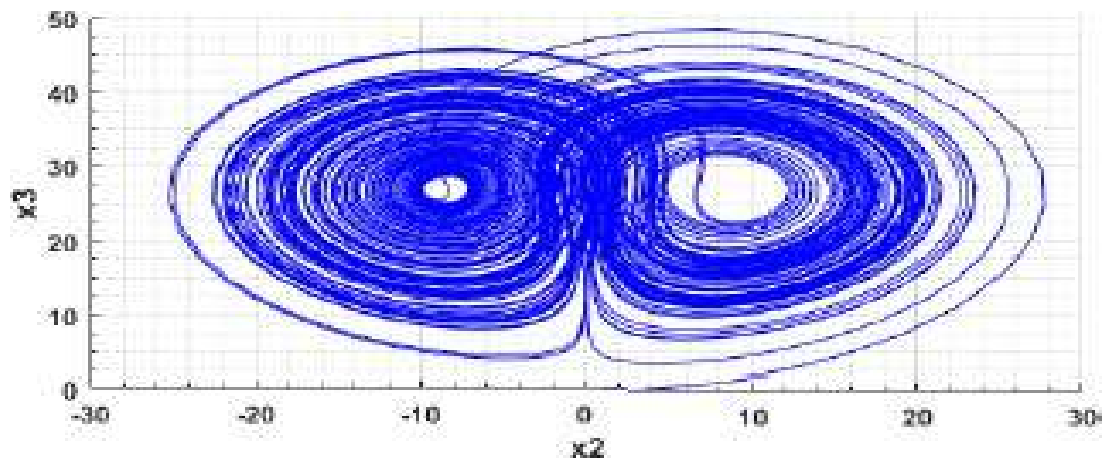


Figure 1.10. Représentation du système chaotique de Lorenz dans l'espace des phases.



Conclusion

Dans ce chapitre nous avons présente quelques notions sur les systèmes dynamiques et la théorie chaos ainsi que leur caractéristique à savoir : plan de phase, point fixe et leur stabilité, bifurcation et les différents scénarios évoluant vers le chaos, les attracteurs.

Nous avons aussi présenté 2 exemples de système chaotique à savoir le système de Lorenz et le système Rossler. Ces notions étudiées dans ce chapitre.

CHAPITRE 2

SYNCHRONISATION DES SYSTEMES CHAOTIQUES ET METHODE D'INSERTION DE MESSAGE

1-INTRODUCTION

L'utilisation du chaos dans les systèmes de télécommunication a été rendue possible depuis la maîtrise de la synchronisation des systèmes chaotiques. En effet le problème de synchronisation du récepteur dans le but de dupliquer le signal chaotique utilisé au niveau du récepteur se pose directement [16][20].

La synchronisation des systèmes chaotiques peut paraître énigmatique et ambiguë. En effet la synchronisation de ces systèmes présente plus de contraintes contrairement au cas d'oscillations périodiques où il n'y a pas d'instabilité intrinsèque.

Dans la littérature plusieurs concepts de synchronisation chaotique ont été proposés tout d'abord avec les travaux de Yamada et Fujisaka [29] qui ont utilisé une approche locale de la synchronisation chaotique. Par la suite Afraimovich et al. [1] ont développé les concepts importants liés à la synchronisation chaotique et ultérieurement Pecora et Carroll [20] [21] ont défini la synchronisation chaotique connue sous le nom de synchronisation identique, développée sur la base de circuits chaotiques couplés, avec l'un maître et l'autre esclave ; Ces travaux ont ouvert la voie des applications du chaos aux télécommunications [17].

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

2-Définition de la synchronisation

Après plusieurs tentatives pour définir un mouvement synchronisé, Brown et Kocarev ont récemment fourni une définition mathématique de la synchronisation. Pour construire la définition, ils supposent qu'un système dynamique, global, de dimension finie et déterministe est divisible en deux sous-systèmes :

$$\frac{dx}{dt} = f_1(x, y, t), \quad \frac{dy}{dt} = f_2(y, x, t)$$

où, $x \in \mathbb{R}^n$ et $y \in \mathbb{R}^m$ sont des vecteurs qui peuvent avoir des dimensions différentes.

3-METHODESDESYNCHRONISATION

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

3-1 SYNCHRONISATION PAR REPARTITION DU SYSTEME

Pour illustrer la méthode de synchronisation par couplage entre deux systèmes chaotiques, nous avons choisi de présenter la synchronisation identique proposée par Pecora et Carroll [20] [21]. L'avantage de cette approche est de représenter une solution simple et performante. L'objectif est qu'un système esclave reproduise le plus fidèlement possible l'état du maître, après un régime transitoire.

L'idée consiste à diviser le système d'origine en deux sous-systèmes de telle sorte que les variables dynamiques de départ soient réparties de part et d'autre de chacun des sous-systèmes. Il s'agit ensuite de reproduire les sous-systèmes à l'identique et de les mettre en cascade. Le signal issu du système de départ (système maître) sert à piloter (synchroniser) le premier des deux sous-systèmes dupliqués mis en cascade, qui lui-même permet de synchroniser le second sous-système dupliqué.

Partant d'un système chaotique défini par la dynamique suivante:

$$\dot{x}(t) = f(x(t))$$

On divise le système initial en deux sous-systèmes avec une réorganisation des variables d'état dans un ordre particulier.

$$S_1 : x^{1} = F^{1}(x^{1}, x^{2})$$

$$S_2 : x^{2} = F^{2}(x^{1}, x^{2})$$

$$(x) = [F^{1}(x); F^{2}(x)]$$

Soit un autre système S' de dynamique identique F^{2} et un vecteur d'état x^{2}

Pecora et Carroll ont démontré que le système S' est candidat pour se synchroniser avec le système initial à la condition nécessaire et suffisante qu'il soit stable, ceci est équivalent à ce que les exposants de Lyapunov soient négatifs.

Une convergence parfaite de trajectoires est ainsi accomplie

$$\lim_{t \rightarrow \infty} \|x^{2}(t) - x^{2}(t)\| = 0$$

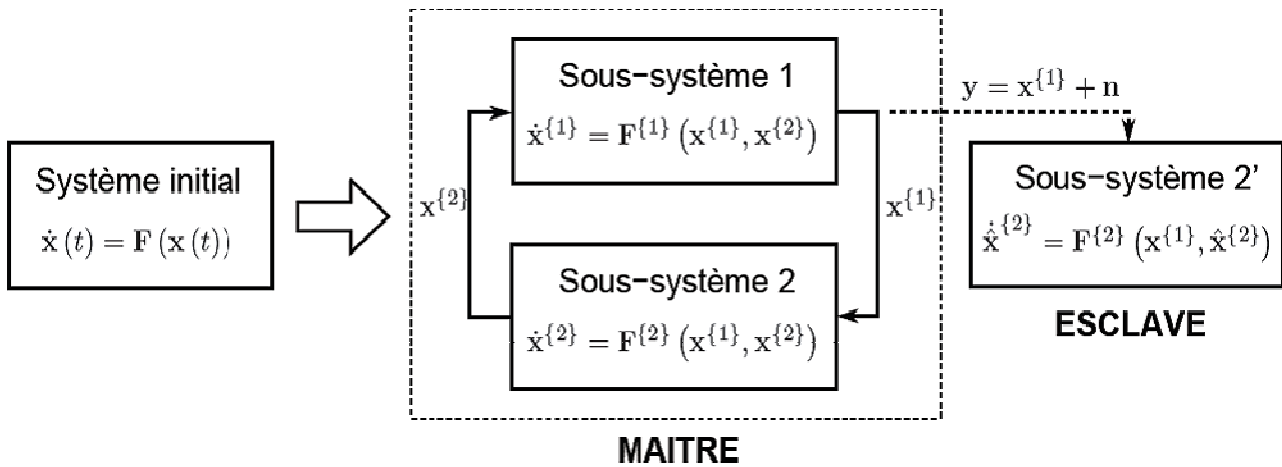


Fig.2.1 Synchronisation maître-esclave

3-2 SYNCHRONISATION GÉNÉRALISÉE

Cette méthode est une généralisation du concept de synchronisation identique. Les deux systèmes se synchronisent, au sens généralisé, il existe une transformation M telle que $\lim_{t \rightarrow \infty} \|x'(t) - Mx(t)\| = 0$.

Les conditions initiales ne sont pas tenues en compte dans ce cas.

Si M est inversible, alors $M^{-1}(x')$ fournit une estimation de l'état x ; dans le cas contraire, il serait impossible de fournir une estimation de l'état x . Ceci présente alors un inconvénient majeur pour les techniques de communication utilisant l'état de l'émetteur pour décrypter le message transmis [5][8].

3-3 SYNCHRONISATION RETARDÉE

Dans ce mode de synchronisation, l'état du système esclave converge vers l'état décalé dans le temps du système maître [33].

$$\lim_{t \rightarrow \infty} \|x'(t) - x(t-r)\| = 0$$

où $x(t)$ est l'état du système émetteur, $x'(t)$ est l'état du système récepteur et r est un retard positif.

3-4 SYNCHRONISATION PROJECTIVE

Dans cette méthode, l'état du système récepteur se synchronise avec un multiple de l'état du système émetteur. Soit a et \square tels que:

$$\lim_{t \rightarrow \infty} \|x'(t) - a(\square)\| = 0$$

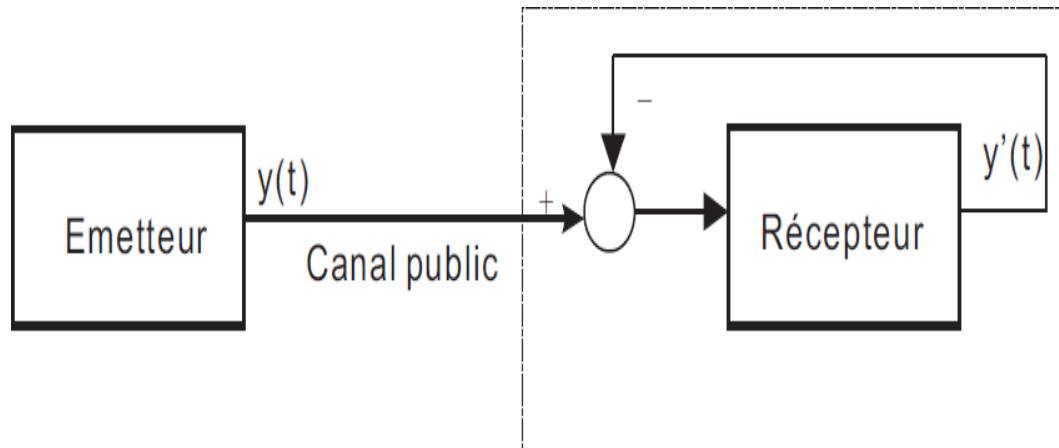
où a est le facteur d'échelle, (\square) est l'état du système émetteur, \square' est l'état du système récepteur et \square est un retard positif.

Cette approche est utilisée pour des systèmes partiellement linéaires et permet de synchroniser à un facteur près les états qui ne peuvent être synchronisés.

3-5 SYNCHRONISATION PAR BOUCLE FERMÉE

La synchronisation de systèmes chaotiques par les méthodes en boucle ouverte implique une sensibilité aux variations paramétriques.

