République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Mouloud MAMMERI, Tizi-Ouzou

Faculté de Génie Electrique et d'Informatique
Département d'Automatique

Mémoire de Fin d'Etudes

En vue de l'obtention du diplôme

Master académique en automatique

Option commande des systèmes

Thème

Etude de dispositifs de transmission sécurisée de données à base de systèmes chaotiques d'ordre entier et fractionnaire

Dirigé par :

M. DJENNOUNE Saïd

Soutenu le : 15/10/12

Présenté par :

M^elle^ FEDDAL Lydia

M^elle^ MERBOUTI Souad

Promotion 2012

Ce travail a été préparé : au laboratoire de conception et conduite des systèmes de production (L2CSP)

Remerciement

Nos remerciements chaleureux a notre promoteur Monsieur ***DJENNOUNE.S*** *professeur à l'UMMTO pour son soutien, son aide, ses réponses a nos diverses questions, mais avant tout pour nous avoir proposé ce sujet très intéressant. Aussi, c'est un honneur pour nous d'avoir eu l'occasion de travailler et d'apprendre aux cotes de personne ayant des qualités humaines exceptionnelles.*

On tient à remercier, au même titre, Monsieur ***HAMICHE .H*** *maitre de conférences classe A. On lui dit un grand MERCI pour ses conseils, son aide, ses encouragements ainsi sa sympathie.*

On aimera également remercier les membres de jury qui nous feront l'honneur d'évaluer ce travail.

Dédicace

Je dédie ce travail

A la femme la plus merveilleuse sur cette terre, à celle qui a donné un sens à mon existence qui était et toujours là pour moi avec son soutien et son grand amour ma chère mère.

A toute ma famille que j'aime énormément.

A toutes mes amies.
A tous ceux qui sont chers à mon cœur.

Lydia

Je remercie d'abord le bon dieu de m'avoir éclairé le droit chemin

Je dédie ce modeste travail :

A mes très chers parents

A mes très chers frères (DJAMEL, ABDERRAHMANE et MUSTAPHA).

A mes très chères sœurs (LATIFA, SOUHILA).

A :

La mémoire de ma très chère grand-mère.

Mon très cher grand-père.

Mes belles sœurs (Siham, Khadîdja, Samira, Ouiza).

Mes très chères nièces (Zineb, Meriem, Nour-Elhouda, Daya).

A Lydia et sa famille.

Mes amies.

La promotion (2011-2012).

Tous ceux qui ont contribué a la réalisation de ce mémoire, de loin ou de près.

Souad

Liste de figures

Les tableaux

Ensembles

$\mathbb{R}$: Ensemble des nombres réels.

$\mathbb{R}^+$: Ensemble des nombres réels positifs.

$\mathbb{N}$: Ensemble des nombres entiers naturels.

$L_f^{n-1}h$: (n-1) ème dérivée de Lie de h dans la direction de f.

$dL_f^{n-1}h$: Le différentiel de $L_f^{n-1}h$.

Matrices et normes

O : la matrice d'observabilité.

J : la matrice Jacobienne.

$\mu_i(J)$: Les valeurs propres de la matrice J

$\|x\|$: La norme euclidiennes de x,

Acronymes

AES: Advanced Encryption Standard

DES : Data Encryption Standard.

RSA : Rivest Shamir Adleman.

SCI : Sensibilité aux Conditions Initiales.

LED : Light Emitting Diode

LASER: Light Amplification by Stimulated of Radiation

PIN : Positive Intrisic Négative.

SNR : Signal Noise Ratio.

Au cours des dernières décennies, une part importante des activités de recherche en automatique s'est focalisée sur le problème de l'observation de l'état des systèmes dynamiques non linéaires. Ceci est motivé par le fait que l'estimation de l'état est une étape importante voir indispensable pour la synthèse de lois de commande, pour le diagnostic ou la supervision des systèmes industriels. Récemment, d'autres applications telles que la synchronisation et le décryptage dans les systèmes de communication, sont devenues l'un des secteurs de recherche les plus dynamiques [26].

En effet, la cryptographie joue un rôle important dans la sécurité et la fiabilité des systèmes de transmission de données, surtout avec le développement du commerce électronique, les utilisateurs cherchent à protéger les données sensibles dans leurs ordinateurs et de garantir la confidentialité des données sur des réseaux publics tels que l'Internet.

Les techniques de cryptographie classique sont basées sur la théorie des nombres et en particulier sur la décomposition d'un entier en éléments simples. Nous pouvons aussi citer les deux algorithmes bien connus : DES, RSA. Mais, avec la révolution de l'informatique, ces algorithmes proposés ne sont pas assez sécurisés. Pour ces raisons, plusieurs chercheurs essayent de mettre en œuvre d'autres « cryptosystèmes ».

Durant ces dernières décennies, la théorie des systèmes non linéaires a été appliquée à la cryptographie afin d'augmenter le degré de sécurité. Grace aux propriétés naturelles des systèmes chaotiques sont devenus de bons candidats pour la cryptographie. De nombreux schémas sont proposés afin d'appliquer les systèmes chaotiques dans le domaine de la cryptographie [23].

L'idée d'utilisation du chaos dans les systèmes de communication a été inspirée de la découverte de Pecora-Carroll en 1990 [18]. Ils ont montré que deux systèmes chaotiques identiques avec des conditions initiales différentes peuvent éventuellement se synchroniser s'ils sont couplés d'une certaine manière convenable, c'est à dire sous certaines conditions. Le développement des systèmes de communication utilisant le chaos a commencé donc avec des schémas de synchronisation très simples de circuits électroniques, visant pour le cryptage et la reconstruction simultanés d'un signal d'information [10]. Par la suite, de nombreuses techniques de cryptage par addition, par commutation, par modulation,… etc, ont été mises au

point pour inclure le message clair dans un signal porteur chaotique, voire dans la dynamique même de l'émetteur. Par un processus de synchronisation, le récepteur est capable d'estimer l'état de l'émetteur, puis d'effectuer le décryptage du message crypté.

Au cours des dernières années, les recherches ont montré qu'on peut aussi prolonger la synchronisation aux systèmes chaotiques à dérivée fractionnaire. La théorie des dérivés d'ordre fractionnaire peut être remontée au 17ème siècle et développée largement en dernier siècle dû à son application dans une grande variété de champs scientifiques et technologiques **[**23**].** Le calcul d'ordre fractionnaire a fait un impact profond dans les domaines de viscoélasticité et rhéologie, génie électrique, électrochimie, biologie, traitement de signal et d'image, mécanique, physique, théorie de commande, cryptage, transmission de données [6]. D'autre part, il y'a aussi des systèmes dynamiques d'ordre fractionnaire bien connus ont montré des bifurcations complexes et des phénomènes chaotiques étranges. Par exemple, le système chaotique d'ordre fractionnaire de Lorenz, le circuit de Chen d'ordre fractionnaires, le circuit de Chua fractionnaire **[**20**]**. Ces systèmes chaotiques d'ordre fractionnaires ont été misent en application dans le domaine de la transmission sécurisée pour renforcer la sécurisation et rendre la cassure de la clé quasiment impossible.

Notre travail a pour objectif principal de proposer un nouveau système de transmission sécurisée. On exploitant dans un premier temps les propriétés des systèmes dynamiques chaotiques, avec la possibilité de synchronisation par observateur dans le but d'utilisation dans une transmission sécurisée et d'autre part, on étudiant la possibilité de synchronisation des systèmes dynamiques chaotiques d'ordre fractionnaire pour améliorer le niveau de sécurité.

Afin d'aborder ce but, on a divisé ce mémoire en quatre chapitres, dont le premier est consacré aux notions de base de la théorie de l'information ainsi que les techniques habituellement utilisés dans le contexte de la transmission sécurisée de l'information.

Dans le deuxième chapitre, nous proposons d'établir un état de l'art sur la théorie des systèmes dynamiques chaotiques, à travers ses caractéristiques essentiels ainsi que ses différents outils d'analyses, dans le but de concevoir un cryptosystème à base du chaos. Ce

deuxième chapitre servira également d'illustration des techniques de synchronisation des systèmes chaotiques.

Dans le troisième chapitre, nous présentons le système de communication complet, composé de l'émetteur, un système chaotique d'ordre entier dit circuit de Chua (un circuit électronique simple permet de générer le chaos) et à la réception un observateur à mode glissant étape par étape permet de reproduire les signaux chaotiques générés par l'émetteur et le message confidentiel. Ensuite, on donne les résultats de simulation pour les deux techniques de cryptage « addition » et « inclusion ».

Le dernier chapitre est consacré à l'étude d'un nouveau dispositif de transmission sécurisée, où nous allons introduire la dérivée fractionnaire au système de transmission étudié au chapitre précédent dans le but de renforcer la sécurité de la transmission.

Enfin, Nous terminons notre mémoire par une conclusion générale récapitulant nos principaux résultats et quelques perspectives.

1.1 Introduction

Les procédés de cryptage constituent un domaine en plein essor. En effet, les processus chargés de sécuriser des données sont au cœur de nombreuses technologies : qu'il s'agisse de communications avec des téléphones portables, de transmission de données chiffrées par l'intermédiaire de cartes bancaires, de sites internet…la cryptographie intervient constamment dans la vie quotidienne.

Nous proposons dans ce chapitre d'établir d'une manière globale un état de l'art sur la transmission sécurisée. L'intérêt se portera essentiellement sur le problème de la cryptographie. Il est en question, dans un premier temps, de donner quelques concepts et notions rencontrées dans la littérature concernant la théorie de l'information ainsi que la transmission de données, car une bonne sécurité de transmission nécessite la bonne compréhension de ces notions. Nous présentons par la suite les techniques de cryptage utilisées habituellement, celles basées sur une clé privée et celles basées sur une clé public.

1.2 Principe de la transmission de données

1.2.1 Définition

La transmission de données concerne toute communication d'un signal électromagnétique, que ce signal transporte l'information sous forme analogique (par des fonctions continues) ou numérique (par une succession de bits 0 et 1) [8].

Tout système de communication est constitué globalement de 3 éléments principaux : Un émetteur, un canal de transmission et un récepteur utilisés pour transmettre une information sur une certaine distance [8].

L'émetteur : il met en forme une information selon un codage donné, pour la préparer à la transmission.

Le récepteur : il permet de récupérer l'information transmise et de la décoder selon le même code que celui utilisé à l'émetteur.

Le canal de transmission : il sert à véhiculer l'information sur une certaines distance.

1.2.2 Canal de transmission

1.2.2.1 Définition

On appelle canal de transmission tout milieu physique servant de support au transfert de l'information entre deux points distants, une source et une cible [8] (figure 1.1)

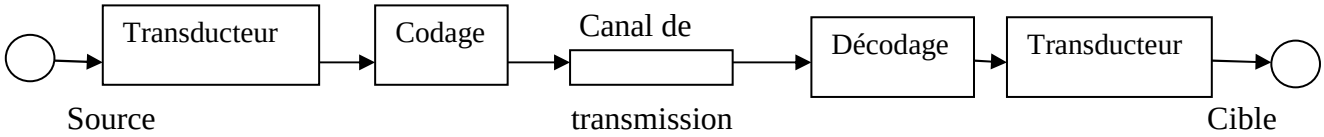


Fig.1.1 La schématisation d'un système de transmission.

1.2.3 Les supports de transmission

1.2.3.1 Transmission par lignes

On appelle ligne tout support physique de transmission constitué d'un milieu matériel fini. On appelle câble de transmission, tout support physique constitué d'un ensemble de lignes [8].

Exemples :

Câble téléphonique aérien, câble informatique, câble TV.

1.2.3.2 Transmission par ondes rayonnées [8]

Les ondes électromagnétiques rayonnées par une antenne se propagent dans l'atmosphère qui constitue un deuxième vecteur important dans la transmission de l'information.

a/ Antenne [8]

Les antennes de transmission permettent la propagation électromagnétique en milieu libre d'un point à un autre, sans la présence d'un câble.

b/ Guide d'ondes [8]

Lorsque la fréquence utilisée du signal à transmettre est très élevée, la transmission sur le support de type ligne devient impossible, en particulier du fait de la très forte atténuation qui en résulterait. Dans le domaine de hyperfréquences ou micro-ondes, c'est-à-dire pour des longueurs d'ondes métriques, centimétriques ou millimétrique, on a souvent recourt à des supports spécifiques appelés guides d'ondes.

c/ Fibre optique

En transmission, on utilise de plus en plus les fibres optiques. En effet, les ondes lumineuses possèdent de hautes fréquences, or la capacité de transport de l'information d'un signal augmente avec la fréquence. Un signal acheminé par fibres optiques peut parcourir de grandes distances avant qu'il ne soit nécessaire de le régénérer au moyen d'un répéteur.

Un système de transmission par fibre optique met en œuvre [18] :

-un émetteur de lumière (transmetteur), constitué d'une diode électroluminescente **LED** (*Light Emitting Diode*) ou d'une diode **LASER** (*Light Amplification by Stimulated of Radiation*), qui transforme les impulsions électriques en impulsions lumineuses.

-un récepteur de lumière, constitué d'une photodiode de type **PIN** (*Positive Intrisic Négative*) ou de type **PDA** qui traduit les impulsions lumineuses en signaux électriques.

-une fibre optique.

1.3 Les caractéristiques des réseaux de transmission

L'évolution des besoins et des applications informatiques conduit à transporter sur un même système physique des flux d'information de natures différentes. Afin de qualifier ces différents flux vis-à-vis du système de transmission, nous définirons brièvement les caractéristiques essentielles d'un réseau de transmission.

1.3.1 Notion de débit binaire [21]

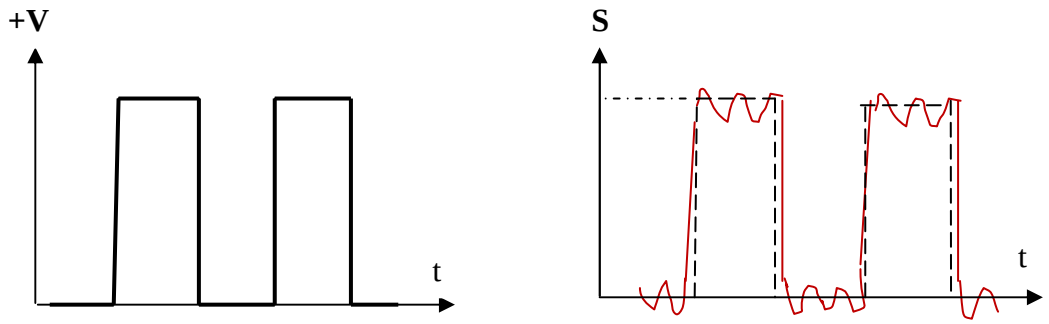
Les systèmes de traitement de l'information emploient une logique à deux états dite «binaire». Pour y être traitée, l'information doit être traduite en symboles compréhensibles et

manipulables par ces systèmes. Selon le type d'information à transformer, l'opération qui consiste à transformer les données en éléments binaires s'appelle le *codage* ou *numérisation*.

On appelle débit binaire (D) le nombre d'éléments binaires, ou nombre de bits, émis sur le support de transmission pendant une unité de temps. Le débit binaire est généralement la grandeur utilisée en premier pour qualifier un système de transmission.

1.3.2 Notion de rapport signal sur bruit [21]

Durant la transmission, les signaux électriques peuvent être perturbés par des phénomènes électriques ou électromagnétiques d'origine externe désignés sous le terme générique de *bruit*. Le bruit est un phénomène qui dénature le signal et qui est susceptible d'introduire des erreurs d'interprétation du signal reçu (figure 1.2).



Signal sans bruit Signal avec bruit

Fig.1.2 Le signal pollué par le bruit.

Les capacités de transport d'information (débit) sont directement liées au rapport entre la puissance du signal utile et celle du signal de bruit. Ce rapport, appelé rapport signal sur bruit (SNR, Signal Noise Ratio que nous noterons s_y/s_b), s'exprime en dB (décibel), formule dans laquelle s_y représente la puissance électrique du signal transmis et s_b la puissance du signal parasite ou bruit affectant le canal de transmission [21].

$$SNR = 20log_{10}(s_y/s_b) \text{ (En puissance)} \quad (1.1)$$

1.3.3 Notion d'erreur et de taux d'erreur [21]

Les phénomènes parasites (bruits) perturbent le canal de transmission et peuvent affecter les informations en modifiant un ou plusieurs bits du message transmis, introduisant ainsi des erreurs dans le message (figure 1.3).

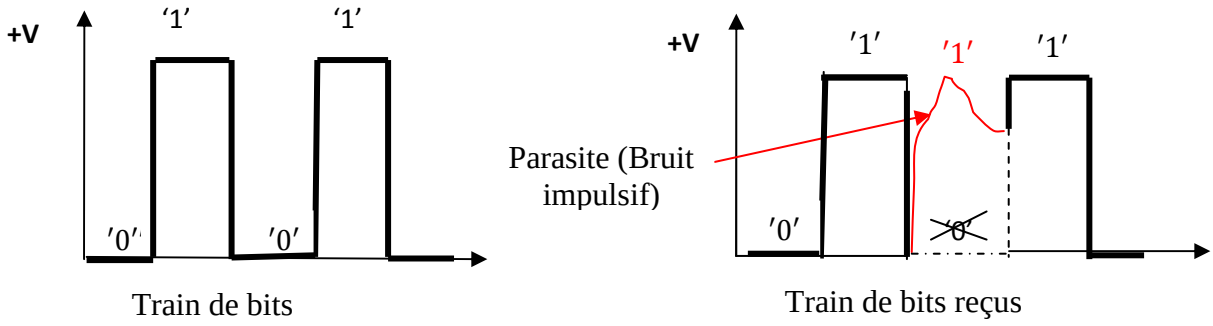


Fig.1.3 L'effet d'une erreur sur le train binaire.

On appelle taux d'erreur binaire Te le rapport du nombre de bits reçus en erreur au nombre de bits transmis.

$$Te = \frac{Nombre\ de\ bits\ en\ erreur}{Nombre\ de\ bits\ transmis}$$

1.3.4 Notion de temps de transfert

Le temps de transfert, appelé aussi temps de transit ou temps de latence, mesure le temps entre l'émission d'un bit, à l'entrée du réseau et sa réception en sortie de ce dernier. Ce temps prend en compte le temps de propagation sur le support et le temps de traitement [21].

1.3.5 Notion de spectre du signal

Le mathématicien français Joseph Fourier (1768-1830) a montré que tout signal périodique de forme quelconque pouvait être décomposé en une somme de signaux élémentaires sinusoïdaux (fondamental et harmoniques) superposée à une valeur moyenne (composante continue) qui pouvait être nulle. L'ensemble de ces composantes forme le spectre du signal ou bande de fréquence occupée par le signal (largeur de bande) [21].

1.4 Notions générales sur la cryptographie

1.4.1 Principe

L'origine du mot cryptographie provient du grec kryptós (caché) et gráfein (écrire). On peut définir la cryptographie comme l'ensemble des techniques permettant de protéger une communication. La cryptographie permet de correspondre de manière sécurisée en utilisant des canaux non sécurisés. Pour cela, une fonction de chiffrement est appliquée au message à transmettre et le résultat de ce chiffrement, appelé texte chiffré, pourra être transmis à l'autre entité qui connait comment déchiffrer ce texte chiffré afin d'obtenir le texte clair. Bien sûr, aucune information ne devra être dévoilée sur le texte clair si le texte chiffré tombe entre les mains de l'ennemi. Pour cela, les fonctions de chiffrement et de déchiffrement doivent rester secrètes. Pour des raisons pratiques, ces fonctions sont décomposées en algorithmes paramétrés par une clé. Le fonctionnement de ces algorithmes est public et seule la valeur des clés est tenue secrète.

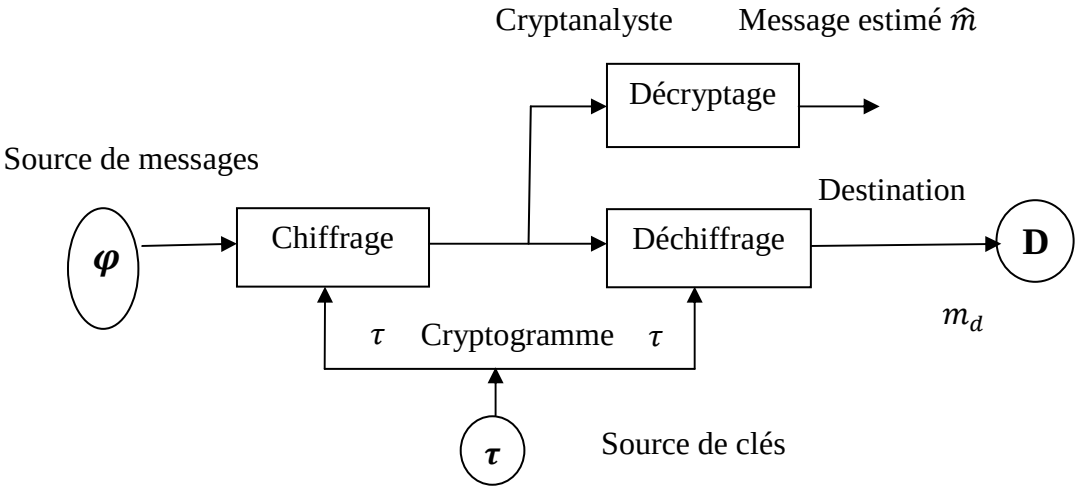


Fig.1.4 Schéma général du chiffrage.

Le texte en clair est noté m, c'est le message à chiffrer. Il peut être un texte, un enregistrement de voix numérisé, ou une image. De toute façon m n'est rien d'autre que de l'information binaire, comme il peut être transmis ou stocké. Le texte chiffré est noté m_c. C'est aussi de l'information binaire, parfois de la même taille que m, parfois plus grand. Les deux fonctions de chiffrement et déchiffrement sont notées respectivement F_c (pour chiffrer)

et F_d (pour déchiffrer). La fonction de chiffrement F transforme m en m_c, ce qui sera notée mathématiquement

$$F_c(m) = m_c \tag{1.2}$$

1.4.2 Quelques définitions et concepts

- *Message clair*: désigne le message original n'ayant pas subi aucune modification.
- Message chiffré: désigne le message ayant subi le chiffrement.
- *Chiffrer* (crypter) : c'est transformer un texte clair en texte codé. L'opération ou son résultat s'appelle un chiffrement.
- *Déchiffrer* : c'est traduire en clair en connaissant la clé. C'est donc le destinataire légitime du message qui déchiffre.
- *Décrypter, cryptanalyser* : c'est traduire un texte en clair en ne connaissant pas la clé. L'opération ou son résultat s'appelle un décryptement.
- *Cryptographie :* Discipline incluant les principes, les moyens et les méthodes de transformation des données, dans le but de masquer leur contenu, d'empêcher leur modification ou leur utilisation illégale.
- *Stéganographie :* contrairement à la cryptographie, la sténographie (en grec « écriture couverte » est l'art de dissimuler un message par l'intermédiaire d'un autre.
- *Cryptanalyse :* est l'art de déchiffrer un message dans le but de le rendre compréhensible.

1.4.4 Les objectifs de la sécurité

De nos jours, la cryptographie consiste à mettre au point les systèmes cryptographiques afin d'assurer les piliers suivant [10] :

1. La confidentialité des données : il s'agit de s'assurer que l'information ne s'ébruite pas en dehors des personnes autorisées à l'obtenir, cela revient à garantir l'identité du destinataire.

2. L'authentification : il s'agit de s'assurer que les interlocuteurs sont bien ceux qu'ils prétendent être, cette fois cela revient à garantir l'identité de l'expéditeur.

3. La non-répudiation : il s'agit de s'assurer qu'un contrat ne peut être remis en cause par l'une des parties. Cela rejoint un peu le point précédent : on doit prouver la participation d'un interlocuteur dans un échange de données.

4. L'intégrité des données : il s'agit de s'assurer que les données ne subissent aucune altération ou destruction volontaire ou accidentelle. D'un point de vu cryptographique, on cherche à vérifier que les données n'ont pas été modifiées.

1.4.5 Cryptanalyse et attaques sur les systèmes cryptographiques

1.4.5.1 Les grands types de menaces [7]

Toute communication sur un canal de transmission peut être soumise à deux types d'attaques, selon qu'elles ne modifient pas les informations transmises (menaces passives) ou qu'elles perturbent le fonctionnement du réseau (menaces actives).

1. Les menaces passives : Dans ce cas, le tiers se contente d'écouter le message. Cette attaque, menace la confidentialité du message. Une information sensible parvient à une autre personne que son destinataire légitime.

2. Les menaces actives : là, le tiers peut modifier le contenu des messages échangés, ce qui menace l'intégrité de l'information. L'information reçue est interprétée comme provenant d'une personne autre que son véritable auteur.

1.4.5.2 Les attaques sur un chiffrement [7]

La cryptanalyse concerne l'étude de la sécurité des procédés de chiffrement utilisés en cryptographie. On distingue quatre niveaux d'attaque :

1. texte chiffré connu : le cryptanalyste dispose du texte chiffré de plusieurs messages, tous ayant été chiffrés avec la même clé. La tache du cryptanalyste est de retrouver le plus grand nombre de messages clairs possibles, ou mieux encore de retrouver la ou les clés qui ont été utilisées, ce qui permettrait de déchiffrer d'autres messages chiffrés avec ces mêmes clés.

2. texte clair connu : le cryptanalyste a non seulement accès aux textes chiffrés de plusieurs messages, mais aussi aux textes clairs correspondants. La tache est de retrouver la ou les clés qui ont été utilisées pour chiffrer ces messages ou un algorithme qui permet de déchiffrer d'autres messages chiffrés avec ces mêmes clés.

3. texte clair choisi : le cryptanalyste a non seulement accès aux textes chiffrés et aux textes clairs correspondants, mais de plus il peut choisir les textes en clair. Cette attaque est plus efficace que l'attaque à texte clair connu, car le cryptanalyste peut choisir des textes en clair spécifiques qui donneront plus d'informations sur la clé.

4. texte chiffré choisi : le cryptanalyste peut choisir différents textes chiffrés et obtenir les textes déchiffrés associés.

1.5 Classification des algorithmes de chiffrement

Si le but traditionnel de la cryptographie est d'élaborer des méthodes permettant de transmettre des données de manière confidentielle, la cryptographie moderne s'attaque en fait plus généralement aux problèmes de sécurité des communications. Le but est d'offrir un certain nombre de services de sécurité (1.4.4). Pour cela, on utilise un certain nombre de mécanismes basés sur des algorithmes cryptographiques. Nous allons voir dans cette partie quelles sont les techniques que la cryptographie fournit pour réaliser ces mécanismes.

1.5.1 Chiffrement classique

1.5.1.1 Chiffrement par substitution [7]

Un « chiffrement par substitution » est un algorithme par lequel chaque caractère du message clair est substitué par un autre caractère dans le message.

En cryptographie classique, quatre types de chiffrement par substitution sont distingués :

- Les substitutions **mono-alphabétiques** (simples) : Chaque lettre est remplacée par une lettre ou un autre symbole. De nos jours, les substitutions simples ne sont plus utilisées que pour les rubriques des journaux.
- Les substitutions **poly-alphabétiques** (à double clé ou à alphabet multiples) : Elles utilisent plusieurs 'alphabets', ce qui signifie qu'une même lettre peut être remplacée par plusieurs symboles.
- Les substitutions **polygrammiques** (aussi appelées polygraphiques) : les lettres ne sont pas chiffrées séparément, mais par groupes de plusieurs lettres (deux ou trois généralement).
- Les substitutions **tomogrammiques** (aussi appelées par fractions de lettres) : Chaque lettre est tout d'abord représentée par des groupes de deux ou plusieurs symboles, qui sont ensuite chiffrés séparément par substitution ou transposition.

1/ Un exemple historique de substitutions simple : *le chiffrement de César*

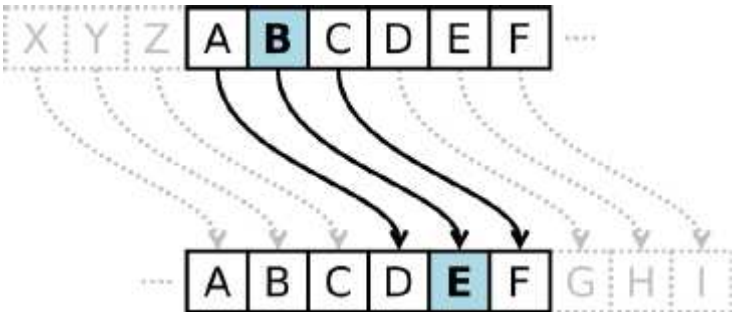


Fig.1.5 décalage de César.

Le code de César est la technique cryptographique la plus ancienne communément admise par l'histoire. Ce code repose sur une simple substitution mono alphabétique, où la substitution est en fait un décalage de lettres.

Ainsi si on choisit un décalage de trois lettres, on obtient :

Texte clair	A	U	T	O	M	A	T	I	Q	U	E
Texte codé	D	X	W	R	P	D	W	M	U	T	H

Tab.1.1 Chiffrement de César utilisant un décalage de 3.

1.5.1.2 Chiffrement par transposition [7]

Le chiffrement par transposition consiste à appliquer une permutation des caractères sur le message clair en entier. Tel que le message chiffré est fait du même matériel que le message clair. Ce chiffrement est de type anagramme, il consiste à modifier l'ordre des caractères du message clair.

On divise le message $\boldsymbol{m}$ en blocs de longueur $\boldsymbol{d}$, puis on prend une permutation **I** de 1, 2 ,3….d et $\boldsymbol{f_I}$ la permutation sur I. La clé de l'algorithme est donnée par la paire $\boldsymbol{\tau} = (d\,, f_I)$. Les blocs successifs de d caractères du message m sont chiffrés en permutant les caractères selon la transformation *f*.

Exemple: On cherche le texte chiffré du message « GENIE ELECTRIQUE », en prenant $d = 5$ et $f_I(i) = 2\ 5\ 3\ 1\ 2$ on obtient le tableau suivant.

Texte clair	G	E	N	I	E	E	L	E	C	T	R	I	Q	U	E
$f_I(i)$	2	5	3	1	2	2	5	3	1	2	2	5	3	1	2
Texte chiffré	E	E	N	G	E	E	T	E	E	L	I	E	Q	R	I

Tab.1.2 Chiffrement par transposition.

Pour de très brefs messages, comme un simple mot, cette méthode est peu sûre car il n'y a beaucoup de variantes. Bien entendu, lorsque le nombre de lettres croît, le nombre d'arrangements augmente rapidement et il devient quasiment impossible de retrouver le texte original sans connaître le procédé de brouillage. Pour notre exemple, les 15 lettres de « GENIE ELECTRIQUE » peuvent être disposées de $15! = 1307674368000$ manières.

1.5.2 Le chiffrement actuel

On distingue deux grands types d'algorithmes de chiffrement moderne, les algorithmes à clé secrète et les algorithmes à clé public. Chacune de ces deux classes possède ses propres avantages et inconvénients, une approche mathématique simple permet de les différencier [4].

1.6.2.1 Le chiffrement symétrique

Le chiffrement à clé secrète, encore appelé chiffrement symétrique ou chiffrement conventionnel : c'est le type de chiffrement le plus répandu. Où les clés de chiffrement et de déchiffrement sont identiques ou facilement déductibles l'une de l'autre, connues uniquement par l'émetteur et le destinataire. L'algorithme est quant à lui public et la confidentialité du message échangé repose uniquement sur le secret de la clé partagée [9].

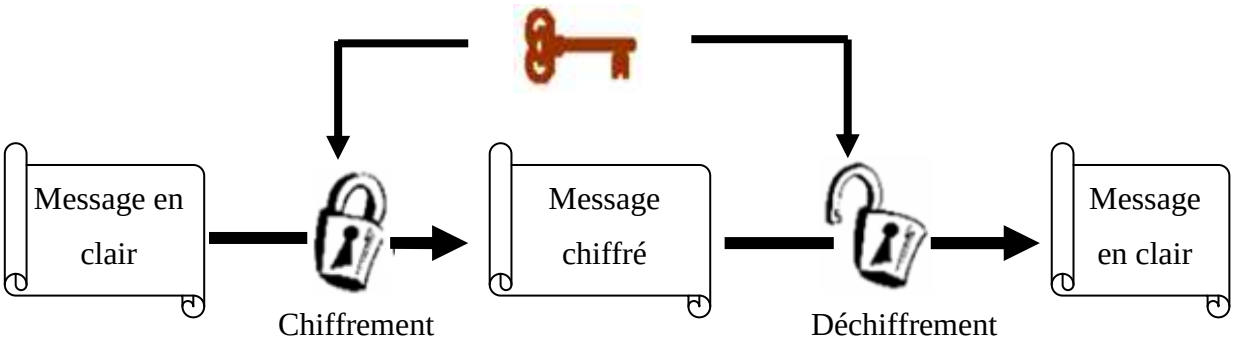


Fig.1.6 Schéma général du chiffrement symétrique

La cryptographie symétrique fait face à deux principaux problèmes. Le premier est celui du partage préalable de la clé entre l'entité qui chiffre et l'entité qui déchiffre. Comme la clé ne doit être connue de personne d'autre, cette transmission doit donc être faite de manière sécurisée. Le second problème est celui de la gestion des clés. En effet dans un système de n personnes, nous avons $n\,(n-1)\,/2$ clés à gérer (c.-à-d. une clé par couple de personnes), nous avons donc un nombre de clés qui évolue au carré par rapport au nombre de personnes. Malgré ces inconvénients, ce type de système a l'avantage, pour des raisons algorithmiques,

d'être extrêmement rapide (comparativement à sa contrepartie à clé public) à un moindre coût, permettant d'atteindre des débits de l'ordre de centaines de mégabits par seconde.

Il existe deux types d'algorithmes de chiffrement symétrique. Le premier type, qui est aussi le plus utilisé en pratique, est le chiffrement par blocs. Dans ce mode, les données sont traitées par bloc de bits, typiquement 64 ou 128 bits. Le second type est le chiffrement par flux. Ce type de chiffrement permet, après une période d'initialisation, de chiffrer bit par bit. Cette seconde méthode est plus rapide que le chiffrement par blocs car il n'y a pas besoin d'attendre la répétition d'un grand nombre de bit pour agir, dès que l'on reçoit un bit de message, on le chiffre.

Nous allons maintenant présenter plusieurs systèmes conventionnels à clé secrète. Dans la suite de cette partie, nous allons décrire les deux cryptosystèmes symétriques les plus utilisés en pratique, les DES et l'AES.

a/ Système de chiffrement par blocs (Block Cipher)

Ranier Ruppel définit la différence entre le chiffrement par blocs et par flux de la manière suivante : « Les systèmes de chiffrement par blocs agissent sur des données avec une transformation fixe des grands blocs de données en clair, les systèmes de chiffrement par flux agissent avec une transformation variant avec le temps des chiffres en clair individuels »

Aujourd'hui les nouveaux algorithmes de chiffrement par blocs peuvent être chainés (appelés de manière successive) et, dans ce cas, si l'on considère des blocs de très petite taille (par exemple 1), les deux systèmes de chiffrement se confondent. Les seules différences qui demeurent sont l'aspect contextuel du chiffrement par bloc, la facilité d'implémentation matérielle (hardware) des algorithmes de chiffrement par flux et les performances logicielles des algorithmes par bocs (*les processeurs travaillant aussi par blocs*) [7].

Le chiffrement par blocs est plus répandu et joue d'une meilleure réputation que le chiffrement par flux. En effet, mathématiquement, le chiffrement par flux est plus facile à analyser, ce qui facilite la cryptanalyse.

Le schéma général du chiffrement par blocs est le suivant :

1) coder l'information source en binaire. On obtient ainsi une chaine composé de 0 et de 1.

2) découper cette chaine en blocs de longueur donnée, par exemple 32 ou 64 bits.
3) chiffrer un bloc en faisant un OU Exclusif (XOR) bit par bit à une clé secrète qui est une suite binaire.

4) déplacer et permuter certains bits du bloc.

5) recommencer éventuellement un certain nombre de fois l'étape précédente.

6) passer au bloc suivant et retourner à l'étape 3 jusqu'à ce que tous les blocs soient chiffrés.

b/ Système de chiffrement par flux [7]

Les algorithmes de chiffrement par flux peuvent être définis comme étant des algorithmes de chiffrement par blocs, où le bloc a une dimension unitaire (1 bit, 1 octet, etc.) ou relativement petite. Leurs avantages principaux viennent du fait que la transformation (méthode de chiffrement) peut être changée à chaque symbole du texte clair et du fait qu'ils soient extrêmement rapides. De plus, ils sont utiles dans un environnement où les erreurs sont fréquentes car ils ont l'avantage de ne pas propager les erreurs. Ils sont aussi utilisés lorsque l'information ne peut être traitée qu'avec de petites quantités de symboles.

c/ Algorithme de chiffrement DES (Data Encryption Standard)

En 1973, le NIST (National Institute of Standards and Technology) adopte le standard de chiffrement DES. Ce chiffrement conçu par IBM sous le nom de LUCIFER a été choisi par le NIST après quelques petites modifications, cet algorithme deviendra officiellement le DES approuvé en novembre 1976 et publié comme standard en en janvier 1977 [5].

c.1/ Description

Ce chiffrement symétrique permet de chiffrer des messages de 64 bits avec une clé τ de 56 bits. Pour chiffrer un texte, il faut d'abord le découper en blocs de 64 bits puis appliquer le chiffrement sur chacun des blocs. Ce chiffrement est constitué de 16 enchainements successifs d'opérations de transposition et de substitution. Les avancées matérielles en informatique permettent aujourd'hui, en un temps raisonnable de « casser » un message

chiffré avec DES par « force brute », en testant toutes les clés possibles grâce à une énumération exhaustive. En 1998, la NIST lança un appel d'offre pour choisir, l' « Advanced Encryption Standard »(AES), le successeur du DES, devenu trop sensible aux attaques par recherches exhaustives [5].

d/ Algorithme de chiffrement AES (Advanced Encryption Standard)

Le standard de chiffrement AES fut adopté en 2000 par le NIST en remplacement du DES. Ce chiffrement est constitué de substitutions, de décalage, de « ou exclusif » et de multiplications dans un corps fini de polynômes fixés ; ces opérations sont élémentaires, simples et rapides à calculer. Il permet de crypter des blocs de128, 192 ou 256bits en utilisant des clés symétriques de 128, 192 ou 256 bits. Le choix de la taille de la clé et de la taille des blocs sont indépendants, il y a donc au total 9 combinaisons possibles. Ceci laisse une grande flexibilité à l'utilisateur d'AES en fonction du niveau de sécurité et de la vitesse de calcul désirés [5].

De tels systèmes ont l'avantage principal d'être efficaces en termes de temps de calcul, tant pour le chiffrement que pour le déchiffrement. En revanche, la faiblesse de ce système vient du secret absolu qui doit entourer la clé. Si le tiers parvient par un moyen quelconque à obtenir cette clé, il pourra déchiffrer tous les messages échangés entre deux interlocuteurs.

1.5.2.2 Le chiffrement asymétrique

D'un point de vue pratique, la cryptographie symétrique présente un inconvénient majeur lié à la gestion des clés utilisées. Pour que deux interlocuteurs puissent communiquer de manière confidentielle, il leur est nécessaire de convenir au préalable d'une valeur secrète de clé [9].

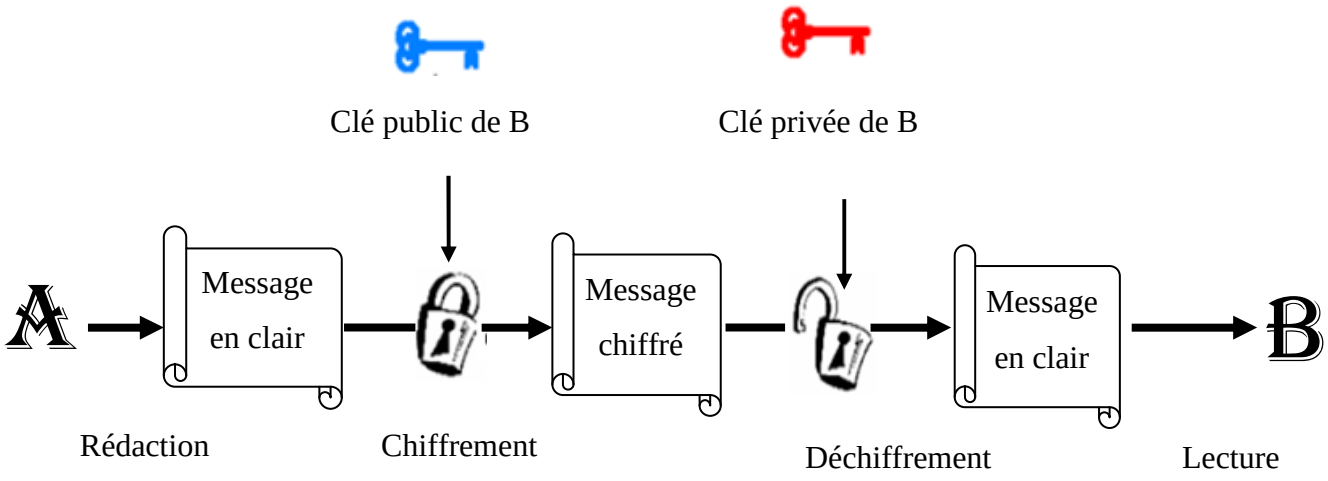


Fig.1.7 Schéma général du chiffrement asymétrique.

Comment partager préalablement le secret entre les deux entités qui vont correspondre de manière sécurisée ? Cette question est sans aucun doute à l'origine de la cryptographie asymétrique. Le concept de cryptographie asymétrique, aussi appelée cryptographie à clé public, est apparu officiellement en 1976 dans le célèbre article de Whitfield Diffie et Martin Hellman, New Directions in Cryptography. Dans un tel système, la clé de chiffrement est connue et la clé de déchiffrement est bien sûr tenue secrète. Dans la plupart des cas, c'est le destinataire qui choisit sa clé de déchiffrement (privée) et utilise une fonction à trappe pour calculer sa clé de chiffrement (public). Cette dernière est connue à toutes les personnes susceptibles de communiquer avec lui.

Les fonctions à trappe utilisées dans la cryptographie asymétrique reposent sur des problèmes mathématiques réputés difficile comme la factorisation des grands nombres. Cependant, l'utilisation de ces problèmes mathématiques implique que les algorithmes de chiffrement à clé public sont beaucoup plus lents que ceux à clé secrète, d'une part à cause de la complexité des opérations mises en jeux mais aussi à cause de la longueur des clés utilisées (d'ordre 2048 bits).

Ceci implique en particulier que la cryptographie à clé public et la cryptographie à clé secrète sont souvent combinées en pratique, la première servant à transmettre la clé qui sera utilisée par la seconde pour effectuer le chiffrement des données à transmettre.

En 1978, Ronald Rivest, Adi Shamir et Leonard Adleman ont proposés le premier exemple de cryptosystèmes à clé publique, appelé RSA du nom de ses inventeurs, qui est sans aucun doute le cryptosystème le plus connu et probablement le plus utilisé dans le monde **[9].**

a/Algorithme de chiffrement *RSA* [5]

Le *RSA* est le premier cryptosystème de chiffrement utilisé en pratique. La sécurité du *RSA* repose sur la difficulté supposée du problème de la factorisation d'entiers.

Plusieurs autres cryptosystèmes à clé public sont apparus après, qui reposant sur d'autres problèmes difficiles.

La génération d'une clé RSA se fait de la manière suivante. Le couple (η, υ) constitue la clé public et (ϑ, η) la clé privée tel que $\eta = \varrho\sigma$ ou ϱ et σ sont deux nombres premiers, $\upsilon\epsilon\{2, \ldots., (\varrho - 1)(\sigma - 1)\}$ et ϑ est calculée tel que $\upsilon\vartheta = 1\, mod(\varrho - 1)(\sigma - 1)$ Pour chiffrer par l'algorithme *RSA* un message m de taille inférieure à n avec la clé public (η, υ) nous calculons :

$$\{\mathrm{m}\}_{(\eta,\upsilon)} = m^{\upsilon}\ mod\ \eta \tag{1.3}$$

Pour retrouver le message original m à partir d'un message chiffré $m_c = \{m\}_{(\eta,\upsilon)}$ nous calculons :

$$m = (m_c)^{\vartheta}\ mod\ \eta \tag{1.4}$$

La connaissance de η donne théoriquement accès à ϱ et σ qui sont par définition les facteurs premiers de η.

La force de la technique *RSA* repose sur l'extrême difficulté à factoriser de grands nombres. Mais le développement de la puissance de calcul des ordinateurs améliore sans cesse les temps de factorisation.

Le choix d'une longueur de clé (la taille de η) est directement lié au niveau de confidentialité recherché. En contrepartie, l'algorithme *RSA* est très lent, ce qui n'est guère pratique pour les fichiers volumineux : de plus la clé est grande, plus le processus de cryptage et de décryptage sont longs. Cette technique est réservée aux messages cours [10].

1.5.2.3 Avantages et inconvénients des chiffrements symétriques et asymétriques

Nous comparons ces deux types de chiffrements qui sont complémentaires et omniprésents dans les protocoles cryptographiques modernes.

Le chiffrement symétrique est plus rapide à calculer et utilise des clés de tailles plus petites qu'un chiffrement asymétrique. De plus, il est basé sur des fonctions mathématiques simples donc la facilité d'implémentions matérielle. Par contre, pour chaque communication avec chaque participant, une clé différente est nécessaire. Il faut donc gérer la distribution d'un grand nombre de clés, sachant que la divulgation de la clé serait catastrophique pour la sécurité de la communication.

La distribution de clés publics est très simple à gérer avec ce genre de chiffrement. De plus, cette méthode de chiffrement utilise des clés de grandes tailles et nécessite un temps de calcul plus long et plus de ressources que lors d'un chiffrement symétrique, ceci à cause de la complexité des opérations à effectuer.

En pratique les cryptosystèmes à clé public sont sensiblement moins rapides que les fonctions de chiffrement symétrique. Ils ne sont donc généralement pas utilisés pour chiffrer-déchiffrer de gros documents, mais plutôt pour échanger de manière sécurisée une clé de chiffrement symétrique. Chiffrer cette clé par un algorithme à clé publique ne sera pas pénalisant puisque c'est une donnée de petite taille, et une fois cette clé échangée avec son interlocuteur il sera possible d'utiliser un algorithme de chiffrement par bloc rapide (l'*AES* par exemple) pour chiffrer un volume important de données [5].

Vu les inconvénients présentés par ces algorithmes de cryptages, les chercheurs essayent de mettre en œuvre d'autres techniques de chiffrement pour améliorer le niveau de sécurité. Dans la suite de ce mémoire, nous présentons d'autres méthodes de cryptage basées sur la synchronisation de système dynamique chaotique, où la sécurité de la transmission se base sur la complexité du système choisi. Ce compromis va s'exprimer dans toutes les techniques que nous présentons aux chapitres suivants.

1.6 Conclusion

Ce chapitre avait comme objectif, la représentation de quelques notions de base sur la théorie et les techniques habituellement utilisées pour résoudre des problématiques de la transmission sécurisée.

Dans un premier temps et sans entrer dans les détails, on a présenté quelques principes de la transmission sécurisée qui se fait au travers de deux fonctions de base : la théorie de l'information qui a pour rôle de mieux transmettre l'information en évitant toute dégradation (bruit et perturbation) et la cryptographie qui consiste à mettre en œuvre les méthodes et les moyens permettant de protéger une communication. Une classification des méthodes de chiffrement a été donné, deux approches ont été distinguées à clé privée et à clé public, où chaque algorithme à présenter ses avantages et ses inconvénients.

2.1 Introduction

Les systèmes dynamiques étranges (chaotiques) sont depuis longtemps connus dans le domaine des mathématiques mais c'est seulement au cours de la dernière décennie que les applications concrètes se sont multipliées en physique, chimie, l'astronomie, biologie, médecine et la transmission sécurisée de l'information par la résolution de problèmes relatifs à la synchronisation de systèmes chaotiques [6]. Notre étude se focalise sur l'usage du chaos pour la transmission sécurisée de données.

Dans les différents paragraphes qui suivent sont présentées certaines définitions utiles à la compréhension du chaos, au sens de la théorie du chaos et des systèmes dynamiques non linéaires. Celles-ci ne sont abordées que comme des notions nécessaires à la compréhension sans rentrer dans les détails mathématiques. Par la suite, nous introduisons quelques définitions concernant la synchronisation des systèmes chaotiques. En effet, la synchronisation joue un rôle primordial dans les schémas de communication.

2.2 Quelques définitions sur les systèmes dynamiques

D'une manière générale, un système dynamique décrit des phénomènes qui évoluent au cours du temps. Le terme « système » fait référence à un ensemble de variables d'état (dont la valeur évolue au cours du temps) [19].

2.2.1 Représentation mathématique des systèmes dynamiques

Mathématiquement, Un système dynamique (discret ou continu) est décrit par une fonction mathématique qui 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. Ces fonctions lient les grandeurs qui caractérisent le système et qui sont, les grandeurs d'entrées, les grandeurs de sorties, et les variables d'états [19].

2.2.1.1 Représentation par des équations différentielles-Systèmes continus [2]

Un système dynamique continu est généralement décrit par un système d'équations différentielles de type :

$$\dot{x} = f(x, u, t) \tag{2.1}$$

où : $x \in X \subseteq \mathbb{R}^n$ est l'état du système, $u \in U \subseteq \mathbb{R}^p$ représente l'entrée du système f est une fonction non linéaire de l'état. U est le vecteur des paramètres.

En temps continu, on définit le système autonome comme une dynamique qui ne dépend pas de l'instant t.

$$\dot{x} = f(x, u) \tag{2.2}$$

2.2.1.2 Fonctions itératives – Systèmes discrets [19]

Les systèmes dynamiques discrets sont généralement décrits par la relation suivante appelée récurrence ou équation aux récurrences:

$$x_{n+1} = f\ (x_n, u_n, n) \tag{2.3}$$

où $x\ \in\ \mathbb{R}^n$ est le vecteur d'état et $u\ \in\ \mathbb{R}^p$ est un vecteur paramètre. x_{n+1}est appelé image ou conséquent de rang 1 de x_n par f et x_n est un antécédent de x_{n+1}.
$x(\ n = 0) =\ x_0$ est appelé condition initiale.

En temps discret, on définit aussi le système autonome comme une dynamique qui ne dépend pas de l'instant n.

$$x_{n+1} = f(\ x_n\ , u_n\ ) \tag{2.4}$$

Dans ce qui suit, nous allons donner uniquement quelques notions sur les systèmes continus.

2.2.2 Définitions

Définition 2.1 *(Système autonome) Un système dynamique non linéaire est dit autonome lorsqu'il ne dépend pas explicitement du temps initial. 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.

Définition 2.2 *(Trajectoire) Si l'on observe l'ensemble des différents états successifs de l'espace d'état, on peut remarquer l'émergence d'une trajectoire dans cet espace. Cette trajectoire est également appelée orbite du système [10].*

Définition 2.3 *(Espace des phases) Un système dynamique est caractérisé par un certain nombre de variables d'état, qui ont la propriété de définir complètement l'état du système à un instant donné. Le comportement dynamique du système est ainsi relié à l'évolution de chacune de ses variables d'état au cours du temps. Pour représenter l'état de ce système, on utilise couramment en physique un espace de dimension N, où N est le nombre de variables d'état. Cet espace est appelé « espace des phases » : chaque point définit un état différent du système [19].*

Définition 2.4 *(Point fixe ou point d'équilibre) On appelle point fixe ou point d'équilibre du système (2.1), le point x_0 tel que* :

$$f(x_0) = 0 \tag{2.5}$$

Dans le cas des systèmes non linéaires, on peut avoir $x_0 \neq 0$ et il peut avoir plusieurs points d'équilibre.

Définition 2.5 *(Cycle limite) Un système non linéaire peut être un siège d'oscillations, auto-soutenues caractérisées par leur amplitude et leur période fixe, indépendantes de la condition initiale x_0, et sans excitation extérieure. Ce siège est appelé cycle limite.*

Définition 2.6 (*attracteur*) *Un attracteur dans l'espace des phases est un objet géométrique vers lequel tendent un ensemble de trajectoires des points de cet espace, c'est-à-dire une situation ou un ensemble de situations vers lesquelles évolue un système dynamique, pour un ensemble des conditions initiales. On peut avoir plusieurs attracteurs dans un même espace des phases. Il existe deux types d'attracteurs : les attracteurs réguliers (le point fixe, le cycle limite, le tore) et les attracteurs étranges (chaotiques)* [19].

2.3 Quelques notions sur le chaos

L'étude théorique approfondie du chaos est loin d'être l'objectif de ce travail de mémoire. Dans cette section, nous nous limitons à définir brièvement le phénomène chaotique apparaissant dans un système non linéaire dynamique déterministe.

2.3.1 Définition du chaos

Quelques systèmes physiques se comportent de manière chaotique. Parmi ces systèmes, on peut citer l'atmosphère, un robinet qui goutte, un pendule excité dans un champ magnétique, le rythme cardiaque [12]. Ces quelques systèmes se démarquent par leurs dimensions et l'origine de leurs mouvements. Il existe plusieurs définitions possibles du chaos. Ces définitions ne sont pas toutes équivalentes, mais elles convergent vers certains points communs caractérisant ainsi le chaos.

Définition 2.7 *On appelle chaotiques des phénomènes complexes, dépendant de plusieurs paramètres et caractérisés par une extrême sensibilité aux conditions initiales [4].*

Remarque 2.1 *Il est à noter que les systèmes linéaires ne possèdent jamais de comportement chaotique, et les phénomènes chaotiques que l'on observe sont souvent dus aux non linéarités que présentent les systèmes, dans des domaines très variés : mécanique, circuits électroniques, réactions chimiques, processus biologiques et systèmes de sécurité de l'information.*

2.3.2 L'histoire du chaos déterministe

En 1963 le météorologue Edward Lorenz expérimentait une méthode lui permettant de prévoir les phénomènes météorologiques. 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. [16].

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 XIX^{e} siècle le mathématicien, physicien et philosophe français Henri Poincaré [1954-1912]

avait déjà mis en évidence le phénomène de sensibilité aux conditions initiales lors de l'étude astronomique du problème des trois corps. On trouve dans le calcul des probabilités d'Henri Poincaré l'affirmation suivante [6] :

« *Une cause très petite, qui nous échappe, détermine un effet considérable que nous ne pouvons pas ne pas voir, et alors nous disons que cet effet est dû au hasard. Si nous connaissions exactement les lois de la nature et la situation de l'univers à l'instant initial, nous pourrions prédire exactement la situation de ce même univers à l'instant ultérieur… une petite erreur sur les premières produirait une erreur énorme sur les derniers. La prédiction devient impossible et nous avons le phénomène fortuit* ».

Henri Poincaré, 1908

Cette citation définit parfaitement le chaos en tant que sensibilité aux conditions initiales mais aussi le déterminisme qui réside dans le fait que si une condition initiale est parfaitement déterminée alors l'évolution du système l'est aussi.

Toujours au XIX^{e} siècle, le mathématicien russe Alexandre Lyapunov effectue des recherches sur la stabilité du mouvement. Il introduit l'idée de mesurer l'écart entre deux trajectoires ayant les conditions initiales voisines, lorsque cet écart évolue exponentiellement on parle de sensibilité aux conditions initiales. Les travaux de Lyapunov, d'abord tombés dans l'oubli, seront plus tard très précieux pour étudier certains aspects de la théorie du chaos.

Les travaux des prédécesseurs de Lorenz ont donc été très importants pour la compréhension du chao déterministe, mais ce qui a permet une étude plus importante du chaos c'est l'ordinateur. En effet, les équations régissant un système chaotique sont nécessairement non linéaires et, sans ordinateur, leur résolution est en général impossible.

Ensuite, Stephen Smale étudia un système dynamique dont le comportement peut s'illustrer par un repliement et un étirement de l'espace des phases, et qui donna une figure ressemblant des comportements très complexes mais ordonnés sur une structure particulière qu'ils nommèrent *attracteur étrange* (1971). Enfin, le mot chaos d'origine grecque, devient un terme scientifique depuis un article « Period three implies chaos » de James Yorke et Tien-Yien Li publié dans une revue de mathématiques en 1975 [6].

2.4 Caractéristiques essentielles du chaos

2.4.1 Déterminisme

Il existe une démarche pour comprendre ou prévoir un phénomène réel. Cette démarche consiste à construire un modèle mathématique qui établit une relation entre un ensemble de causes et un ensemble d'effets. Autrement dit, à partir de conditions initiales connues, le modèle permet de prévoir l'évolution d'un système au cours du temps. La notion de déterminisme est ainsi intrinsèquement liée à tous les systèmes dont l'évolution est définie par un ensemble d'équations différentielles [2].

Durant ces 40 dernières années, des chercheurs ont réussi à mettre les systèmes chaotiques en équation et remarqué qu'il existe un côté déterministe dans ce qui paraît être à première vue aléatoire. Bien que ses équations définissent complètement son évolution, il est imprédictible à long terme. Cette non prédictibilité à long terme provient du fait que les systèmes chaotiques sont très sensibles aux conditions initiales [16].

Depuis la découverte des phénomènes chaotiques la prévisibilité n'est plus systématiquement liée au déterminisme.

2.4.2 La sensibilité aux conditions initiales

La sensibilité aux conditions initiales est une caractéristique fondamentale des systèmes dynamiques chaotiques, qui été découverte par Lorenz, c'était une explication scientifique de « l'effet papillon ».

La citation de Lorenz lors d'un congrès international

« *Le battement d'aile d'un papillon, aujourd'hui à Brésil, engendre dans l'air des remous qui peuvent se transformer en tempête le mois prochain à Texas* »

Edward Lorenz (Brésil 1963)

En effet, deux trajectoires de phases initialement voisines s'écartent toujours l'une de l'autre, et ceci quelle que soit leur proximité initiale. Il est en particulier clair que la moindre erreur ou simple imprécision sur la condition initiale interdit de décider à tout temps quelle sera la trajectoire effectivement suivie et, en conséquence, de faire une prédiction autre que

statistique sur le devenir à long terme du système. Ainsi, bien que l'on traite de systèmes déterministes, il est impossible de prévoir à long terme leurs comportements [26].

Illustrons ce phénomène de SCI (sensibilité aux conditions initiales) par une simulation numérique effectuée sur le système chaotique de Lorenz modélisé par les équations suivantes :

$$\begin{cases} \dot{x}_1 = -10x_1 + 10x_2 \\ \dot{x}_2 = 28x_1 - x_2 - x_1x_3 \\ \dot{x}_3 = x_1x_2 - (8/3)\,x_3 \end{cases} \tag{2.6}$$

On affecte à ce système chaotique deux conditions initiales très proches. Dans un premier temps, les deux systèmes évoluent de la même manière ; mais, très vite, leur comportement devient différent. Ceci est illustré à la figure suivante.

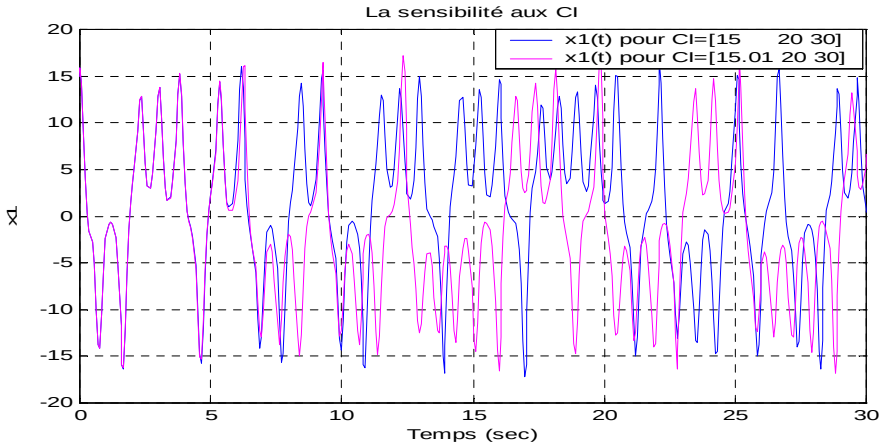


Fig.2.1 Evolution dans le temps pour deux conditions initiales très proches.

2.4.3 Le caractère pseudo aléatoire

La courbe précédente (Figure 2.1) illustre la sensibilité aux conditions initiales. Cependant, une autre caractéristique des systèmes chaotiques peut être observée sur la courbe précédente. En effet, un système chaotique évolue d'une manière qui semble aléatoire.

La courbe suivante permet de comparer une évolution simple $y(t) = 18\sin 5t$, périodique et donc prédictible d'un système classique avec l'évolution plus complexe, non périodique et non prédictible du système de Lorenz.

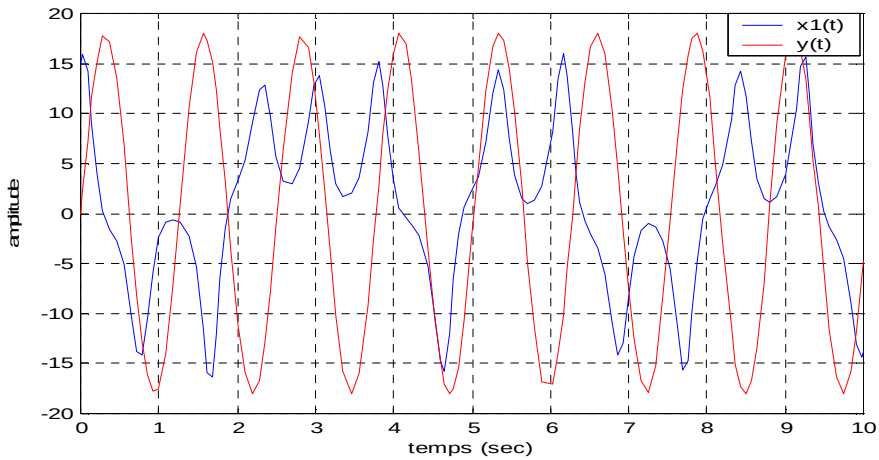


Fig. 2.2 Evolution dans le temps d'un système chaotique, comparé à une sinusoïde.

Le caractère pseudo-aléatoire confère qualitativement aux signaux chaotiques des propriétés semblables à celles d'un bruit : pas de périodicité décelable, désordre apparent et imprédictibilité de l'évolution [26]. Notons que les systèmes chaotiques obéissent tout de même aux lois de la physique. Si on se place dans l'approximation de la physique classique, on peut affirmer que le système est totalement déterministe.

2.4.4 Attracteur étrange

Le terme attracteur étrange a été utilisé pour la première fois par David Ruelle et Floris Takens en 1971, afin de décrire l'attracteur obtenu par une série de bifurcations d'un système modélisant le courant d'un liquide. En fait, avant l'article de Ruelle et Takens, les attracteurs avaient déjà fait l'objet de publications mais ils sont restés ignorés. Cette appellation d'attracteur étrange fait appel à leur propriété peu commune, qui est leur dimension fractale [3].

Définition 2.8 *(Dimension fractale) La dimension d'un espace correspond au nombre minimum de coordonnées nécessaires pour spécifier de manière unique la position d'un point ou encore la dimension d'un système dynamique. En géométrie classique, un point est défini*

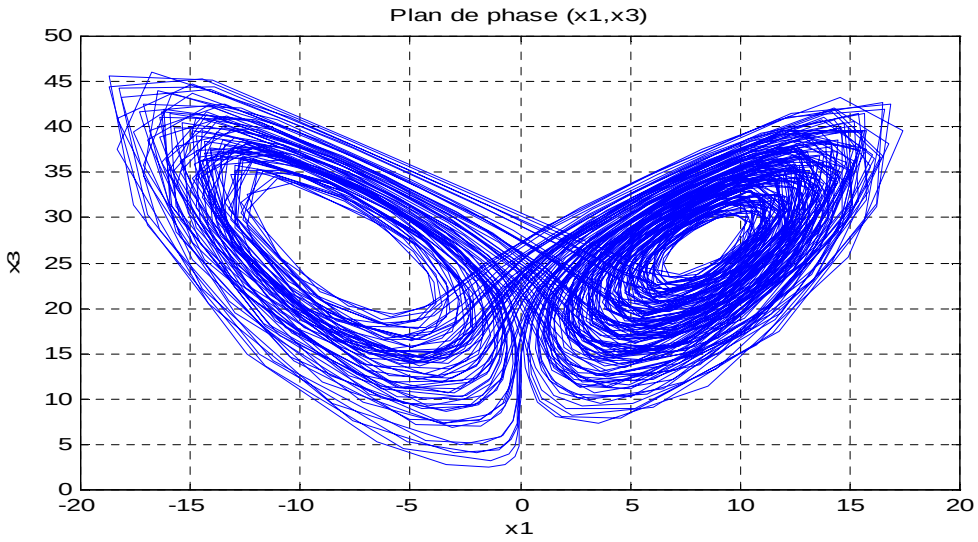
par 3 coordonnées que l'on mesure dans un repère d'axe, c'est l'espace euclidien à 3dimensions. On définit la dimension fractale d'un système chaotique comme une 4^{ième} dimension introduite, par exemple un point peut se situer dans un espace à 3.4 dimensions.

En effet la structure géométrique des trajectoires générées par un système chaotique est extrêmement complexe à cause des étirements, repliements et contractions s'opérant dans une région bornée de l'espace d'état. Les caractéristiques de l'attracteur étrange sont alors :

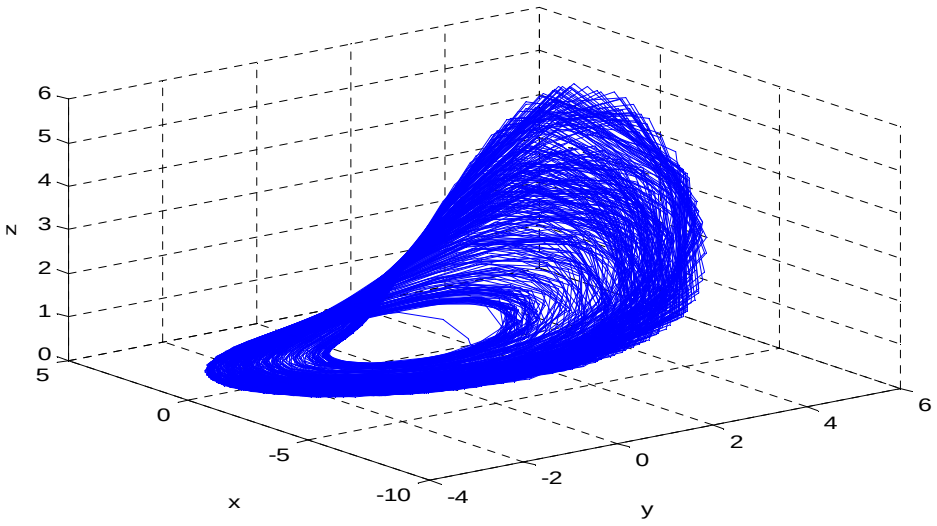
- il est contenu dans un espace fini, sa dimension est fractale et non entière. Sa trajectoire est complexe.
- presque toutes les trajectoires sur l'attracteur ont la propriété de ne jamais passer deux fois par le même point.
- deux trajectoires proches à un instant « t » localement leur distance (les 2 trajectoires) augmente 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 [10].

Un système chaotique est donc contraint d'évoluer de manière « imprévisible » dans une région bien définie de l'espace des phases. L'attracteur étrange le plus célèbre, qui a contribué au succès médiatique de la théorie du chaos, prend la forme *d'ailes de papillon* déployées. Ce fameux papillon est devenu en quelque sorte le symbole de la théorie du chaos un peu comme la pomme de Newton est devenue le symbole de la gravité.

Dans ce qui suit, nous allons présenter deux exemples d'attracteurs. Le premier est l'attracteur de Lorenz et le deuxième est celui de Rössler.



(a) Attracteur de Lorenz.



(b) Attracteur de Rössler

Fig. 2.3 Attracteurs chaotiques « célèbres » dans leur espace des phases.

En résumé, le chaos est rencontré dans des systèmes dynamiques (différentiels ou itératifs) grâce à la présence de non-linéarités. Lorsque le chaos est obtenu, il présente les caractéristiques décrites précédemment. L'analyse de ces comportements se fait dans la

pratique avec des outils spécifiques (espace des phases, exposants de Lyapunov) ou avec des outils classiques de traitement du signal (spectres, auto-corrélation). Nous allons maintenant présenter certains de ces outils.

2.5 Outils de caractérisation du chaos

2.5.1 Le spectre de puissance et fonction d'auto-corrélation

Une façon simple de caractériser le chaos consiste à calculer le spectre de Fourrier de l'évolution temporelle d'une des variables du système [3]. En effet, le spectre d'un signal périodique ou quasi-périodique est constitué de raies discrètes correspondant aux fréquences du système. En revanche, dans le cas d'un signal chaotique, on obtient un spectre continu. Ce spectre chaotique continu peut être de plus ou moins bonne qualité en termes de porteuse chaotique pour le cryptage [19].

Pour le calcul du spectre d'un signal, il faut extraire ses composantes fréquentielles donc utiliser la transformée de Fourier. La fréquence, l'amplitude et la phase de chaque composante sinusoïdale sont calculées en fonction du signal temporel selon la relation suivante en faisant intervenir les deux variables réciproques, t le temps, et f_r la fréquence :

$$\tilde{x}(f_r) = \int_{-\infty}^{+\infty} x(t) e^{-2j\pi f_r t} dt \tag{2.7}$$

Le spectre de puissance est la transformée de Fourier de la fonction d'auto-corrélation, d'après le théorème de Wiener-Kintchine est définie par :

$$C(\tau) = \frac{1}{t_2 - t_1} \int_{t_1}^{t_2} x(t).x(t+\tau) dt \tag{2.8}$$

Cette fonction mesure la ressemblance de la variable x, à un instant donné t, avec sa valeur à un instant ultérieur $t + \tau$. En faisant varier progressivement l'intervalle, on construit la fonction $C(\tau)$ qui traduit le taux de similitude du signal avec lui-même quand le temps s'écoule.

- Si $x(t)$ est constant, périodique ou quasi-périodique, $C(\tau)$ ne tendra pas vers zéro quand τ tendra vers l'infini. Les signaux périodiques gardent donc leur similitude interne quand le temps s'écoule. Le comportement du système est

prédictible puisque sa connaissance pendant un laps de temps suffisant permet de savoir, par simple comparaison, ce qu'il sera à tout instant ultérieur.

- Si $x(t)$ est chaotique, $C(\tau)$tend vers zéro quand τ augmente.

2.5.2 Les exposants de Lyapunov

Le mathématicien russe Alexander Lyapunov s'est penché sur le phénomène de sensibilité aux petites variations des conditions initiales et a développé une quantité permettant de mesurer la vitesse à laquelle ces petites variations peuvent s'amplifier. Cette quantité appelée "exposant de Lyapunov" mesure en fait le degré de sensibilité d'un système dynamique.

Par définition, un exposant de Lyapunov est le taux exponentiel moyen de divergence ou de convergence de trajectoires voisines de l'espace des phases [10]. L'écart entre les deux trajectoires peut être approximé par e^{kt}. Le nombre d'exposants de Lyapunov est égal à la dimension de l'espace des phases : un exposant de Lyapunov est associé à chaque direction de l'espace des phases. Si l'exposant est positif, les trajectoires divergeront et si l'exposant est négatif, celles-ci convergeront. Pour un exposant nul, les trajectoires sont confondues.

Ceci est illustré par la figure (2.4) ci-dessous

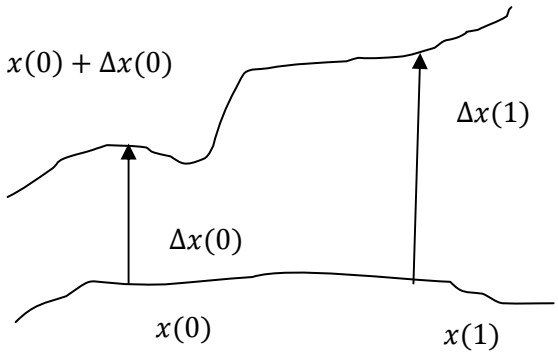


Fig. 2.4 Evolution de deux trajectoires dans l'espace de phase.

l'exposant de Lyapunov est tel que $e^k = \left|\frac{\Delta x(1)}{\Delta x(0)}\right|$, alors

$$k = \ln \left| \frac{\Delta x(1)}{\Delta x(0)} \right|$$

La quantité $\ln \frac{|\Delta x(1)|}{|\Delta x(0)|}$ est l'exposant de Lyapunov local qui mesure le taux de l'étirement au point $x = x(0)$.

2.5.2.2 Exposants de Lyapunov d'un attracteur étrange

L'extrême sensibilité des systèmes chaotiques aux conditions initiales se traduit par une petite perturbation $\delta x_p(t)$ au voisinage d'un point x_p où le système a été linéarisé ou des exposants de Lyapunov positifs. Donc, un attracteur étrange possèdera toujours au moins un exposant de Lyapunov positif avec la propriété $\sum_{i=0}^{n} k_i < 0$. De plus, pour un attracteur étrange, un des exposants de Lyapunov est toujours nul. Cela signifie que pour respecter la condition
$\sum_{i=1}^{n} k_i < 0$, un attracteur étrange doit avoir au minimum trois exposants de Lyapunov. Donc, un système continu dans le temps doit être au moins de dimension supérieure ou égale à trois pour produire du chaos [19].

2.5.2.3 Comportement du système en fonction des exposants de Lyapunov

On étudiant les exposants de Lyapunov d'un système non linéaire, on peut définir le type d'attracteur généré par le système [10].

- $k_n \leq \cdots \leq k \leq 0$: des exposants de Lyapunov négatifs montrent l'existence d'un point fixe.
- $k_1 = 0 , k_n \leq \cdots \leq k_2 \leq 0$: l'attracteur est une orbite fermée.
- $k_1 = k_2 = 0 , k_n \leq \cdots \leq k_3 \leq 0$: l'attracteur est quasi périodique (2fréquences).
- $k_1 = \cdots = k_j = 0 , k_n \leq \cdots \leq k_{j+1} \leq 0$: l'attracteur est quasi périodique (j fréquences).
- $k_1 > 0 , \sum_{i=1}^{n} k_i < 0$: l'attracteur est chaotique.

-$k_1 > \cdots > k_j > 0$, $\sum_i k_i < 0$: l'attracteur est hyper-chaotique.

L'étude du spectre de Lyapunov constitue un outil intéressant de quantification du degré de complexité d'un attracteur.

En conclusion, plus on aura un nombre important d'exposants de Lyapunov supérieurs à 0, plus l'attracteur chaotique est complexe, et sera donc intéressant à priori pour la cryptographie par chaos.

Exemple 2.1 : Dans la figure (2.5), est représenté les exposants de Lyapunov du système chaotique Chen [6] obtenu par un programme sous Matlab.

Le modèle de Chen :

$$\begin{aligned} \dot{x}_1 &= a(x_2 - x_1) \\ \dot{x}_2 &= (c-a)x_1 - x_1x_3 + cx_2 \\ \dot{x}_3 &= x_1x_2 - bx_3 \end{aligned} \tag{2.9}$$

Avec $(a, b, c) = (35,3,28)$

Le système possède trois exposants de Lyapunov (k_1, k_2) sont négatifs et k_3 est positif le système est donc chaotique.

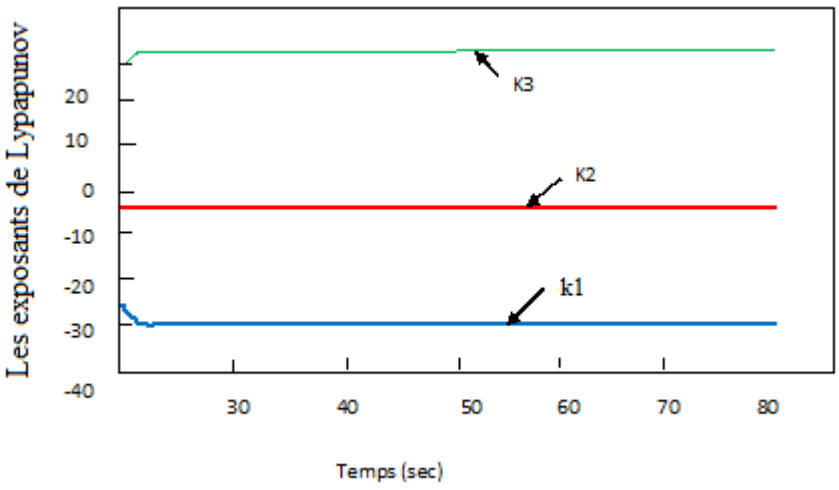


Fig. 2.5 Exposants de Lyapunov relatifs au système de Chen [3].

En résumé, pour dire qu'un système est chaotique, les exposants de Lyapunov doivent remplir trois conditions:

- au moins l'un d'eux est positif pour expliquer la divergence des trajectoires
- au moins l'un d'eux est négatif pour justifier le repliement des trajectoires.
- la somme de tous les exposants est négative pour expliquer qu'un système chaotique est dissipatif c'est-à-dire qu'il perd de l'énergie

La valeur du plus grand exposant de Lyapunov quantifie le degré de chaos du système mais le fait que les trois conditions énoncées ci dessus soient réunies ne suffit pas à conclure qu'un système est chaotique.

Il faut toujours mettre les résultats du calcul des exposants de Lyapunov avec ceux fournis par d'autres outils d'analyse non-linéaire.

2.5.3 La notion de bifurcation

Un système dynamique non-linéaire peut présenter de multiples comportements (point fixe, oscillations périodiques, quasi-périodiques, chaos) en fonction de la valeur de ses paramètres. Il passe d'un comportement à un autre en fonction des changements de certains paramètres du système.

Les transitions entre régimes dynamiques se font par bifurcation et le paramètre qui est responsable de ce changement de dynamique est appelé paramètre de bifurcation.

L'ensemble de l'évolution dynamique d'un système peut se représenter sous la forme d'un diagramme de bifurcation [14].

On distingue trois scénarios théoriques d'évolution vers le chaos, toutes ces évolutions ont permis de classer certains phénomènes expérimentaux comme « chaotiques déterministes ». On obtient l'apparition du chaos en modifiant la valeur d'un paramètre, que ce soit de manière théorique ou expérimentale.

- *Le doublement de période* : L'augmentation d'un paramètre provoque, pour un système périodique, l'apparition d'un doublement de sa période. La période est ensuite multipliée par 4, 8, 16. . .

A partir d'une certaine valeur de ces paramètres la période devient infinie, et les mouvements deviennent chaotiques. Ce scénario peut être observé dans un grand nombre d'expériences comme un robinet qui fuit.