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



4- technique de cryptage par le chaos :

4-1 Insertion du message par addition:

Le principe de cette méthode est d'ajouter directement notre signal informationnelle $m(t)$ avec le signal de notre oscillateur chaotique de Sprott $x(t)$ et de récupérer ensuite par synchronisation chaotique. Le même oscillateur est utilisé à la fois au niveau de l'émetteur et au niveau du récepteur, avec la différence que le récepteur est contrôlé par le signal reçu de l'émetteur pour obtenir la synchronisation. Au niveau du récepteur après synchronisation grâce au signal reçu, on récupère le message original par une simple soustraction.

Par conséquent, un intrus ne soupçonnera pas qu'un message est transmis, même s'il intercepte le signal $S(t)$ (porteuse chaotique plus le message). Donc il ne cherchera pas à appliquer des techniques de décryptage.

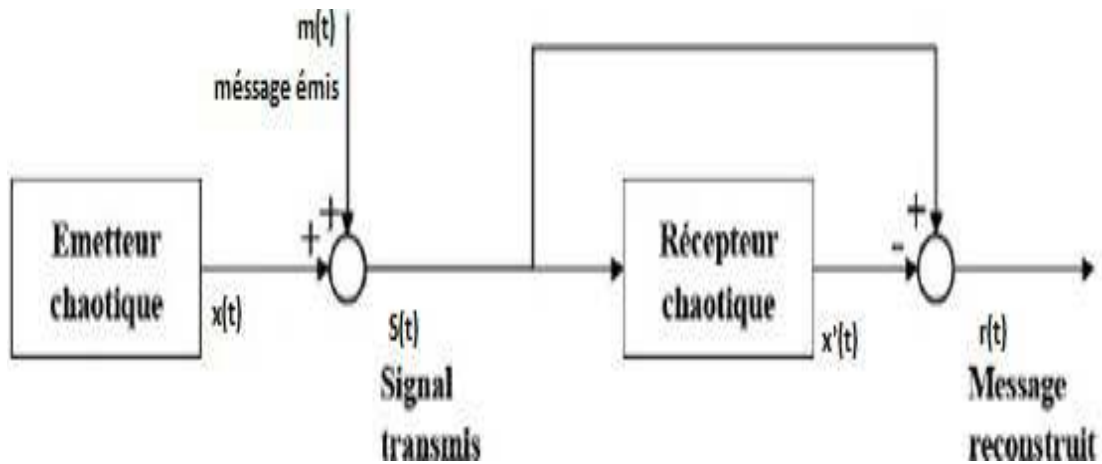


Figure 2.3: Cryptage par addition [3].

Le principal avantage de cette méthode réside dans la simplicité du cryptage. On peut souligner que cette technique peut être appliquée à des messages continus ou discrets. L'inconvénient de cette méthode est qu'il faut garantir la synchronisation, le message doit être au moins de 20 à 30 dB inférieur à la sortie de l'émetteur. Toutefois, en présence d'un bruit de canal d'une puissance proche de celle du message, il devient difficile de détecter l'information. De plus, cette méthode reste sensible aux attaques extérieures.

4-2 Insertion du message par modulation paramétrique:

L'approche par modulation utilise le message contenant l'information pour moduler un ou plusieurs paramètres θ de l'émetteur chaotique. Un contrôleur adaptatif est chargé de maintenir la synchronisation au niveau du récepteur, tout en suivant le changement du paramètre modulé. Les schémas correspondants sont présentés par la figure 2.4.

À un niveau de l'émetteur, le fait de moduler un ou plusieurs paramètres impose à la trajectoire un changement continu de l'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.

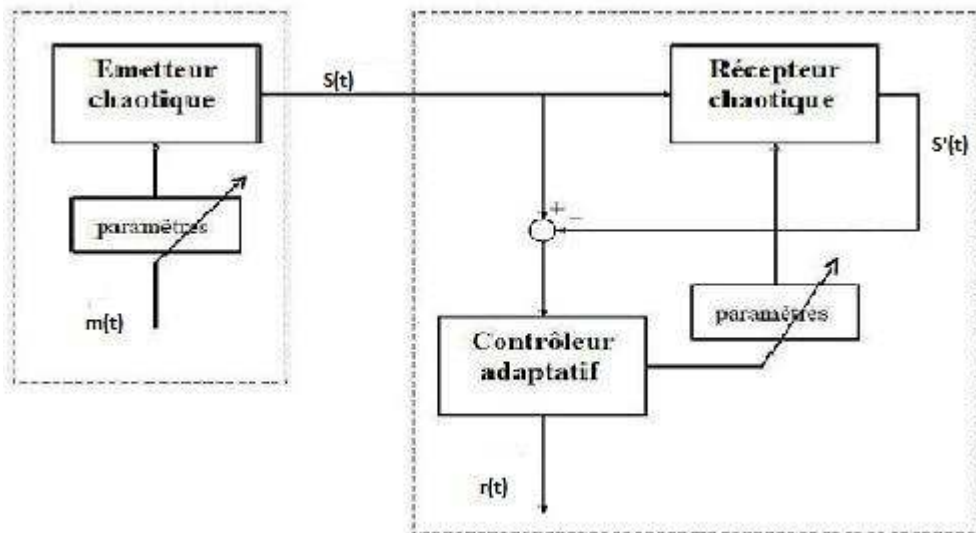


figure2.4: Cryptage par modulation paramétrique

4-3 Insertion du message par inclusion:

Cette technique de cryptage consiste à injecter le message dans la dynamique de l'émetteur.

La restauration de l'information se fait principalement par deux techniques, reposant soit sur les observateurs à entrées inconnues soit sur l'inversion du système émetteur. Cette méthode présente beaucoup d'avantages et est très utilisée en pratique.

4-4 Insertion du message mixte:

Afin de faire face aux problèmes de sécurité des méthodes précédentes, une nouvelle technique combinant les principes de la cryptographie standard et la synchronisation chaotique a été proposée. Le message $u(t)$ contenant l'information est crypté grâce à une clé $c(t)$ générée par l'émetteur chaotique.

Le message crypté est alors injecté dans la dynamique du système chaotique, pour le rendre plus complexe. Ensuite, un signal $y(t)$ fonction des variables d'état de l'émetteur est transmis au récepteur, qui établit une synchronisation avec l'émetteur. La clé est alors reconstruite par le récepteur, qui peut finalement décoder le message. Le principe général de cette méthode est illustré par la figure 2.5.

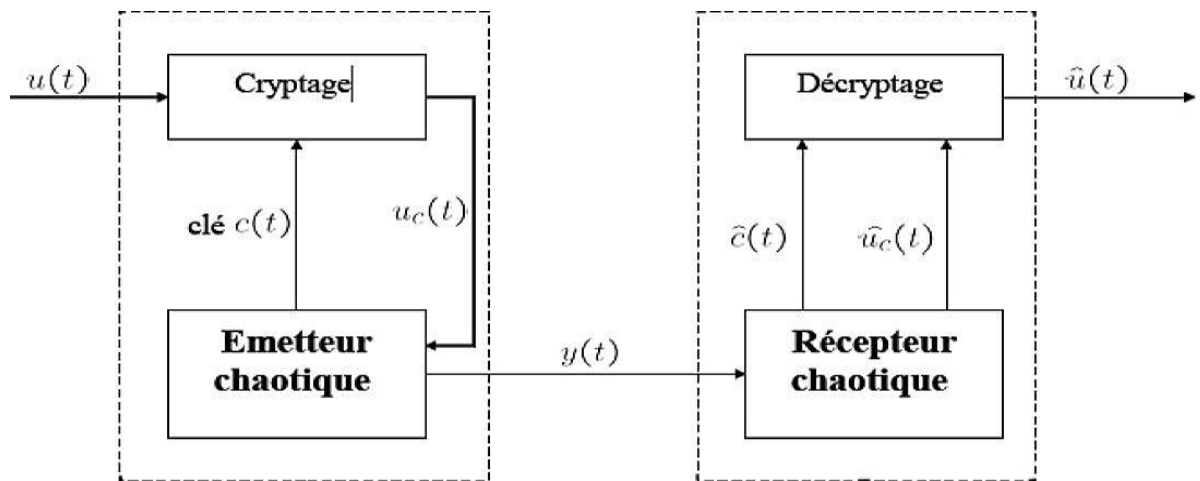


Figure 2.5: Cryptage mixte

CONCLUSION :

Dans ce chapitre, nous avons expliqué le concept de synchronisation des systèmes chaotiques ainsi que les différents modes de synchronisation. Cette démarche nous sera très utile pour notre système de transmission.

La cryptographie chaotique peut s'effectuer sous différents schémas, il s'agit de définir la façon d'introduire le message dans l'émetteur.

Dans le chapitre qui suit nous nous intéresserons à la méthode de synchronisation impulsive. Les concepts de base y seront énoncés et la façon de l'appliquer dans ce travail de mémoire sera développée avec plus de détail.

CHAPITRE 3

CRYPTAGE ET DECRYPTAGE D'IMAGE PAR

LE SYSTEME CHAOTIQUE

Introduction :

Dans ce chapitre, nous allons parler aux concepts de base sur l'imagerie et l'imagerie numérique. Puis nous allons parler sur les attributs et les types et les formats d'image. Enfin nous avons parlé sur ces différents modes de couleurs.

3-2 Notions de base sur l'image

Définition de l'image

Une image peut être définie comme une fonction bidimensionnelle, $f(x, y)$, où x et y sont des coordonnées spatiales (plan), et l'amplitude de f à n'importe quelle paire de coordonnées (x, y) s'appelle l'intensité ou le niveau de gris de l'image à ce point

L'imagerie numérique

Une image numérique est composée des cases appelées « pixels ». Ces pixels seront affectés de nombres binaires permettant de définir des teintes de gris ou des couleurs

Les attributs des images

1) Pixels

Le pixel représente la plus petite unité d'une image numérique appelé en anglais (PICTure Element). Les nombres des pixels de ligne et les nombres des colonnes déterminent la dimensions de l'image, et chaque pixel représente une valeur (couleur).

2) La taille

La taille de l'image est la place qu'elle occupe dans le codage binaire. Son unité est « l'octet » [13].

Taille = nombre d'octets pour chaque pixel \times définition

3) Résolution

La résolution d'une image c'est le nombre de pixels par unité de longueur dpi (dot per inch).

Si la résolution est élevée alors la meilleure qualité d'image est obtenue

Types d'imagerie numérique.

Il existe deux types d'images numériques :

1) Les images matricielles

Formée d'une grille composée de pixels. Plus on zoom, plus les pixels deviennent apparents .

Les formats d'images bitmap : BMP, PCX, GIF, JPEG, TIFF. On obtient également des images matricielles à l'aide d'un appareil photo numérique, d'une caméra vidéo numérique ou d'un scanner .

2) Les images vectorielles

L'image vectorielle utilise également la technique du Pixel, mais cette fois, leur position

et leur couleur.

Autrement dit, pour afficher une ligne par exemple, le logiciel détermine le point de départ, le point d'arrivée puis la trajectoire à suivre. Ensuite, il calcule et positionne l'ensemble des pixels nécessaires pour afficher cette ligne

3-2-2 Les différents formats d'images

1) JPEG

JPEG (Joint Photographic Experts Group) est une méthode de compression avec perte, Les images JPEG compressées sont généralement stockées dans le format de fichier JFIF (JPEG Interchange File Format). Le format de fichier d'image est le plus utilisé. Les formats JPG est plus utilisé dans les appareils photo numériques et les pages Web .

2) TIFF

Le format TIFF (Tagged Image File Format), Il permet de stocker des images de haute qualité en noir et blanc, couleurs RVB jusqu'à 32 bits par pixels. Il supporte aussi les images indexées faisant usage d'une palette de couleurs, les calques et les couches alpha (transparence) [29,30].

3) GIF

GIF (Graphics Interchange Format), C'est un format léger pour les animations. Et de transparence compression efficace Très répandu sur le Web malgré ses faiblesses et un problème de droit sur son format de compression. À déconseiller pour les photos

4) PNG

Le format de fichier PNG (Portable Network Graphics), Il permet de stocker des images en noir et blanc (jusqu'à 16 bits par pixels), en couleurs réelles (True color, jusqu'à 48 bits par pixels) ainsi que des images indexées, faisant usage d'une palette de 256 couleurs. Il offre enfin une couche alpha de 256 niveaux pour la transparence

3-Cryptage d'image :

3-3-1 : introduction a la cryptographie :

La cryptographie est l'étude de technique mathématiques liée a la sécurité de l'information. Par sécurité de l'information , on entend confidentialité des données, intégrité des données, authentification des donnée des communicants et non répudiation des données. La confidentialité consiste a grader des données secrète pour tous ce qui ne sont pas autorisés à les connaitre. L'intégrité des données a pour but de préserver les données de toute altération non autorisée. L'authentification de données consiste a faire un lien entre les données et leur expéditeur. L'authentification des entités consiste à s'assurer de leur identité. La non répudiation consiste a éviter que , par la suite, la communication nient leurs actions. L'émetteur nie avoir envoyé un message et le récepteur nie avoir reçu un message.

3-3-2 Cryptographie par chaos :

Dans les différentes applications actuellement envisagées, les signaux chaotiques servent soit à véhiculer l'information soit à réaliser le cryptage de données.

Nous nous intéressons au cryptage de données à transmettre et plus particulièrement dans un contexte de transmission sécurisée. En effet, un signal chaotique apparaît comme un «

bruit» pseudo-aléatoire .Il peut être utilisé lors du cryptage de données, pour masquer les informations dans une transmission sécurisée ; il suffit de le «mélanger » de manière appropriée au message à envoyer confidentiellement [26].

3-3-3 Méthode proposée :

cryptage d'image sous simulink avec le système chaotique de Qi :

Tout d'abord on va utiliser le logiciel Matlab qui est spécialisé dans le traitement d'image

On va utiliser une image binaire de 8 bit Dans cette méthode de cryptage d'image on utilise le bloc « display » qui permet de mesurer les valeurs des pixels qui sont comprises entre 0 et 255. C'est cette sortie q'on va l'utiliser pour la modulation paramétrique avec le paramètre b dans le chapitre suivant.

Et on expliquera le rôle de chaque bloc de traitement aussi dans le travaille qui suit , donc la simulation de ce processus est longue mais elle fonctionne. L'imaeg est de taille 256*256 pixels, le temps de la simulation est de $256*256=65536$

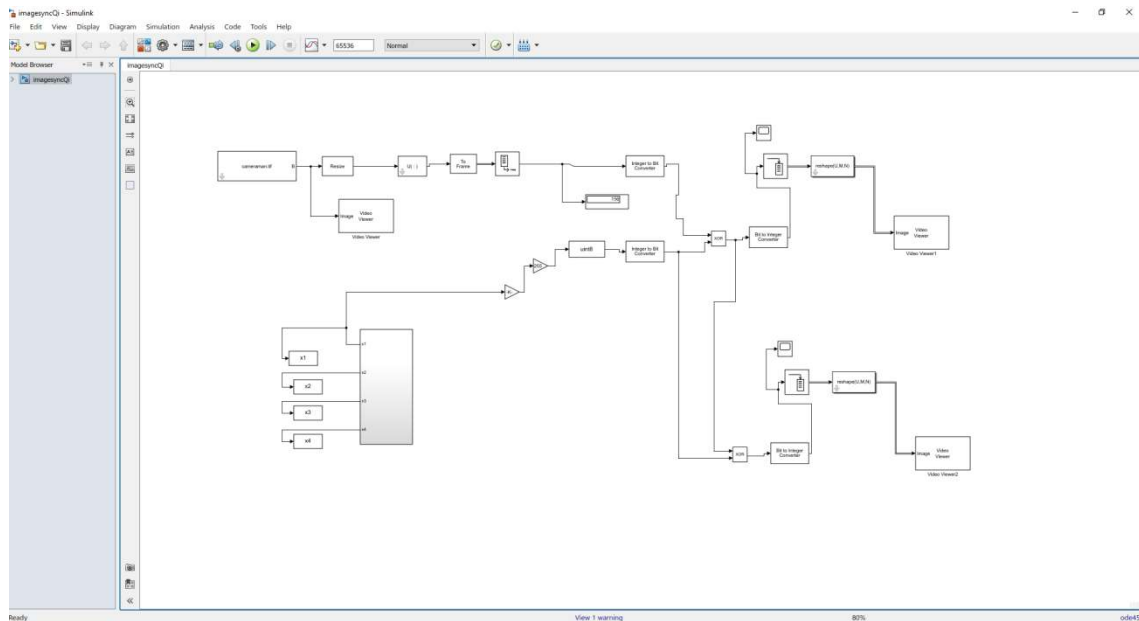


Figure 3-1 : cryptage d'image sous matlab simulink avec le système de Chen



Figure 3-2 : image à crypter

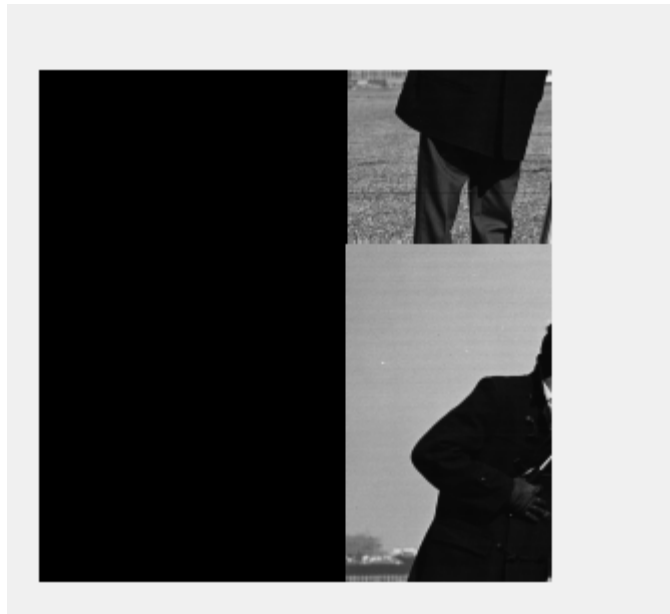


Figure 3-3 : image en cour de décryptage

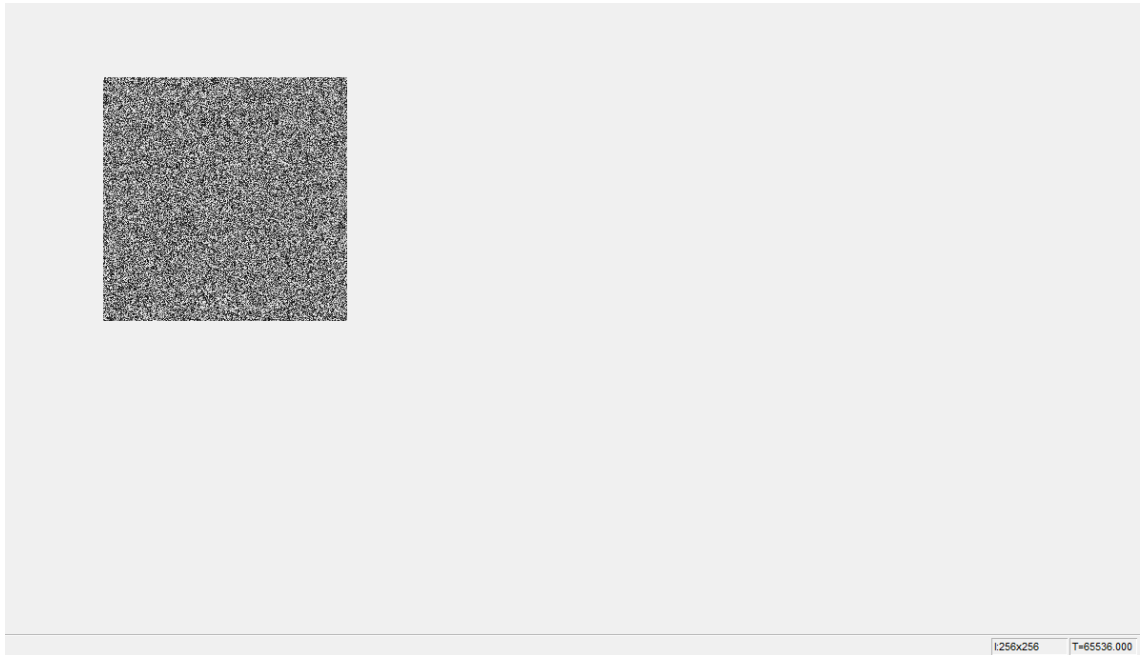


Figure 3-4 : image démontre le processus et l'opération de décryptage et fin du temps de simulation



Figure 3-5 : image récupérée

Conclusion :

Aujourd'hui, le monde connaît un grand développement dans le domaine de réseaux de communication. Donc, la plupart des recherches se concentrent sur l'amélioration des méthodes de la cryptographie pour augmenter le taux de sécurité et de confidentialité des données. Méthode proposée basée sur Matlab Simulink bloc Qi, pour éliminer la complexité de calcul l'inverse de clé du déchiffrement, ainsi, facilite la transmission de cette clé. Et une technique de permutation des pixels pour assurer les propriétés de confusion et diffusion.

CHAPITRE 4

INSERTION ET RECUPERATION DE MESSAGE

AVEC MODULATION

PARAMETRIQUE ET SYNCHRONISATION

ADAPTATIVE

4-introduction

Insertion et récupération de message du système chaotique avec la synchronisation adaptative et modulation paramétrique

Introduction : Dans ce chapitre, nous expliquons plus en détails le contenu et le rôle de chaque bloc du schéma de cryptage d'image avec simulink et la modulation paramétrique

4-1 Etude del'émetteur

Nous développons le système chaotiques émetteur.