- *L'intermittence* : L'intermittence se caractérise plutôt par un mouvement périodique stable entrecoupé par des bouffées chaotiques. L'augmentation d'un paramètre produit l'augmentation de la fréquence des perturbations, puis le chaos domine le comportement du système. Ce scénario a été observé dans des réactions chimiques.
- *Le quasi périodicité* : le troisième scénario fait intervenir, pour un système périodique, l'apparition d'une deuxième période dont le rapport avec la première n'est pas rationnel. Ce régime est appelé « quasi périodique ». Il peut, de lui-même ou avec l'apparition d'une troisième fréquence gigantesque, donner un régime chaotique. Ce scénario peut être observé dans le déroulement des séismes.

Pour mieux comprendre l'aspect de bifurcation nous présentons l'exemple suivant :

Exemple 2.2 : Considérons le diagramme de bifurcation de récurrence logistique, utilisée par le biologiste Robert May en 1976, décrit l'évolution de la population d'une espèce. Elle est de dimension 1 et a pour représentation d'état :

$$x_{j+1} = \theta_{x_j}(1 - x_j) \tag{2.10}$$

Avec $0 < \theta < 4$. Le vecteur d'état $x_j \in [0,1]$ représente la population à l'annéej, et le paramètre θ représente un facteur de croissance de la population.

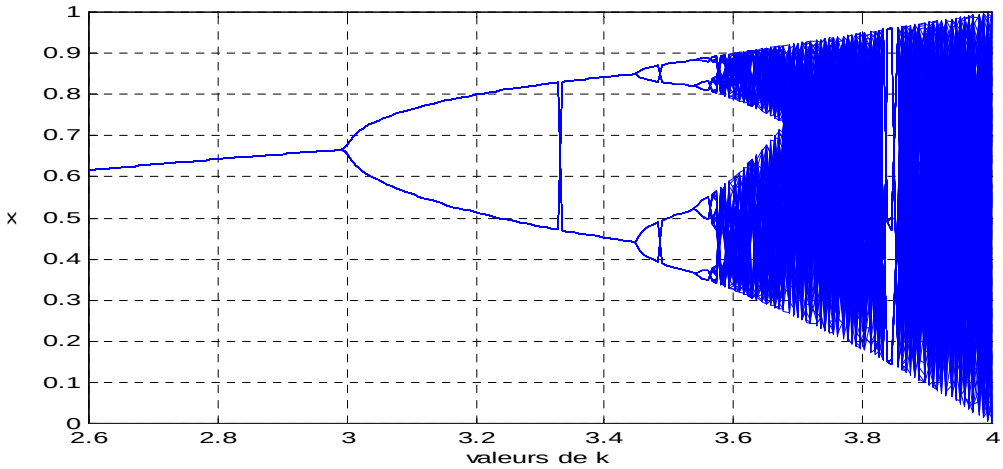


Fig. 2.6 Le diagramme de bifurcation du modèle de May**.**

L'évolution x_j est représentée en fonction de k sur la figure 2.6. En augmentant k, l'évolution commence par un point fixe croissant. Ensuite, il y a une bifurcation de période 2 et la population augmente puis diminue périodiquement sur un cycle de 2 ans. Si k augmente encore, le régime périodique évolue vers un cycle de 4,8, 16…années et atteint finalement un régime complexe, c'est-à-dire, un régime chaotique. Le modèle présente une cascade de bifurcation par dédoublement de période dans une route vers le chaos.

2.5.4 La section de Poincaré

Pour observer les trajectoires d'un attracteur, il est parfois très utile de réduire la dimension d de l'espace des phases. Une section d'observation $\sum$ à dimension $d-1$ transforme la trajectoire continue en une succession de points de passage discontinus à travers $\sum$ [10].

Exemple 2.3 *La section de Poincaré appliquée à un attracteur*

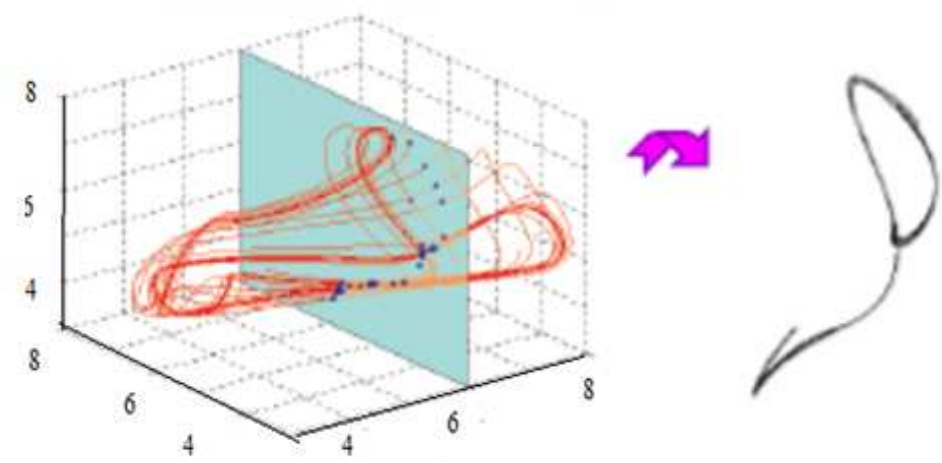


Fig. 2.7 Section de Poincaré [16].

L'intérêt de cette coupe est non seulement de donner une représentation plus claire de la dynamique du système en 3D (la dynamique est ainsi plus facile à étudier), mais aussi de permettre de mesurer la dimension fractale [16].

La figure (2.7) correspond à un faible rapport (T/τ), ce qui permet d'avoir des régimes chaotiques de faible dimension.

2.5.5 Résumé-Propriétés d'un système chaotique

Nous récapitulons ici les caractéristiques essentielles d'un système chaotique présentées dans les paragraphes précédents.

- Le comportement chaotique est le résultat de phénomènes essentiellement non linéaires.

-Il s'agit d'un système déterministe dont l'évolution est gouvernée par certaines lois qui se présentent sous forme d'un ensemble d'équations différentielles.

-L'évolution d'un système dynamique chaotique est imprédictible en ce sens qu'elle est sensible aux conditions initiales.

-Une trajectoire chaotique se situe sur un attracteur étrange, dans un espace des phases de dimension supérieure ou égale à 3.

-La structure géométrique des trajectoires générées par un système chaotique est extrêmement complexe.

-Son spectre de puissance est caractérisé par un large spectre.

-Son attracteur étrange possèdera toujours au moins un exposant de Lyapunov positif avec la propriété $\sum_{i=0}^{n} k_i < 0$.

Un système est dit chaotique lorsque dans certaines conditions il se comporte de manière chaotique. Cependant, dans d'autres conditions, il peut avoir un comportement non chaotique. Il est donc utile de chercher des moyens de caractériser a priori un régime dynamique et a posteriori, s'il s'agit d'un régime chaotique, de savoir dans quelle mesure il est chaotique. Ci pour cela qu'on fait appel aux outils cités précédemment tels que diagramme de bifurcation, le spectre de puissance, fonction d'auto-corrélation el le calcul des exposants de Lyapunov.

Nous allons maintenant présenter certains de ces caractéristiques tout en les illustrant sur un circuit électronique particulier de Chua, fort étudié dans la littérature des systèmes dynamiques non-linéaires.

2.6 Exemple de système chaotique « Circuit de Chua »

Lors d'une visite au Japon en 1983, Leon Chua fut témoin d'une tentative infructueuse de génération de chaos à partir d'une réalisation électrique inspirée des équations de Lorenz.

Ceci le poussa à développer son propre circuit électronique. Rapidement, le comportement dynamique de ce circuit fut mis en évidence à la fois par la simulation et par l'expérience.

Dans le domaine de l'électronique, l'exemple type de système engendrant des phénomènes dynamiques complexes est le circuit de Chua qui a fait et qui continue de faire l'objet de nombreuses études.

Le circuit de Chua est un circuit électronique qui se compose de cinq éléments : une résistance R, une inductance L, deux condensateurs C_1 , C_2 et une résistance non linéaire NR appelée diode de Chua comme représenté dans la figure suivante.

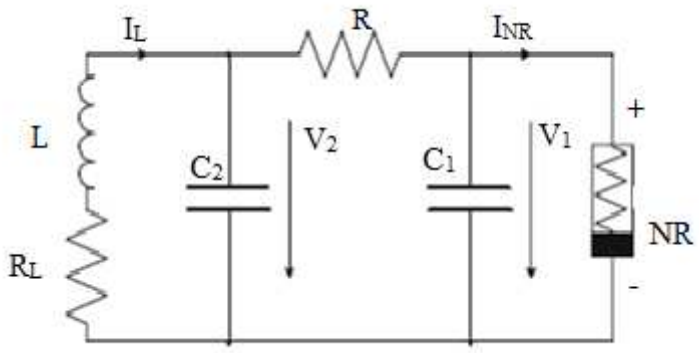


Fig. 2.8 Circuit de Chua.

La résistance non-linéaire peut s'obtenir avec deux amplificateurs opérationnels et des résistances.

En utilisant la loi des mailles et la loi des nœuds, nous pouvons établir trois équations différentielles aux variables indépendantes, caractéristiques du circuit :

$$\frac{dV_1(t)}{dt} = \frac{1}{C_1}[G\big(V_2(t) - V_1(t)\big) - f(V_1(t))]$$

$$\frac{dV_2(t)}{dt} = \frac{1}{C_2}[G\big(V_1(t) - V_2(t)\big) + I_L(t)] \qquad (2.11)$$

$$\frac{dI_L(t)}{dt} = \frac{1}{L}[-V_2(t) - R_L I_L(t)]$$

Avec la conductance $G = \frac{1}{R}$, $I_L(t)$ le courant qui traverse l'inductance L, $V_1(t)$ et $V_2(t)$sont les tensions respectivement aux borne des capacités C_1 et C_2 et $f(V_1(t))$ la fonction non-linéaire qui caractérise la diode de Chua a pour expression :

$$I_{NR}(t) = f(V_1(t)) = G_b V_1(t) + \frac{1}{2}(G_a - G_b)(|V_1(t) + E| - |V_1(t) - E|) \qquad (2.12)$$

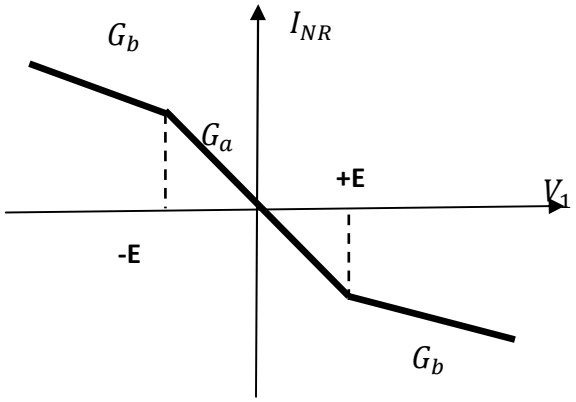


Fig. 2.9 La caractéristique de la non-linéarité de la diode de Chua.

avec E est la tension de palier de la diode, $G_a < 0$; $G_b < 0$ sont les pentes de la non-linéarité

En effectuant les changements de variables suivants :

$x_1 = \frac{v_1}{E}$ $x_2 = \frac{v_2}{E}$ $x_3 = \frac{I_L}{E.G}$ $\alpha = \frac{C_2}{C_1}$ $\beta = \frac{C_2}{(LG)^2}$ $\gamma = \frac{C_2.R_L}{L.G}$

$m_1 = \frac{G_b}{G}$, $m_0 = \frac{G_a}{G}$ **.**L'échelle de temps est remplacé par $\tau = t(\frac{G}{C_2})$.

Le modèle (2.11) prend alors la forme suivante, appelée modèle sans dimension du circuit de Chua :

$$\begin{cases} \dot{x_1} = -\alpha x_1 + \alpha x_2 - \alpha f(x_1) \\ \dot{x_2} = x_1 - x_2 + x_3 \\ \dot{x_3} = -\beta x_2 - \gamma x_3 \end{cases} \qquad (2.13)$$

$f(x_1)$ représente la non-linéarité du circuit figure (2.8) et décrite par l'équation :

$$f(x_1) = m_1 x_1(t) + \frac{1}{2}(m_0 - m_1).(|x_1(t) + 1| - |x_1(t) - 1|) \qquad (214)$$

Avec

$$f(x_1) = \begin{cases} m_1 x_1 + (m_0 - m_1) & si\ x_1 \geq 1 \\ m_0 x_1 & si\ |x_1| < 1 \\ m_1 x_1 - (m_0 - m_1) & si\ \ x_1 \leq 1 \end{cases} \quad (2.15)$$

Les points d'équilibre du système sont donnés par :

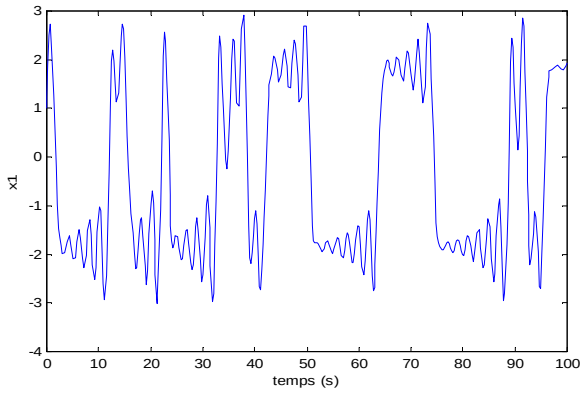
$C_{01} = (0,0,0)$, ainsi que deux points fixes

$$C_{02} = \left(\frac{m_1 - m_0}{m_1 + 1}, 0, \frac{m_0 - m_1}{m_1 + 1}\right); \quad C_{03} = \left(\frac{m_0 - m_1}{m_1 + 1}, 0, \frac{m_1 - m_0}{m_1 + 1}\right)$$

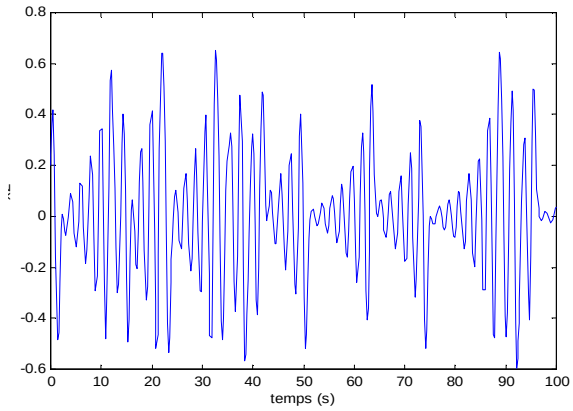
Pour certaines valeurs des différents paramètres $(\alpha, \beta, \gamma, m_0, m_1)$ et différentes conditions initiales imposées aux variables d'états $x_1(t), x_2(t)\ et\ x_3(t)$, ce circuit présente des régimes de fonctionnement oscillatoires chaotiques.

Lors des simulations sous Matlab de ce modèle, nous avons pris $\alpha = 10;\ \ \beta = 14.87;\ \gamma = 0.$ et les conditions initiales $(x_{10}, x_{20}, x_{30}) = (1\ \ 0.2\ \ 0)$. On a obtenu les résultats suivants :

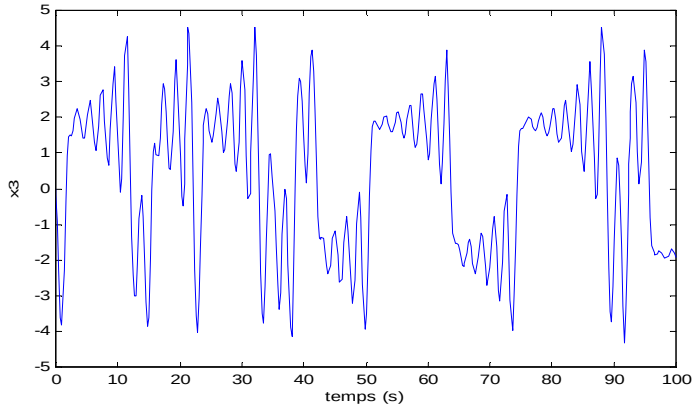
1/ Aspect aléatoire



1. L'état x_1



2. L'état x_2



3. L'état x_3

Fig. 2.10 Trajectoires des trois états du système (2.13).

La figures ci-dessus représente l'aspect aléatoire des trois états du circuit de Chua Ce système chaotique évolue d'une manière semble aléatoire mais tout en restant déterministe. Pour mieux distinguer cet aspect aléatoire on a comparé une évolution simple, périodique d'une fonction sinusoïdale avec le signal chaotique de la variable x_1 du système (2.13)). Le résultat est représenté à la figure suivante :

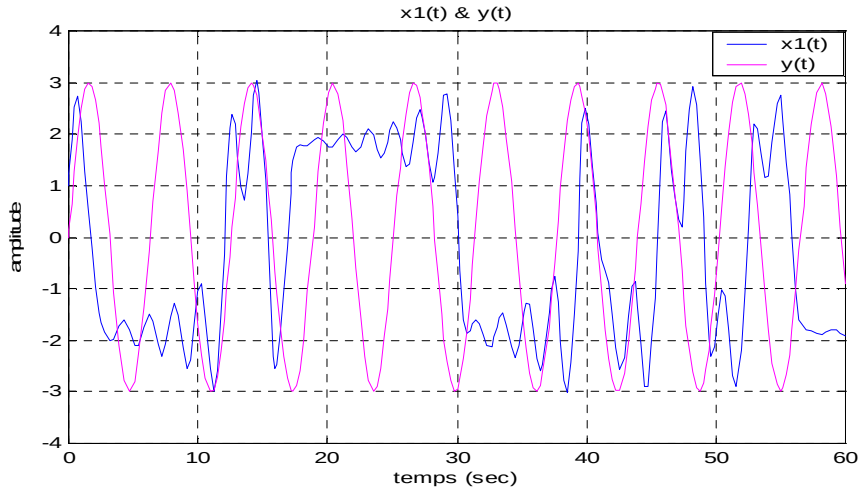


Fig. 2.11 Représentation de la différence d'aspect entre un signal périodique et le signal de la variable $x_1(t)$du système (2.13).

2/ Sensibilité aux conditions initiales

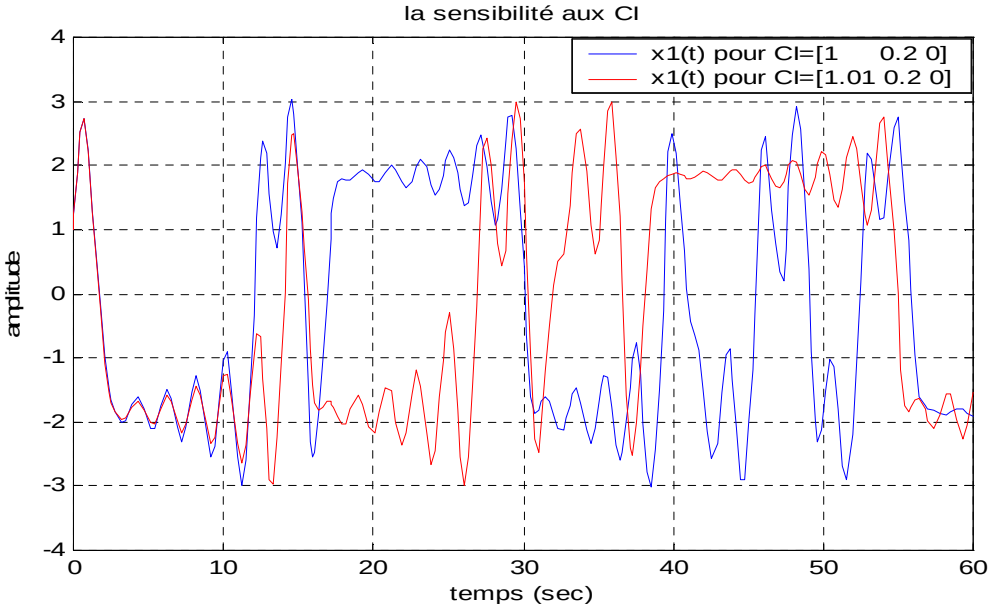


Fig. 2.12 illustration de la sensibilité aux conditions initiales du signal $x_1(t)$du système (2.18).

Cette courbe illustre le phénomène de sensibilité aux conditions initiales. Dans un premier temps, on voit que les deux courbes évoluent de la même manière mais très vite à $t = 1.4\ s$ les deux trajectoires divergent l'une par rapport à l'autre et ça revient a l'extrême sensibilité aux conditions initiales.

3/ L'attracteur étrange

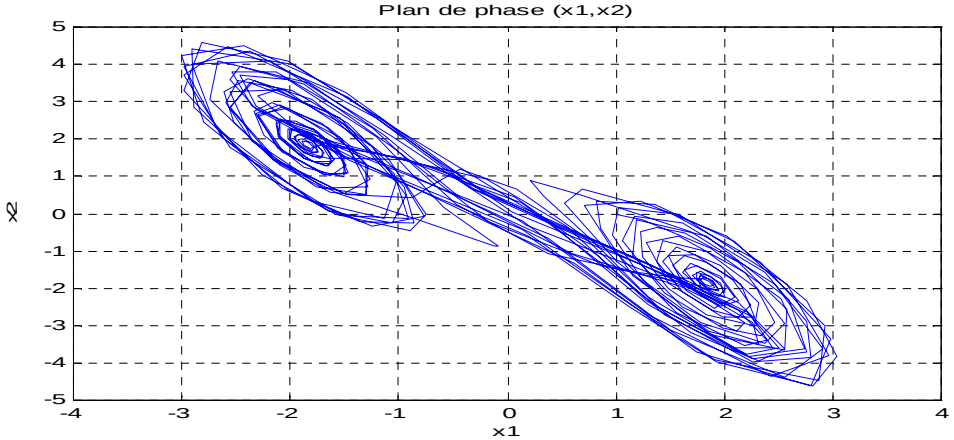
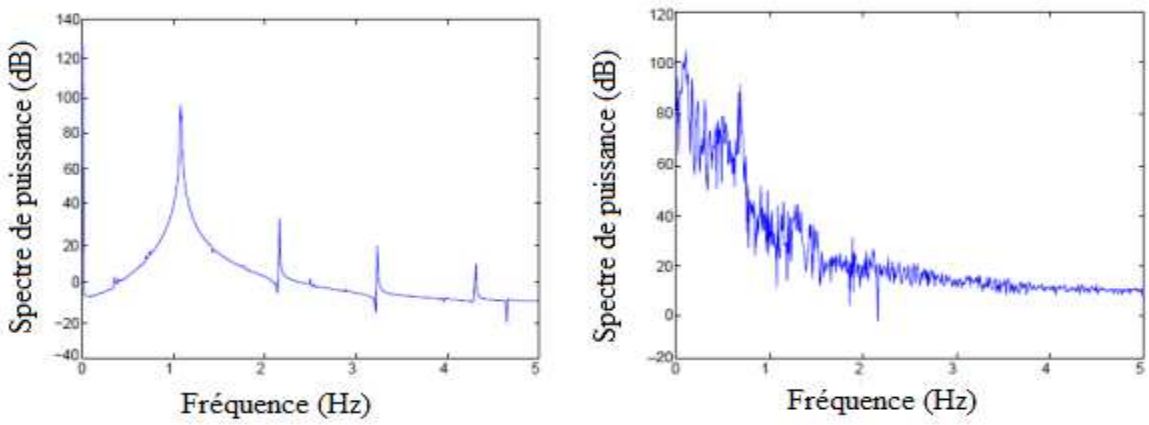


Fig. 2.13 Représentation de l'attracteur de Chua.

Cette figure représente l'attracteur correspondant au circuit de Chua, on voit que cet attracteur évolue sans jamais se répéter, mais en restant confiné dans un espace borné et c'est la caractéristique de l'attracteur étrange du chaos.

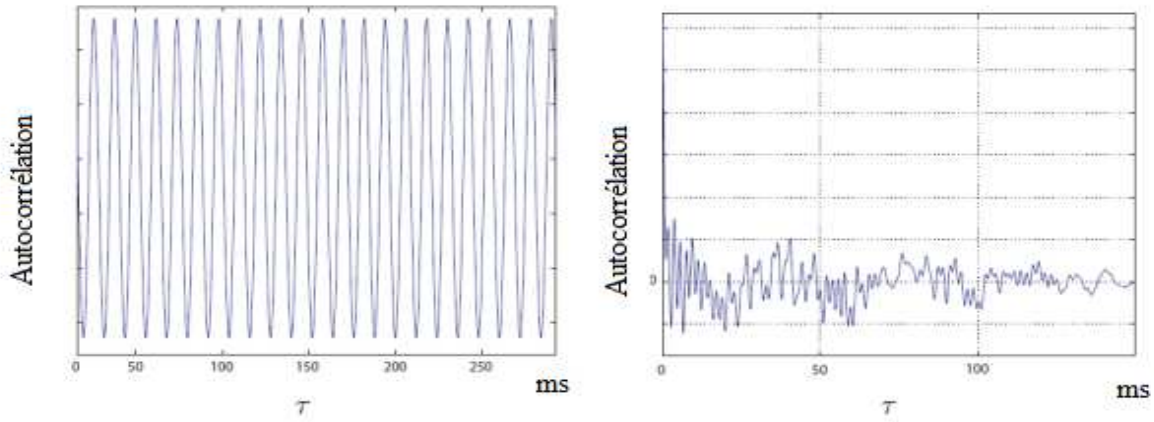
3/ Le spectre de puissance et la fonction d'auto-corrélation



a)régime périodique b) régime chaotique

Fig. 2.14 Spectres d'amplitude du circuit de Chua en régime périodique et en régime chaotique [19].

La figure 2.14b montre le spectre d'amplitude du circuit de Chua en régime chaotique, le spectre présente plusieurs fréquences, signe d'une grande richesse dans la dynamique.



a)régime périodique b) régime chaotique

Fig. 2.15 Auto-corrélation pour un circuit de Chua en régime période et en régime chaotique [19].

La figure 2.15b représente la fonction d'auto-corrélation d'un signal chaotique généré par le circuit de Chua : où la similitude du signal avec lui-même diminue, et disparait quasiment à des instants suffisamment éloignés l'un de l'autre.

2.7 Les applications du chaos [6]

Ingénierie	Contrôle de vibration, stabilisation des circuits, réactions chimiques, turbines, étages de puissance, lasers, combustion, et beaucoup plus.
Ordinateurs	Commutation des paquets dans des réseaux informatiques. Cryptage. Contrôle du chao les systèmes robotiques.
Communication	Compression et stockage d'image. Conception et management des réseaux d'ordinateurs.
Médecine et biologie	Cardiologie, analyse du rythme du cœur (EEG), prédiction et contrôle d'activité irrégulière du cœur.
Management et finance	Prévisions économique, analyse financière, et prévision du marché.

Tab 2.1 : Domaine d'application du chaos.

Contrôle	Première application du chaos est le contrôle du comportement irrégulier dans les circuits et les systèmes.
Synchronisation	Communication sécurisée, cryptage, radio.
Traitement d'information	Codage, décodage et stockage d'information dans des systèmes chaotiques, tel que les éléments de mémoires et les circuits.
Prédiction à court terme	Les maladies contagieuses, température, économie.

Tab 2.2 Les applications du chaos.

2.8 Communiquer avec le chaos

L'idée d'utilisation du chaos dans les systèmes de communication a été inspirée de la découverte de Pecora-Carroll en 1990 [18]. Ils ont montré que deux systèmes chaotiques identiques avec des conditions initiales différentes peuvent éventuellement se synchroniser

s'ils sont couplés d'une certaine manière convenable, c'est à dire sous certaines conditions [26]. Le développement des systèmes de communication utilisant le chaos a commencé donc avec des schémas de synchronisation très simples de circuits électroniques, visant pour le cryptage et la reconstruction simultanés d'un signal d'information [10].

2.8.1 Principe de la synchronisation

Le terme « synchronisation » vient de grec « συγ » (syn) qui signifie « avec », et « χρονος » (chronos) qui signifie, « temps ». On peut donner une première définition de la synchronisation, à savoir : la synchronisation est un phénomène qui caractérise deux systèmes se comportant de la même façon en même temps. En fait, le phénomène de synchronisation est observé depuis le XVII^{e} siècle lorsque le mathématicien hollandais Huygens (1629-1695) remarqua ce phénomène en étudiant deux horloges de fréquences légèrement différentes. Il constata qu'en les reliant l'une à l'autre avec un morceau de bois, elles affichaient toutes les deux la même heure : elles se synchronisaient. Des exemples de synchronisation existent dans la nature, dans le domaine de la science de la vie et de la terre, ainsi que dans les domaines techniques [4].

2.8.2 Synchronisation des systèmes chaotiques

La notion de synchronisation est en général liée à un mouvement périodique. Deux signaux sont synchronisés si leur période ainsi que leur phase sont identiques. Cette définition n'est plus valable dans le cas de signaux chaotiques. Deux signaux chaotiques seront dits synchronisés s'ils sont asymptotiquement identiques lorsque t tend vers l'infini **[3]**.

Dans le contexte de la communication, nous signifions par synchronisation qu'un système esclave se force à se synchroniser avec un système maitre. Considérons la figure (2.16) suivante.

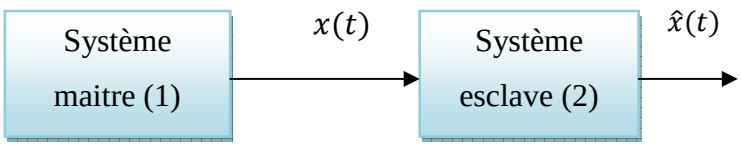


Fig. 2.16 Système maitre-esclave pour réaliser la synchronisation.

dans laquelle, le système (2), dit système esclave, sera synchronisé avec le système (1) (système maître) [19]

Le *système maître* peut être décrit par un système différentiel

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

avec le vecteur d'état $x \in \mathbb{R}^n$, la condition initiale $x(0)$ et une sortie $y = h(x)$
Par analogie, le *système esclave* est défini par le système différentiel

$$\dot{\hat{x}}(t) = \hat{f}\big(\hat{x}(t), y(t)\big)$$

avec le vecteur d'état $\hat{x} \in \mathbb{R}^n$ et la condition initiale $\hat{x}(0)$.

Nous disons que le *système maître* se synchronise avec le *système esclave* si

$$\lim_{t\to\infty} \|x - \hat{x}\| = 0 \qquad (2.16)$$

pour tout $(x(0), \hat{x}(0)) \in \mathbb{R}^n \times \mathbb{R}^n$. Ce type de synchronisation est appelé *synchronisation d'état*.

A priori, il paraît impossible d'arriver à synchroniser deux exemplaires d'un même système chaotique. D'une part parce que dans les systèmes réels, il est extrêmement difficile de construire deux circuits à l'identique à cause de la tolérance sur les composants ainsi que du bruit présent dans tout système électronique [26]. D'autre part, en supposant que l'on dispose de deux circuits identiques, il se pose le problème de la sensibilité aux conditions initiales. Une infime différence entre les conditions initiales des deux circuits conduira à des signaux totalement différents. Cela signifie que reproduire ces conditions initiales dans un système réel est impossible.

2.8.3 Méthode de synchronisation

Les méthodes traditionnelles de synchronisation chaotique sont en général basées sur l'utilisation des circuits identiques. Supposons deux systèmes chaotiques identiques oscillant

de façon totalement indépendante. Si par un moyen quelconque, on leur permet d'échanger de l'énergie, action que l'on nomme « couplage », les deux systèmes finirent 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. Par contre, dans le couplage bidirectionnel, l'élément de couplage permet d'échange de l'énergie dans les deux sens. Les deux types de couplage –unidirectionnel et bidirectionnel- peuvent aussi être appliqués aux systèmes non identiques. Le couplage unidirectionnel de circuits non identiques qui sera traité dans ce mémoire [12].

En plus du couplage simple, d'autres méthodes ont été proposées pour la synchronisation des systèmes chaotiques. Ainsi pour la synchronisation unidirectionnelle on peut citer la méthode par décomposition du système, la synchronisation impulsive ou la synchronisation par 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 les comportements des deux circuits et détruire le phénomène de synchronisation.

2.8.3.1 Auto-synchronisation : Principe de Pecora-Carroll [26]

Certains systèmes chaotiques possèdent la propriété d'auto-synchronisation, c'est-à-dire qu'on peut les décomposer en deux sous-systèmes, l'un *maître*, l'autre *esclave*. Ces derniers peuvent se synchroniser sous l'effet d'un couplage avec un signal commun.

Dans le schéma de synchronisation proposé par Pecora et Carroll, un système chaotique

$$\dot{x}(t) = f(x(t)) \tag{2.17}$$

Où le vecteur d'état x est décomposé de la manière suivante :

$$(\Sigma)\ \dot{x}(t) = \begin{pmatrix} \dot{x}_1(t) \\ \dot{x}_2(t) \end{pmatrix}$$

avec une sortie scalaire $y = h(x)$ est décomposé en deux sous-systèmes dont les états sont x_1 et x_2 respectivement :

$$(\Sigma_1)\ \dot{x}_1(t) = f_1\big(x_1(t), x_2(t)\big) \tag{2.18a}$$

$$(\Sigma_2)\ \ \dot{x}_2(t) = f_2(x_1(t), x_2(t)) \tag{2.18b}$$

Ensuite, on crée un nouveau sous-système (Σ'_2) identique au sous-système (Σ_2), dont l'entrée est x_1 :

$$(\Sigma'_2)\ \ \dot{x}'_2(t) = f_2(x_1(t), x'_2(t)) \tag{2.19}$$

Le système (Σ_1, Σ_2)est appelé système *maître*, et le sous-système Σ'_2 est appelé système *esclave*. On définit alors les notions suivantes :

Définition 2.9 (*Exposants de Lyapunov conditionnels) Les exposants de Lyapunov du système esclave (2.19) dont l'entrée est une trajectoire particulière $x_1(t)$ sont appelés exposants de Lyapunov conditionnels.*

Pecora et Carroll ont établi le résultat suivant :

Définition 2.10 *Les systèmes* (2.18) *et* (2.19) *sont synchronisés si et seulement si tous les exposants de Lyapunov conditionnels de* (2.19) *sont négatifs.*

En gros, le problème dans le principe de Pecora-Carroll est de trouver une décomposition (2.18)- (2.19) convenable, c'est à dire telle que les ELCs de (2.19) soient négatifs.

Ce principe peut être résumé par la figure (2.17).

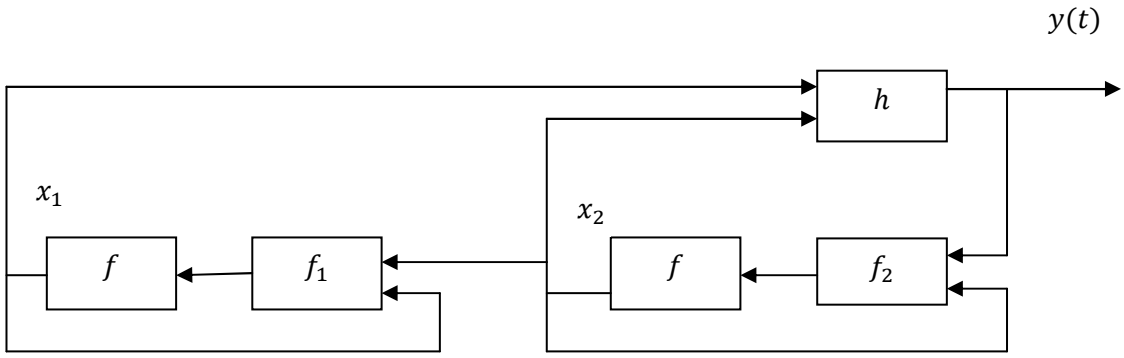


Fig. 2.17 Principe de Pecora-Carrol.

2.9 Conclusion

Ce chapitre avait comme objectif l'introduction de quelques notions élémentaires concernant les systèmes dynamiques chaotiques, pour tirer des propriétés de ce dernier afin de concevoir un générateur chaotique. Ce générateur, une fois validé, est utilisé pour effectuer le masquage de l'information pour réaliser une transmission sécurisée à la suite de ce mémoire.

Dans la première partie de ce chapitre, nous avons présenté les caractéristique essentielles du chaos (le déterminisme, la sensibilité aux conditions initiales, caractère pseudo aléatoire, attracteur étrange) et les outils d'analyse applicables aux systèmes dynamiques chaotiques (le diagramme de bifurcation, le spectre d'auto-corrélation et les exposants de Lyapunov).En suite nous avons cherché à illustrer ces notions sur un exemple simple tel que circuit de Chua. En dernier, on a abordé le phénomène de synchronisation et son application pour la communication, et présenté par la suite les principales méthodes utilisées pour la synchronisation des systèmes chaotiques.

3.1 Introduction

Les besoins actuels de confidentialité dans les télécommunications modernes stimulent de plus en plus le développement de nouveaux systèmes de cryptage. Le cryptage par chaos est actuellement un axe de recherche en plein essor qui a déjà donné naissance à plusieurs réalisations de circuits électroniques chaotiques comme les circuits de Colpitts, Chua, Chen [17].

Dans ce chapitre, nous étudions la possibilité d'utiliser le chaos pour chiffrer l'information dans une transmission sécurisée. Le système de cryptage est composé d'un émetteur chaotique et d'un récepteur. L'émetteur est un oscillateur de Chua-Hartley, le message est injecté dans cet oscillateur par deux méthodes de cryptage inclusion et addition. Seulement, un des états de l'émetteur est transmis au récepteur via un canal public. Le récepteur est un observateur à mode glissant étape par étape, conçu pour reconstruire tous les états de l'émetteur, ainsi que le message transmis. Les résultats de simulation sont présentés afin d'étudier les performances de cet observateur ainsi que ces méthodes de cryptage.

3.2 Méthode de couplage unidirectionnel choisie : l'approche par observateur

Lorsque l'émetteur est représenté par un système dynamique avec les variables d'état $x(t)$ la synchronisation consiste donc à concevoir l'émetteur de telle façon que l'émetteur se synchronise avec le récepteur. On doit donc concevoir un système avec les variables d'état $\hat{x}(t)$ pour le récepteur tel que l'erreur $e(t)$ tende vers zéro. On fait appel aux observateurs pour donner ce récepteur. La synchronisation revient donc à concevoir un observateur au système décrivant l'émetteur.

3.2.1 Principe de synchronisation à base d'observateurs

Après la découverte de Pecora-Carroll, le problème de synchronisation a été rapidement relié au problème plus général de l'observation d'état non linéaire classique. Dans cette approche, le système *maître* est un système chaotique quelconque et le système *esclave* est un observateur d'état correspondant. La figure 3.1 illustre ce principe de synchronisation [26].

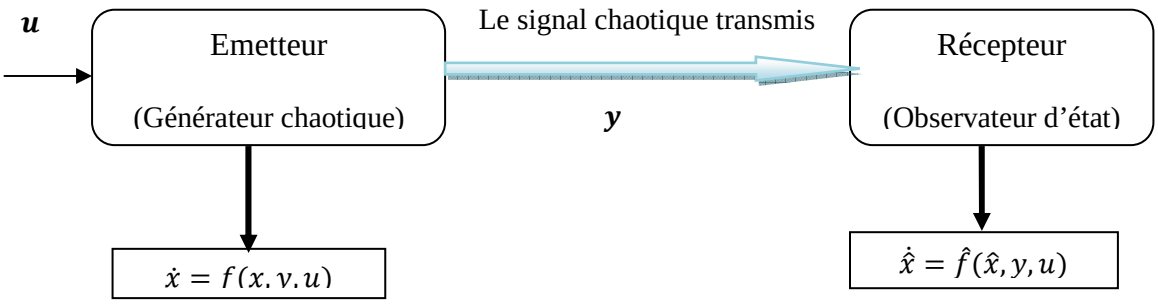


Fig. 3.1 Principe de synchronisation à base d'observateur.