1-Présentation des équations de système chen:

Notre étude se porte sur le système de Chen qui a quatre dimensions, il est régi par le système d'équations suivant.

$$\dot{x}_1 = a(x_2 - x_1) + x_4$$

$$\dot{x}_2 = dx_1 - x_1x_3 + cx_2$$

$$\dot{x}_3 = x_1x_2 - bx_3$$

$$\dot{x}_4 = x_2x_3 + rx_4$$

2.Définition desparamètres

a=35 et b=3 c= 12 d=7 et r=0.085

ces paramètres sont définit l'orque le système et chaotique

3. simulation du système

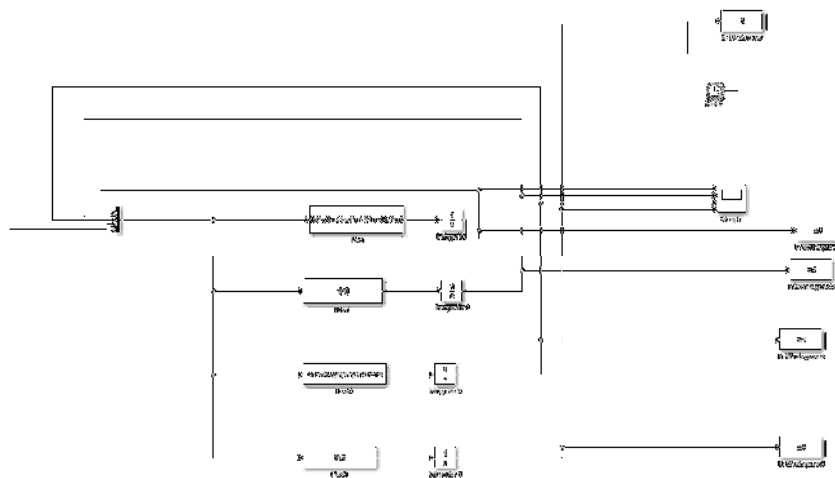


Figure 4-1 : schéma bloc du système de Chen

Ce système nous permet d'étudier le comportement du système et les courbes des signaux

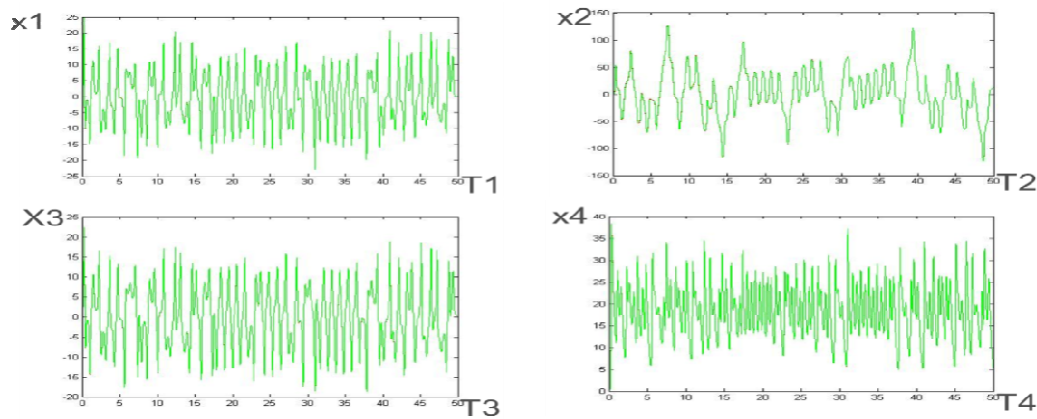


figure4-2 : les signaux du système de Chen en fonction du temps

4-2 étude de l'émetteur complet en fonction du système de Chen

4-2-1 : méthode utilisée :

La méthode utilisée pour la conception de l'émetteur est la modulation paramétrique
 Rappel : la modulation paramétrique consiste à utiliser un signal de nature binaire pour moduler l'un des paramètres du système chaotique avec une relation mathématique telle :
 $M(t) = a_0 + m(t)$

a_0 : est le paramètre à moduler

$m(t)$: est le message

avec une condition $m(t) < a_0$ pour que le système préserve ces propriétés chaotiques (condition de bifurcation)

donc dans notre travail on va construire un système émetteur de sorte qu'on envoie un message qui est l'image puis le récupérer on garde les propriétés chaotiques

4-2-2 étude et réalisation

On a notre système est chaotique a des paramètres $a=35$ $b=3$ $c=12$ et $d=7$
 Donc on doit faire l'analyse de bifurcation pour choisir le paramètre modulé qui rentre dans la réalisation

Donc on choisit le paramètre $b=3$ de sorte que
 $2 < b < 4$ analyse de bifurcation (l'étude de changement de comportement d'un système lorsque les paramètres changent)

Donc notre message qu'on le doit insérer est une image binaire de 8 bits on reprend notre image précédente

Elle varie entre 0 et 255

$$0 < m_i < 255$$

4-3-2 calcul du paramètre b moduler

Pour calculer le paramètre b moduler

On a la relation suivante : (modulation paramétrique)

$$P(t) = \frac{mi}{10} \times d + b$$

Calcul de la constante $= \frac{mi}{10} \times d$

Et mi elle dépend du mode de l'image

Mode : Noir=0

Blanche =255

Donc on prend le max mi=255

On aura $p(t) = \left(\frac{1}{10} \times 255\right) + 3$

$P(t)=bmoduler =3.1$ condition vérifiée

4-3 : réalisation du système émetteur

Après avoir étudié le système de Chen et calculer le paramètre b avec l'analyse de bifurcation maintenant passons à la réalisation avec insertion de l'image et paramètre b Et qu'on doit adapter pour le système émetteur du bloc du traitement d'image et le schéma bloc du système de Chen

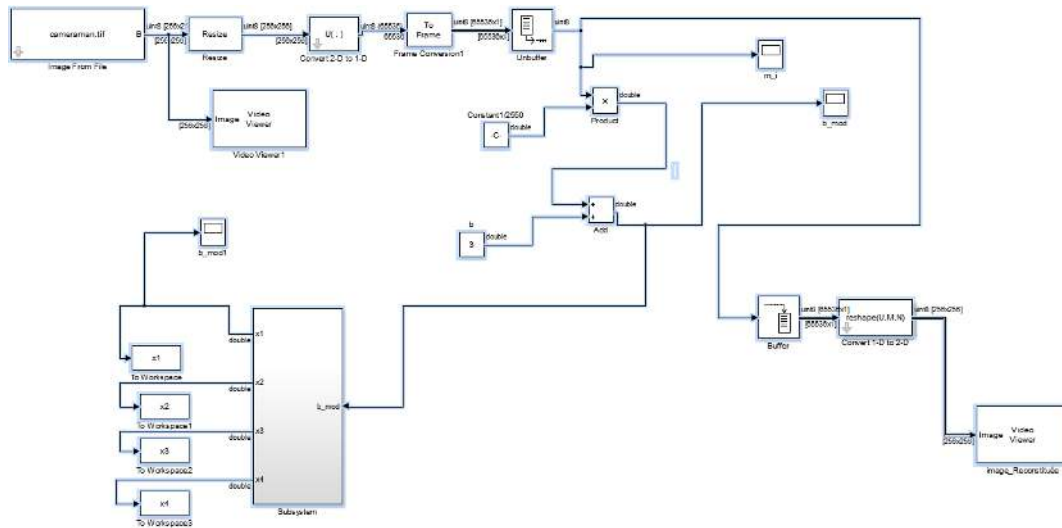


Figure 4-3 :schéma bloc du système émetteur sous Matlab Simulink

4-3-1 explication détaillée de chaque bloc du traitement

1) from file : c'est le fichier qui contient l'image notre image (cameraman) il permet de lire une image d'un fichier spécial

2) Bloc resize :il permet de redimensionné l'image en %

3) Bloc convert :ce bloc permet de faire une transformation d'une image matricielle en un vecteur a une seule dimension

4) Bloc to frame : Le bloc Conversion de trame transmet l'entrée à la sortie et définit le mode d'échantillonnage de sortie sur la valeur du paramètre Mode d'échantillonnage du signal de sortie, qui peut être basé sur la trame ou sur l'échantillon. Le mode d'échantillonnage de sortie peut également être hérité du signal

(référence) port d'entrée, que vous rendez visible en cochant la case Hériter le mode d'échantillonnage de sortie du port d'entrée <Ref>.

Le bloc Frame Conversion n'apporte aucune modification au signal d'entrée autre que le mode d'échantillonnage. En particulier, le bloc ne remet pas en mémoire tampon ou ne redimensionne pas les entrées 2D. Étant donné que les vecteurs 1-D ne peuvent pas être basés sur des trames, lorsque l'entrée est un vecteur 1-D de longueur M et que le bloc est en mode basé sur des trames, la sortie est une matrice M-par-1 basée sur des trames, c'est-à-dire un canal unique.

5)Bloc unbuufer : C'est-à-dire que les entrées ne sont pas mises en mémoire tampon par ligne de sorte que chaque ligne de la matrice devienne un échantillon de temps indépendant dans la sortie. Le taux auquel le bloc reçoit des entrées est généralement inférieur au taux auquel le bloc produit des sorties.



Figure 4-4 image reconstitué

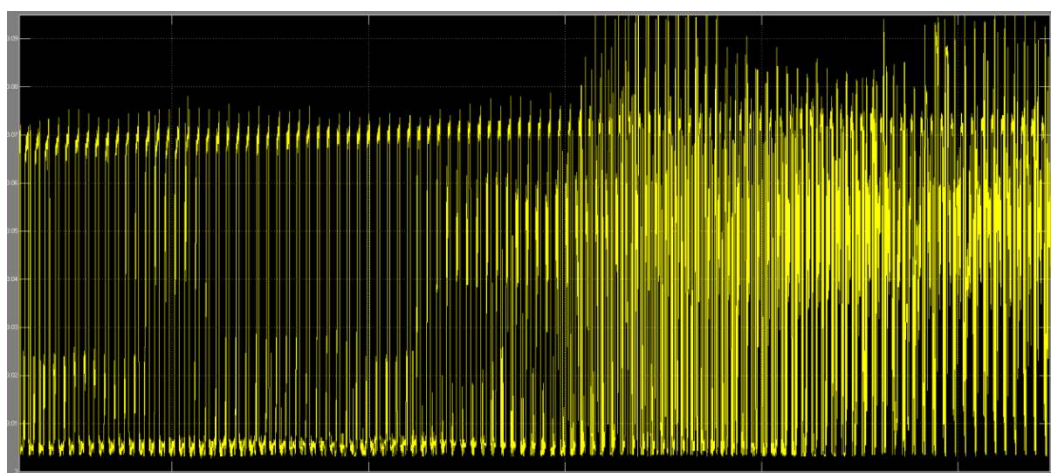


Figure-4-5 graphe variation du paramètre b modulé

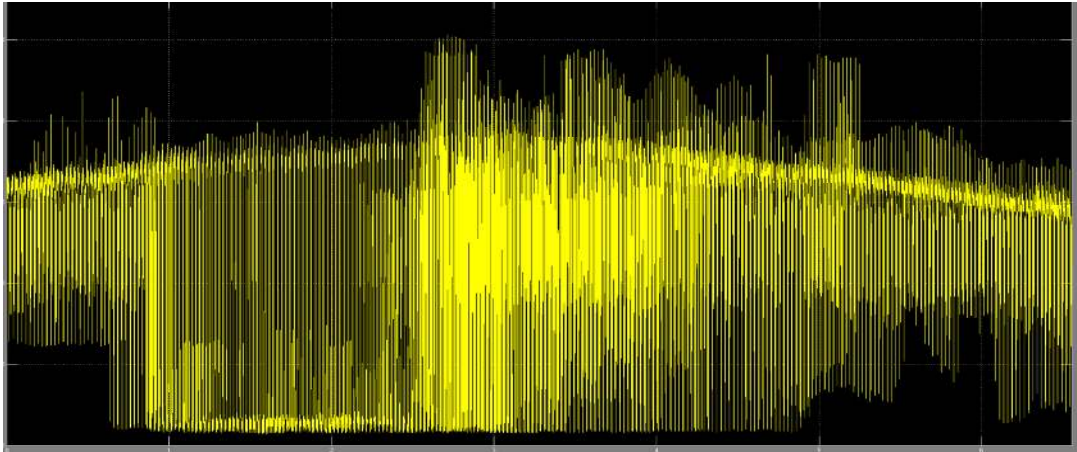


Figure 4-6
sign

al amplitude des pixels d'image

4-4 étude du récepteur

4-4-1 introduction :

L'utilisation d'observation est proposée pour estimer les états inconnus d'un système qui ne sont pas mesurables directement. Un système dynamique est dit observable si on peut récupérer toutes grandeurs par une combinaison de mesures et de leurs dérivées. En 1997, Nijmeijer et Mareels [31]. Ont montré que la synchronisation unidirectionnelle de deux systèmes chaotiques peut être considérée comme un problème d'observateur non linéaire et par conséquent, les théories d'automatique peuvent être utilisés pour analyser ce phénomène[31].

4-4-2 méthode utiliser :

la synchronisation adaptative :

Donc pour construire le récepteur il va falloir faire des calculs de la synchronisation adaptative

4-4-3 les étapes de la synchronisation adaptative :

On a notre système qui est constitué de deux systèmes

S1 : (maître)

$$\dot{x}_1 = a(x_2 - x_1) + x_4$$

$$\dot{x}_2 = dx_1 - x_1x_3 + cx_2$$

$$\dot{x}_3 = x_1x_2 - bx_3$$

$$\dot{x}_4 = x_2x_3 + rx_4$$

S2 : (esclave)

$$\dot{z}_1 = \hat{a}(z_2 - z_1) + z_4 - k_1e_1$$

$$\dot{z}_2 = \hat{d}z_1 - z_1y_3 + \hat{c}z_2 - k_2e_2$$

$$\begin{aligned} \dot{z}_3 &= x_1 \times z_2 - \hat{b}z_3 - k_3e_3 \\ \dot{z}_4 &= z_2 \times z_3 + \hat{r}z_4 - k_4e_4 \end{aligned}$$

Erreur de synchronisation :

$$\begin{aligned} \dot{e}_1 &= a \times e_2 + (x_2 - x_1)e_a + e_4 - k_1e_1 \\ \dot{e}_2 &= x_1 \times e_d - x_1 \times e_3 + x_2 \times e_c - k_2e_2 \\ \dot{e}_3 &= x_1 \times e_2 - x_3 \times e_b - k_3e_3 \\ \dot{e}_4 &= y_2 \times e_3 + x_4 \times e_r - k_4e_4 \end{aligned}$$

1^{er} étape calcul de l'erreur :

On a : l'erreur = $x - y$, $e = x - y$ et $a_1 = a + \hat{a}$

Pour pouvoir calculer l'erreur et déterminer les équations et les paramètres il va falloir utiliser les relations suivantes :

On a : $v = v_1 + v_2 \geq 0$

Et la fonction de Lyapunov : $v_1 = \frac{1}{2} (e_1^2 + e_2^2 + e_3^2 + e_4^2)$ et

$$v_2 = \frac{1}{2} \left(\frac{e_a^2}{a} + \frac{e_b^2}{b} + \frac{e_c^2}{c} + \frac{e_d^2}{d} + \frac{e_r^2}{r} \right)$$

$$\frac{Dv}{dt} < 0$$

$$\begin{aligned} de_1 &= x_4 - z_4 + e_1k_1 - a(x_1 - x_2) + a_1(z_1 - z_2) \\ de_1 &= e_4 + e_1k_1 - ax_1 + ax_2 + (a + \hat{a})(z_1 - z_2) \\ de_1 &= e_4 + e_1k_1 - ax_1 + ax_2 + az_1 + az_2 + \hat{a}z_2 - \hat{a}z_1 - \hat{a}z_2 \\ e_1de_1 &= e_1(e_4 + e_1k_1 - ae_1 - ae_2 + \hat{a}z_1 - \hat{a}z_2) \\ e_1de_1 &= e_1e_4 + e_1^2k_1 - ae_1^2 - ae_2e_1 + \hat{a}e_1z_1 - \hat{a}e_1z_2 \\ e_1de_1 &= e_1^2(k_1 - a) + e_1 \times (e_4 - ae_2 + \hat{a}z_1 - \hat{a}z_2) \end{aligned}$$

On a : $u = \frac{1}{a} \times e_a \times \dot{e}_a$

$$\begin{aligned} e_1de_1 &= e_1^2 \times (k_1 - a) + e_1 \times (e_4 - ae_2 + \hat{a}z_1 - \hat{a}z_2) + \frac{1}{a} \times e_a \times \dot{e}_a \\ e_1de_1 &= e_1^2 \times (k_1 - a) + e_1e_4 - ae_1 \times e_2 + e_1e_a \times z_1 \\ e_1de_1 &= e_1^2 \times (k_1 - a) + e_1e_4 - ae_1 \times e_2 + e_a \left(e_1z_1 - e_1z_2 + \frac{1}{a} \times \dot{e}_a \right) \times e_1(z_1 - z_2) \quad (1) \end{aligned}$$

$$\begin{aligned} de_2 &= e_2k_2 + cx_2 + dx_1 + c_1z_2 - d_1z_1 - x_1x_3 + z_1z_3 \\ de_2 &= e_2k_2 + cx_2 - (c + \hat{c})z_2 + dx_1 - (d + \hat{d})z_1 - x_1x_3 + z_1z_3 \\ de_2 &= e_2k_2 + ce_2 - \hat{c}z_2 + de_1 - \hat{d}z_1 - x_1x_3 + z_1z_3 \\ e_2de_2 &= e_2 \times (e_2k_2 + ce_2 - \hat{c}z_2 + de_1 - \hat{d}z_1 - x_1x_3 + z_1z_3) \\ e_2de_2 &= e_2^2k_2 + ce_2^2 - \hat{c}e_2z_2 + de_2e_1 - \hat{d}e_2z_1 - x_1x_3 \times e_2 + z_1z_3 \times e_2 \\ e_2de_2 &= e_2^2(k_2 + c) + e_2(-\hat{c}z_2 + de_1 - \hat{d}z_1 - x_1x_3 + z_1z_3) \end{aligned}$$

On a $u = \frac{1}{c} \times e_c \times \dot{e}_c$

$$e_2de_2 = e_2^2(k_2 + c) - e_2z_2 + \frac{1}{c} \times e_c \times \dot{e}_c$$

$$\begin{aligned}
e_2 de_2 &= e_2^2(k_2 + c) + ec \times \left(-e_2 z_2 + \frac{1}{c} \times ec\right) \\
e_2 de_2 &= e_2^2(k_2 + c) + e_2(de_1 - \hat{d}z_1) + \frac{1}{d} \times ed \times ed \\
e_2 de_2 &= e_2^2(k_2 + c) + ed \left(-e_2 z_1 + \frac{1}{d} \times ed\right) + e_2 \times e_1 d \quad (2)
\end{aligned}$$

$$\begin{aligned}
de_3 &= e_3 k_3 - bx_3 + b_1 z_3 + x_1 x_2 - z_1 z_2 \\
de_3 &= e_3 k_3 - bx_3 + (b + \hat{b})z_3 + (x_1 x_2) - (z_1 z_2) \\
de_3 &= e_3 k_3 - be_3 + \hat{b}z_3 + x_1 x_2 - z_1 z_2 \\
de_3 &= e_3 k_3 - be_3 + \hat{b}z_3 + x_1 x_2 \times e_3 - z_1 z_2 \\
e_3 de_3 &= e_3 \times (e_3 k_3 - be_3 + \hat{b}z_3 + x_1 x_2 - z_1 z_2) \\
e_3 de_3 &= e_3^2 \times k_3 - be_3^2 + \hat{b}e_3 z_3 + x_1 x_2 - z_1 z_2 \times e_3 \\
e_3 de_3 &= e_3^2 \times (k_3 - b) + e_3 \times (\hat{b}z_3 + x_1 x_2 - z_1 z_2) \\
\text{On a : } u &= \frac{1}{b} \times e_b \times e_b \\
e_3 de_3 &= e_3^2 \times (k_3 - b) + e_3 \times (\hat{b}z_3 + x_1 x_2 - z_1 z_2) \\
e_3 de_3 &= e_3^2 \times (k_3 - b) + e_3 - e_b * z_3 + e_3 \times x_1 x_2 + e_3 \times z_1 z_2 + \frac{1}{b} \times e_b \times e_b \\
e_3 de_3 &= e_3^2 \times (k_3 - b) + e_3 \times x_1 x_2 - e_3 \times z_1 z_2 + e_b \left(e_3 \times z_3 + \frac{1}{b} \times e_b\right) (3) \\
de_4 &= e_4 k_4 + rx_4 - r_1 z_4 + x_2 x_3 - z_2 z_3 \\
de_4 &= e_4 k_4 + rx_4 - (r + \hat{r})z_4 + x_2 x_3 - z_2 z_3 \\
de_4 &= e_4 k_4 + rx_4 - rz_4 - \hat{r}z_4 + x_2 x_3 - z_2 z_3 \\
de_4 &= e_4 k_4 + re_4 + x_2 x_3 - z_2 z_3 \\
e_4 de_4 &= e_4^2 k_4 + e_4^2 r + e_4 \times x_2 x_3 - e_4 * z_2 z_3 - e_4 \times \hat{r} \times z_4 \\
e_4 de_4 &= e_4^2 (k_4 + r) + e_4 (-\hat{r}z_4 + x_2 x_3 - z_2 z_3) + \frac{1}{r} \times er \times er \\
e_4 de_4 &= e_4^2 (k_4 + r) + e_4 \times e_r \times z_4 + e_4 \times x_2 x_3 - e_4 \times z_2 z_3 + \frac{1}{r} \times er \times er \\
e_4 de_4 &= e_4^2 (k_4 + r) + e_4 (x_2 x_3 \times z_2 z_3) + e_r \times \left(e_4 z_4 + \frac{1}{r} \times er\right) \quad (4)
\end{aligned}$$

2ème étape : détermination des cst k1 k2 k3 k4

Etude et détermination des cts k :

$$e_1^2(k_1 + a) > 0$$

$$e_1^2 > 0 \quad k_1 + 35 > 0$$

$$k_1 < -35$$

$$e_2^2(-k_2 + c) > 0$$

$$-k_2 + c > 0$$

$$-k_2 + 12 > 0$$

$$k_2 < 12$$

$$e_3^2(-k_3 + b) > 0$$

$$k_3 + 3 > 0$$

$$k_3 > -3$$
$$k_4 + 0.085 > 0$$
$$k_4 < -0.085$$

4-4-4 réalisation du récepteur

Le récepteur est constitué de deux étages:

- un premier étage qui correspond à la synchronisation adaptative permettant de récupérer les valeurs des paramètres du système chaotique et en particulier la valeur de b modulée.
- un deuxième étage qui correspond à la démodulation paramétrique, c'est à dire l'opération inverse de la modulation permettant ainsi de récupérer les valeurs estimées des pixels pour la reconstitution de l'image.

La partie principale du récepteur est la synchronisation adaptative. Le deuxième étage (démodulation)

4-4-4-1 : les étapes à suivre pour la réalisation du récepteur :

Dans le schéma du récepteur avec la synchronisation adaptative, il faut faire apparaître les blocs suivant :

- le bloc émetteur $x(t)$
- le bloc récepteur $y(t)$
- le bloc erreur $e(t)$
- le bloc paramètre estimé

Il faut relier les différents blocs en fonction de nos équations.