Pour ce principe, nous disons que l'émetteur et le récepteur se synchronisent si le système $\dot{\hat{x}} = \hat{f}(\hat{x}, u)$ est un observateur convergent pour le système $\dot{x} = f(x, u),\ y = h(x)$. Autrement dit, le problème de synchronisation revient à déterminer une fonction $\hat{f}$ telle que :

$$\|x(t) - \hat{x}(t)\| \to 0, \text{ quand } t \to +\infty$$

Dans ce qui suit, nous allons rappeler quelques définitions liées à la notion d'observabilité et les conditions de recouvrement d'observabilité des systèmes non linéaires (en temps continu) et le type d'observateur utilisé pour la transmission sécurisée.

3.3 Observateurs d'état des systèmes non linéaires

Le domaine de l'estimation d'état des systèmes non linéaires est encore largement ouvert. Même si de nombreuses méthodes ont été développées pour concevoir des observateurs non linéaires, le problème reste sans solution dans un grand nombre de cas. C'est un domaine de recherche actif, car la connaissance de l'état d'un système est nécessaire dans de multiples applications, à savoir la commande de procédés, la surveillance de systèmes, le diagnostic et la détection de défauts…etc. [26].

3.3.1 Principe d'estimation d'état

D'une manière générale, un observateur est un système dynamique qui permet la reconstruction de l'état d'un système, à partir de ses entrées, de ses sorties, et de la connaissance de son modèle dynamique, qui sont les seules informations disponibles. Ce principe est illustré par la figure suivante :

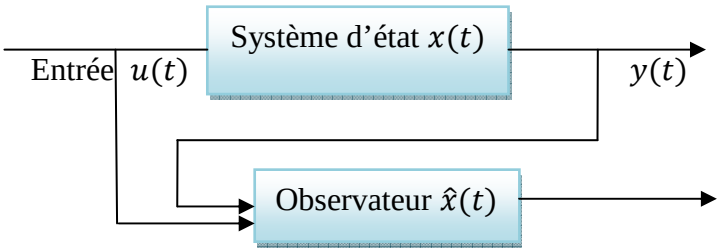


Fig. 3.2 Principe d'un observateur non-linéaire.

Théoriquement, le problème de la conception d'un observateur pour un système (non linéaire) donné est posé comme suit [4] :

On considère le système non linéaire suivant :

$$\begin{cases} \dot{x} = f(x) + g(x)u \\ y = h(x) \end{cases} \tag{3.1}$$

Avec $t \geq 0$.

Où les variables : $x \in X \subset \mathbb{R}^n$, $u \in U \subset \mathbb{R}^m$ et $y \in Y \subset \mathbb{R}^p$ représentent respectivement l'état, l'entrée ou la commande et la sortie du système. f et h sont des champs de vecteurs supposés suffisamment continûment dérivables sur X et les conditions initiales sont données par $x_0 = x(0)$.

La structure d'observateur la plus utilisé est:

$$\begin{cases} \dot{\hat{x}} = f(\hat{x}) + g(\hat{x})u + \eta(y, \hat{x}) \\ y = h(x) \end{cases} \tag{3.2}$$

Avec $\hat{x} \in R^n$ l'état estimé.

Le problème de synthèse d'un observateur consiste donc à trouver une copie du modèle plus un terme correcteur $\eta(y, \hat{x})$ qui assure la convergence de l'état estimé $\hat{x}$ du (3.2) vers l'état réel x du système (3.1). Pour étudier la convergence de l'observateur d'un système, des outils concernant la stabilité des systèmes dynamiques sont utilisés, et notamment la théorie élaborée par Lyapunov (voir l'annexe A).

Pour les systèmes non linéaires, étant donné l'espace de l'état $X \subseteq \mathbb{R}^n$ et l'ensemble U des entrées, la notion d'observabilité est basée sur la possibilité de différencier deux conditions initiales distinctes. On parlera ainsi de la distinguebilité d'un couple de conditions initiales.

Définition 3.1 (Distinguebilité) [12] *Deux états initiaux* x_{10}, $x_{20} \in X$ *tel que* $x_{10} \neq x_{20}$ *sont dits distinguables dans* X *si* $\exists t \geq 0$ *et l'entrée admissible* $u : [0, t] \to U$ *telle que les trajectoires des sorties* $y(t, x_{10}, u(t))$ *et* $y(t, x_{20}, u(t))$ *issues, respectivement de* x_{10} *et* x_{20}, *restent dans* X *pendant la durée* $[0, t]$ *et vérifient* $y(t, x_{10}, u(t)) \neq y(t, x_{20}, u(t))$. *Dans ce cas, on dira que* u *distingue* x_{10} *et* x_{20} *dans* X. *Réciproquement, deux états initiaux* $x_{10}, x_{20} \in X$ *tel que* $x_{10} \neq x_{20}$ *sont dites inditinguables si* $\forall t \geq 0$ *et* $\forall u : [0, t] \to U$ *pour lesquels les trajectoires issues de* x_{10}, x_{20} *restent dans* X *on a :* $y(t, x_{10}, u(t)) = y(t, x_{20}, u(t))$.

Définition 3.2 (Observabilité et observabilité locale faible) [12] *Un système est observable en* $x_{10} \in X$ *si tout autre état* $x_{20} \neq x_{10}$ *est distinguable de* x_{10} *dans* X. *Un système est globalement observable s'il est distinguable en tous points de X. Un système est localement faiblement observable en* $x_{10} \in X$, *s'il existe un voisinage* $X'(x_{10}) \subset X$ *contenant* x_{10}, *tel que pour tout voisinage* $X'' \subset X'(x_{10})$ *de* x_{20}, *pour tout point* $x_{20} \in X''(x_{20})$, *les couples* (x_{10}, x_{20}) *sont distinguables et les trajectoires* $y(t, x_{10}, u(t))$ *et* $y(t, x_{20}, u(t))$ *évoluent à l'intérieur de* $X''(x_{10})$.

Dans la pratique, ces notions sont relativement difficiles à vérifier et souvent on fait recours à la linéarisation du système au tour d'un point d'équilibre pour s'affranchir de l'observabilité ou pas du système au voisinage de ce point d'équilibre.

Définition 3.3 (Observabilité au sens du rang)

On dit que la paire (f, h) est observable au sens du rang si :

$$Rang\{dh, dL_f h, \dots, dL_f^{n-1} h\}^T = n$$

Où l'écriture de $dL_f^k h$ *est donnée par le vecteur :*

$$dL_f^k h = \left[\frac{\partial \mathrm{L_f^k}}{\partial \mathrm{x_1}}, \frac{\partial \mathrm{L_f^k}}{\partial \mathrm{x_2}} \ldots \frac{\partial \mathrm{L_f^k}}{\partial \mathrm{x_n}}\right]$$

3.3.2 Méthode d'inversion à gauche et condition de recouvrement d'observabilité [10]

Dans la transmission de données par synchronisation de systèmes chaotiques, il est important de pouvoir estimer l'entrée inconnue du système en plus de la synchronisation des états. En effet, l'entrée inconnue peut être un défaut, une perturbation ou dans notre cas un message confidentiel. La transmission d'information avec la méthode par inclusion (section 3.6.2.2) est non seulement un problème d'observabilité mais aussi un problème d'inversion à gauche, c'est-à-dire reconstruire tous les états ainsi que le message inconnue (entrée inconnue) à partir de la sortie du système et de ses dérivées.

Soit le système :

$$\begin{cases} \dot{x} = f(x,u), \quad x_0 \in D \subseteq \mathbb{R}^n \\ y(t) = h(x,u) \end{cases} \tag{3.3}$$

dans lequel $x \in \mathbb{R}^n$ est l'espace d'état, $u \in \mathbb{R}^m$ est le vecteur d'entrée, et $y \in \mathbb{R}^p$ représente la sortie du système, $t \in T = [0,\ t_f]$. Les fonctions $f(x,u)$, $h(x,u), u(t)$ sont considérées suffisamment dérivables. Le problème d'inversion du système consiste à reconstruire x, u ou une partie de ceux-ci à partir de la sortie $y(.)$ du système. Le système (3.3) génère le « mapping » suivant (pour la condition initiale x_0 soit connue):

$$\phi(u): U \subseteq C^N(T, \mathbb{R}^m) \to C^N(T, \mathbb{R}^p): u \to x(., x_0, u) \longrightarrow y(.) = h(x,u)$$

On considère un ensemble U défini sur le domaine D_α constitué de fonctions et de leurs dérivées d'ordre 1 à α. Alors nous avons : $U = U(D_\alpha)$ où :

$D_0 = \bigcup_{t\in T} u(t)$, $D_1 = \bigcup_{t\in T}(u(t), \dot{u}(t))$,…, $D_\alpha = \bigcup_{t\in T}(u(t), \ldots, u(t)^{(\alpha)})$, $D_i \subseteq \mathbb{R}^{(i+1)m}$

Définition 3.4 *Le système (3.3) est inversible dans le domaine $D \times D_\alpha \times T$ si pour tout $x_0 \in D$ et deux entrées différentes $u_1(t)$, $u_2(t) \in D_\alpha$ il existe un instant $t \in T$ tel que $h(\phi(x_0, u_1)) \neq h(\phi(x_0, u_2))$.*

Nous écrivons le système (3.3) de la façon suivante :

$$\begin{cases} \dot{x} = f(x) + g(x)m \\ y = h(x) \end{cases} \tag{3.4}$$

Dans lequel l'entrée m est considérée bornée et les champs des vecteurs $f, g: X \subset \mathbb{R}^n \to \mathbb{R}^n$ et $h: X \subset \mathbb{R}^n \to \mathbb{R}$ sont des réels analytiques. Le vecteur de sortie de ce système est transmis au récepteur, qui doit générer un vecteur de sortie qui convergera asymptotiquement vers le vecteur d'entrée de l'émetteur. Ce problème constitue le problème d'inversion à gauche.

Afin d'étudier l'observabilité du circuit de Chua-Hartley (voir dans la section 3.7.1) et la condition de recouvrement d'observabilité de l'émetteur chaotique (circuit de Chua incluant le message), on doit vérifier les conditions posées dans les hypothèses suivantes :

Hypothèse 3.1 : l'entrée inconnue (message confidentiel) est bornée.

Hypothèse 3.2 : $span\{dh, dL_f h, \dots, dL_f^{n-1} h\}$ est de $rang\ n$.

Hypothèse 3.3 : $\begin{bmatrix} dh \\ dL_f h \\ \vdots \\ dL_f^{n-1} \end{bmatrix} . g(x) = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ \theta \end{bmatrix}$

où θ signifie une fonction non nulle presque partout dans $X \subset \mathbb{R}^n \to \mathbb{R}$.

La condition donnée dans l'hypothèse 3.3 est appelée condition de recouvrement d'observabilité, cette condition garantie la propriété d'inversibilité à gauche, c'est-à-dire la possibilité de retrouver tous les états et le message à partir de y et de ses dérivées.

3.4 Observateurs à modes glissants [12]

Dans un observateur à modes glissants, le terme correcteur d'erreur d'estimation est une fonction discontinue de type $sign$. La construction de l'observateur à modes glissants est une approche basée sur la théorie des systèmes à structure variable.

L'observateur à modes glissants a été proposé dans différentes applications, dans notre cas, il est utilisé pour la synchronisation des systèmes chaotiques. Dans ce qui suit, nous

allons donner quelques définitions liées aux modes glissants. Ensuite, nous construisons un observateur à mode glissants étape par étape pour reconstruire les variables d'état et l'entrée inconnue de notre émetteur chaotique.

On considère le système non linéaire (3.1) :

$$\begin{cases} \dot{x} = f(x) + g(x)u \\ y = h(x) \end{cases}$$

La structure d'observateur par modes glissants pour le système (3.1) s'écrit :

$$\begin{cases} \dot{\hat{x}} = f(\hat{x}) + g(\hat{x})u + \lambda sign(y - \hat{y}) \\ \hat{y} = h(\hat{x}) \end{cases} \quad (3.5)$$

C'est une copie du modèle, à laquelle on ajoute un terme correcteur, qui assure la convergence de $\hat{x}$ vers x. La surface de glissement dans ce cas est donnée par :

$$S = y - \hat{y} \quad (3.6)$$

Le terme de correction utilisé est proportionnel à la fonction discontinue $sign$ appliquée à l'erreur de sortie où $sign(x)$ est définie par :

$$sign(x) = \begin{cases} 1 & si\ x > 0 \\ 0 & si\ x = 0 \\ -1 & si\ x < 0 \end{cases}$$

Définition 3.5 : *Une surface $S = 0$ est attractive pour un domaine de convergence donné si toute trajectoire évoluant dans le domaine d'attraction est dirigée vers cette surface.*

Définition 3.6 : *Une surface $S = 0$ est invariante si toute trajectoire débutant dans cette surface ou atteignant cette surface, ne peut en sortir et évolue donc sur cette surface. La surface S=0 divise l'espace d'état en deux régions. La première région ε^+ correspond à s>0 et la seconde notée ε^- correspond à S<0. Si l'état du système est de côté ε^+ de l'espace d'état (ou du côté ε^-), il rejoindra forcément la surface $S = 0$. S'il dépasse de l'autre côté ε^- (ou du côté ε^+), il se ramènera vers $S = 0$ (figure 3.3). Cette surface $S = 0$ est donc*

appelée surface glissante et le mouvement sur cette surface est un mode glissant dont l'équation détermine la dynamique désirée du système.

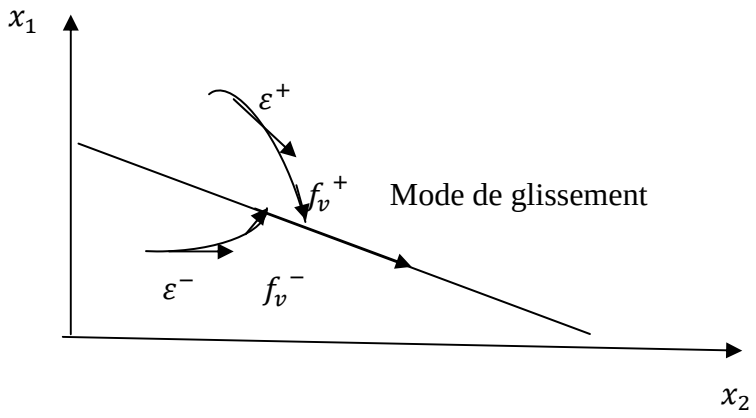


Fig. 3.3 Mode de glissement idéal

Une surface de discontinuité $S = 0$ *, suivant que l'état du système est sur* ε^+ *ou sur* ε^- *, il atteint la surface respectivement avec les vitesses* $f_v{}^+$ *ou* $f_v{}^-$.

Avec : ε^+ *et* ε^- *sont respectivement* $S > 0$ *et* $S < 0$, f^+ *et* f^- *sont les vecteurs de vitesse* où *:*

$$f_v = \begin{cases} f_v{}^+ \ si \ S > 0 \\ f_v{}^- \ si \ S < 0 \end{cases}$$

L'étude de l'existence d'un mode de glissement, comme l'étude de la stabilité d'un point d'équilibre, est basée sur la deuxième méthode de Lyapunov. La condition d'existence du mode de glissement est l'attractivité de la surface de commutation $S = 0$. Géométriquement, les vecteurs vitesses $f_v{}^+$ et $f_v{}^-$ vont être dirigés vers la surface de commutation. Cependant, dans certains cas, le glissement n'a pas lieu sur n'importe quel point de la surface de commutation car l'attractivité de cette dernière n'est assurée que dans un domaine restreint D_g, que l'on appelle domaine de glissement. Alors pour que la surface $S = 0$ soit attractive sur tout le domaine de fonctionnement, il faut que cette condition soit satisfaite :

$$S\dot{S} < 0 \quad \forall s \neq 0$$

Cette condition est appelée « condition d'attractivité (« reaching condition »).

- Nous étudions la stabilité asymptotique de la surface de glissement S en posant une fonction de Lyapunov V de la façon suivante :

$$V = \frac{1}{2}S^2$$

Alors la condition de stabilité est déduite :

$$\frac{dV}{dt} < 0 \Rightarrow S\frac{dS}{dt} < 0; \ \forall S \neq 0$$

3.4.1 Observateur à modes glissants étape par étape [27]

Considérons le système analytique (3.1) mono entrée– mono sortie, avec f, g, h sont des vecteurs de fonction analytiques de dimension appropriées. De plus, pour tout $x \in \mathbb{R}^n$, $g(x,0) = 0$ et le système (3.1) est supposé avoir des états bornés et son entrée bornée aussi.

Afin de transformer le système (3.1) en un système triangulaire, la condition du rang d'observabilité donnée dans la définition 3.3 doit être satisfaite et aussi pour tout $u \in \mathbb{R}^m$, le vecteur g doit vérifier la condition suivante :

$$dL_g L_f^i h \in span\{dh, \dots, dL_f^i h\} \quad 0 \leq i \leq n-1 \ \ \forall i \in \{0, \dots, n-1\}$$

Nous pouvons maintenant écrire la forme triangulaire du système (3.1) à l'aide d'un difféomorphisme au voisinage de x de la forme :

$$\begin{cases} \dot{x}_1 = x_2 + \bar{g}_1(x_1, u) \\ \dot{x}_2 = x_3 + \bar{g}_2(x_1, x_2, u) \\ \vdots \\ \dot{x}_{n-1} = x_n + \bar{g}_{n-1}(x_1, \dots, x_{n-1}, u) \\ \dot{x}_n = \bar{f}_n + \bar{g}_n(x, u) \\ y = x_1 \end{cases} \tag{3.7}$$

avec $g_i(u=0) = 0$ pour $\in \{1, \dots, n\}$, si et seulement si les conditions données ci-dessus sont satisfaites au voisinage de x.

3.4.2 Observateur à modes glissants pour le système triangulaire [12]

La structure de l'observateur proposé pour le système triangulaire est :

$$\begin{cases} \dot{\hat{x}}_1 = \hat{x}_2 + \bar{g}_1(x_1, u) + \lambda_1 sign_1(x_1 - \hat{x}_1) \\ \dot{\hat{x}}_2 = \hat{x}_3 + \bar{g}_2(x_1, \tilde{x}_2, u) + \lambda_2 sign_2(\tilde{x}_2 - \hat{x}_2) \\ \vdots \\ \dot{\hat{x}}_{n-1} = \hat{x}_n + \bar{g}_{n-1}(x_1, \tilde{x}_2 \dots, \tilde{x}_{n-1}, u) + \lambda_{n-1} sign_{n-1}(\tilde{x}_{n-1} - \hat{x}_{n-1}) \\ \dot{\hat{x}}_n = \bar{f}_n + \bar{g}_n(x_1, \tilde{x}_2, \dots, \tilde{x}_n, u) + \lambda_n sign_n(\tilde{x}_n - \hat{x}_n) \end{cases} \tag{3.8}$$

Où les variables $\tilde{x}_i$ sont données par :

$$\begin{cases} \tilde{x}_2 = \hat{x}_2 + \lambda_1 sign_1(x_1 - \hat{x}_1) \\ \tilde{x}_3 = \hat{x}_3 + \lambda_2\, sign_1\ (\tilde{x}_2 - \hat{x}_2) \\ \vdots \\ \tilde{x}_n = \hat{x}_n + \lambda_n\, sign_n(\tilde{x}_{n-1} - \hat{x}_{n-1}) \end{cases} \tag{3.9}$$

Et dans lequel $sign_i = E_i sign$ avec $E_i = 1$ $si\ E_1 = \cdots = E_{i-1} = 1$ et $x_1 - \hat{x}_1 = 0$, sinon $E_i = 0$. Dans la structure de l'observateur, la fonction $sign_i$ permet la convergence de $\tilde{x}_i - \hat{x}_i$ vers zéro si toutes les $\tilde{x}_j - \hat{x}_j; j < i$ sont convergés vers zéro.

Remarque 3.1 : *Si on considère que le système (3.7) vérifie les hypothèses 3.2 et 3.3 (la condition d'observabilité à gauche), nous pouvons choisir les gains λ_i de l'observateur à modes glissants tels que l'état $\hat{x}$ de l'observateur converge vers x en temps fini, et si l'entrée inconnue m est continue ou au moins continue par morceaux, alors son estimation $\hat{m}$ converge vers m en temps fini.*

Dans ce travail nous avons utilisé la forme originale du système de Chua-Hartley normalisé afin de construire un observateur à mode glissant étape par étape.

3.5 Phénomène de réticence ou chattering [26]

Un mode de glissement idéal ne peut pas exister en pratique car cela nécessite la présence d'une commande ou d'un correcteur d'erreur d'estimation qui commute à une fréquence infinie. En présence des limitations sur le temps de commutation, la discontinuité

produit un comportement dynamique particulier caractérisé par des fortes oscillations autour de la surface. Ce phénomène est appelé réticence (figure 3.4)

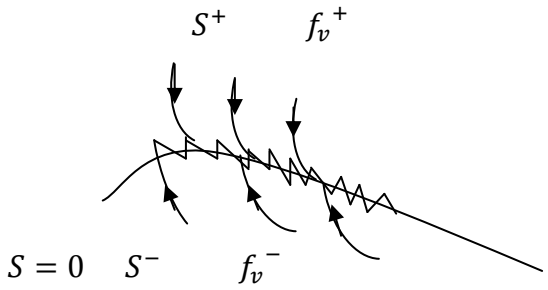


Fig. 3.4 Mode glissant avec réticence.

Le phénomène de réticence constitue un inconvénient majeur non négligeable, car même s'il est possible de le filtrer à la sortie du processus, il est susceptible d'exciter des modes de hautes fréquences qui n'ont pas été pris en compte lors de la modélisation du système. Ceci peut dégrader les performances et même conduire au problème d'instabilité [27]. Dans le but de réduire ce phénomène, de nombreuses solutions ont été proposées. Dans notre travail, la fonction $sign$ est remplacée par une fonction plus lisse de forme $[\frac{2}{\pi}\arctan(\frac{S}{\varepsilon})]$.

Une fois que la synchronisation entre le récepteur et l'émetteur est réalisé, il est possible d'utiliser ce phénomène pour transmettre une information $x_{info}(t)$. Il existe pour cela plusieurs techniques qui permettent de plus une transmission sécurisée. Il s'agit donc de méthodes de cryptage basées sur l'utilisation de signaux chaotiques. Décrivons brièvement quelques principales techniques qui nous intéressent dans ce travail.

3.6 Les cryptosystèmes chaotiques

Cette génération de systèmes de communication représentée à la figure 3.5 a été développée en 1997. Cette méthode combine la technique de cryptographie classique et la synchronisation du chaos afin d'améliorer le degré de sécurité à un niveau beaucoup plus élevé que les précédentes déjà étudiées au premier chapitre.

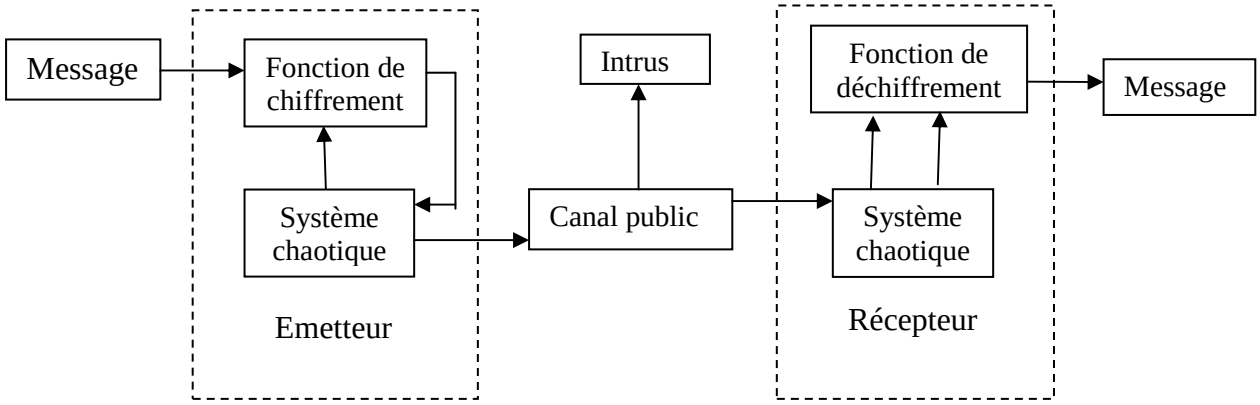


Fig. 3.5 Schéma de communication en utilisant les cryptosystèmes chaotiques.

3.6.1 Techniques d'insertion du message [4]

Dans un système cryptographique, l'objectif est de transmettre de manière sécurisée un message entre l'émetteur et le récepteur. Diverses techniques existent pour encoder le message sur la porteuse chaotique, certaines ayant été développées spécifiquement pour l'encodage de signaux numériques, tandis que d'autres permettent l'encodage de signaux analogiques.

Il existe pour les systèmes chaotiques quatre schémas classiques pour crypter le message : masquage par chaos (*Chaos Masking*), cryptage par commutation de clé chaotique (*Chaos Shift Keying*), cryptage par modulation (*Chaos Modulation*) et cryptage par inclusion [26]. Chaque méthode de cryptage présente des avantages, des inconvénients et des contraintes par rapport à la qualité cryptographique du système.

L'objectif de l'émetteur, rappelons-le, est de transmettre une information cryptée de telle manière qu'un espion ne puisse pas décrypter l'information, mais qu'un récepteur autorisé puisse le faire.

3.6.2 Les méthodes de transmission sécurisée

On dispose dans la littérature de différents schémas de communications chaotiques nécessitant la synchronisation. Il existe de nombreuses techniques de cryptage/décryptage utilisant comme étape centrale la synchronisation du chaos. On s'intéresse dans ce mémoire à

l'étude de deux cryptosystèmes chacun avec son moyen de transmission sécurisée et sa technique de cryptage.

3.6.2.1 Cryptage par addition [10]

Cette méthode appelée, masquage chaotique, est la première chronologiquement qui introduit la synchronisation du chaos. L'émetteur est un système chaotique autonome dont le signal de sortie $y(t)$ est ajouté au signal du message $m(t)$. La somme des deux signaux est transmise au récepteur à travers le canal de transmission, qui est un canal public.

Après la synchronisation des deux systèmes émetteur-récepteur, le message est extrait à l'aide d'une opération de soustraction. Le schéma représentant cette méthode est donné par la figure suivante :

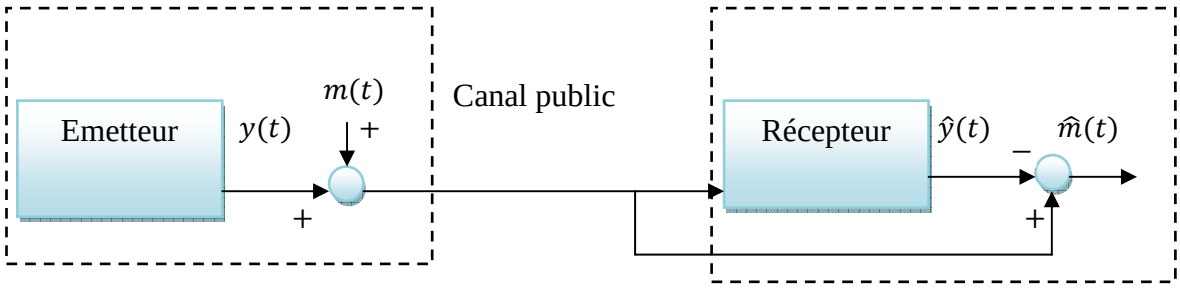


Fig. 3.6 Principe du cryptage par addition.

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. Dans les deux cas, l'amplitude du message original doit être plus petite que celle de la porteuse chaotique, d'une part pour ne pas perturber l'établissement de la synchronisation au niveau du récepteur, et d'autre part pour garantir le secret de la transmission.

Dans tous les cas, à cause de la présence du message, la synchronisation ne peut être parfaite. En outre, la fréquence du message doit être comprise dans le spectre du signal chaotique.

3.6.2.2 Cryptage par inclusion

Cette technique de cryptage consiste à injecter le message dans la dynamique de l'émetteur, sans toutefois réaliser une modulation de paramètre. 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 [10].

a/ Observateur à entrées inconnues

Le schéma de la figure (3.7) illustre un problème classique d'estimation d'état non linéaire à entrées inconnues : il faut reconstruire l'état $x(t)$ du système émetteur et également l'entrée inconnue $m(t)$.Différentes techniques de synthèse d'observateurs à entrées inconnues ont été utilisées dans la littérature, et peuvent être utilisées à des fins de décryptage.

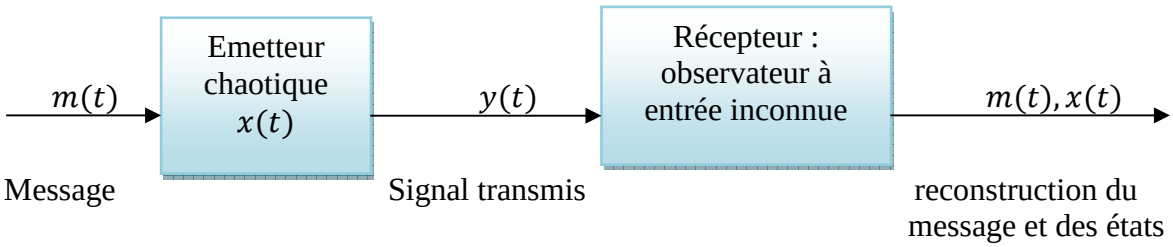


Fig. 3.7 Observateur à entrée inconnue.

b/ Décryptage par inversion

Le récepteur est conçu en inversant le modèle de l'émetteur. La figure (3.8) présente le principe général de cette approche.

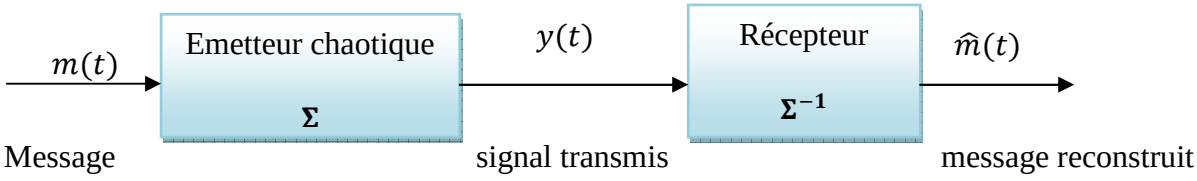


Fig. 3.8 Principe de cryptage par inversion.

Dans toutes ces méthodes de cryptage, la clé de cryptage est constituée par l'ensemble des paramètres du générateur de chaos qui permettent de produire le signal chaotique transmis. En effet la première condition pour que le récepteur génère le même signal chaotique que l'émetteur est qu'il soit réglé à l'identique. Une fois cette condition vérifiée, la synchronisation est envisageable.

3.6.2.3 Transmission à deux voies [26]

Dans le schéma présenté à la figure (3.9), l'émetteur envoie deux signaux au récepteur. Le premier y_1, permet la synchronisation du récepteur. Le second, y_2 envoyé éventuellement sur un autre canal est un signal chaotique qui contient l'information à transmettre.

Parmi les avantages de cette méthode, on peut souligner d'une part que le signal y_1 ne contient aucune information sur le message, par conséquent la synchronisation peut s'établir de façon optimale. D'un autre côté, le second signal y_2 contient l'information qui peut être soit cryptée par une fonction non linéaire de l'état x, soit simplement masquée par un signal chaotique généré par l'émetteur, qui sert de porteuse. On peut noter également que 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.

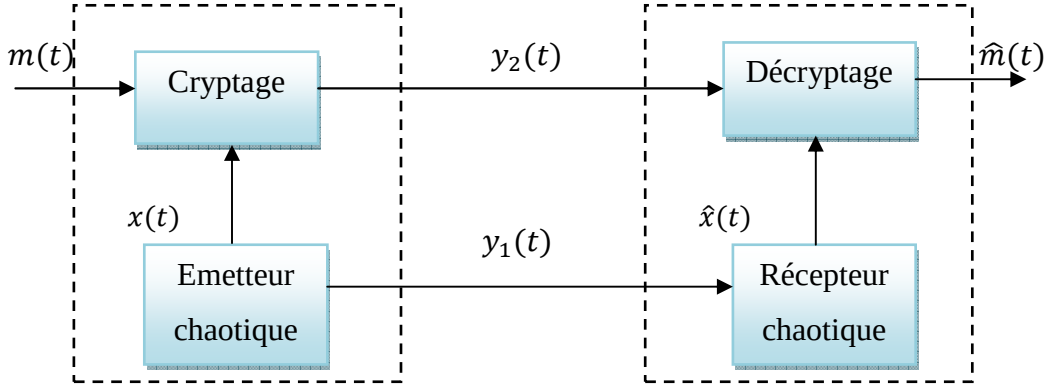


Fig. 3.9 Transmission à deux voies

3.7 Description du système émetteur-récepteur

Dans cette section, nous présentons le système de transmission sécurisée complet composé d'un émetteur, récepteur et les deux techniques de cryptages utilisées.

3.7.1 L'émetteur « circuit de Chua-Hartley »

Il est existe plusieurs modèle de représentation du circuit de Chua, dans notre mémoire, nous avons opté pour le « Chua-Hartley ». Ce choix est indiqué par le fait que l'équivalent d'ordre fractionnaire de ce circuit est proposé dans la littérature [11] et fera l'objet d'étude au chapitre suivant.

Le système de Chua-Hartley est différent du système de Chua habituel (voir le chapitre 2) où la non-linéarité par morceaux est remplacée par une non-linéarité cubique appropriée, ce qui rapporte un comportement très semblable.

Soit le modèle de représentation du circuit de Chua-Hartley suivant :

$$\begin{cases} \dot{x}_1 = \alpha(x_2 + \frac{x_1 - 2x_1^3}{7}) \\ \dot{x}_2 = x_1 - x_2 + x_3 \\ \dot{x}_3 = -\beta x_2 = -\frac{100}{7} x_2 \end{cases} \tag{3.10}$$

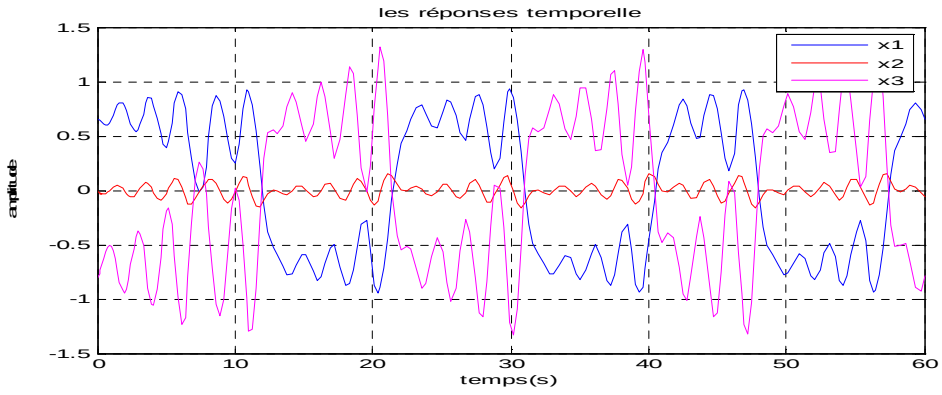
Où la non-linéarité cubique est : $f(x_1) = \frac{x_1 - 2x_1^3}{7}$

$$x_1 = \frac{V_1}{\xi}, \qquad x_2 = \frac{V_2}{\xi}, \qquad x_3 = \frac{I_L}{\xi . G}$$

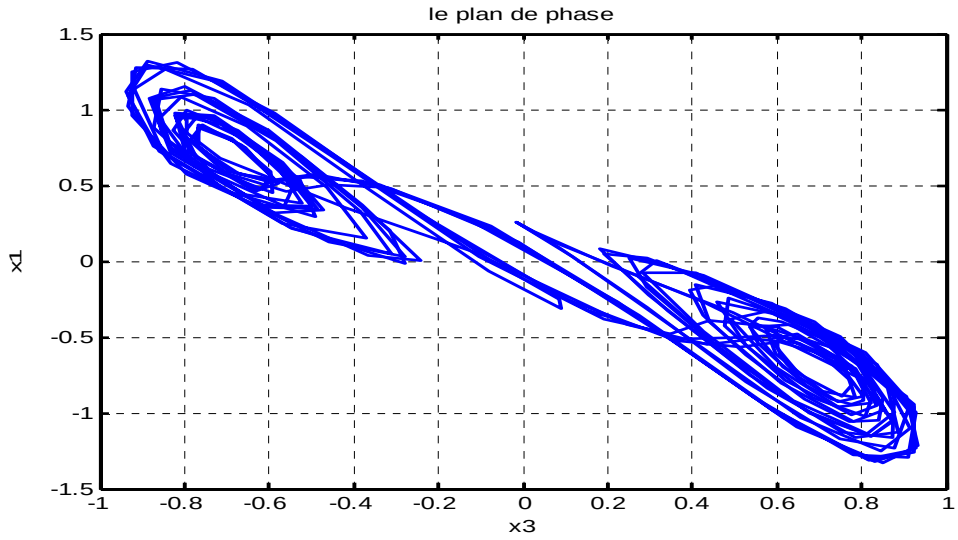
ξ est la tension de palier de la diode.

- **<u>Le comportement chaotique du système</u>**

  Lors des simulations sous Matlab, on a pris $\alpha = 9.5$, $\beta = -\frac{100}{7}$ et les conditions initiales $(x_{10}, x_{20}, x_{30}) = (0.65, 0, -0.8)$



a)Réponses temporelles



b) plan de phase $(x_1 x_3)$

Fig. 3.10 Le comportement chaotique du circuit de Chua-Hartley.

Ces deux figues représentent les caractéristiques chaotiques du circuit de Chua-Hartley, tels que l'aspect aléatoire observé sur les réponses temporelles des trois états et l'attracteur chaotique étrange illustré par le portrait de phase dans le plan de phase $(x_1 x_3)$.

Remarque 3.2 *Dans le cas des systèmes dynamiques non-linéaire de dimension 3, un point d'équilibre "selle" est un point sur lequel le modèle linéarisé équivalent a au moins une valeur propre dans la région stable et une valeur propre dans la région instable. Dans le même système, un point "selle" est appelé point "selle" d'indice 1 si l'une des valeurs propres est instable et les autres sont stables. Aussi, un point "selle" d'indice 2 est un point "selle" avec une valeur propre stable et deux valeurs propres instables. Aux systèmes chaotiques, il est prouvé que les rouleaux sont générés à autour des points "selles" d'indice 2.*

- **La stabilité des points d'équilibres :**

Le système de Chua-Hartley possède trois points d'équilibre :

$p_{01} = (0,0,0)$; $p_{02} = (\frac{-\sqrt{2}}{2}, 0, \frac{\sqrt{2}}{2})$; $p_{03} = (\frac{\sqrt{2}}{2}, 0, \frac{-\sqrt{2}}{2})$

La matrice jacobienne du système est alors donnée par :

$$J = \frac{\partial x}{\partial x_i} = \begin{pmatrix} \alpha\left(\frac{1-6x_1^2}{7}\right) & \alpha & 0 \\ 1 & -1 & 1 \\ 0 & -\frac{100}{7} & 0 \end{pmatrix}$$

Le calcul de la matrice J aux points d'équilibre p_{01}, p_{02}, p_{03} conduit respectivement à :

$$J_1 = \begin{pmatrix} \frac{\alpha}{7} & \alpha & 0 \\ 1 & -1 & 1 \\ 0 & -\frac{100}{7} & 0 \end{pmatrix}$$ pour le point p_{01}

$$J_2 = \begin{pmatrix} \frac{-2\propto}{7} & \alpha & 0 \\ 1 & -1 & 1 \\ 0 & -\frac{100}{7} & 0 \end{pmatrix}$$ pour les points (p_{02}, p_{03})

Les valeurs propres de la matrice J_1sont : $\mu_1 = 2.3676$, $\mu_2 = -1.0052 + 2.6792i$ et $\mu_3 = -1.0052 - 2.6792i$ tandis que les valeurs propres de la matrice J_2 sont : $\mu_1 = -4.1552$, $\mu_{2,3} = 0.2204 \pm 3.0469i$. Le point d'équilibre p_{01} est stable alors que les deux autres points (p_{02}, p_{03}) sont instables. Effectivement on a obtenu 2 points selle d'ordre2, où l'attracteur de Chua-Hartley est généré autour de ces deux points selles d'indices 2.