Après la réalisation du récepteur sur Matlab simulink on doit analyser tout système et on montre le tracé des graphes x (émetteur) en fonction du temps puis en fonction d'erreur pour rassurer que la synchronisation est faite

Les figures (4-7—4-10) ci-dessous montrent le tracé de x (émetteur) en fonction du temps

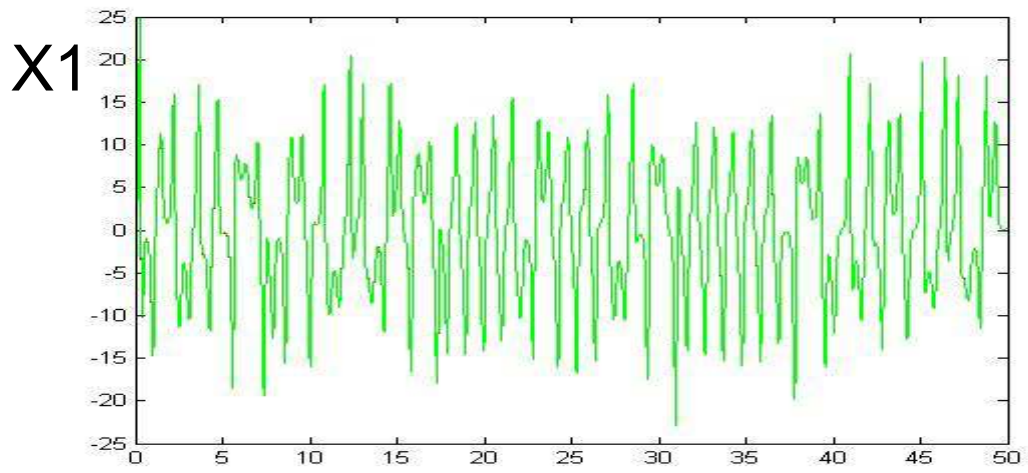


figure4-7
Représente le tracé x1 en fonction de t

T

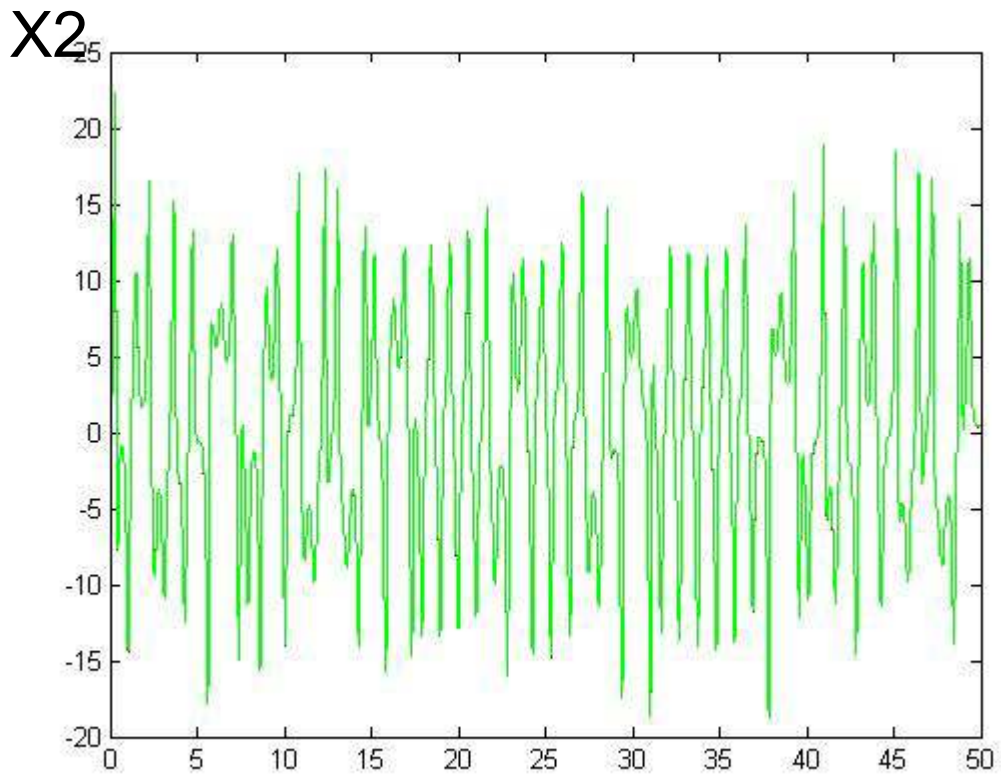


Figure 4-8
Représente le tracé x2 en fonction de t

T

X3

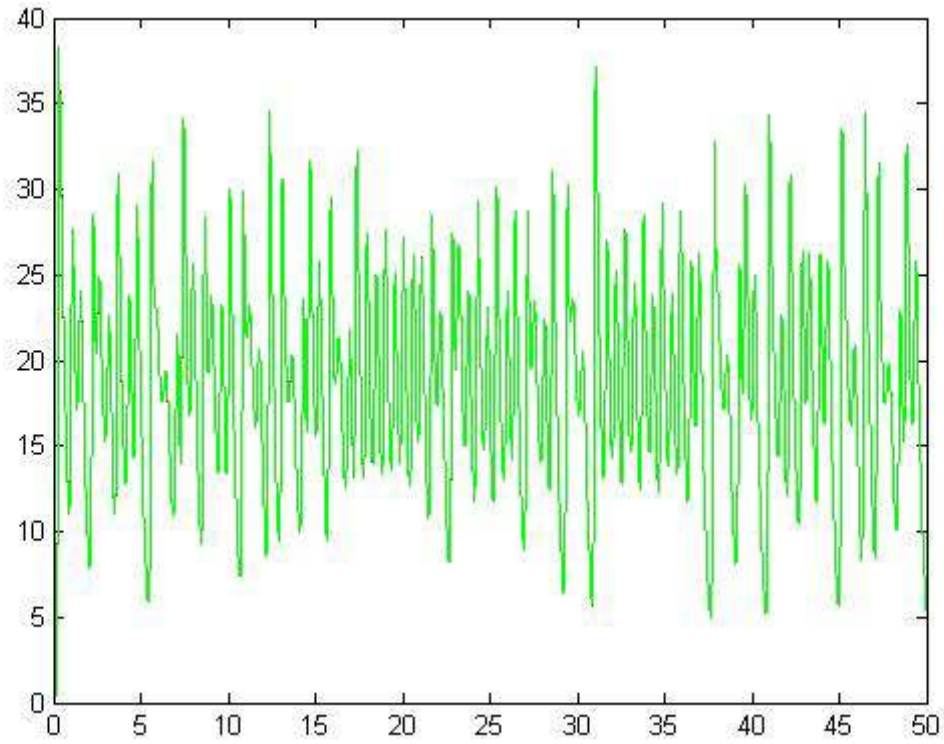


Figure 4-9 Représente le tracé X3 en fonction de T

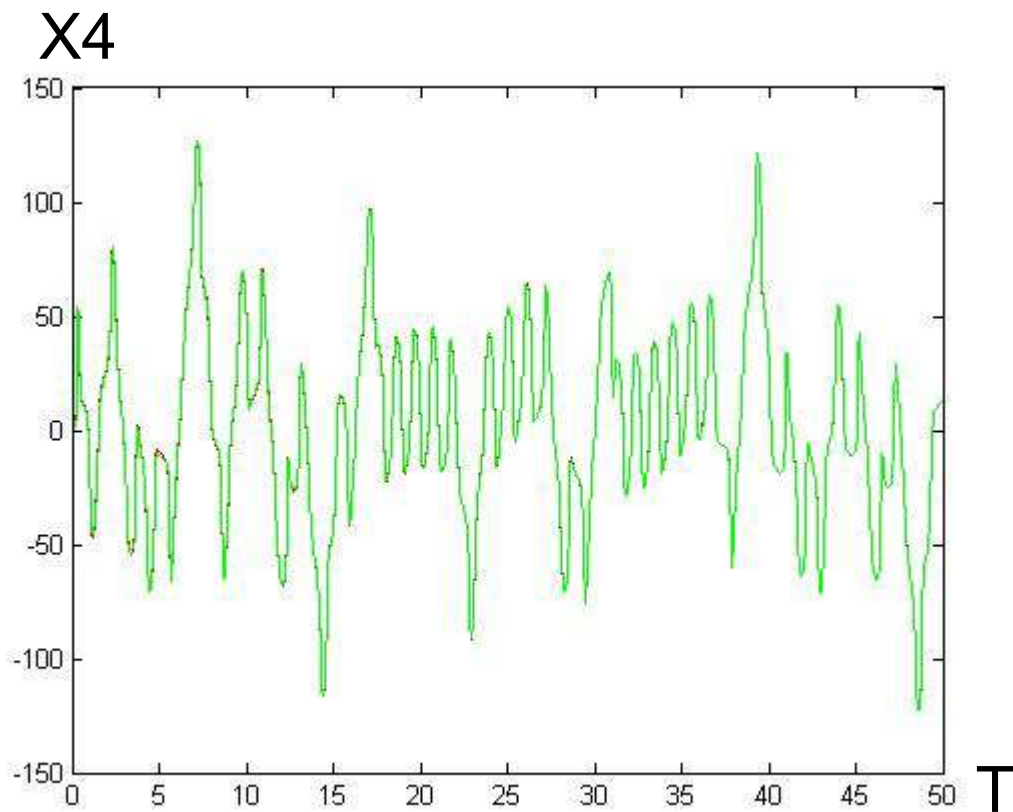


Figure4-10

Représente le tracé x_4 en fonction de t

Les figures(4-11—4-14) ci-dessous montrent le tracé entre émetteur x et l'erreur

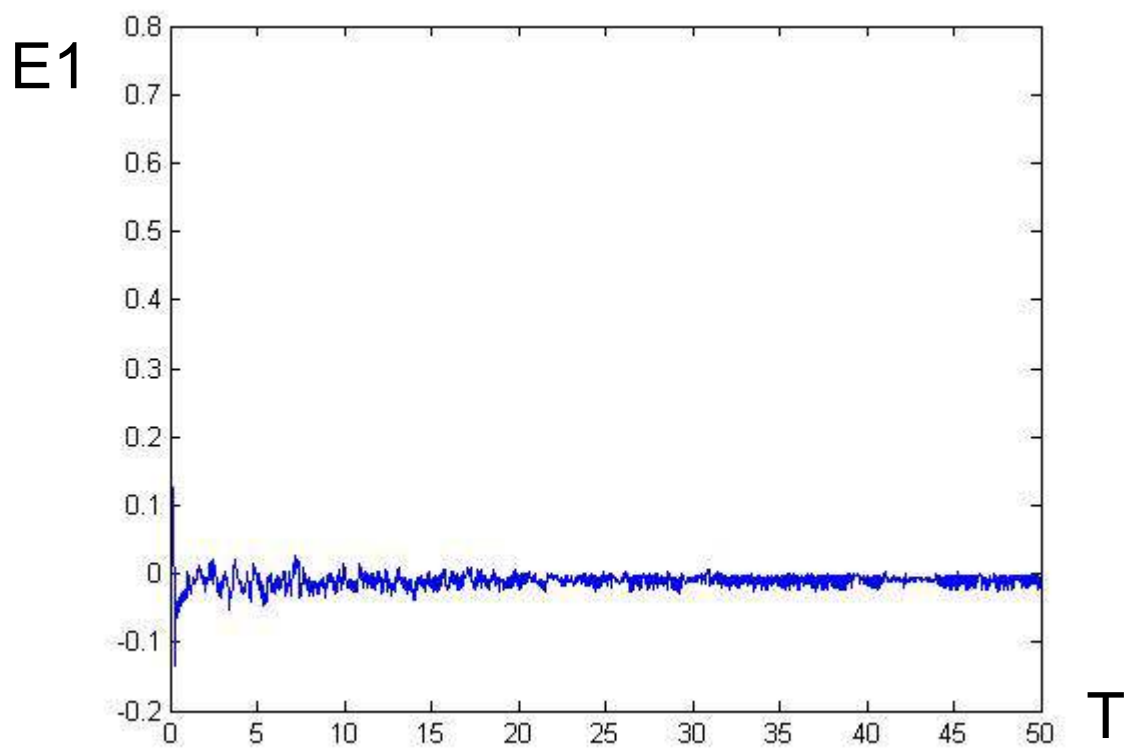
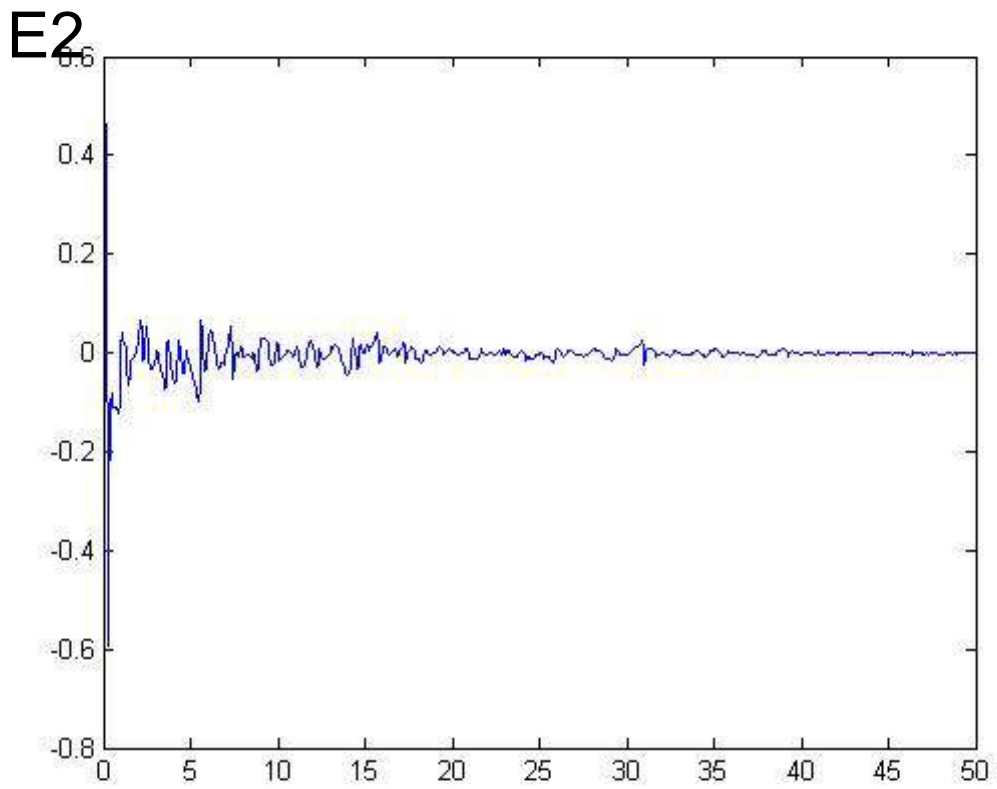
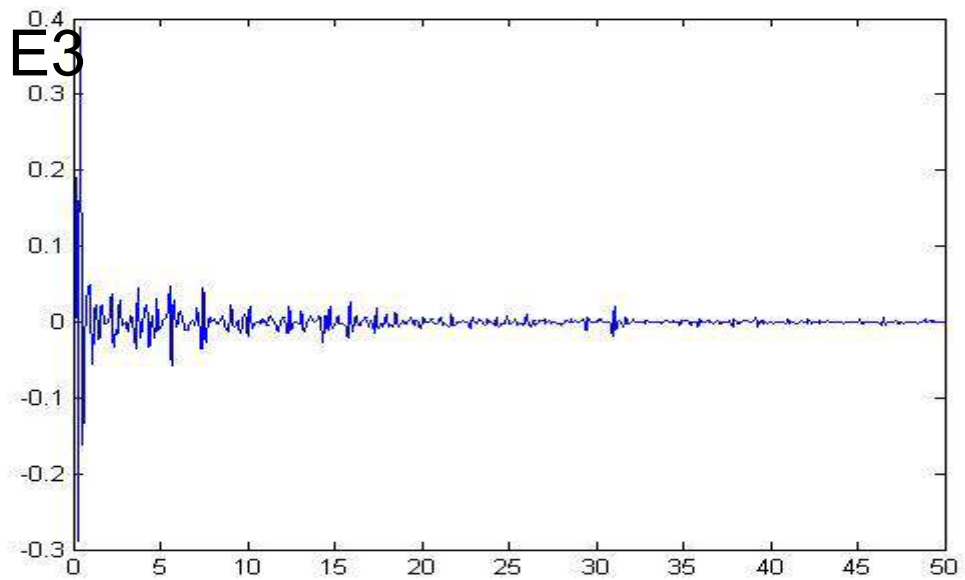


Figure 4-11
Représente le tracé e1 en fonction de t



T

Figure4-12
Représente le tracé e2 en fonction de t



T

igure

4-13

Représente le tracé e3 en fonction de t

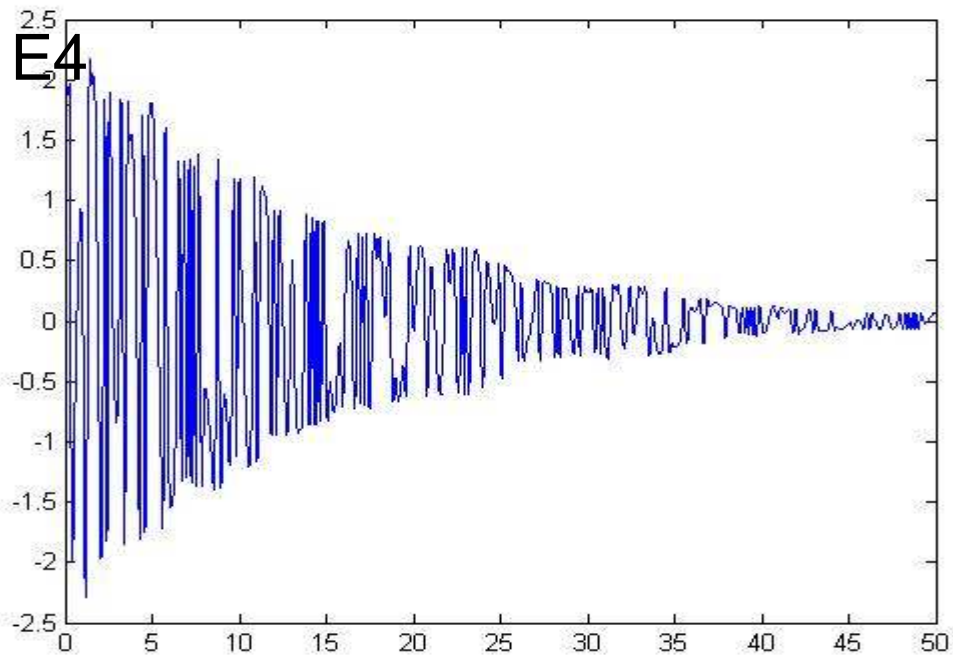


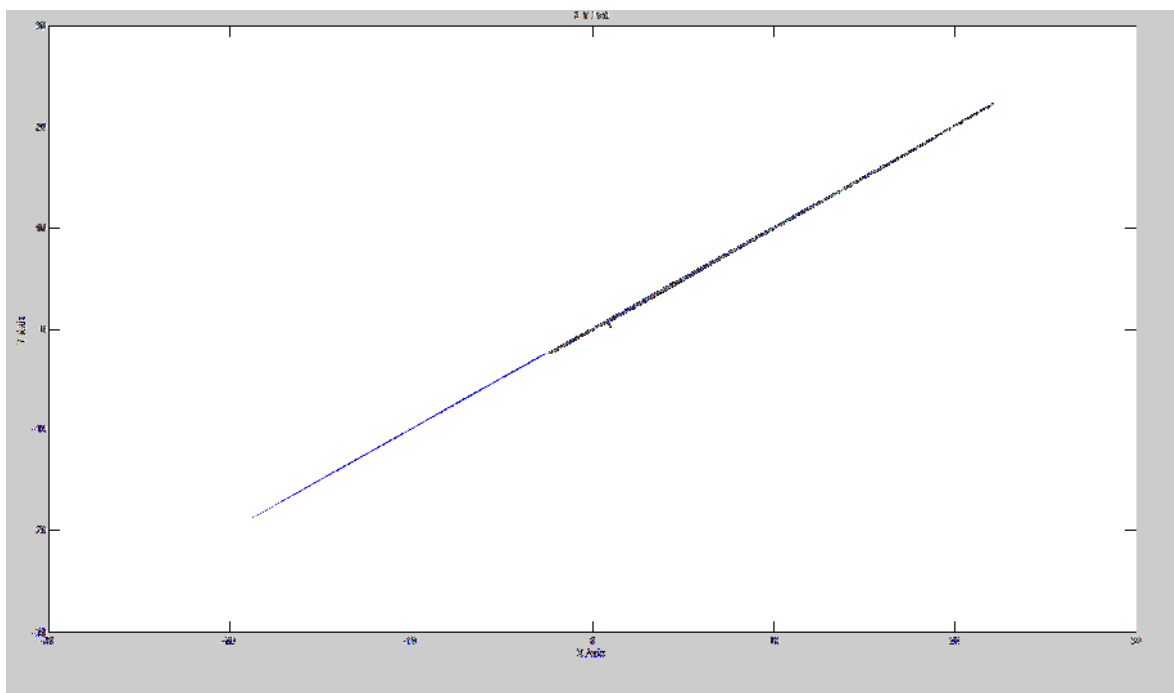
Figure 4-14

Représente le tracé e4 en fonction de t

Remarque : dans notre système nous remarquons que l'erreur tend vers 0
Le système esclave converge vers le système maître .