- **<u>L'étude de l'observabilité de l'émetteur</u>**

Considérons le système de circuit de Chua-Hartley, l'émetteur de notre schéma de transmission:

$$\begin{cases} \dot{x}_1 = \alpha\left(x_2 + \frac{x_1 - 2x_1^3}{7}\right) \\ \dot{x}_2 = x_1 - x_2 + x_3 \\ \dot{x}_3 = -\frac{100x_2}{7} \\ y = x_1 \end{cases} \quad (3.11)$$

Remarque 3.3 *Nous avons les trois états du système* (x_1, x_2, x_3)*et le message m confidentiel sont bornés.*

Teste d'observabilité :

Nous avons $h = [x_1\ 0\ 0]$ et $dh = [1\ 0\ 0]$. Vérifiant maintenant l'observabilité du système (3.11) au sens du rang comme suit :

$$Rang\{dh, dL_f h, \dots, dL_f^{n-1} h\}^T = n$$

D'où : $O = \begin{bmatrix} dh \\ dL_f h \\ dL_f^2 h \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ \alpha(\frac{1-6x_1^2}{7}) & \alpha & 0 \\ \alpha\rho\left(\frac{1-6x_1^2}{7}\right) + \alpha & \alpha(\rho - 1) & \alpha \end{bmatrix}$

avec :

$$\rho = \alpha\,(\frac{1 - 6x_1^2}{7})$$

On a obtenu $rang(O) = 3 = n$ donc le système (3.11) est observable. Nous étudions maintenant la condition de recouvrement d'observabilité et l'inversibilité à gauche de ce système.

- **L'étude de la condition de recouvrement d'observabilité et d'inversibilité à gauche**

  A ce stade, les hypothèses 3.1 et 3.2 sont vérifiées pour le système de Chua-Hartley. Nous étudions maintenant la condition de recouvrement d'observabilité et l'inversibilité à gauche de l'émetteur chaotique (le système de Chua-Hartley incluant le message confidentiel donné en (3.11)), soit la possibilité de retrouver le message injecté dans l'émetteur. Si ses deux conditions sont satisfaites, l'hypothèse 3.3 est vérifiée et nous pourrons construire un observateur pour le système. Nous écrivons le système (3.11) sous la forme :

$$\begin{cases} \dot{x} = f(x) + g(x)m \\ y = Cx \end{cases}$$

Avec $m(t)$ l'information à envoyer et $g(x) = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$

-On vérifie maintenant la troisième hypothèse 3.3: $\begin{bmatrix} dh \\ dL_f h \\ \vdots \\ dL_f^{n-1} \end{bmatrix} . g(x) = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ \theta \end{bmatrix}$

On aura :

$$O.g(x) = \begin{bmatrix} 1 & 0 & 0 \\ \alpha(\frac{1-6x_1^2}{7}) & \alpha & 0 \\ \alpha\rho\left(\frac{1-6x_1^2}{7}\right)+\alpha & \alpha(\rho-1) & \alpha \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \alpha = \theta \end{bmatrix}$$

Avec $\alpha = 9.5 \neq 0$. Ainsi, la condition de recouvrement d'observabilité de l'émetteur chaotique est vérifiée ainsi que l'inversibilité à gauche. Il est possible d'extraire le message m à l'aide d'un observateur à mode glissants.

3.7.2 Le récepteur « observateur à modes glissants »

Dans la section précédente nous avons vérifié l'observabilité du circuit de Chua et la condition de recouvrement d'observabilité de l'émetteur chaotique donnée en (3.12). De plus, le système possède des états bornés et le message est lui aussi borné. Nous pouvons alors construire un observateur à modes glissants pour le système (3.11) dans le but de reconstruire tous les états du circuit et le message à partir de l'état connu x_1, qui est ici la sortie du système (3.17) transmise au récepteur.

Pour que cet observateur à mode glissant fonctionne étape par étape, le système doit se mettre sous une forme triangulaire d'observation, donc le vecteur g doit vérifier la condition suivante :

$$dL_g L_f^2 h \in span\left\{dh, dL_f^1 h, dL_f^2 h\right\}$$

Nous avons

- $dh = [1 \quad 0 \quad 0]$

- $dL_f h = [\alpha\left(\frac{1-6x_1^2}{7}\right) \quad \alpha \quad 0]$
- $dL_f^2 h = [\alpha p\left(\frac{1-6x_1^2}{7}\right) + \alpha \quad \alpha(p-1) \quad \alpha]$
- $dL_g L_f^2 h = [0 \;\; 0 \;\; 0]$

D'où

$$dL_g L_f^2 h \in span\left\{dh, dL_f^1 h, dL_f^2 h\right\}$$

Nous pouvons maintenant écrire la forme triangulaire d'observation suivante

$$\begin{cases} \dot{\hat{x}}_1 = \alpha\left(\hat{x}_2 + \frac{x_1 - 2x_1^3}{7}\right) + \lambda_1 sign(x_1 - \hat{x}_1) \\ \dot{\hat{x}}_2 = x_1 - \tilde{x}_2 + \hat{x}_3 + E_1\lambda_2 sign(\tilde{x}_2 - \hat{x}_2) \\ \dot{\hat{x}}_3 = -\frac{100}{7}\hat{x}_2 + E_2\lambda_3 sign(\tilde{x}_3 - \hat{x}_3) \end{cases} \tag{3.12}$$

avec λ_i sont les gains de l'observateur.

Les états auxiliaires sont :

$$\begin{cases} \tilde{x}_2 = \hat{x}_2 + \frac{1}{\alpha}\lambda_1 E_1 sign(x_1 - \hat{x}_1) \\ \tilde{x}_3 = \hat{x}_3 + E_2\lambda_2 sign(\tilde{x}_2 - \hat{x}_2) \end{cases}$$

Cet observateur fonctionne étape par étape comme suit

- lorsque $\hat{x}_1 = x_1$, alors $E_1 = 1$ sinon $E_1 = 0$.

Donc quand $E_1 = 1$, l'observateur reconstruit l'état suivant c'est-à-dire x_2.

De la même manière :

- lorsque$\hat{x}_2 = \tilde{x}_2$, alors $E_2 = 1$ sinon $E_2 = 0$.

Quand $E_2 = 1$, on passe à l'étape suivante, soit la reconstruction de x_3.

- Enfin lorsque $\hat{x}_3 = \tilde{x}_3$ et $E_3 = 1$ alors le message est reconstruit par l'observateur.

Remarque 3.4 : *si les hypothèses 1, 2 et 3 sont vérifiées, alors l'observateur à modes glissants (3.12) converge en temps fini étape par étape, c'est-à-dire que l'erreur d'estimation* $e_i = x_i - \hat{x}_i$ *tend vers zéro au bout d'un temps fini (voir la démonstration dans [12], [27]).*

- **<u>L'étude de convergence de l'observateur à mode glissant</u> :**

Les dynamiques d'erreur d'estimation ($e = x - \hat{x}$) sont données par :

$$\begin{cases} \dot{e}_1 = \alpha e_2 - \lambda_1 sign(e_1) \\ \dot{e}_2 = e_1 - (x_2 - \tilde{x}_2) + e_3 - E_1\lambda_2 sign(\tilde{x}_2 - \hat{x}_2) \\ \dot{e}_3 = -\frac{100}{7} e_2 - E_2\lambda_3 sign(\tilde{x}_3 - \hat{x}_3) \end{cases} \quad (3.13)$$

Avec « $sign$ » représente la fonction $sign$ usuelle.

En considérant la fonction de Lyapunov $V = \frac{1}{2}e_1^2$ ou $e_1 = x_1 - \hat{x}_1$, on montre l'attractivité de la surface de glissement $S = e_1$ comme suit : on dérive la fonction V et on obtient :

$$\dot{V} = e_1\dot{e}_1 = e_1(\alpha e_2 - \lambda_1 sign(e_1))$$

$\dot{V} < 0$ lorsque $\lambda_1 > \alpha|e_2|_{max}$, l'utilisation de la fonction « $sign$ » et la fonction de Lyapunov décroissante permettent la convergence en temps fini t vers la surface de glissement $S = 0$.

Donc pour $\lambda_1 > \alpha|e_2|_{max}$, $\hat{x}_1$ converge vers x_1 et reste égal à x_1 pour $t > t_0$. autrement dit $|e_2|_{max}^{t_0}$ décroit et converge vers zéro après l'instant t_0, ou $|e_2|_{max}^{t_0}$ est le maximum de e $\forall t \in [0, t_0]$.

On peut calculer le temps de convergence t sachant que $S = e_1$, de la façon suivante :

$$S\dot{S} = e_1(\alpha e_2 - \lambda_1 sign(e_1))$$

Si $\lambda_1 = 2\alpha|e_2|_{max}$, nous avons :

$$S\dot{S} \leq e_1(\alpha|e_2|_{max} - 2\alpha|e_2|_{max}) = -e_1(\alpha|e_2|_{max}) = -e_1\frac{\lambda_1}{2} = -S\frac{\lambda_1}{2}$$

Par intégration, on obtient :

$$|S(t)| - |S(0)| \leq \frac{\lambda_1}{2} t$$

D'où le temps de convergence est donné par :

$$t_0 = \frac{2S(0)}{\lambda_1}$$

Avec $S(0) = x_1(0) - \hat{x}_1(0)$ est la condition initiale.

L'état auxiliaire $\tilde{x}_2$ s'obtient lorsque $\dot{e}_1 = 0, \forall t > t_0$ c'est-à-dire à partir de l'équation : $e_2 = \frac{\lambda_1}{\alpha} sgn(e_1)$. Alors $\tilde{x}_2$ devient égal à x_2 au bout d'un temps fini, pour $t > t_0$.

Remarque 3.5 *Dans cette partie, on vient de monter aussi la stabilité asymptotique (l'attractivité) de la surface de glissement s.*

Dans ce qui suit, nous allons faire une comparaison des résultats obtenus pour chaque cryptosystème, en utilisant le même émetteur et récepteur. Seules les méthodes de cryptage et l'insertion du message qui diffère. Le premier cryptosystème « transmission à deux voies » avec la méthode de cryptage par addition, le second « transmission à une seule voie » avec la méthode de cryptage par inclusion.

3.7.2 Le premier cryptosystème « cryptage par addition »

Nous allons maintenant construire un système de transmission sécurisée à deux voix qui sépare totalement l'étape de la synchronisation et l'étape de cryptage de l'information.

La synchronisation des états entre le système émetteur-récepteur se fait par la ligne y_1, en suite pour le cryptage, on injecte le message à la deuxième ligne de transmission y_2.

Le système émetteur « *Chua-Hartley » est* décrit par les équations suivantes:

$$\begin{cases} \dot{x}_1 = \alpha(x_2 + \dfrac{x_1 - 2x_1^3}{7}) \\ \dot{x}_2 = x_1 - x_2 + x_3 \\ \dot{x}_3 = -\beta x_2 = -\dfrac{100}{7} x_2 \\ y = x_1 \end{cases}$$

Nous avons choisi un message sinusoïdal qui varie lentement par rapport aux dynamiques de l'oscillateur chaotique.

Le message est $m(t) = 1 \sin \omega t$ avec $\omega = 1\, rad/sec$ et de fréquence $= 0.159\, Hz$ **,** qui est représenté à la figure suivante.

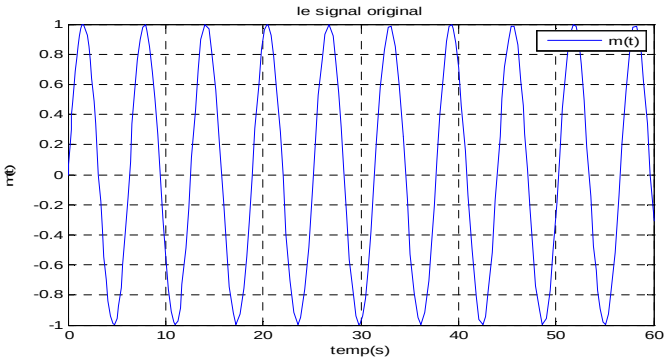


Fig. 3.11 Le message original $m(t)$

❖ **Processus de chiffrement**

Pour le chiffrement avec cette méthode, on ajoute le message dans la deuxième ligne de transmission y_2 par une simple fonction d'addition comme suit :

$$m_c = y + m = x_1 + m$$

où m_c est le message crypté.

Le message correspondant au signal crypté (envoyé à travers un canal de transmission vers le récepteur), $m_c = \psi(x, s)$, est représentée à la figure 3.12.

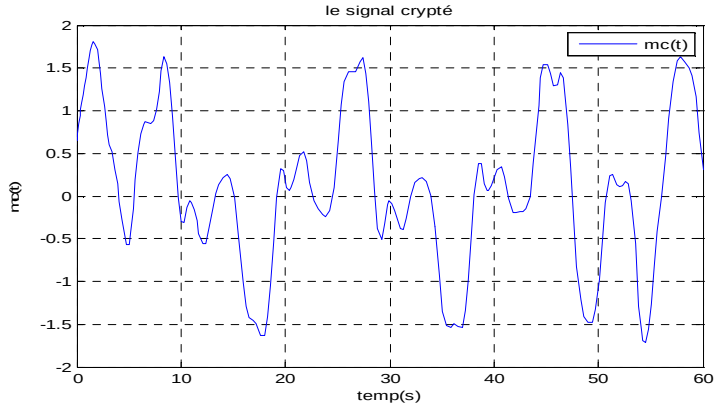


Fig. 3.12 Le message crypté $m_c(t)$

❖ **Processus de synchronisation**

Cette étape est utilisée pour la récupération des états de l'émetteur ainsi que le message confidentiel. On choisit comme signal de sortie $y_1 = x_1$,. $h = [x_1\ 0\ 0]$. Ce signal, ne contenant aucune information du message m, est utilisé seulement pour la synchronisation. Il est envoyé via un deuxième canal de transmission séparé du premier.

Pour les deux méthodes de cryptage, on prend les mêmes conditions initiales et la même valeur de $\alpha = 0.95$:

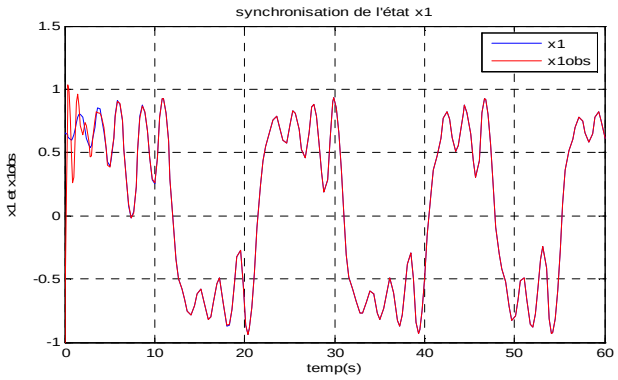
-Les conditions initiales de l'émetteur sont : $(x_{10}, x_{20}, x_{30}) = (0.65, 0, -0.8)$.

-Les conditions initiales du récepteur : $(\hat{x}_{10}, \hat{x}_{20}, \hat{x}_{30}) = (-0.6, -0.2, 0)$.

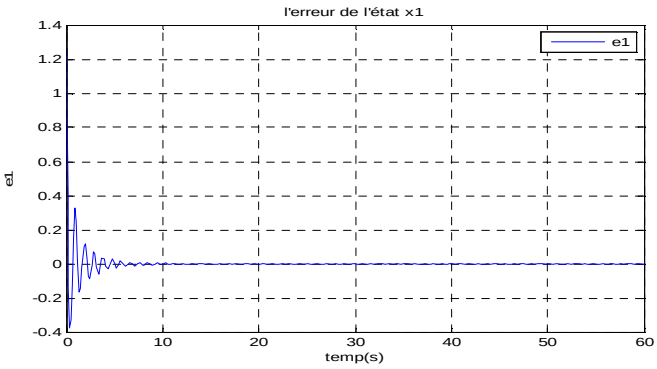
-Les valeurs des gains de l'observateur sont : $\lambda_1 = \lambda_2 = \lambda_3 = 10$

Pour diminuer l'effet du chattering, nous avons remplacé la fonction signe par la fonction « arc tangente ».

Les résultats de simulation du système de communication utilisant la méthode de cryptage par addition sont montrés sur les figures (3.13, 3.14, 3.15). D'après ces résultats, les états du système sont reconstruits, les erreurs de synchronisation (e_1, e_2 et e_3) convergent vers zéro en un temps fini respectivement $t_{e1} = 8\,\text{sec}$, $t_{e2} = 10\,\text{sec}$, $t_{e3} = 12sec$. Nous remarquons aussi que le chattering apparait juste pendant les premiers instants du régime transitoire.

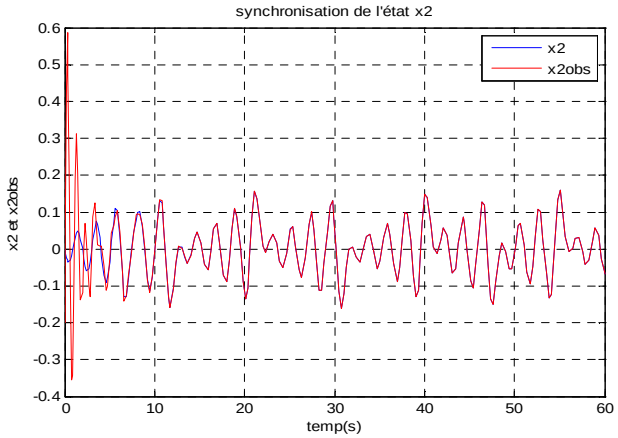


a)Les états $x_1 et\ \hat{x}_1$

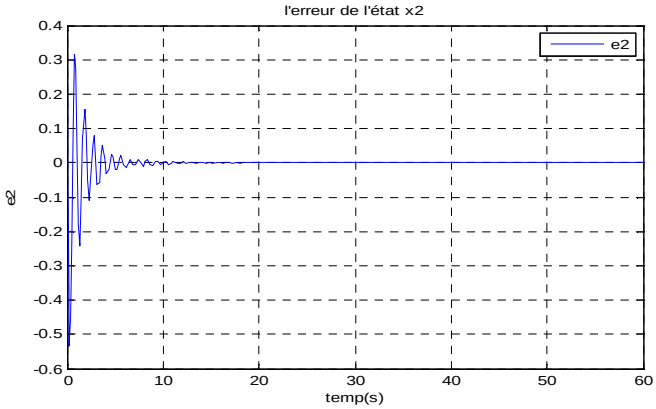


b) L'erreur de synchronisation de l'état x_1

Fig. 3.13 Le résultat de synchronisation des états x_1 et $\hat{x}_1$.

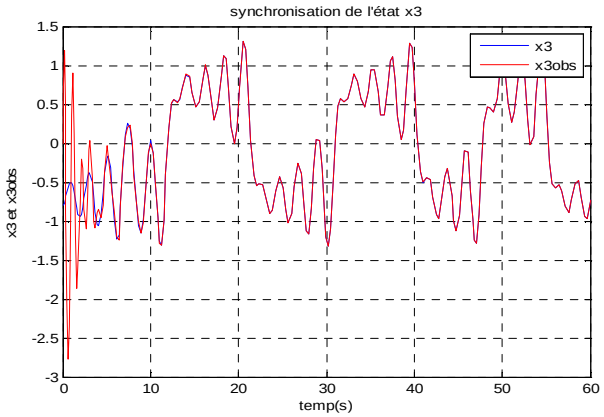


a) Les états $x_2 et\ \hat{x}_2$

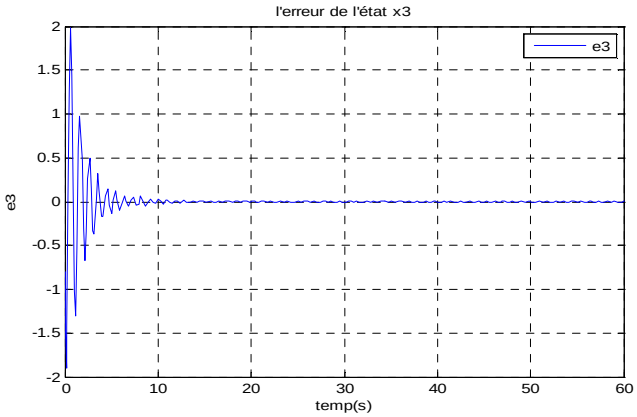


b) L'erreur de synchronisation de l'état x_2

Fig. 3.14 Le résultat de synchronisation des états x_2 et $\hat{x}_2$.



a) Les états $x_3 et\ \hat{x}_3$



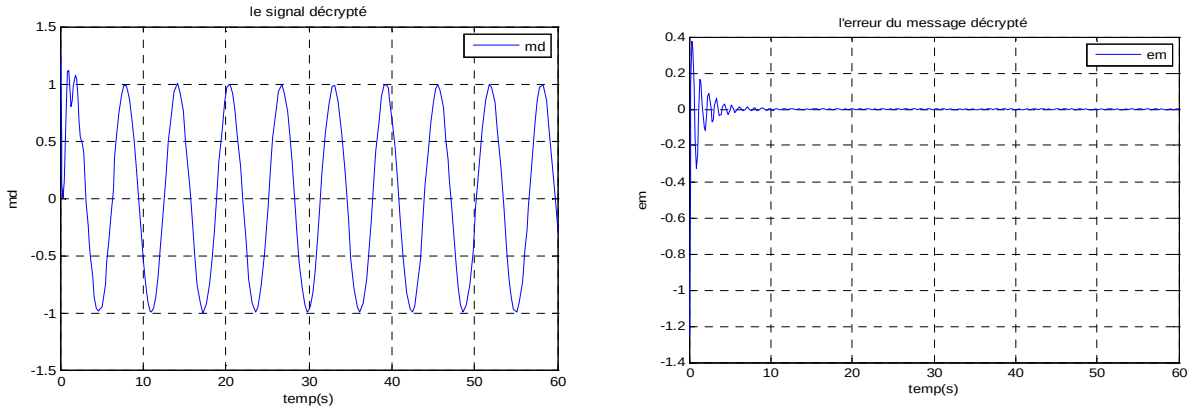
b) L'erreur de synchronisation de l'état x_3

Fig. 3.15 Le résultats de synchronisation des états x_3 et $\hat{x}_3$.

❖ **Processus de déchiffrement**

Cette étape sert à reconstruire le signal de départ. Pour déchiffrer le message transmis à l'aide du système (3.11), nous utilisons dans un premier temps l'observateur à modes glissant étape par étape (3.12) pour la synchronisation qui est présenté à la section 3.7.2, ensuite une simple fonction de soustraction nous permet de récupérer le message original comme suit:

$$m_d = m_c - \hat{x}_1$$



a) message déchiffré $m_d(t)$ **b)** L'erreur du message déchiffré e_m

Fig. 3.16 Le message déchiffré m_d.

La figure 3.16 montre le message déchiffré, juste pendant les premiers instants du régime transitoire qu'on observe le phénomène du chattering et l'erreur du message déchiffré tende vers zéros en un temps fini grâce à l'observateur à mode glissant qui assure un temps fini de convergence.

3.7.4 Le deuxième cryptosystème « cryptage par inclusion »

Dans cette seconde technique, l'état de l'émetteur et le signal d'information correspondant au signal à transmettre sont reconstruits simultanément par la méthode de cryptage dite par inclusion devant celle de la porteuse. On a choisi comme émetteur chaotique le système de *Chua-Hartley* décrit par les équations :

$$\begin{cases} \dot{x}_1 = \alpha(x_2 + \dfrac{x_1 - 2x_1^3}{7}) \\ \dot{x}_2 = x_1 - x_2 + x_3 \\ \dot{x}_3 = -\dfrac{100}{7}x_2 + m \\ y = x_1 \end{cases}$$

Avec cette méthode de cryptage il y'a qu'une seule ligne de transmission y, nous ajoutons le message m à la dynamique de l'état x_3. Notons que le message est le dernier état à reconstruire par des dérivations successives des sorties de l'observateur. Cela constitue un moyen pour satisfaire la condition de recouvrement d'observabilité. Le message original choisi est $m(t) = 0.3\sin\omega t$ de pulsation $\omega = 1\,rad/sec$ et de fréquence $f = 0.159Hz$.

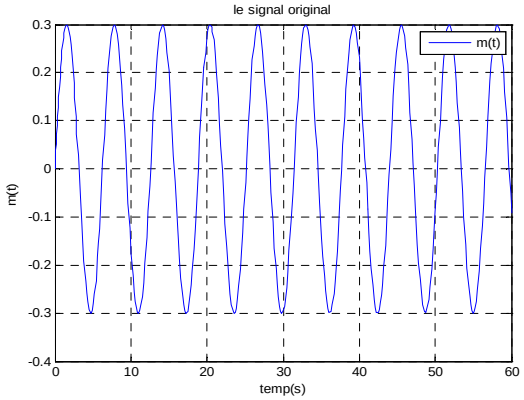


Fig. 3.17 Le message original m(t)

❖ **Processus de cryptage**

Pour le cryptage avec cette méthode, le message est injecté à la dynamique de l'état x_3 comme suit :

$$\begin{cases} \dot{x}_1 = \alpha\left(x_2 + \dfrac{x_1 - 2x_1^3}{7}\right) \\ \dot{x}_2 = x_1 - x_2 + x_3 \\ \dot{x}_3 = -\beta x_2 + m = -\dfrac{100}{7}x_2 + m \\ y = x_1 \end{cases}$$

Où m_c est le message crypté.

Le message correspondant au signal crypté (envoyé à travers un canal de transmission vers le récepteur), m_c est représentée à la figure 3.18.

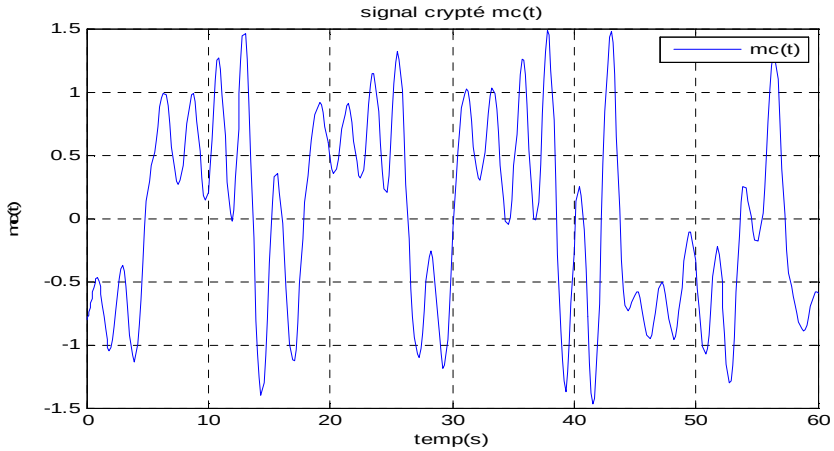


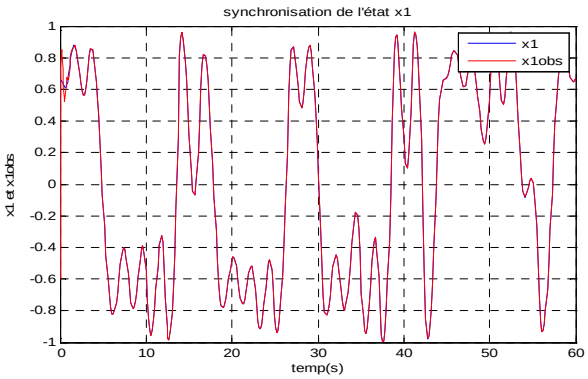
Fig. 3.18 Le message crypté $m_c(t)$

❖ **Processus de synchronisation**

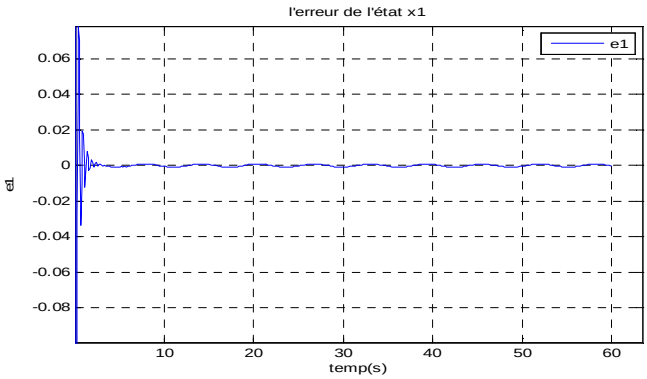
Cette étape est utilisée pour la récupération des états de l'émetteur et le message confidentiel.

Les valeurs des gains de l'observateur à mode glissant sont : $\lambda_1 = 30,\ \lambda_2 = 18,\ \lambda_3 = 22$

Les résultats de simulation du système de communication utilisant la méthode de cryptage par inclusion sont montrés sur les figures (3.19, 3.20, 3.21). D'après ces résultats, les états du système sont reconstruits, les erreurs de synchronisation (e_1, e_2 et e_3) convergent vers zéro juste le chattering qui apparait aux premiers instants du régime transitoire de chaque état.

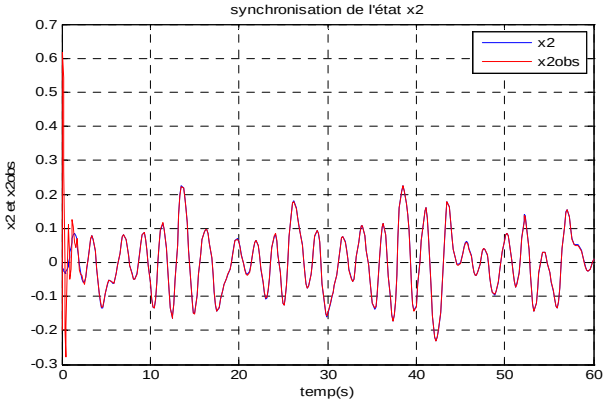


a) Les états $x_1 et\ \hat{x}_1$

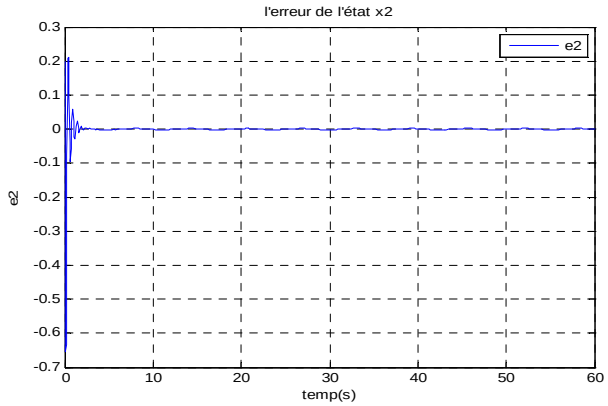


b) L'erreur de synchronisation de l'état x_1

Fig. 3.19 Le résultat de synchronisation de l'état x_1.

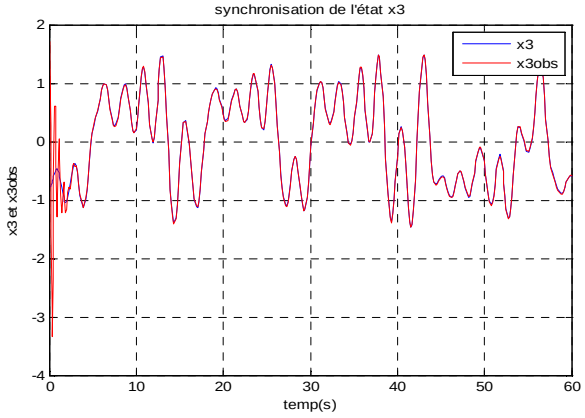


a) Les états $x_2 et\ \hat{x}_2$

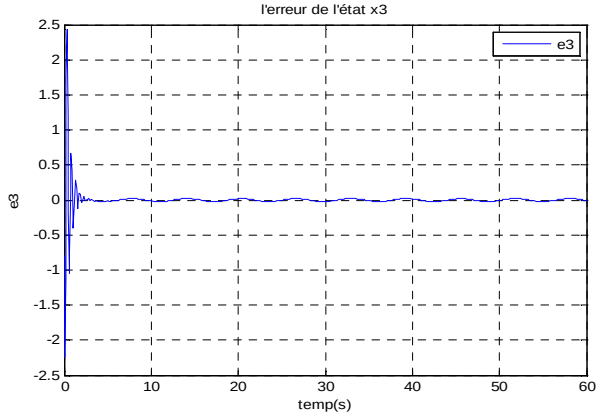


b) L'erreur de synchronisation de l'état x_2

Fig. 3.20 Le résultat de synchronisation de l'état x_2



a) Les états $x_3 et\ \hat{x}_3$



b) L'erreur de synchronisation de l'état x_3

Fig. 4.21 Le résultat de synchronisation de l'état x_3

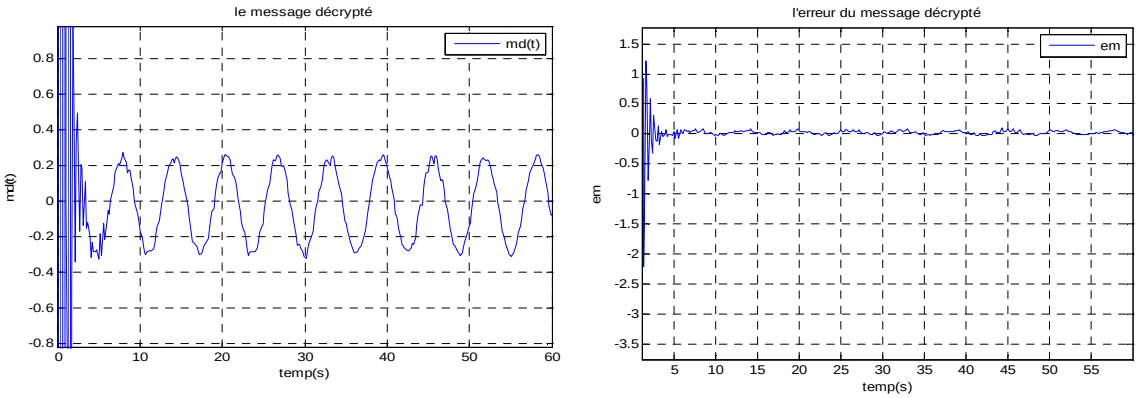
❖ **Processus de déchiffrement**

Pour déchiffrer le message transmis à l'aide du système (3.11), nous utilisons l'observateur à modes glissant étape par étape.

Lorsque $\hat{x}_3 = \tilde{x}_3$, le message sera reconstruit par l'observateur. Pour déchiffrer le message nous utilisons l'équation suivante :

$$\tilde{m} = E_3 \lambda_3 sign(\tilde{x}_3 - \hat{x}_3)$$

où $\widetilde{m}$ est le message décrypté



a) le message déchiffré $m_d(t)$ **b)** L'erreur du message déchiffré e_m

Fig. 3.22 Le message déchiffré m_d

La figure (3.22) montre le résultat de reconstitution du message original, où l'erreur du message déchiffré tende vers zéro mais le chattering perturbe tout le régime transitoire et apparait même au régime permanent.

3.8 Robustesse aux bruits de transmission et aux variations des paramètres

3.8.1 Robustesse aux bruits de transmission

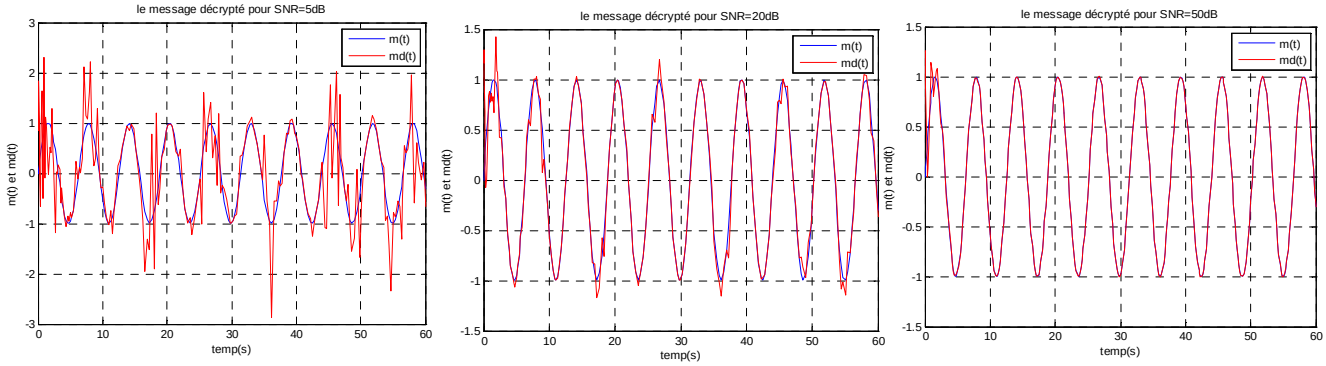
La robustesse aux bruits se pose pour tout système de communication analogique ou numérique : l'émetteur est relié au récepteur par un canal, l'élément physique qui permet de transmettre les informations selon la nature du canal (des notions déjà vu au chapitre 1). Quelque soit le canal utilisé, le bruit perturbe le signal en lui ajoutant une grandeur qui peut rendre le message plus ou moins compréhensible par le récepteur [4].

Dans cette partie, nous étudions l'impact, sur la qualité de restauration du message (signal sinusoïdal), du bruit affectant le signal dévolu à la synchronisation. On considère un bruit additif b(t) gaussien, normal centré perturbant le signal $y(t)$. Pour quantifier le rapport entre l'amplitude du signal et celle du bruit qui l'affecte, on rappelle la définition du rapport signal sur bruit, exprimé en décibels **:**

$$SNR(y,b) = 20\log_{10}\frac{\|y(t)\|}{\|b(t)\|}$$

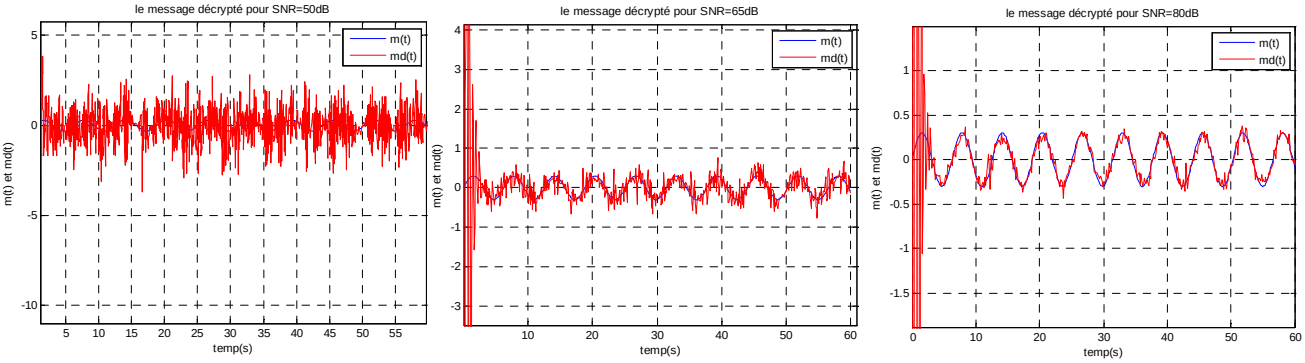
Plus ce rapport est grand, moins le bruit perturbe le signal original.

- ***Les résultats de simulation***



a) SNR = 5 dB b) SNR = 20 dB c) SNR = 35 dB

Fig. 3.23 Le message déchiffré en présence de bruit de transmission pour différents SNR



a) SNR = 50 dB b) SNR = 65 dB c) SNR = 80dB

Fig. 3.24 le message déchiffré en présence de bruit de transmission pour différents SNR.

On a représenté les résultats de simulation de robustesse aux bruits de transmission pour les deux cryptosystèmes. Les figures 3.23 et 3.24 montrent respectivement les messages reconstruits pour différentes SNR (SNR = 5dB, 20dB, 35dB) pour le premier cryptosystème et (SNR = 50dB, 65dB, 80dB) pour le deuxième.

La présence du bruit sur le signal transmis, comme nous venons de le voir apporte des erreurs dans l'estimation des états de l'émetteur (système (3.11)). Par conséquence, le message est complètement perdu, le cas du premier cryptosystème voir la figure 3.23a pour

une valeur de $SNR = 5dB$ et le deuxième cryptosystème pour une $SNR = 50dB$ voir la figure 3.24a.

D'après ces résultats, nous constatons que les deux cryptosystèmes sont sensibles au bruit de transmission, mais la restauration reste meilleure pour le premier cryptosystème tel qu'on peut récupérer le message jusqu'à une valeur de $SNR = 35dB$ qui correspond à un grand niveau de bruit.

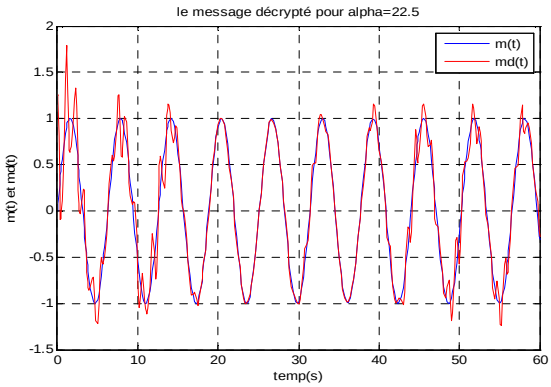
3.8.2 Robustesse aux variations de paramètres

Dans ce paragraphe, nous testons la robustesse et la capacité d'adaptation du système de communication pour les deux méthodes de cryptage proposé face à un pirate possédant des paramètres proches des valeurs réels du système. Notons que dans ce contexte, la transmission est d'autant plus sécurisée que le système est plus sensible aux variations des paramètres c'est-à-dire qu'il doit être plus robuste. Rappelons que les paramètres du système constituent la clé de sécurité. Plus le nombre de paramètres est grand, plus la transmission est sécurisée. On note $\grave{k}$ la clé de décryptage$\grave{k} = f(\grave{\alpha}, \beta)$, pour éviter toute confusion, on choisit les paramètres de la clé de déchiffrement $k = f(\alpha = 10.5;\ \beta = 100/7)$ au niveau de l'émetteur différents des paramètres de la clé de décryptage.

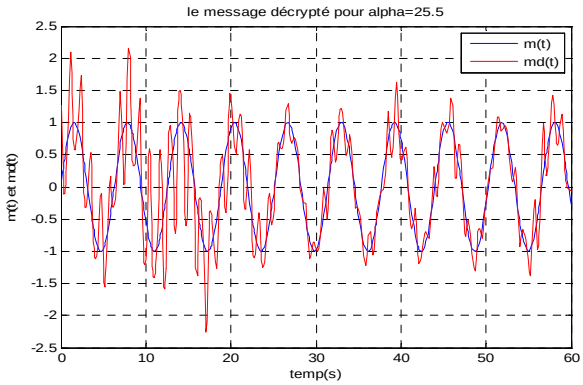
On doit considérer une variation du paramètre α pour la première méthode de cryptage par inclusion et d'autres variations du même paramètre α pour la deuxième méthode de cryptage par addition, le paramètre β est gardé constant. Dans cette section, nous considérons le cas d'une transmission d'un signal sinusoïdal identique à celui utilisé précédemment. Cette propriété s'énonce comme suit : deux clés aussi proches que l'on veut dans l'espace des clés, ou deux messages clairs très peu différents produisent des signaux décryptés totalement différents.

Nous allons réaliser la simulation suivante : on transmet trois fois le même message, le premier cryptosystème étant réalisé grâce à trois clés de décryptage très peu différentes. La première clé $\alpha = 12$, la seconde clé $\alpha = 22.5$, et la troisième clé $\alpha = 27.5$ voir la figure 3.25. Le deuxième cryptosystème étant réalisé aussi grâce à trois clés de décryptage La première clé $\alpha = 10$, la seconde clé $\alpha = 10.5$, et la troisième clé $\alpha = 11.5$ voir la figure 3.26.

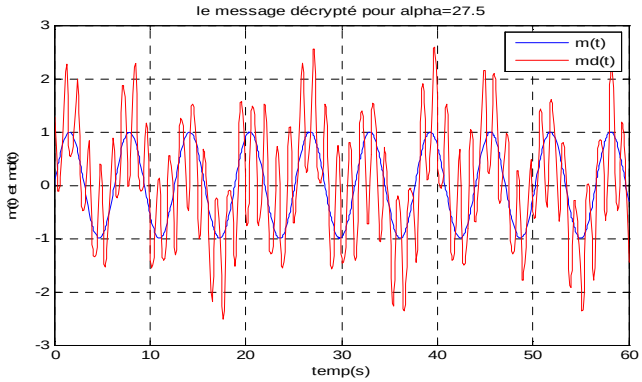
➢ ***Résultat de simulation***



$a)\ \alpha = 22.5$



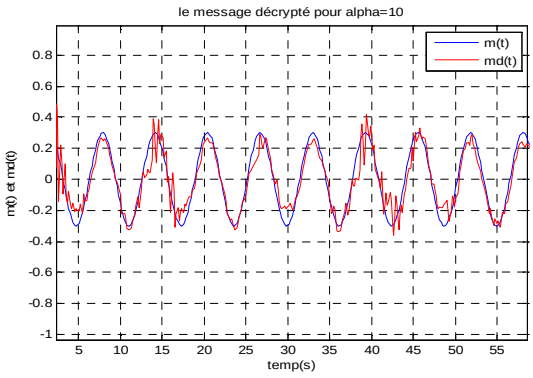
$b)\alpha = 25.5$



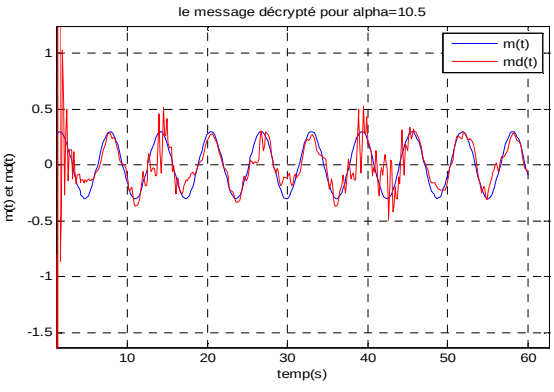
$c)\alpha = 27.5$

Fig. 3.25 La reconstitution du message m pour quelques valeurs de α « le cryptage par addition »

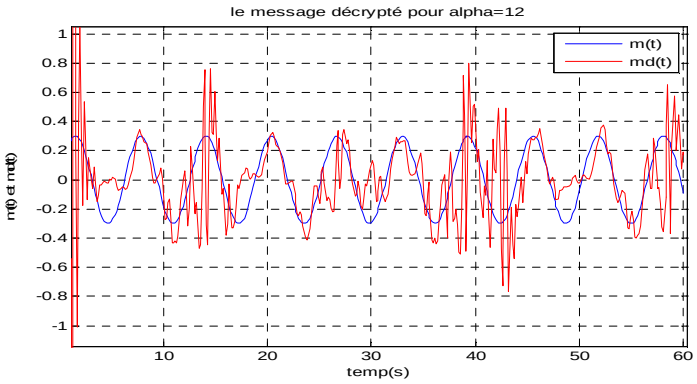
Ce premier cryptosystème est peu sensible à la variation de la clé de décryptage, pour perdre le message il faut varier $\grave{\alpha}$ jusqu'à 22.5 ($\grave{\alpha} = \alpha + 13$) voir la figure 3.35a, donc ce cryptosystème n'est pas robuste en sécurité.



a) $\alpha = 10$



b) $\alpha = 10.5$



c) $\alpha = 12$

Fig.3.26 La reconstitution du message m pour quelques valeurs de α « cryptage par inclusion ».

La variation du paramètre α, comme nous venons de le voir apporte des modifications dans l'estimation du message confidentiel. Pour une légère variation de $\grave{\alpha}$ $(\grave{\alpha} = \alpha + 2)$, le message n'est pas complètement reconstruit voir la figure 3.26c.

D'après ces résultats, nous constatons que le deuxième cryptosystème qui est plus sécurisé cela se traduit par sa sensibilité à la variation du paramètre α. Par contre le premier cryptosystème est peu sensible ce qui rend le système plus menacé aux tentatives des pirates.

3.9 Comparaison des performances des deux cryptosystèmes

Les résultats de simulation obtenus ont montrés que la reconstitution de l'information masquée dépend de la synchronisation du système (le choix de l'émetteur et récepteur) ainsi que de la méthode de cryptage utilisée.

Le message secret a été reconstitué avec les deux méthodes de cryptage sous l'hypothèse de conditions parfaites (ni bruit, ni retard dans la transmission), mais avec le premier cryptosystème que le message a été mieux reconstruit, car on a utilisé la technique de transmission à deux voies donc le message ne change la dynamique du système et la technique de cryptage n'influence pas sur la synchronisation. Mais pour le deuxième cryptosystème, on a utilisé une seule voie de transmission où le message est injecté à la dynamique du système donc il va jouer un rôle sur sa synchronisation.

En suite, on a envisagé le cas où le cryptosystème proposé est perturbé par la présence de bruit de transmission. L'observateur robuste détaillé dans ce chapitre, choisi comme récepteur, a permet d'atténuer l'influence d'un bruit additif sur le signal $x(t)$ et sur l'erreur de synchronisation des états et par conséquent sur la récupération du message confidentiel. Les simulations, pour différents niveaux de bruit, montrent que la restauration du message est meilleure à partir d'un ($SNR = 35$, pour le premier cryptosystème, $SNR = 80$ pour le deuxième), Au contraire, lorsque le SNR est petit (par exemple $SNR = 5dB$ pour le premier cryptosystème, $SNR = 50$ pour le deuxième) la restauration du message n'est pas possible, donc le premier cryptosystème qui est moins sensible au bruit. Par la suite, nous avons testé la sensibilité du schéma de communication face à la variation de sa clé secrète de déchiffrement. On a trouvé que le deuxième cryptosystème qui est plus sécurisé où le message reconstruit est très sensible aux variations des paramètres de la clé de décryptage.

3.10 Conclusion

A travers ce troisième chapitre, nous avons présenté une application importante de la synchronisation à base d'observateur sous la forme d'un système de communication sécurisée. La problématique est celle de la restauration du message, avec des contraintes de sécurité supplémentaires. Les résultats de simulation ont montrés que la reconstitution de l'information déchiffrée dépend de la synchronisation entre le système émetteur-récepteur et la méthode de cryptage. Le message secret a été bien reconstruit pour le premier cryptosystème mais il présente moins de sécurité. Par contre le deuxième cryptosystème est plus sécurisé, même si que le message déchiffré n'est pas parfaitement reconstruit (le chattering apparait pendant les premiers instants du régime transitoire).

Au chapitre suivant, on va voir un autre moyen pour renforcer la résistance du processus de communication sécurisée.

4.1 Introduction

Le calcul d'ordre fractionnaire axé sur les opérateurs intégro-différentiels d'ordre non entier est un vieux concept mathématique introduit par Leibniz et L'Hopital en 1695. Depuis, de nombreux ouvrages traitant des fondements mathématiques de cet outil ont été édités [23].

Ces dernières années, un intérêt considérable pour le calcul fractionnaire a été stimulé par les applications de plus en plus grandissantes de cet outil dans la modélisation de manière plus précise de certains phénomènes physiques. Ces phénomènes sont liés aux aspects héréditaire, de diffusion ou de viscoélasticité rencontrés dans plusieurs domaines de la physique comme en mécanique, en électricité voire même en biologie [17].

Dans la théorie du contrôle, cet outil a été exploité pour la conception de contrôleurs d'ordre fractionnaire qui possèdent la qualité de robustesse vis-à-vis des variations de certains paramètres du système à contrôler, de nombreux contrôleurs fractionnaires ont été proposés citons part exemple le contrôleur CRONE, le PID fractionnaire [17].

L'idée de concevoir des systèmes non linéaires chaotiques d'ordre fractionnaire a été aussi investie par plusieurs auteurs. Dans [20] Ivo Petras expose une synthèse des systèmes non linéaires chaotiques d'ordre fractionnaires. Cette idée consiste à étendre le comportement chaotique des systèmes d'ordre entier au cas où on remplace les dérivées premières d'ordre entier dans le modèle d'état par des dérivées d'ordre non entier.

Dans ce chapitre, nous allons présenter le système chaotique d'ordre fractionnaire de Chua-Hartley. Ce système est l'équivalent fractionnaire du système de Chua-Hartley d'ordre entier. Le comportement chaotique n'est maintenu que pour certaines valeurs de l'ordre de dérivation [11]. Ensuite, ce système est utilisé dans un processus de transmission sécurisée de données. La même démarche entreprise au chapitre précédent est reconduite dans ce chapitre. La synchronisation avec les deux méthodes de cryptage est étudiée. L'utilisation des systèmes fractionnaire dans la transmission de données, trouve son intérêt dans le fait que les ordres de dérivation sont de nouveaux paramètres de clé et renforcent ainsi la sécurité de la transmission.

4.2 Théorie de la dérivation non entière

4.2.1 Introduction au calcul fractionnaire

On peut généraliser les opérateurs d'intégration et de différentiation en un seul opérateur fondamental ${}_aD_t^q$ défini comme suit [20] :

$$ {}_{\mathrm{a}}D_t^q = \begin{cases} \frac{d^q}{dt^q} & q > 0 \\ 1 & q = 0 \\ \int_a^t (d\,\tau)^{-q} & q < 0 \end{cases} \tag{4.1} $$

où $q \in \mathbb{R}$, est l'ordre de l'opération et a , t désignent respectivement la condition initiale et la variable par rapport à laquelle on applique l'opérateur de dérivation fractionnaire.

4.2.1.1 Outils de base

1. La fonction Gamma [16] :

La fonction gamma (Γ) d'Euler est une fonction qui prolonge la factorielle aux valeurs réelles et complexes, définie pour les nombres entiers positifs, elle est donnée par :

$$ \Gamma(z) = \int_0^{+\infty} t^{z-1} e^{-t} dt\,, \quad z > 0 \tag{4.2} $$

2. La fonction Béta est définie par [16] :

$$ \beta(p,z) = \int_0^l \tau^{p-1}(1-\tau)^{z-1}\, d\tau = \frac{\Gamma(\mathrm{p})\Gamma(\mathrm{z})}{\Gamma(\mathrm{p+z})} \quad \text{avec} \quad Re(p) > 0 \; et \; Re(z) > 0 \tag{4.3} $$

4.2.1.2 Intégration non entière [20]

Soit $q \in \mathbb{R}^+$ et f une fonction localement intégrable définie sur$[t_0, \infty)$. L'intégrale d'ordre q de f de borne inférieure t_0 définie par :

$$ {}_{t_0}I_t^q f(t) = \frac{1}{\Gamma(\mathrm{q})} \int_{t_0}^t (t-\tau)^{q-1}\; f(\tau) d\tau \tag{4.3} $$

est appelée intégrale d'ordre fractionnaire de Riemann-Liouville avec $\Gamma(q)$ la fonction Gamma d'Euler.

4.2.2 Définitions et propriétés de la dérivation non-entières

Nombreuses sont les définitions de cet opérateur de dérivation fractionnaire, malheureusement toutes les définitions proposées ne sont pas toutes équivalentes. Nous présentons dans cette partie celles qui sont les plus utilisées.

4.2.2.1 Définition de Riemann-Liouville (R-L) [20]

Soient $q \in \mathbb{R}$ avec $q > 0$, n un entier positif, $t_0 \in \mathbb{R}$ et f une fonction localement intégrable définie sur $[t_0, +\infty)$. La dérivée d'ordre q de f de borne inférieur $t_0$est définie par :

$$ {}_{t_0}D_t^q f(t) = \frac{d^n}{dt^n}\left({}_{t_0}I_t^{(n-q)} f(t)\right) = \frac{1}{\Gamma(n-q)}\frac{d^n}{dt^n}\int_{t_0}^{t}(t-\tau)^{n-q-1} f(\tau)d\tau \qquad (4.4)$$

Où le nombre entier *n* est tel que $(n-1) < q < n$.

4.2.2.2 Définition de Caputo [20]

A la fin des années 60, dans le cadre de ses travaux sur la dissipation dans un matériau viscoélastique linéaire, Caputo a introduit une autre définition de la dérivation d'ordre fractionnaire. L'expression mathématique de cette définition est :

$$ {}_{t_0}D_t^q f(t) = I^{n-q} D^n f(t) = \frac{1}{\Gamma(n-q)}\int_{t_0}^{t}\frac{f^{(n)}(\tau)}{(t-\tau)^{q-n+1}}d\tau \qquad (4.5)$$

Où n est un entier positif vérifiant $(n-1) < q < n$.

$f^{(n)}(\tau)$, étant la dérivée d'ordre entier n, par rapport à τ, de la fonction $f(\tau)$, ${}_{t_0}D_t^q f(t)$désigne la dérivée d'ordre fractionnaire q de la fonction $f(t)$ entre t_0 et t selon la définition de Caputo.

4.2.2.3 Définition de Grünwald-Letnikov (G-L) [20]

Une autre généralisation, basée sur la définition usuelle de la dérivation entière, est proposée par Grünwald-Letnikov basée sur la généralisation de la dérivée classique d'une fonction $f(t)$ d'ordre $n \epsilon \mathbb{N}$ de la forme :

$$D^n f(t) = \lim_{h\to 0} \frac{1}{h^n} \sum_{j=0}^{\infty} (-1)^k \binom{n}{j} f(t - jh) \tag{4.6}$$

$$\binom{n}{j} = \frac{n!}{j!(n-j)!} \tag{4.7}$$

En remplaçant l'entier n par $q \epsilon \mathbb{R}$ ($q > 0$), l'expression (4.9)s'écrit

$$\binom{q}{j} = \frac{\Gamma(q+1)}{j!\ \Gamma(q-j+1)} \tag{4.8}$$

La dérivée d'ordre fractionnaire d'ordre $q > 0$ de G-L est donc

$${}_aD_t^q f(t) = \lim_{h\to 0} \frac{1}{h^q} \sum_{j=0}^{\left[\frac{t-q}{h}\right]} (-1)^j \binom{\alpha}{j} f(t - jh) \tag{4.9}$$

Où [.]dénote la partie entière d'un nombre réel, h est la période d'échantillonnage.

Remarque 4.1 : Ces différentes définitions nous montrent que la dérivée d'ordre non entier prend en compte les valeurs de $f(t)$ à tous les instants passés grâce à l'intégration qui y apparait. Elle fournit donc une caractérisation globale de $f(t)$. C'est cet effet « mémoire » qui fait de l'opérateur de dérivation non entière un excellent outil de modélisation des phénomènes de diffusion connus pour être à « mémoire longue »

4.2.2.4 Propriétés de la dérivation d'ordre fractionnaire [20]

Les principales propriétés des dérivées et intégrales d'ordre fractionnaire sont les suivantes ;

1) Si $f(z)$ est une fonction analytique en z, alors sa dérivée fractionnaire ${}_aD_t^q f(z)$ est une fonction analytique en z et q.

2) Pour $q = n$, où n est un nombre entier, l'opérateur ${}_aD_t^q$ produit le même résultat que la dérivation classique d'ordre entier.

3) Opération identité

Pour $q = 0$, l'opérateur ${}_aD_z^q$ est l'opérateur identité :

$$ {}_aD_z^q f(z) = f(z) $$

4) Linéarité

La dérivation non entière est une opération linéaire. Ainsi, si f et g sont deux fonctions continues et (a, b) des nombres réels, on a :

$$ D^{(q)}(a.f + b.g) = a.D^{(q)}(f) + b.D^{(q)}(g) \tag{4.10} $$

5) La loi additive

$$ {}_0D_t^{q1}\ {}_0D_t^{q2} f(t) = {}_0D_t^{q2}\ {}_0D_t^{q1} f(t) = {}_0D_t^{q1+q2} f(t) \tag{4.11} $$

Avec $q_1 et\ q_2$ deux nombres réels.

4.2.3 Transformée de Laplace de la dérivée fractionnaire [16]

La transformée de Laplace F, en fonction de l'opérateur de Laplace *s*, d'une fonction f, est définie par la relation :

$$ F(s) = L\{f(t), s\} = \int_0^\infty f(t).e^{-s.t}\, dt \tag{4.12} $$

La transformation de Laplace d'une dérivée d'ordre q de la fonction f est donnée par la relation:

$$ L\{\ D^{(q)}\ [f(t)], s\} = s^q\ L\{f(t), s\} \tag{4.13} $$

Nous citons dans ce qui suit la transformée de Laplace de Riemann-Liouville.

4.2.3.1 Au sens de Riemann-Liouville [16]

$$ \mathcal{L}\{\ {}_0D_t^q f(t)\} = s^q\ F(s) - \sum_{k=0}^{n-1} s^k\ [\ {}_0\ D^{q-1-k} f(t)]_{t=0} \tag{4.14} $$

Avec $(n-1) < q < n$ cette transformée de Laplace de la dérivée de Riemann-Liouville est bien connue. Mais son applicabilité en pratique est limitée à cause de l'absence d'interprétation physique des valeurs limites des dérivées d'ordre fractionnaire pour $t = 0$.

4.3 Systèmes d'ordre fractionnaire

4.3.1 Systèmes fractionnaires d'ordres commensurable et non commensurable

Un système est dit fractionnaire s'il est modélisé par des équations différentielles comprenant des dérivées d'ordre fractionnaire. En général, on considère les systèmes non linéaires fractionnaires comme suit :

$$ {}_0D_t^q x_i(t) = f_i(x_1(t), x_2(t), \dots, x_n(t), t) \tag{4.15a} $$

$$ x_i\,(0) = c_i\ ,\ i = 1\,,2, \dots, n \tag{4.15b} $$

où les variables c_i désignent les conditions initiales. On peut également représenter le système (4.15) sous la forme suivante

$$ D^q x = f(x) \tag{4.16} $$

où $x \in \mathbb{R}^n$, $q_i = [\, q_1, q_2, \dots, q_n]^T \; et \; 0 < q_i < 2, (i = 1, 2, \dots, n)$.

Si les ordres de dérivation de l'équation différentielle fractionnaire qui régit le système (4.16) sont des multiples entiers d'ordre de base q, le système est dit commensurable si non le système est non commensurable.

4.3.2 Stabilité des systèmes fractionnaires

Dans la théorie de la stabilité des systèmes linéaires à temps invariant et à dérivée d'ordre entier, nous savons bien qu'un système est stable si les racines du polynôme caractéristique sont à parties réelles strictement négatives, donc situées sur la moitié gauche du plan complexe. Par ailleurs, dans le cas des systèmes fractionnaires linéaires à temps invariant, la définition de la stabilité est différente des systèmes d'ordre entier. En effet, les systèmes fractionnaires ou d'ordre non entier peuvent bien avoir des racines dans la moitié droite du plan complexe et être stables (c'-à-d sont à parties réelles strictement négatives).

Considérons le système linéaire fractionnaire suivant :

$$ \begin{cases} D^q x(t) = Ax(t) + Bu(t) \\ \qquad y(t) = Cx(t) \end{cases} \tag{4.17} $$

Avec q un réel fractionnaire d'ordre commensurable.

Désignons par μ_i les valeurs propres de la matrice A. Le système (4.17) est dit stable si la condition (4.18) est vérifiée.

$$|\arg(\mu_i)| > q\frac{\pi}{2}\ ,\ 1 \le i \le n \tag{4.18}$$

Remarque 4.1

1/ Pour $q = 1$, on retrouve la condition de stabilité des systèmes d'ordre entier.

2/ Désignons par p_i les pôles du système (4.17), ces pôles sont définis comme étant solutions de l'équation $\det(s^q I - A)$. Ils sont donnés par l'expression (4.19).

$$p_i = \mu_i^{\,1/q} \qquad 1 \le i \le n \tag{4.19}$$

Alors, la condition de stabilité dans le sens entrée bornée-sortie bornée est réalisée si la condition (4.20) est vérifiée :

$$|\arg(p_i)| > \pi/2 \tag{4.20}$$

D'après cette condition sur la stabilité, il en découle les différentes régions stables et instables, voir la figure suivante [20].

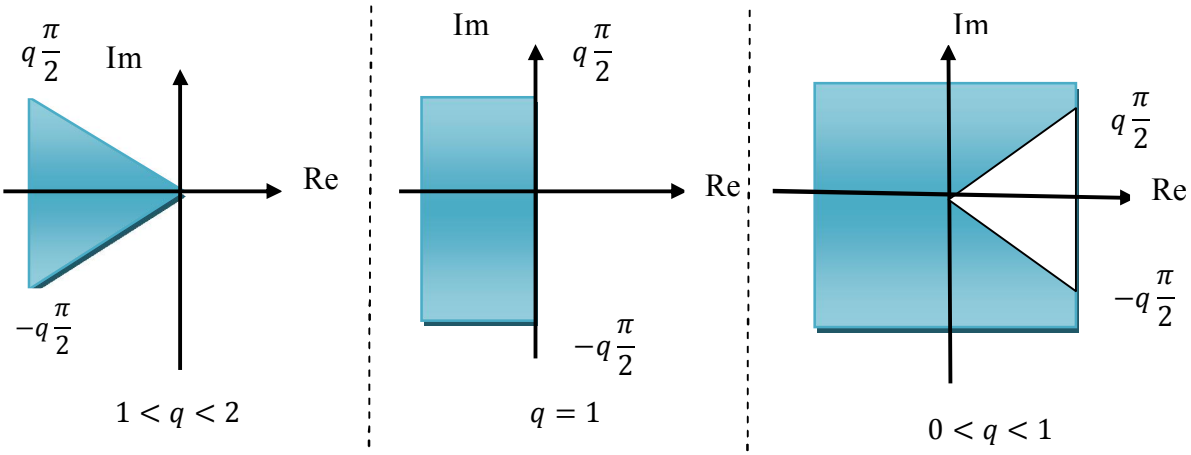


Fig. 4.1 Domaines de stabilité des systèmes commensurables dans le plan complexe.

Remarque 4.2 Dans le cas du système non linéaire (4.21)

$$D^q x = f(x) \tag{4.21}$$

Où $0 < q < 1$ et $x \in \mathbb{R}^n$

La forme linéarisé du système (4.21) peut s'écrire :

$$D^q x = Ax \tag{4.22}$$

avec A est la matrice Jacobienne de f et puis on applique la condition (4.18) précédente aux points d'équilibre.

Remarque 4.3

Supposons le système chaotique de dimension 3 suivant :

$$D^q x = f(x) \tag{4.23}$$

Où $0 < q < 1$ et $x \in \mathbb{R}^n$

Donc il ne dispose que de trois points d'équilibre. Par conséquent, si ce système a un double attracteur de défilement, l'un des points d'équilibre est un point "selle" d'indice 1 et les autres points sont d'indice 2.

Supposons que μ est une valeur propre instable de l'un des points "selle" d'indice 2, une condition nécessaire pour que le système fractionnaire (4.23) demeure chaotique est le maintien de la valeur propre μ dans la région instable. Cela signifie :

$$\tan\left(q.\frac{\pi}{2}\right) > \left|\frac{Im(\mu)}{Re(\mu)}\right| \implies \quad q > \frac{2}{\pi}\tan^{-1}\left(\left|\frac{Im}{Re}\right|\right) \tag{4.24}$$

4.4 Méthodes d'approximation analogique des opérateurs fractionnaires

D'habitude les simulations sont effectuées avec un logiciel préparé pour traiter seulement les puissances d'ordre entier de *s*. Alors il est très important de trouver des approximations d'ordre entier pour des fonctions de transfert d'ordre fractionnaire. Autrement dit, les fonctions de transfert d'ordre fractionnaire sont remplacées par des fonctions de transfert d'ordre entier, avec un comportement assez identique à celles désirées, mais beaucoup plus facile à manipuler. L'implantation d'un tel système dans un calculateur par exemple, nécessite donc de faire des approximations qui se traduisent par une limitation du nombre de fréquence transitionnelle ω_k [13].

Il existe différentes méthodes pour trouver de telles approximations, les approximations disponibles dans le domaine *s* sont appelées des approximations analogiques

ou des approximations du domaine fréquentiel. Ces méthodes d'approximation analogique sont [13] :

- Méthode EFC (Expansion Fractionnaire Continue)
- Méthode de Carlson
- Méthode de Matsuda
- Méthode d'Oustaloup
- Méthode de Charef
- Autres méthodes (Roy,Wang, Jones...)

4.4.1 La méthode d'approximation de Charef [1]

La méthode d'approximation de Charef a été introduite pour représenter et analyser le comportement dynamique des systèmes fractals dits également « pôles à puissance fractionnaire » .Caractérisé par un diagramme d'amplitude de bode à pente fractionnaire.

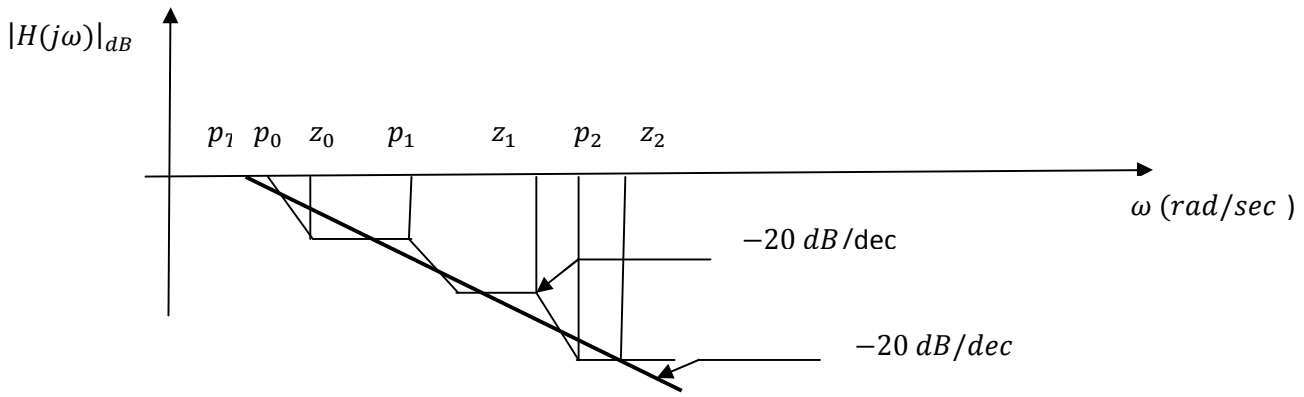


Fig. 4.2 Diagramme asymptotique d'amplitude de Bode de H(s) et son approximation.

Les systèmes fractals sont représentés par une transmittance de la forme :

$$H(s) = \frac{1}{s^q} \tag{4.25}$$

Où $s = j\omega$ est la fréquence complexe et $n \in \mathbb{R}$ est la dimension fractale. Généralement les systèmes fractals présentent une amplitude finie en basses fréquences, une représentation par un pôle à puissance fractionnaire est de ce fait plus appropriée [1]**:**

$$H(s) = \frac{1}{(1+\frac{s}{p_T})^q} \tag{4.26}$$

p_T est la fréquence de cassure et $0 < n < 1$.

La figure (4.2) montre en trait gras le diagramme asymptotique d'amplitude de Bode de la réponse en fréquence de H(s). La droite de pente $-20\,dB/dec$ est approximée par une ligne en zigzag de pente $0\,dB/dec$ et $-20\,dB/dec$ en alternance, ces pentes représentent les contributions individuelles des singularités : poles p_i et zéros z_i [2].

Avec $0 < q < 1$, on peut réécrire la fonction de l'équation (4.26) comme suit:

$$\widehat{H}(s) = \frac{1}{(1+\frac{s}{p_T})^q} = \lim_{N\to\infty} \frac{\prod_{i=0}^{N-1}(1+\frac{s}{z_i})}{\prod_{i=0}^{N}(1+\frac{s}{p_i})} \tag{4.27}$$

où $(N+1)$ est le nombre total des singularités qui peut être déterminé par la bande de fréquences du système. L'équation (4.26) peut être tronquée à un nombre fini N, et l'approximation devient :

$$\widehat{H}(s) = \frac{1}{(1+\frac{s}{p_T})^q} \approx \frac{\prod_{i=0}^{N-1}(1+\frac{s}{z_i})}{\prod_{i=0}^{N}(1+\frac{s}{p_i})} \tag{4.28}$$

Charef utilise comme paramètre principal l'écart maximale, $\varepsilon > 0$ (en décibel), entre la ligne d'approximation en zigzag et la droite de pente $-20dB/dec$, les pôles et les zéros seront ensuite obtenus par un simple calcul géométrique.

$p_0 = p_T\sqrt{b}$, $p_i = p_0(a.b)^i$, $z_i = a.p_0(ab)^i$

Avec

$a = 10^{[\varepsilon/10(1-m)]}$, $b = 10^{[\varepsilon/10.m]}$, $a.b = 10^{[\,\varepsilon/10m(1-m)]}$,

$$N = partie\ entière\left[\frac{\log(\omega_{max}/p_0)}{\log(a.b)}\right] + 1$$

ω_{max} est la bande de fréquence d'approximation.

Pour pouvoir approximer la fonction intégrale fractionnaire bornée en fréquence. Il suffit d'exécuter l'algorithme de Charef, en suite imposer la fréquence de coupure $p_T = \omega_b$ et l'erreur d'approximation en dB. En fin l'algorithme développé permet l'approximation de l'intégrateur fractionnaire borné en fréquence**.**

4.5 Etude des systèmes chaotiques fractionnaires

L'une des applications importantes du calcul fractionnaire est la théorie du chaos [23]. Ce chapitre est ainsi dédié à l'étude des systèmes chaotiques fractionnaires, dont leurs propriétés intrinsèques peuvent être utilisées dans les schémas de synchronisation et de cryptographie. Parmi les systèmes chaotiques fractionnaires on a, le circuit de Chua-Hartley le système de Newton-Leipnik, le système de Lu, le système de Lorenz , le système de Chen, le système de Rossler et Duffing…etc [20].

Le chaos ne peut se produire dans les systèmes dynamiques continus lorsque l'ordre total est inférieur à trois [11]. Cette affirmation est basée sur les concepts habituels d'ordre, tels que le nombre d'états dans un système où le nombre total d'intégrations ou de différentiations dans le système. Le modèle d'un système peut être réorganisé en trois équations différentielles simples, où les équations contiennent des dérivées fractionnaires. L'ordre total du système sera dans ce cas, la somme de l'ordre de chaque dérivée fractionnaire de l'état du système, qui par conséquent sera inférieur à 3. Ce qui nous amène à dire qu'on peut observer le phénomène du chaos dans un système dynamique fractionnaire où l'ordre total du système est inférieur à 3 [11]**.**

4.5.1 Extension de la synchronisation aux systèmes fractionnaires

La définition de la synchronisation maitre-esclave définie pour un système à dérivée entier reste valable pour les systèmes à dérivées fractionnaires c'est-à-dire :

Considérons le système maitre décrit par un système différentiel fractionnaire

$$\frac{d^q x}{dt^q} = f(x,t) \tag{4.29}$$

Par analogie, le système esclave est défini par le système différentiel fractionnaire

$$\frac{d^q \hat{x}}{dt^q} = \hat{f}(\hat{x},y,t) \tag{4.30}$$

Nous disons que le système maitre fractionnaire se synchronise avec le système esclave si

$$\lim_{t\to\infty}|x(t)-\hat{x}(t)| \tag{4.31}$$

4.6 La description du système de transmission

Pour notre application de transmission sécurisée de l'information, on utilise comme émetteur le circuit de Chua-Hartley et l'observateur à mode glissant vus au chapitre précédent mais maintenant on va introduire une autre propriété à ce système qui est la dérivée fractionnaire pour avoir plus de complexité et de sécurité dans ce nouveau cryptosystème.

4.6.1 L'approximation de l'opérateur intégrateur fractionnaire

Dans le but de simulation de notre système chaotique fractionnaire, on a cherché le système approximé en utilisant la méthode de Charef, mais avant d'arriver à cette approximation on a cherché la transformée de Laplace équivalente au sens de Riemann-Liouville comme suit :

$$\mathcal{L}\{D^q x(t)\} = s^q\, X(s) - \sum_{k=0}^{n-1} s^k \left[D^{q-1-k}\, x(t)\right]_{t=0}$$

Puisque $0 < q < 1$, donc $n = 1$

$$\Longrightarrow X(s) = \frac{1}{s^q}\ \mathcal{L}\{D^q x(t)\} + \frac{1}{s^q}\{D^{q-1}\, x(t)|_{t=0}\}$$

On prend $\tilde{x}_0 = D^{q-1}\, x(t)|_{t=0}$ comme la condition initiale pour notre système fractionnaire approximé, mais ça ne représente pas la valeur de x à l'instant $t = 0$.

d'où $$X(s) = \frac{1}{s^q}\ \mathcal{L}\{D^q x(t)\} + \frac{1}{s^q}\,\tilde{x}_0$$

Le schéma fonctionnel sera représenté comme suit :

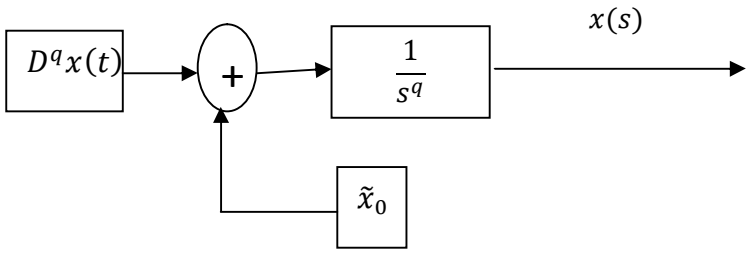


Fig. 4.3 Schéma fonctionnel de l'approximation d'un modèle fractionnaire.

Pour notre application on a choisi le système chaotique fractionnaire non commensurable de Chua-Hartley avec ordre de dérivation $q_1 = 0.94$, $q_2 = 0.96$ et $q_3 = 0.94$.