Les figures(4-15---4-18) ci-dessous montrent la synchronisation et le plan de phase

Z1



X1

Figure 4-15
Représente le tracé de z1 en fonction de x1

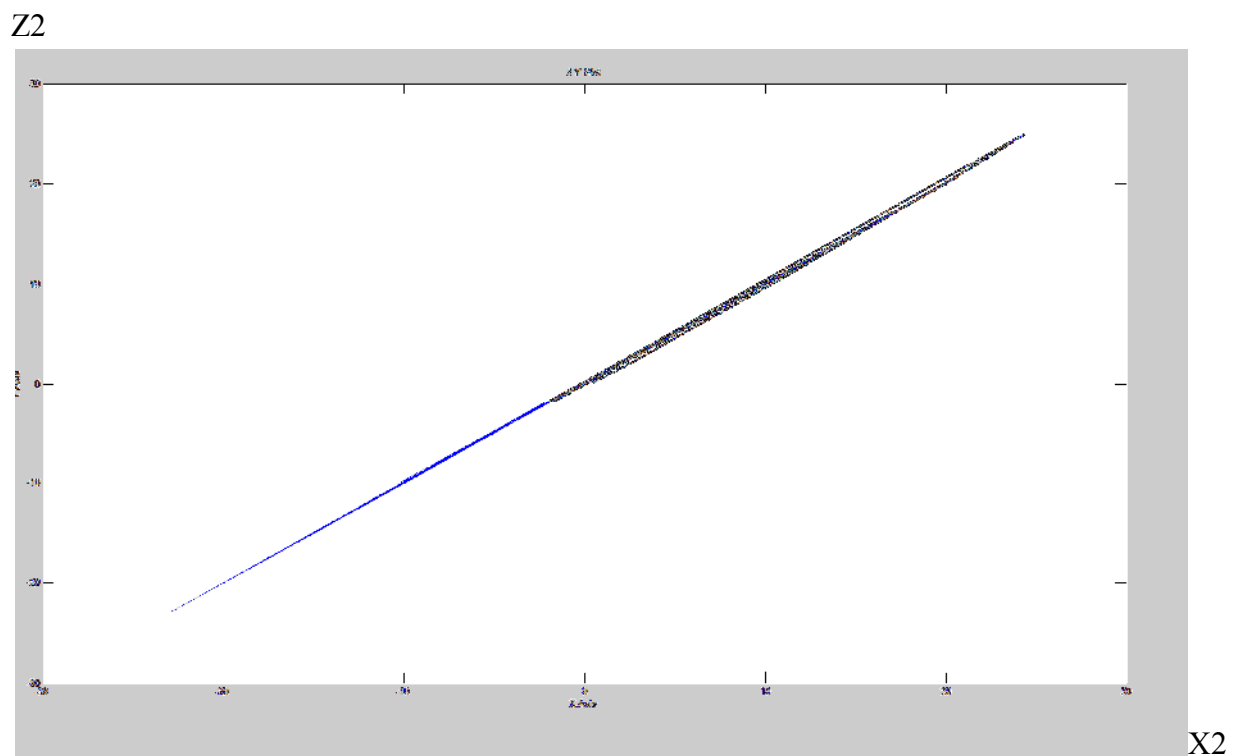


Figure 4-16
Représente le tracé de z2 en fonction de x2

Z3

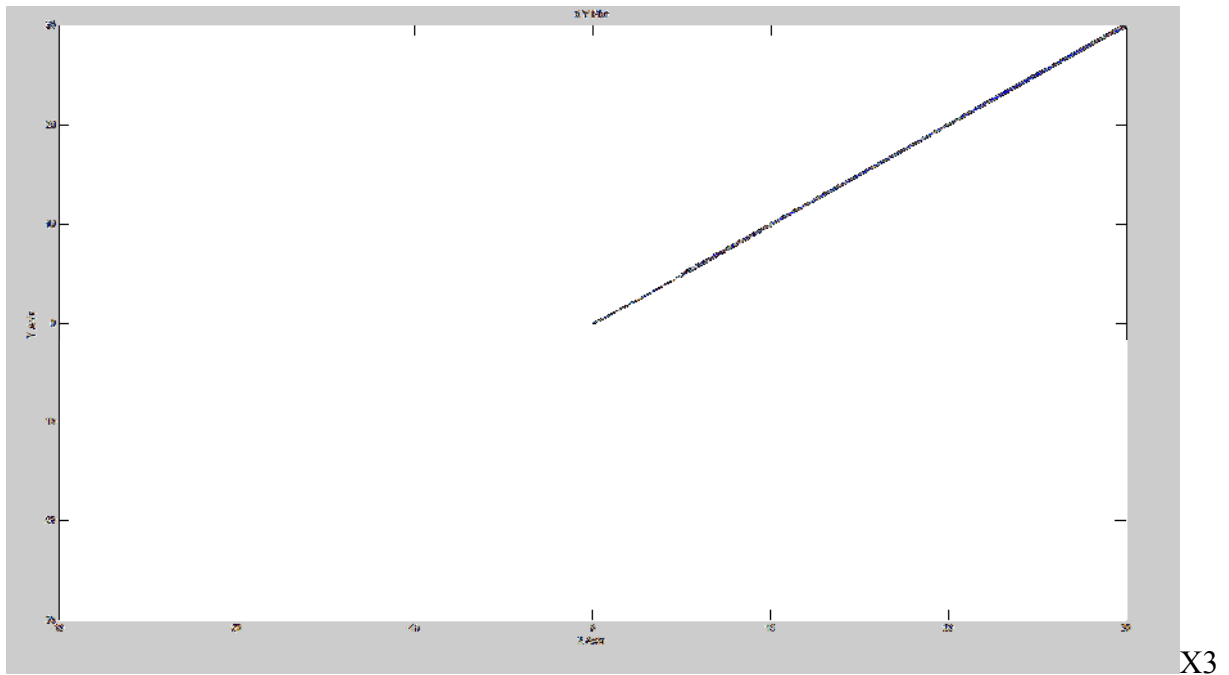


Figure 4-17
 Représente le tracé de z3 en fonction de x3

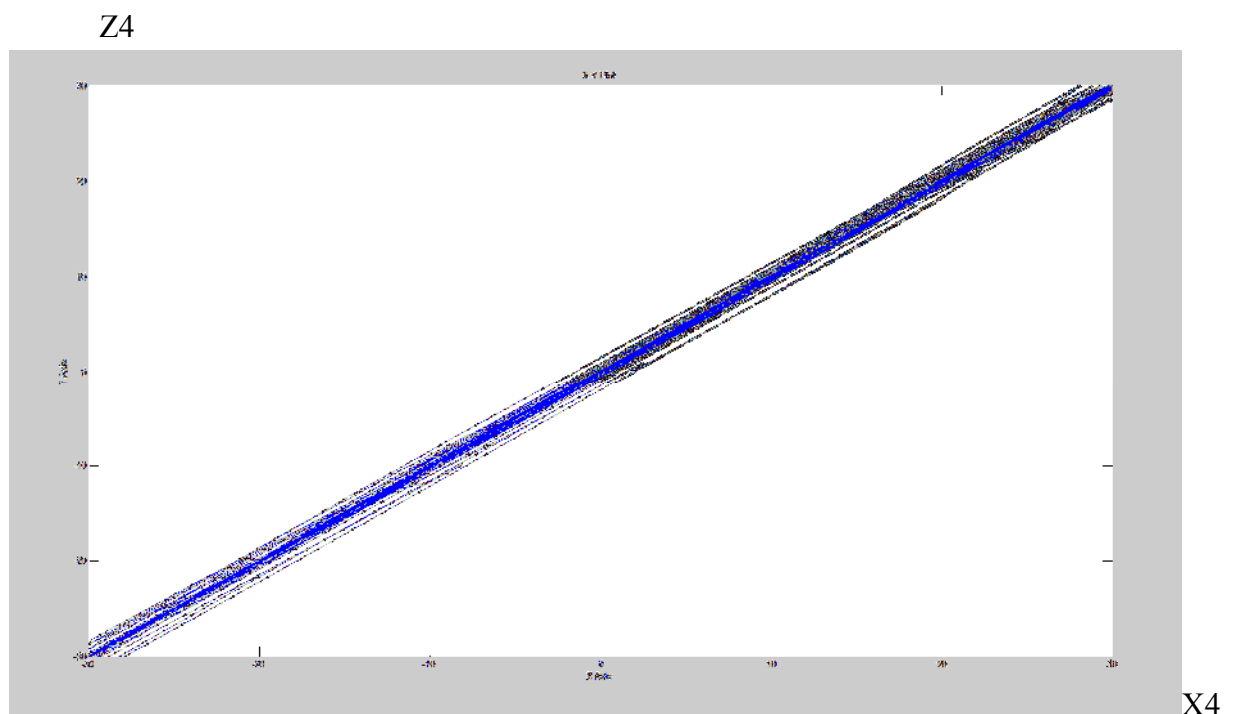


Figure 4-18
 Représente le tracé de z4 en fonction de x4

Remarque : nous remarquons que le tracé du plan de phase est une droite

Conclusion : dans cette étape on a fait la synchronisation adaptative pour déterminer les paramètres estimée pour construire le récepteur qui se compose de bloc émetteur erreur et paramètres estimé. à la fin on peut dire qu'on a simuler et vu le plan de phase qui est une droite qui passe par l'origine $y=x$ qui signifie que le synchronisation elle est bonne.

Conclusion générale :

Dans notre thèse on a étudié le système chaotique en particulier le système de Lorenz. Puis on a fait le cryptage d'image sous MatlabSimulink pour étudier la cryptographie par le chaos pour qu'on s'intéresse à étudier et réaliser un système émetteur et récepteur de message chaotique tout d'abord on a étudié le système de Chen pour adapter ce système avec le bloc Simulink de cryptage d'image Qi a pour construire l'émetteur et envoyer le message à la base par la modulation paramétrique qui est le point essentiel d'insertion de message puis la deuxième étape on a fait la synchronisation adaptative pour déterminer les paramètres estimée pour construire le récepteur qui se compose de bloc émetteur erreur et paramètres estimé. à la fin on peut dire qu'on a simuler et vu le plan de phase qui est une droite qui passe par l'origine $y=x$ qui signifie que le synchronisation elle est bonne.

bibliographie

- [1] E. cherrier, "Estimation de l'état et des entrées inconnues pour une classe de systèmes non linéaires", thèse de doctorat, institut national polytechnique de Lorraine, 2006.
- [2] O. Megherbi, "Etude et réalisation d'un système sécurisé à base de système chaotiques", thèse de magister, Université Mouloud Memmeri Tizi-Ouzou, 10\10\2013.
- [3] H. Dang-Vu, C. Delcarte, "Bifurcation set et chaos: Introduction à la dynamique contemporaine avec des programmes en Pascal, Fortran et Mathematica", Ed. Ellipses, Paris, Septembre 2000.
- [4] N. Witkowski, P. Bergé, "Le chaos dans les magazines scientifiques européens Archimède", 13 janvier 1998.
- [5] M. Maizi, "Etude et contrôle des systèmes dynamiques chaotiques", thèse de Master, université de Tébessa, 29/06/2016.
- [6] CH. Benhabib, "Etude d'un système chaotique pour la sécurisation de communications optiques", thèse de Master, université de Tlemcen, Juin 2014A.
- [7] A. Ikhlef, "Contrôle, chaotification et hyper chaotification des systèmes dynamiques", thèse de Master, Université de Mentouri Constantine, 2007.
- [8] G. Assael, L. Blaizot et G. Huizinga, "la Théorie du chaos", Saint Eloi, 2013.
- [9] D. Peltier, T Nguyen Hoang, D. P. Tran, O. Abdelmalki, K. Alaoui et K. Leroux, "Etude d'un système physique non dissipatif «chaotique»", Projet de Physique P6-3STPI/P6-3/2009.
- [10] H. Azira, M. Khettaal, "Analyse et Implémentation du Système chaotique de Qi", université de Saad Dahlab de Blida, thèse de master, 2015.
- [11] I. Talbi, "Système Dynamique non linéaires et phénomènes de chaos", Thèse de master, Université Mentouri de Constantine, 29\06\2010.
- [12] E. N. Lorenz, "Deterministic no periodic flow", Journal of Atmospheric Sciences, 20:130-141, 1963.
- [13] T. Hamaizia, "Systèmes Dynamiques et Chaos" Application à l'optimisation à l'aide de l'algorithme Chaotique", thèse pour l'obtention de Doctorat, Université de Constantine, 2013, pp.22.
- [14] F. Alain, "Contribution à la prédiction et au contrôle des comportements aperiodiques dans les convertisseurs électromécaniques. Application de la théorie du chaos", université de Reims France, 2005.
- [15] D. Ruelle, et F. Takens, "On the nature of turbulence, Commun Math Phys, 20, 167-192, 1971.