Maintenant on cherche l'approximation de l'intégrateur fractionnaire $\frac{1}{s^{0.94}}$, on utilisant l'approximation de Charef développée au paragraphe (4.4.1) basé sur l'opérateur d'intégration borné en fréquences. Ensuite nous comparons les diagrammes de bode de l'intégrateur fractionnaire et son approximé.

On commence par exécuter l'algorithme de Charef, ensuite on donne l'erreur d'approximation $\varepsilon = 2dB$ et $\omega \in [10^{-2}, 10^{2}]$. En fin, on obtient l'approximation de l'intégrateur fractionnaire d'ordre d'intégration $q = 0.94$ comme suit :

$$\widehat{H}(s) = \frac{2.298\, e^{-0.13} s^3 + 6.125 e^{-0.05} s^2 + 4.64 s + 99.94}{2.3 e^{-0.05}\, s^3 + 2.845 s^2 + 100 s + 1}$$

- **La caractérisation fréquentielle de $H(s)$**

  $H(s) = \frac{1}{s^{0.94}}$

Le diagramme de gain est caractérisé par une droite oblique de pente

$-20 * \boldsymbol{q}\, dB/dec = -18.8\ dB/dec$.

Le diagramme de phase est caractérisé par une droite horizontale d'ordonnée $\varphi = -q.\frac{\pi}{2} = -84{,}6^{\circ}$.

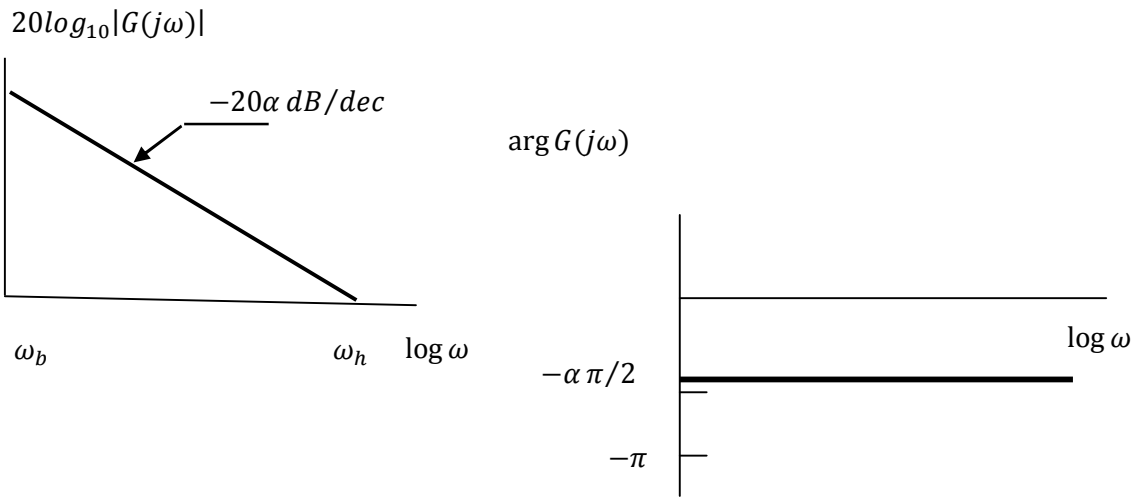
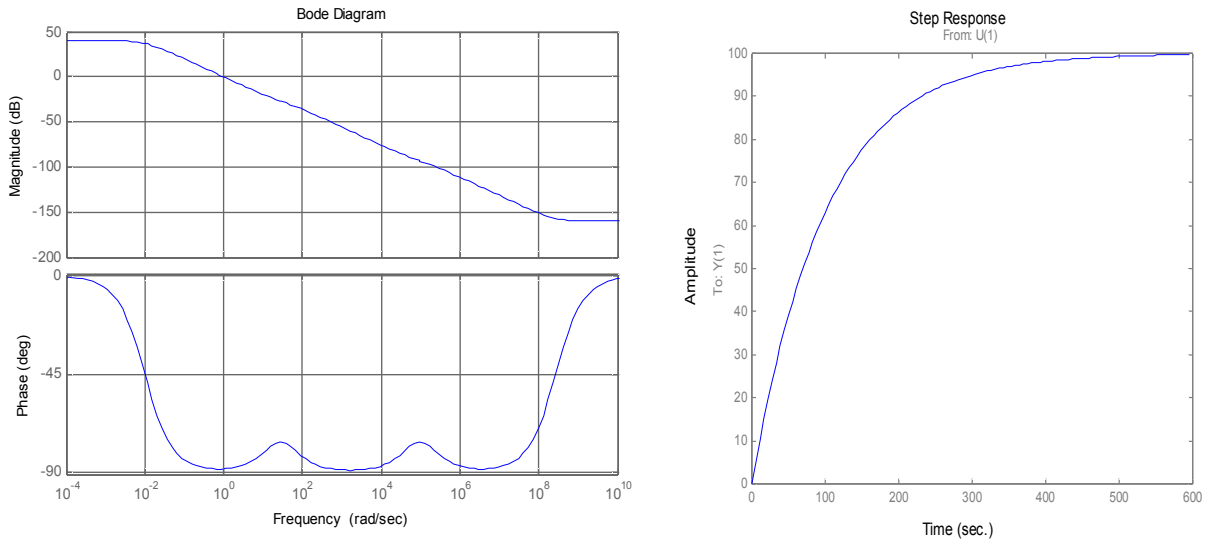


Fig. 4.4 Le diagramme de Bode de l'intégrateur fractionnaire borné en fréquence.

- **La caractérisation fréquentielle de $\widehat{H}(s)$**

Puisqu'il s'agit d'une fonction de transfert d'ordre entier, on peut tracer son diagramme de Bode sous Matlab.



(a) Le diagramme de Bode. (b) La réponse indicielle.

Fig. 4.5 Les caractéristiques de l'intégrateur fractionnaire approximé $\widehat{H}(s)$.

La pente de gain de $\widehat{H}(s)$ égale à $-\frac{150}{8} = -18.75\,dB/dec$, elle est approximativement égale à celle trouvée pour l'intégrateur fractionnaire $H(s)$.

4.6.2 Etude de l'émetteur « Système chaotique fractionnaire de Chua-Hartley »

On a déjà étudié le circuit de Chua-Hartley au chapitre précédent avec les paramètres suivants $\alpha = 9.5$, $\beta = \frac{100}{7}$, et l'ordre de dérivation $q = 1$.

Maintenant, laissez-nous introduire la version fractionnaire (4.32), où les dérivées d'ordre entier(q_1, q_2, q_3) sont remplacées par des dérivées fractionnaires commensurables ou non commensurables, tel que le comportement chaotique est maintenu pour certaines valeurs de l'ordre de dérivation. Le premier signal $x_1(t)$ du système (4.32) est choisit pour la synchronisation avec les deux méthodes de cryptage (par addition et inclusion).

Le modèle de l'émetteur est donné par :

$$\begin{cases} \frac{d^{q_1}x_1}{dt^{q_1}} = \alpha(x_2 + \frac{x_1 - 2x_1^3}{7}) \\ \frac{d^{q_2}x_2}{dt^{q_2}} = x_1 - x_2 + x_3 \\ \frac{d^{q_3}x_3}{dt^{q_3}} = -\beta x_2 = -\frac{100}{7}x_2 \\ y = x_1 \end{cases} \tag{4.32}$$

Dans [11], ils ont vérifié que le chaos peut exister même quand l'ordre total du système est inferieur à 3. Ceci a été déterminé, en calculant les exposants de Lyapunov pour chaque simulation donc pour $q = 0.9\ ;1\ et\ 1.1$ .Ces résultats sont données à la table 1.

L'ordre mathématique du système	L'ordre du système approximé	La valeur de α	Valeur propre μ_1	μ_2	μ_3
2.7	9	12.75	0.338	-0.000201	-0.132
3.0	3	9.5	0.248	-0.00412	-3.07
3.3	18	7	0.318	*	*

Tab 4.1 Les exposants de Lyapunov selon la configuration de l'espace d'états pour $q = 0.9\ ;1\ et\ 1.1$.

L'ordre mathématique du système est $\tilde{n} = \sum q_i$. Pour rester dans le domaine du chaos [11] q doit varier dans plage suivante $q_i \in [0.8\ \ 1.1]$.

Afin d'obtenir par simulation le comportement chaotique pour le circuit de Chua-Hartley nous fixons les paramètres aux valeurs suivantes $\alpha = 10.5$; $\beta = \frac{100}{7}$

-les ordres de dérivation commensurables sont $(q_1, q_2, q_3) = (0.94 \;\; 0.94 \;\; 0.94)$

- les ordres de dérivation non commensurables sont $(q_1, q_2, q_3) = (0.94 \;\; 0.96 \;\; 0.94)$

-les conditions initiales de l'émetteur sont $(x_{10}, x_{20}, x_{30}) = (0.5 \;\; 0 \;\; -0.7)$.

Les attracteurs fractionnaires commensurables et non commensurables de Chua-Hartley sont tracés, respectivement sur les figures (4.6) et (4.8).

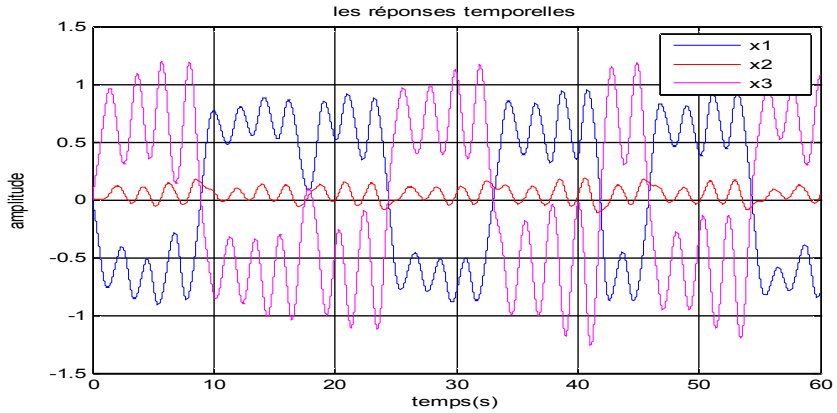
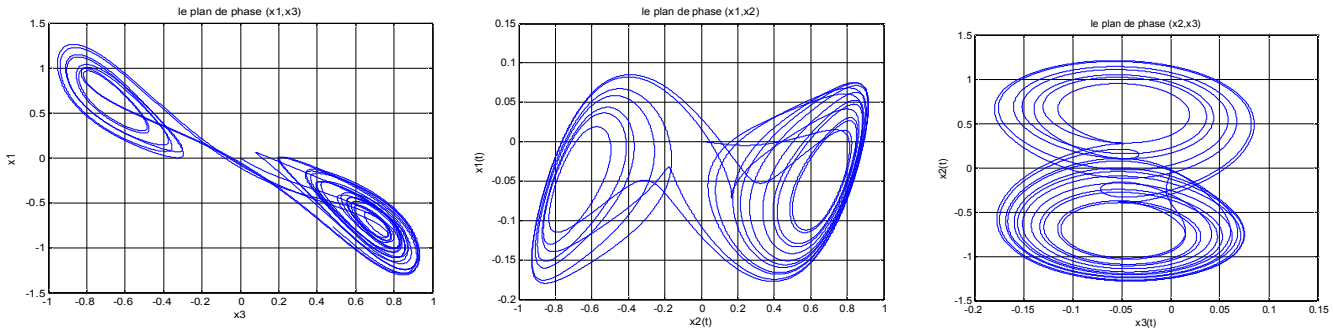


Fig. 4.6 Les réponses temporelles du système commensurable.



1. plan de phase $(x_1 x_3)$ 2. plan de phase $(x_1 \; x_2)$ 3. plan de phase $(x_2 \; x_3)$

Fig. 4.7 Attracteur fractionnaire de Chua-Hartley d'ordre commensurable.

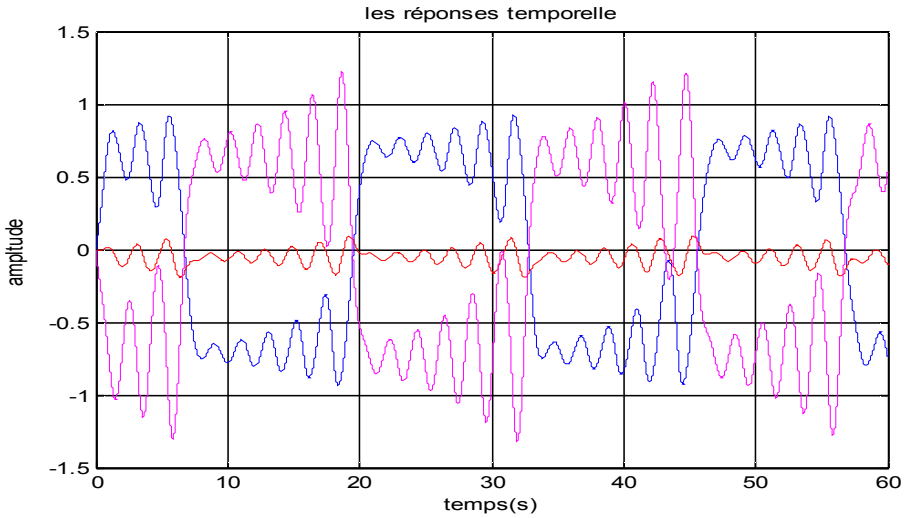
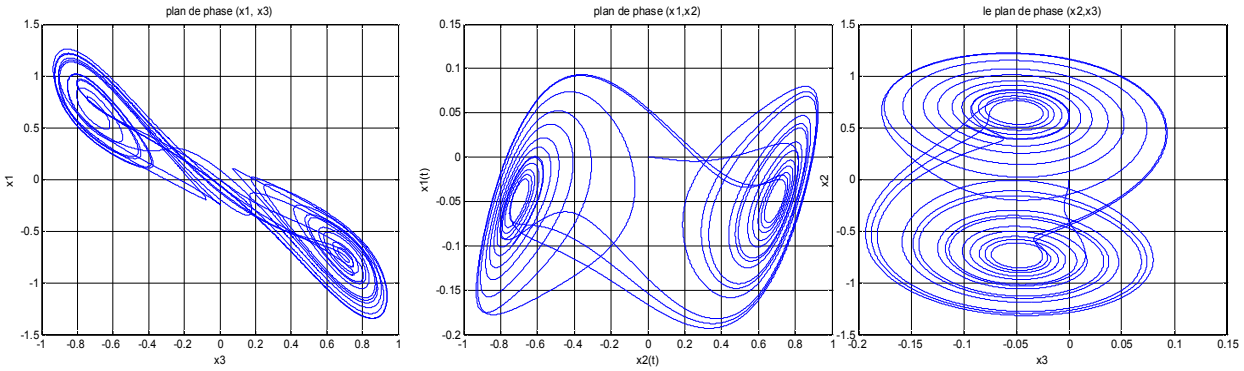


Fig. 4.8 Les réponses temporelles du système non commensurables.



1. plan de phase $(x_1 x_3)$ 2. plan de phase $(x_1\ x_2)$ 3. plan de phase $(x_2\ x_3)$

Fig. 4.9 Le circuit de Chua-Hartley fractionnaire non commensurable.

Ces figures représentent deux caractéristiques essentielles du chaos, telles que l'aspect aléatoire de ces 3 états ainsi que l'attracteur étrange dans les trois plan de phase.

Remarque 4.5

On a vérifié au chapitre précédent l'observabilité, la condition de recouvrement d'observabilité et l'inversibilité à gauche de notre émetteur chaotique d'ordre entier, mais ces trois conditions sont difficiles à les démontrées avec l'ordre fractionnaire, donc on suppose qu'ils sont toujours vérifiées même dans le cas fractionnaire pour pouvoir construire un observateur à la réception de notre système de transmission, pour récupérer le message en clair à partir de la sortie de l'émetteur et ses dérivées d'ordre non entier.

4.6.3 Etude du récepteur « observateur à modes glissants fractionnaire »

Nous avons le système (4.32) possède des états bornés et le message $m(t)$ est lui aussi borné, donc on peut utiliser un observateur à mode glissant fractionnaire afin de réaliser la synchronisation entre l'émetteur chaotique de Chua-Hartley et cet observateur. Maintenant on suppose que le système (4.32) peut se mettre sous la forme triangulaire d'observation, donc nous pouvons écrire la forme de l'observateur à mode glissant fractionnaire étape par étape comme suit :

$$\begin{aligned} \frac{d^{q_1}\hat{x}_1}{dt^{q_1}} &= \alpha\left(\hat{x}_2 + \frac{x_1 - 2x_1^3}{7}\right) + \lambda_1 sgn(x_1 - \hat{x}_1) \\ \frac{d^{q_2}\hat{x}_2}{dt^{q_2}} &= x_1 - \tilde{x}_2 + \hat{x}_3 + E_1\lambda_2 sgn(\tilde{x}_2 - \hat{x}_2) \\ \frac{d^{q_3}\hat{x}_3}{dt^{q_3}} &= -\frac{100}{7}\hat{x}_2 + E_2\lambda_3 sgn(\tilde{x}_3 - \hat{x}_3) \end{aligned} \tag{4.33}$$

Avec les ordres de dérivation de l'observateur sont $(q_1, q_2, q_3) = (0.94\ \ 0.96\ \ 0.94)$ et de conditions initiales $(\hat{x}_{10}, \hat{x}_{20}, \hat{x}_{30}) = (0, 0, 0)$.

Remarque 4.4 La convergence de l'observateur sera justifiée par les résultats de simulation. A notre connaissance, il y'a aucun travail dans la littérature qui traite les observateurs par mode glissant étape par étape pour les systèmes non linéaires d'ordre fractionnaire.

4.7 Les Résultats de simulation

Pour pouvoir établir une comparaison avec le procédé de transmission sécurisée que nous avons élaboré, deux techniques de cryptages ont été testées pour la transmission sécurisée d'un signal numérique.

On suit les mêmes étapes de synchronisation, chiffrement et déchiffrement déjà vues au chapitre précédent. Dans le premier cryptosystème, la transmission se fait à deux voies avec la technique de cryptage par addition. Pour le deuxième cryptosystème, la transmission se fait à une seule voie avec la méthode de cryptage par inclusion, la seule différence par rapport à l'application précédente réside dans l'emploie des ordres fractionnaires, pour renforcer la sécurité de la transmission.

4.7.1 Le premier cryptosystème

Le message $m(t)$ étant un signal sinusoïdal ajouté à la ligne de transmission y_2, tel que l'étape de synchronisation et de cryptage sont séparés.

$$m(t) = 1 \sin wt$$

Avec $\omega = 1\,rad/sec$ $f = 0.159Hz$ la fréquence du message.

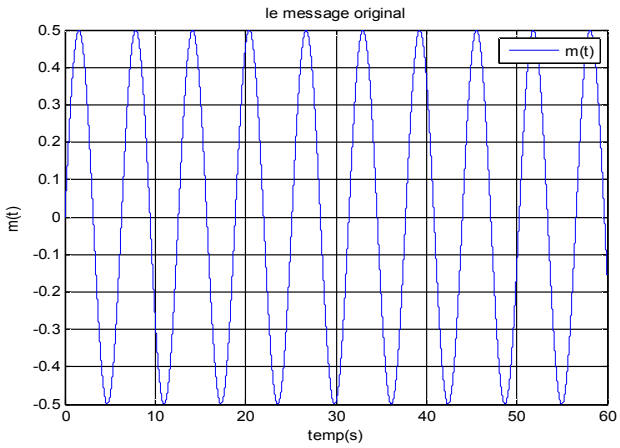


Fig. 4.10 Le message original $m(t)$

❖ **Processus de cryptage**

Pour le cryptage avec cette méthode, le message est ajouté à la deuxième ligne de transmission y_2 par une simple opération d'addition comme suit :

$$m_c = y_2 + m$$

où m_c est le message crypté.

Le message correspondant au signal crypté m_c est représentée à la figure 4.11.

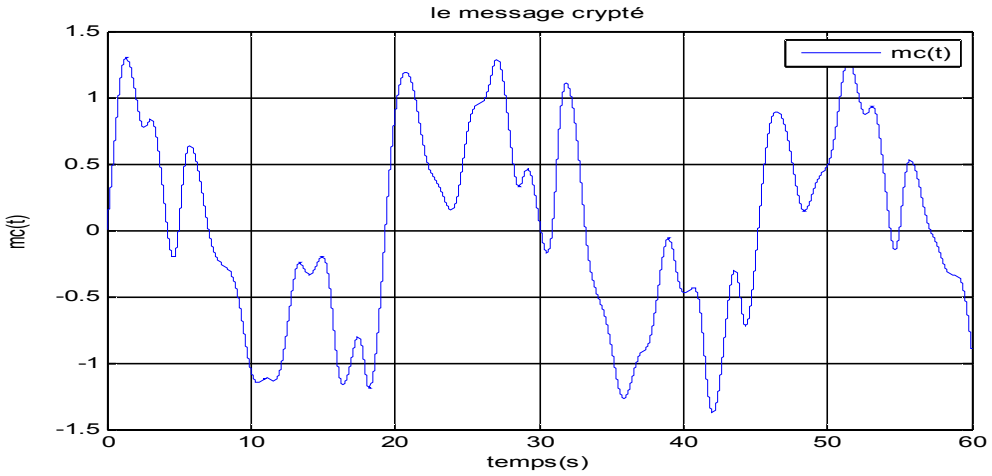
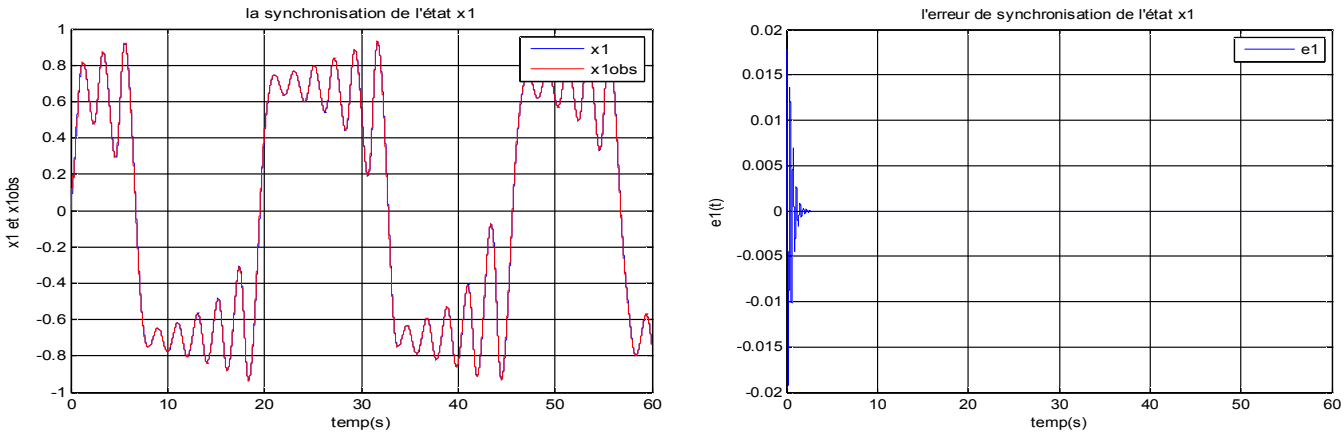


Fig. 4.11 Le message crypté $m_c(t)$.

❖ **Processus de synchronisation**

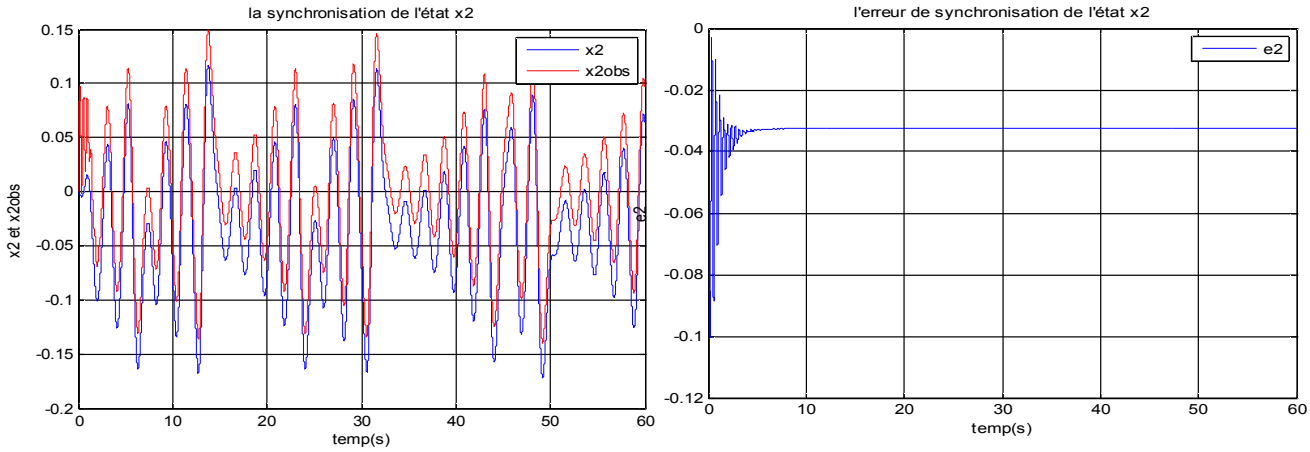
On choisit comme signal de sortie $y_1 = x_1$ et les valeurs des gains de l'observateur sont : $\lambda_1 = \lambda_2 = 30,\ \lambda_3 = 35$

Nous allons présenter les résultats de la synchronisation pour vérifier la robustesse de l'observateur utilisé.



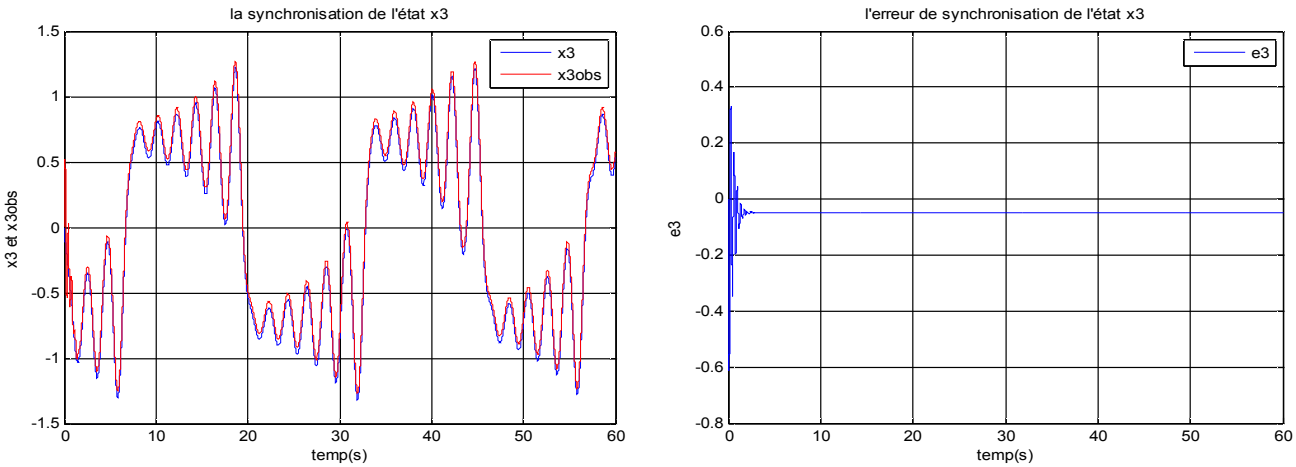
a) Les états $x_1 et\ \hat{x}_1$ **b)** L'erreur de synchronisation de l'état x_1

Fig. 4.12 Le résultat de synchronisation des états x_1 et $\hat{x}_1$



a)Les états a) $x_2 et\ \hat{x}_2$ **b)** L'erreur de synchronisation de l'état x_2

Fig. 4.13 Le résultat de synchronisation des états x_2 et $\hat{x}_2$.



a) Les états $x_3 et\ \hat{x}_3$ **b)** L'erreur de synchronisation de l'état x_3

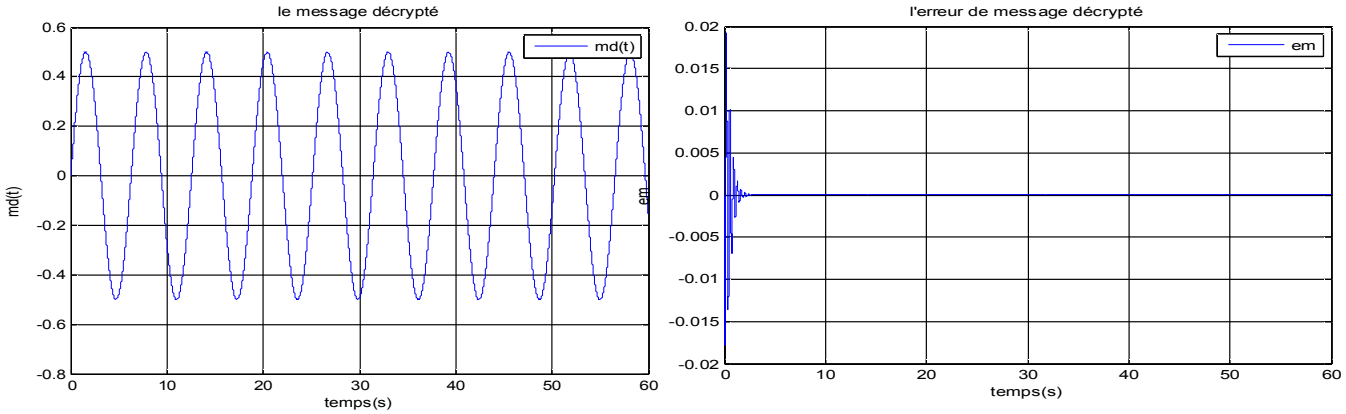
Fig. 4.14 Le résultat de synchronisation des états x_3 et $\hat{x}_3$

Les figures (4.12, 4.13, 4.14) montrent respectivement les états et leurs erreurs de synchronisation. A travers ces figures, nous constatons bien que l'erreur de synchronisation de l'état x_1 converge rapidement vers zéros, mais les deux autres erreurs e_2 et e_3 sont asymptotiquement convergées et ça revient au fonctionnement de l'observateur à mode glissant étape par étape et le choix de la surface de glissement s.

❖ **Processus de déchiffrement**

Cette étape sert à reconstruire le signal de départ. Pour déchiffrer le message transmis à l'aide du système (4.39), nous utilisons dans un premier temps l'observateur à mode glissant fractionnaire étape par étape pour la synchronisation, ensuite une simple fonction de soustraction nous permet de récupérer le message original comme suit:

$$m_d = m_c - \hat{x}_1$$



a) Le message déchiffré $m_d(t)$. **b)** L'erreur du message déchiffré e_m.

Fig. 4.15 Le message déchiffré $m_d(t)$.

La figure 4.15 montre que le message original est bien déchiffré, on observe aussi le chattering pendant les premiers instants du régime transitoire, mais il est diminué par rapport à l'ordre entier. Donc, on peut dire qu'avec ce premier cryptosystème fractionnaire, le message est bien reconstruit grâce à l'observateur à mode glissant qui assure un meilleur temps de convergence.

4.7.2 Le deuxième cryptosystème

Pour ce cryptosystème on utilise une seule voie de transmission y pour le cryptage et la synchronisation, avec la méthode de cryptage par inclusion où le message $m(t)$ est injecté à la dynamique de l'état x_3. Notons que le message est le dernier état à reconstruire par des dérivations successives des sorties de l'observateur. Le message original étant une sinusoïde de forme $m(t) = 0.3 \sin \omega t$ avec une fréquence $f = 0.159Hz$.

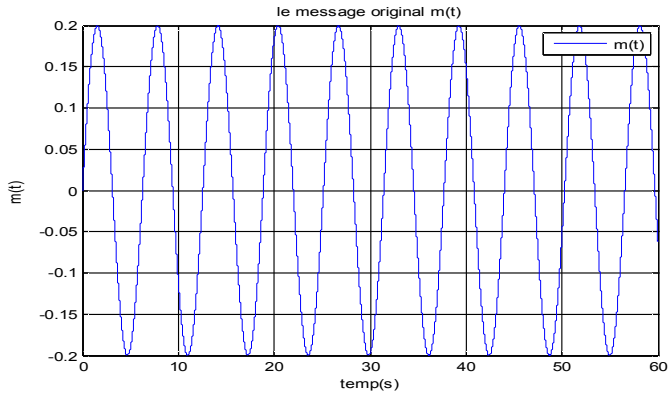


Fig. 4.16 Le message original $m(t)$.

❖ **Processus de cryptage**

Pour le cryptage avec cette méthode, le message est injecté à la dynamique de l'état x_3 ensuite envoyé par la ligne de transmission y.

$$\frac{d^{q_3}x_3}{dt^{q_3}} = -\beta x_2 + m = -\frac{100}{7}x_2 + m$$

Le message correspondant au signal crypté envoyé à travers un canal de transmission vers le récepteur est représentée à la figure 4.17.

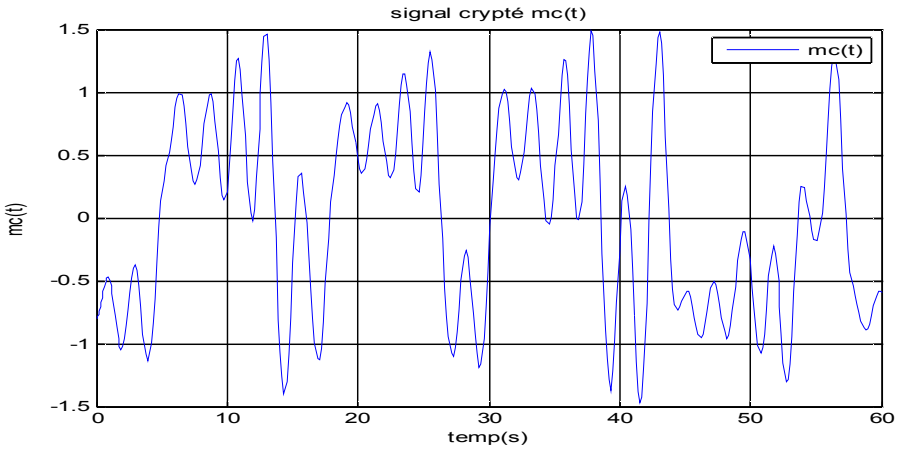
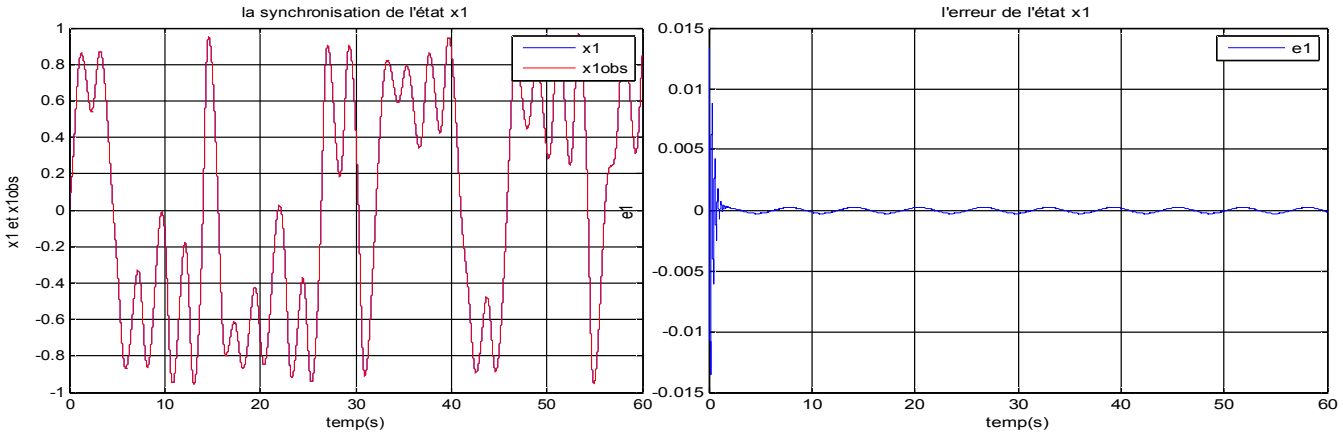


Fig. 4.17 Le message crypté $m_c(t)$

❖ **Processus de synchronisation**

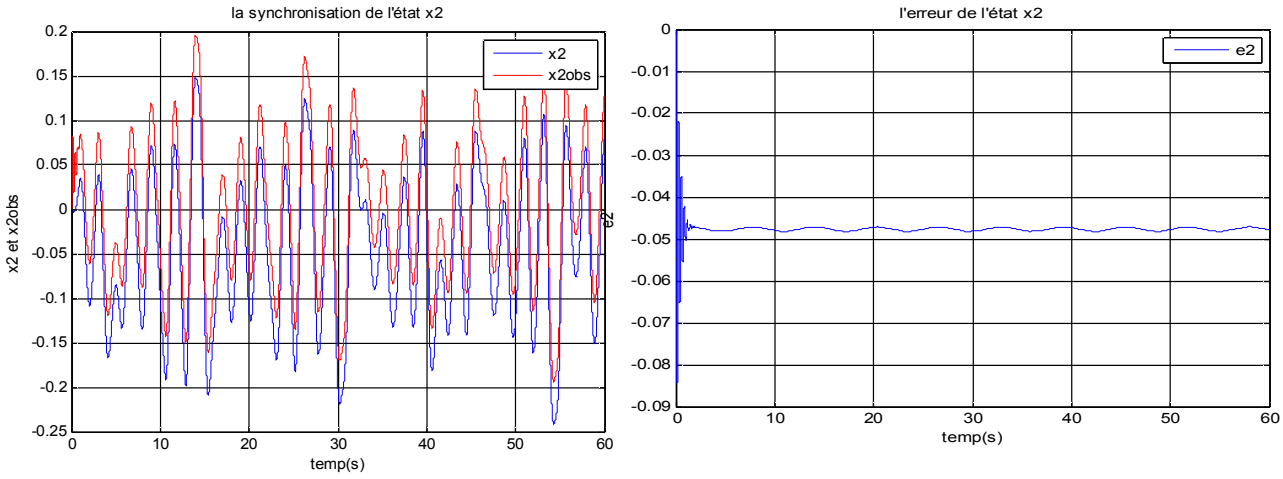
On utilise toujours les mêmes conditions initiales pout l'émetteur et récepteur. Les valeurs des gains de l'observateur sont : $\lambda_1 = 20,\ \lambda_2 = 30,\ \lambda_3 = 25.$

Les résultats de la synchronisation sont :



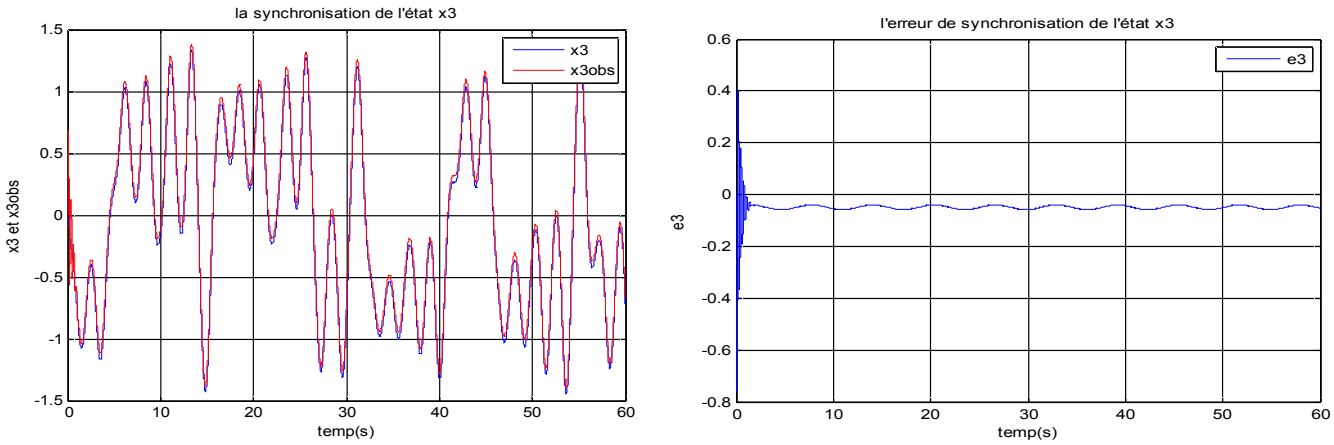
a) Les états $x_1 et\ \hat{x}_1$ **b)** L'Erreur de synchronisation de l'état x_1

Fig. 4.18 Le résultat de synchronisation de l'état x_1



a) Les états $x_2$et $\hat{x}_2$ **b)** Erreur de synchronisation de l'état x_2

Fig. 4.19 Le résultat de synchronisation de l'état x_2



a) Les états $x_3$et $\hat{x}_3$ **b)** L'erreur de synchronisation de l'état x_3

Fig. 4.20 Le résultat de synchronisation de l'état x_3

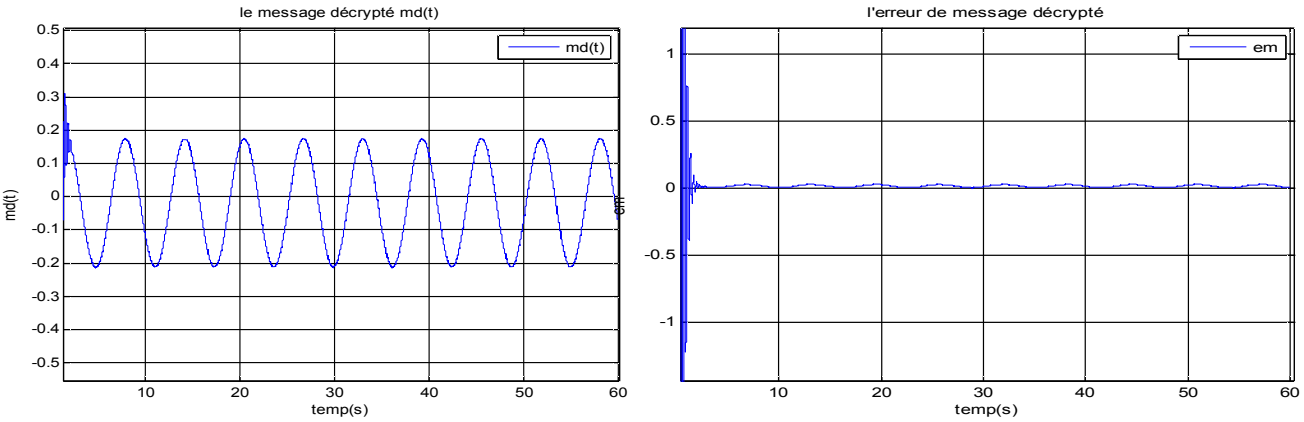
Les figures (4.18, 4.19, 4.20) montrent respectivement les états et leurs erreurs de synchronisation. A travers ces figures, nous constatons que l'erreur de synchronisation e_1 converge vers zéros, mais les deux autres erreurs e_2 et e_3 sont asymptotiquement synchronisées et ça revient toujours au fonctionnement de l'observateur étape par étape, le choix de la surface de glissement et la méthode de cryptage qui joue un rôle sur la dynamique du système.

❖ **Processus de déchiffrement**

Pour déchiffrer le message transmis à l'aide du système (4.39), nous utilisons dans un premier temps l'observateur à modes glissant étape par étape pour la synchronisation, lorsque $\hat{x}_3 = \tilde{x}_3$ le message chiffré sera reconstruit par l'observateur, pour le déchiffrer on utilise l'équation suivante :

$$\tilde{m} = E_3 \lambda_3 sgn(\tilde{x}_3 - \hat{x}_3)$$

où $\tilde{m}$ est le message décrypté.



a) le message décrypté $m_d(t)$ **b)** L'erreur du message décrypté e_m

Fig. 4.21 Le message déchiffré $m_d(t)$.

La figure (4.21) montre que l'erreur du message tend vers zéro, donc le message est reconstruit même pour le deuxième cryptosystème.

$\hat{x}_3$

En comparant les résultats donnés pour la synchronisation d'un système fractionnaire avec ceux obtenus par le système entier, nous constatons une meilleure vitesse de convergence pour l'observateur à mode glissant, grâce à sa convergence en un temps fini et aussi on remarque la diminution du phénomène de chattering. L'observateur à mode glissant étape par étape choisi est plus robuste au sens de synchronisation pour les deux cryptosystèmes.

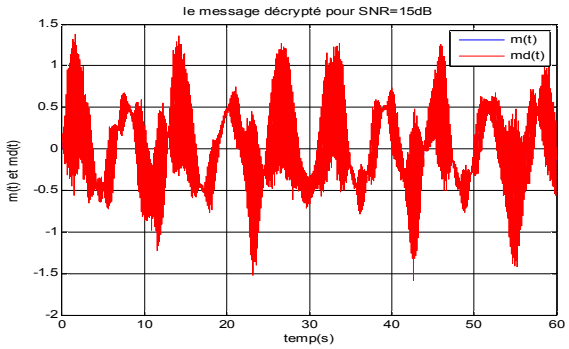
4.8 Robustesse aux bruits de transmission et aux variations des paramètres

4.8.1 Robustesse aux bruits de transmission

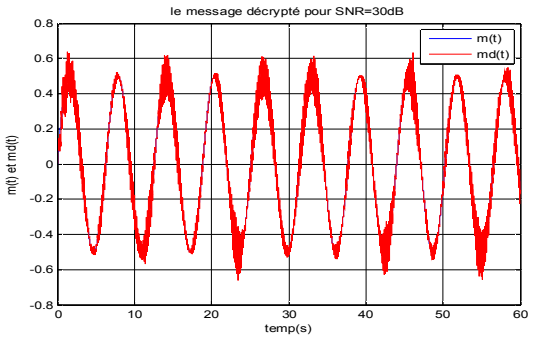
Dans cette partie, nous étudions l'impact, sur la qualité de restauration du message (signal sinusoïdal), du bruit affectant le signal dévolu à la synchronisation. Pour quantifier le rapport entre l'amplitude du signal et celle du bruit qui l'affecte. On considère un bruit additif b(t) gaussien, normal centré perturbant le signal $y(t)$.

➢ ***Les résultats de simulation***

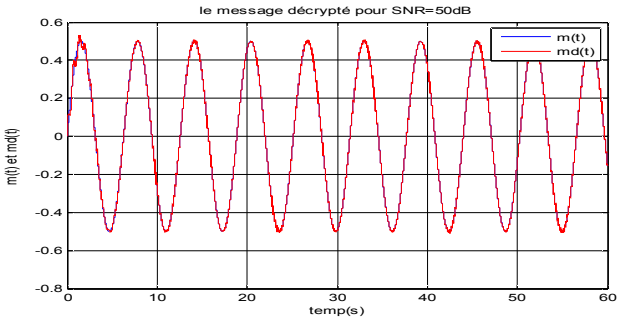
1/ Le premier cryptosystème :



(a) $SNR = 15dB$



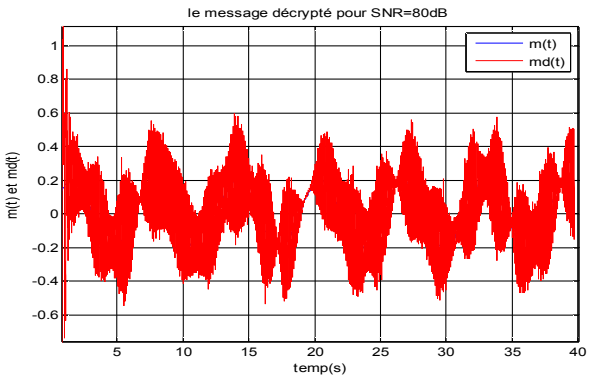
(b) $SNR = 30dB$



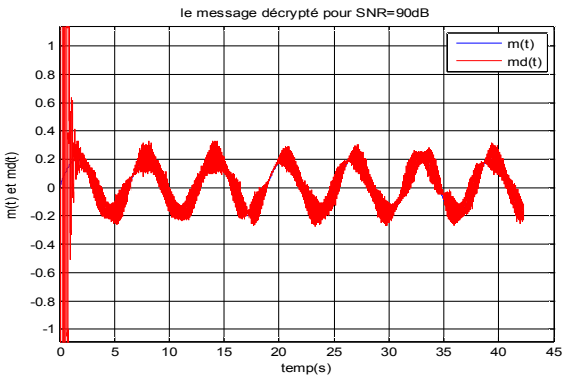
(c) $SNR = 50dB$

Fig. 4.22 Les messages décryptés en présence de bruit de transmission pour différents SNR.

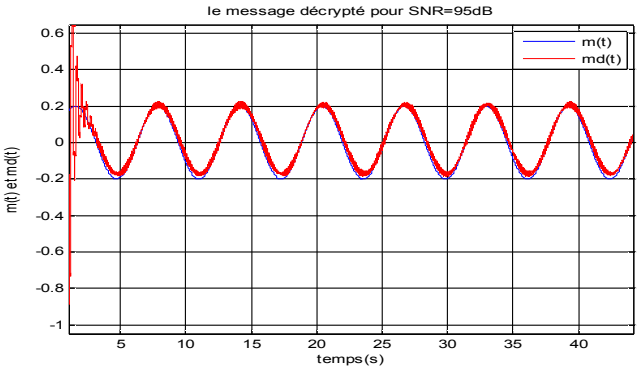
2/ Le deuxième cryptosystème :



(a) $SNR = 80dB$



(b) $SNR = 90dB$



(c) $SNR = 95dB$

Fig. 4.23 Les messages décryptés en présence de bruit de transmission pour différents SNR.

On a représenté les résultats de simulation de robustesse aux bruits de transmission pour les deux cryptosystèmes. Les figures 4.22 et 4.23 montrent respectivement les messages reconstruits pour deux différents SNR (SNR = 15dB , 30dB 50dB) pour le premier cryptosystème et (SNR = 80dB, 90dB, 95dB) pour le deuxième.

La présence du bruit sur le signal transmis, comme nous venons de le voir apporte des erreurs dans la récupération du message reconstruit. Par conséquence, le message est complètement reconstruit le cas du premier cryptosystème pour une valeur de $SNR = 50dB$ et on le perd complètement pour une valeur de $SNR = 15dB$ qui correspond à un grand niveau de bruit voir les figures (4.28a et 4.28c). Le deuxième cryptosystème, on récupère le message pour une valeur de $SNR = 95dB$ et le message est perdu complètement pour une valeur de $SNR = 80dB$ qui correspond à un faible niveau de bruit par rapport au premier bruit, voir les figures (4.29a et 4.29c). D'après ces résultats, nous constatons que le premier cryptosystème qui est plus robuste face aux bruits on le comparant au deuxième cryptosystème.

4.8.2 Robustesse aux variations de paramètres

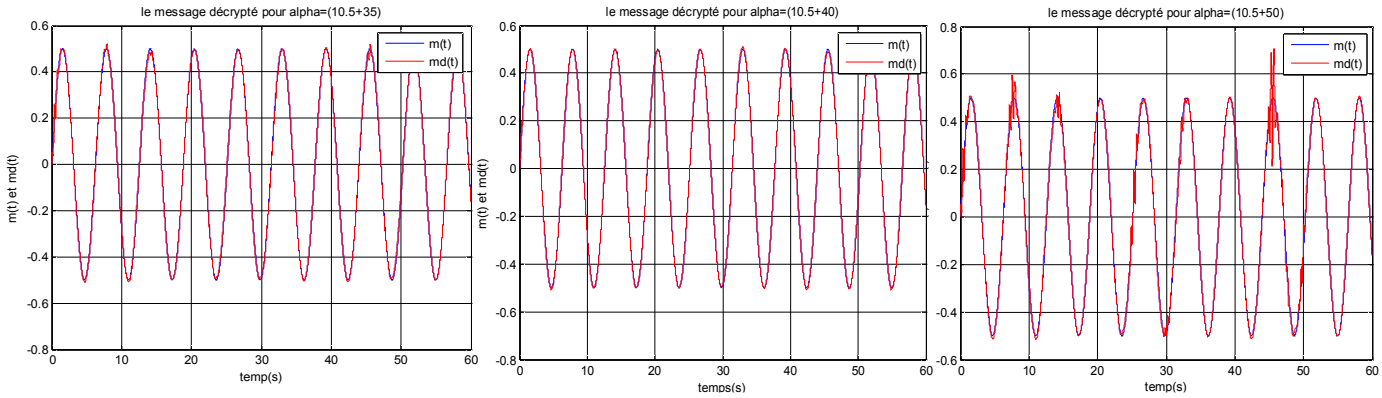
Dans cette partie, nous testons la robustesse et la capacité d'adaptation du système de communication pour les deux méthodes de cryptage proposé face à un pirate possédant des paramètres proches des valeurs réels de la clé de déchiffrement,

On note $\grave{k}$ la clé de décryptage $\grave{k} = f(\grave{\alpha}, \beta, \grave{q}_1, \grave{q}_2, \grave{q}_3)$, pour éviter toute confusion, on choisit les paramètres de la clé de déchiffrement ($\alpha = 10.5$; $\beta = 100/7$; $q_1 = 0.94$; $q_2 = 0.96$; $q_3 = 0.94$) au niveau de l'émetteur différents des paramètres de la clé de décryptage.

On doit considérer une variation des paramètres de la clé de décryptage et prendre les signaux décryptés avec ces clés. Nous allons réaliser la simulation suivante : pour chaque cryptosystème on transmet neuf fois le même message grâce à neuf clés très peu différentes. On fait varier le paramètre α, ensuite les ordres de dérivation (q_1, q_2, q_3).

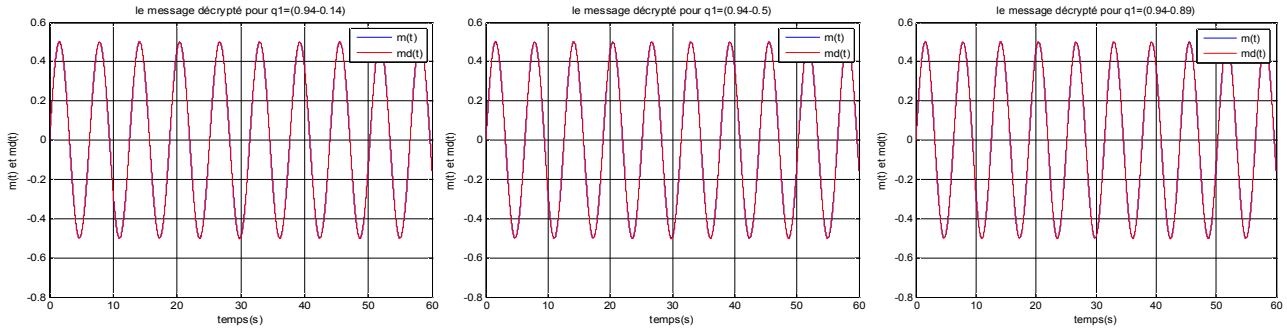
- ***Les résultats de simulation :***

1/ Le premier cryptosystème



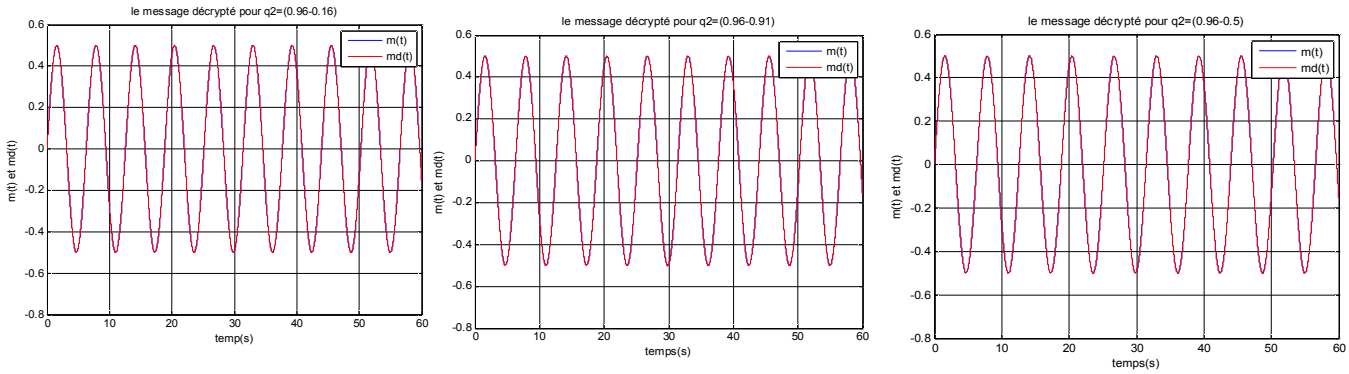
$k_1 = (45.5; \beta; 0.94; 0.96; 0.94)$ $k_2 = (50.5; \beta; 0.94; 0.96; 0.94)$ $k_3 = (60.5; \beta; 0.94; 0.96;\ 0.94)$

Fig. 4.24 le message décrypté pour différentes valeurs de α.



$k_4 = (10.5;\ \beta; 0.8; 0.96; 0.8)$ $k_5 = (10.5;\ \beta; 0.44; 0.96; 0.44)$ $k_6 = (10.5;\ \beta; 0.05; 0.96; 0.05)$

Fig. 4.25 le message décrypté pour différentes valeurs de $q_1 (q_1 = q_3)$.

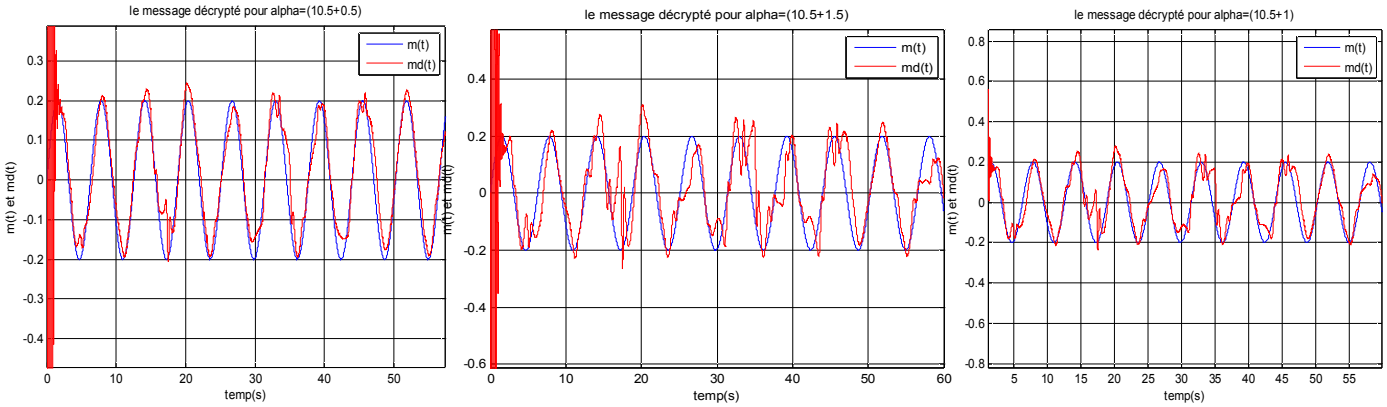


$k_7 = (10.5;\ \beta; 0.94; 0.8; 0.94)$ $k_8 = (10.5;\ \beta; 0.94; 0.05; 0.94)$ $k_9 = (10.5;\ \beta; 0.94; 0.02; 0.94)$

Fig. 4.26 le message décrypté pour différents valeurs de q_2.

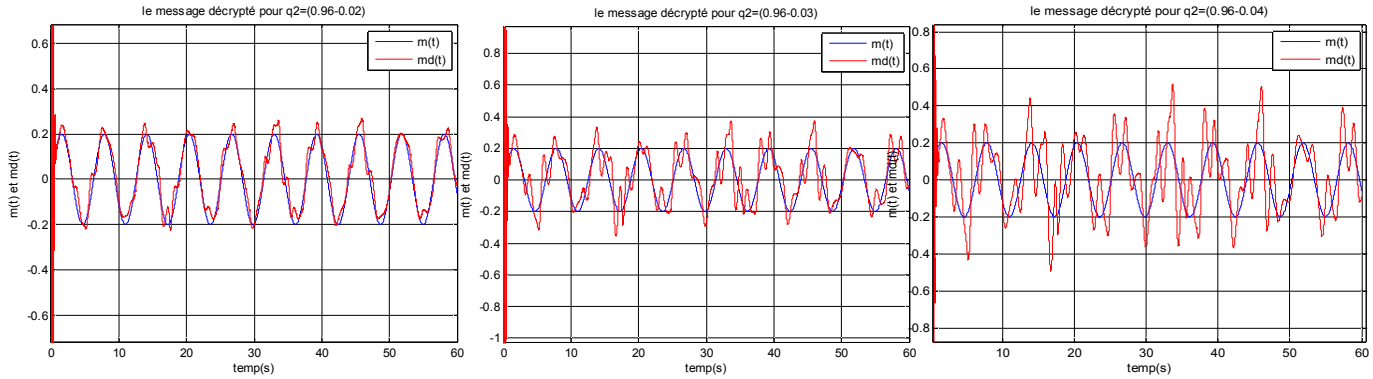
D'après les résultats de simulation obtenus, on remarque que ce premier cryptosystème est insensible aux variations de la clé de décryptage et le message est toujours reconstruit même si qu'on fait varier le paramètre α, donc cette méthode de cryptage n'est pas robuste en sécurité.

2/ Le deuxième cryptosystème



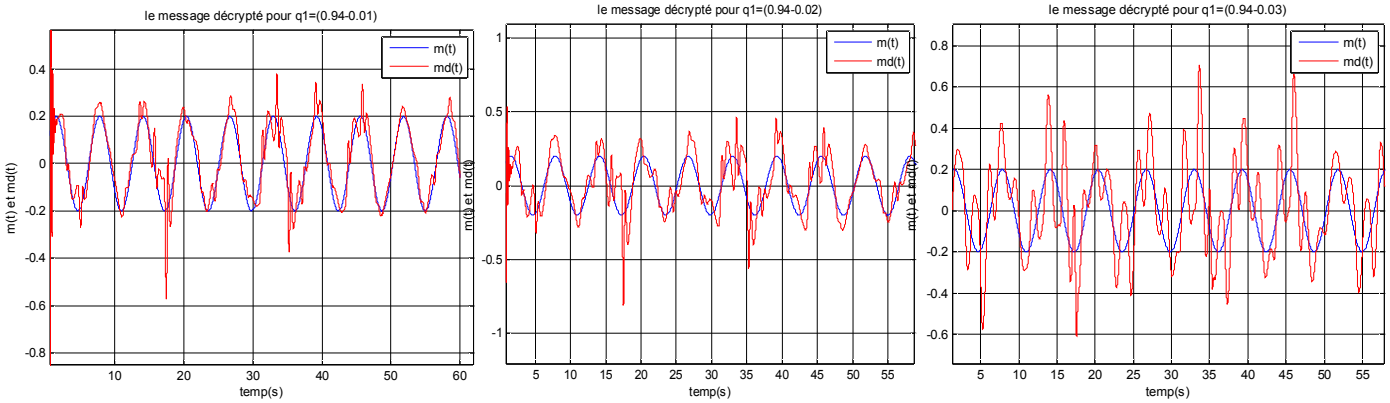
$k_1 = (11;\ \beta; 0.94; 0.96; 0.94)$ $k_2 = (11.5;\ \beta; 0.94; 0.96; 0.94)$ $k_3 = (12;\ \beta; 0.94; 0.96; 0.94)$

Fig. 4.27 le message décrypté pour différentes valeurs de α.



$k_4 = (10.5;\ \beta; 0.94; 0.94; 0.94)$ $k_5 = (10.5;\ \beta; 0.94; 0.93; 0.94)$ $k_6 = (10.5;\ \beta; 0.94; 0.92; 0.94)$

Fig. 4.28 le message décrypté pour différents valeurs de q_2.



$k_7 = (10.5;\ \beta; 0.93; 0.96; 0.93)$ $k_8 = (10.5;\ \beta; 0.92; 0.96; 0.92)$ $k_9 = (10.5;\ \beta; 0.91; 0.96; 0.91)$

Fig. 4.29 le message décrypté pour différents valeurs de q_1 ou q_3.

La variation des paramètres du deuxième cryptosystème $\dot{\alpha}$ et $(\dot{q}_1, \dot{q}_2, \dot{q}_3)$, comme nous venons de le voir apportent des modifications dans l'estimation du message confidentiel. Par conséquence, on perd complètement le message et pour une légère variation des ordres de dérivation du système $\dot{q}_2 = 0.92$ et $\dot{q}_1 = \dot{q}_3 = 0.92$, et aussi pour le paramètre $\alpha = 12$.

D'après ces résultats, nous constatons que le deuxième cryptosystème qui est plus sécurisé cela se traduit par sa sensibilité à la variation des paramètres de la clé de décryptage $\dot{k} = f(\dot{\alpha}, \beta, \dot{q}_1, \dot{q}_2, \dot{q}_3)$ et surtout par rapport aux ordres de dérivation. Donc on peut dire qu'avec cette méthode de cryptage l'ajout des dérivées fractionnaires, renforcent la sécurité du système de transmission.

En résumé, le premier cryptosystème ne peut pas assurer une transmission sécurisée de l'information, mais il est robuste face aux bruits de transmission. Le deuxième cryptosystème permet de garantir un grand niveau de sécurité lors de la transmission, mais il est très sensible aux bruits à cause du système fractionnaire qui fonctionne comme un demi-intégrateur donc filtre moins le bruit.

III.9 Conclusion

A travers ce dernier chapitre, nous avons présenté un nouveau procédé de transmission sécurisée de l'information à base d'un cryptosystème chaotique à dérivée fractionnaire. Les résultats de simulation ont montrés que l'effet du chattering a diminué et la dérivée fractionnaire effectivement renforce la sécurité du système de transmission avec la méthode de cryptage par inclusion seulement, telle qu'une légère variation des ordres de dérivation du système rend le système sensible et perd le message confidentiel et ça représente un avantage au sens de la sécurité mais le seul problème reste celui de bruit qui affecte le message.

Conclusion générale

L'objectif de ce travail de mémoire était l'étude de deux dispositifs de transmission sécurisée de données à base de systèmes chaotiques d'ordre entier et fractionnaire.

Afin de situer au mieux notre travail, un état de l'art a été proposé dans le premier chapitre. Il s'articule autour de deux thèmes principaux. Nous avons d'abord rappelé les résultats principaux de la transmission de l'information. Ensuite on a détaillé les techniques commerciales de cryptage actuellement mises en œuvre, qui reposent sur deux principes fondamentalement éloignés : le cryptage asymétrique et le cryptage symétrique. Le deuxième chapitre avait comme objectif l'introduction de quelques notions élémentaires concernant les systèmes dynamiques et notamment les systèmes chaotiques, pour tirer des propriétés de ce dernier afin de concevoir un générateur chaotique.

Dans le troisième chapitre, on a présenté le premier dispositif de transmission sécurisée à base d'un système chaotique d'ordre entier. La première démarche a été alors de choisir un système qui génère la porteuse chaotique destinée à chiffrer un message confidentiel. Pour cela, nous avons choisi un circuit simple et bien connu de Chua-Hartley. Ce choix est indiqué par le fait que l'équivalent d'ordre fractionnaire de ce circuit est proposé dans la littérature [11].

La deuxième partie de ce chapitre a consisté à la conception du récepteur pour notre émetteur chaotique. Il a été montré dans la littérature que la synchronisation unidirectionnelle des systèmes non linéaires (voire chaotique) peut être considérée comme un problème d'observateur. Ceci a été notre motivation principale dans l'utilisation d'observateur en tant que récepteur. En général, le message est considéré comme une entrée inconnue pour l'émetteur. Cette entrée inconnue est retrouvée par le récepteur, une fois que celui-ci a été synchronisé avec l'émetteur. Comme récepteur on a choisi l'observateur à mode glissant, il fonctionne étape par étape et permet de récupérer tous les états du système ainsi que le message confidentiel et aussi possède la propriété de convergence en temps fini. Nous avons proposé deux techniques de cryptage pour notre système de transmission sécurisée : la technique de cryptage par addition et la technique de cryptage par inclusion. Nous avons testé notre schéma de transmission sécurisée par l'envoie d'un message confidentiel qui est dans notre application un signal sinusoïdal.

On peut conclure des divers tests effectués sur ce premier système de transmission que :

- l'observateur à mode glissant atteint étape par étape les erreurs de synchronisation e_i (des états et le message confidentiel) situées sur un voisinage suffisamment proche de zéros.

-Les cryptosystèmes proposés avec les deux techniques de cryptage exploitent au mieux les propriétés fondamentales des systèmes chaotiques, et le principe de leur synchronisation. Les résultats de sécurité ont montrés que la technique de cryptage par inclusion présente plus de sécurité que la technique de cryptage par addition.

-le chattering et le bruit apportent des erreurs dans la récupération du message reconstruit.

Au dernier chapitre, nous avons testé un autre schéma de transmission sécurisée, exploitant les propriétés fondamentales des systèmes chaotiques à dérivée fractionnaire. Les résultats de simulation obtenus ont montré que le message secret a été bien récupéré, le phénomène du chattering a été diminué pour les deux techniques de cryptage, mais la méthode de cryptage par inclusion qui a présenté plus de sensibilité à la variation de la clé de décryptage (les ordres de dérivation fractionnaires), donc le cryptosystème chaotique fractionnaire avec la méthode de cryptage par inclusion a prouvé effectivement son efficacité en terme de sécurité pour les schémas de transmissions sécurisée.

Le problème de la synthèse et de la cryptanalyse des schémas de chiffrement restera toujours un problème ouvert. Les technologies informatiques (ressources mémoires, processeurs,…) évoluant constamment, elles permettent une analyse plus poussée de la robustesse des schémas de chiffrement et obligent donc de concevoir des schémas de plus en plus sophistiqués. Les perspectives de ce travail sont :

- L'augmentation de la fréquence de fonctionnement du système émetteur.
- Etude de la possibilité d'utilisation d'un observateur à mode glissant d'ordre supérieur afin de diminuer l'effet du chattering.
- Utilisation d'une modulation-démodulation de fréquence (FM) entre l'émetteur et le récepteur afin d'éviter en partie les problèmes posés par le canal de transmission (le bruit).
- La réalisation analogique des systèmes de cryptages chaotiques d'ordre fractionnaire.

- Ce travail ouvre la voie à d'autres développements qui restent ouverts notamment en ce qui concerne la synthèse d'observateur pour les systèmes d'ordres fractionnaires.

A.1 Stabilité au sens de Lyapunov

L'analyse de stabilité d'un système consiste à étudier son comportement lorsqu'il est déplacé d'un point d'équilibre. Cela passe par l'analyse de la trajectoire de l'état du système lorsque son état initial est proche d'un point ou d'une trajectoire d'équilibre.

Les principales notions de stabilité sont présentées ici, à savoir la stabilité asymptotique, la stabilité exponentielle, en relation avec la théorie de Lyapunov.

On considère l'ensemble des systèmes non linéaires décrits par l'équation dynamique suivante

$$\dot{x}(t) = f(x(t), t) \qquad (A.1)$$
$$x(t_0) = x_0$$

où $x(t) \in \mathbb{R}^n \; et \; f: \mathbb{R}^n \times \mathbb{R}^+ \rightarrow \mathbb{R}^n$ est continue.

Définition 1.1 *(Stabilité de l'origine)*

On dit que l'origine est un point d'équilibre stable (au sens de Lyapunov) si toute trajectoire de conditions initiales proches de $x_e = 0$ en t_0 reste suffisamment proche de x_e pour $t > t_0$, autrement dit, si :

$$\forall \rho > 0, \; \forall t_0 \geq 0, \exists \delta > 0 \; / \; \|x_0\| < \delta \implies \|x(t, t_0, x_0)\| < \rho \qquad (A.2)$$

Dans le cas contraire, on dit que l'origine est instable.

Définition 1.2 *(Attractivité)*

On dit que $x_e = 0$ est un point d'équilibre attractif pour le système (A.1) si :

$$\exists \Delta > 0 \quad / \quad \forall t \geq t_0 \; \|x_0\| < \Delta \implies \lim_{t \rightarrow \infty} x(t, t_0, x_0) = 0 \qquad (A.3)$$

Lorsque $\Delta \rightarrow \infty$, on dit que l'origine est globalement attractive.

La notion d'attractivité signifie que, après un certains temps toute trajectoire du système convergera vers son état d'équilibre. Cependant, un système attractif n'est pas nécessairement stable, au sens de la définition 1.2, c'est pourquoi on introduit alors la notion de stabilité asymptotique qui garantit que l'état du système converge vers son état d'équilibre sans trop s'en éloigner.

Définition 1.3 *(Stabilité asymptotique)*

On dit que l'origine est un point d'équilibre (globalement) asymptotiquement stable s'il est stable et (globalement) attractif.

Définition 1.4 *(Stabilité exponentielle)*

On dit que l'origine est un point d'équilibre localement exponentiellement stable du système (A.1) si :

$$\exists\, a, b > 0 \quad / \quad \forall\, t \geq t_0,\ \forall\, x_0 \in B(0,r) \quad \|x\,(t, t_0, x_0\| \leq a e^{-b(t-t_0)} \qquad \text{(A.4)}$$

$\|.\|$ étant une norme, par exemple, euclidiennes de x, $\|x\| = \sqrt{x^T x}$

où $A(0,r)$ est la boule ouverte de centre zéro, de rayon $r > 0$. Lorsque $A(0,r) = \mathbb{R}^n$, on parle de stabilité exponentielle globale.

A.2 Méthode directe de Lyapunov

La philosophie de cette méthode s'appuie sur une observation fondamentale de la physique : si l'énergie totale d'un système est dissipée de manière continue alors le système devra rejoindre finalement un point d'équilibre. On pourra donc conclure à la stabilité d'un système par l'examen de la variation d'une fonction scalaire V , représentant l'énergie totale.

Définition 2.1

Soit $V(x,t)$: $\mathbb{R}^n \times \mathbb{R}^+ \rightarrow \mathbb{R}^+$ une fonction continue. V est dite propre définie positive si :

$(i)\ \forall\, t \in \mathbb{R}^+,\ \forall x \in \mathbb{R}^n \{0\},\ \ V(x,t) > 0$

$(ii)\ \forall\, t \in \mathbb{R}^+,\ V(x,t) = 0 \implies x = 0$

$(iii)\ \forall\, t \in \mathbb{R}^+,\ \lim_{|x| \to \infty} V = \infty$

Définition 2.2 *(Fonction de Lyapunov)* **:** Une fonction $V(x,t)$ est une fonction de Lyapunov locale (respectivement globale) au sens large pour le système (A.1) si elle est propre, définie positive et s'il existe un voisinage de l'origine V_0 tel que :

$$\forall\, x \in V_0 (\text{respectivement} \in \mathbb{R}^n,\ \dot{V}(x,t) = \frac{\partial V}{\partial t}(x,t) + \left[\frac{\partial V(x,t)}{\partial x}\right]' f(x,t) \leq 0) \qquad (A.5)$$

Si $\dot{V}(x,t) < 0$, V est appelée fonction de Lyapunov au sens strict pour (A.1).
La méthode directe de Lyapunov donne une condition suffisante garantissant la stabilité du point d'équilibre 0.

Définition 2.3 *(Méthode directe de Lyapunov).*

Si le système différentiel (A.1) admet une fonction de Lyapunov locale au sens large (respectivement au sens strict), alors l'origine est un point d'équilibre localement stable (respectivement asymptotiquement stable).

Si la fonction de Lyapunov est globale, on parle alors de stabilité globale (respectivement de stabilité asymptotique globale).

Définition 2.4

L'origine de (A.1) est localement exponentiellement stable s'il existe des constantes $a, b, c > 0$, un entier $p \geq 0$, et une fonction de Lyapunov locale $V(x,t)$: $V_0 \times \mathbb{R}^+ \to \mathbb{R}^+$ tels que, pour tout $x \in V_0$:

$(i)\quad a\|x\|^d \leq V(x,t) \leq b\,\|x\|^d$
$(ii)\quad V(x,t) < -c\,V(x,t)$
Si $V_0 = \mathbb{R}^n$, l'origine est globalement exponentiellement stable.

Il n'existe, en général (sauf dans le cas linéaire), aucune méthode systématique pour trouver une fonction candidate de Lyapunov. Il est toutefois assez classique d'utiliser une fonction de Lyapunov quadratique, de type $V(x,t) = x^T(t) M\, x(t)$, où la matrice M est symétrique et définie positive. Ce choix présente l'avantage d'être simple à mettre en œuvre. Par ailleurs, si aucune fonction convenable n'est trouvée, on ne peut rien dire quant à la stabilité éventuelle du point d'équilibre.

Annexe B le tableau d'approximation des intégrateurs fractionnaires

Le tableau d'approximation :

L'ordre de dérivation	La fonction d'approximation
$q = 0.1$	$\frac{1}{s^{0.1}} = \frac{0.08495s^3 + 39.67s^2 + 110.4s + 1.83}{0.2154s^3 + 60.31s^2 + 100.6s + 1}$
$q = 0.2$	$\frac{1}{s^{0.2}} = \frac{0.0005623s^5 + 1.06s^4 + 106.3s^3 + 597.7s^2 + 188.4s + 3.162}{0.003162s^5 + 3.351s^4 + 189s^3 + 597.7s^2 + 106s + 1}$
$q = 0.3$	$\frac{1}{s^{0.3}} = \frac{0.0004984s^6 + 9.409s^5 + 78.93s^4 + 1098s^3 + 1700s^2 + 290.6s + 4.984}{0.005179s^6 + 3.37s^5 + 220.1s^4 + 1586s^3 + 1272s^2 + 112.6s + 1}$
$q = 0.4$	$\frac{1}{s^{0.4}} = \frac{0.02539s^6 + 9.409s^5 + 446.3s^4 + 3049s^3 + 3041s^2 + 436.7s + 8.028}{0.3162s^6 + 54.4s^5 + 1198S^4 + 3798s^3 + 1758s^2 + 117.2s + 1}$
$q = 0.5$	$\frac{1}{s^{0.5}} = \frac{3.192.10^{-5}\, s^7 + 0.06012\, s^6 + 15.49s^5 + 619.1s^4 + 3906s^3 + 3891s^2 + 601.2s + 12.71}{0.001585s^7 + 1.188s^6 + 121.9s^5 + 1939s^4 + 4872s^3 + 1932s^2 + 118.8s + 1}$
$q = 0.6$	$\frac{1}{s^{0.6}} = \frac{0.006351s^6 + 3.455s^5 + 240.5s^4 + 2412s^3 + 3531s^2 + 744.3\, s + 20.08}{0.3162\, s^6 + 54.4\, s^5 + 1198\, s^4 + 3798\, s^3 + 1758\, s^2 + 117.2\, s + 1}$
$q = 0.7$	$\frac{1}{s^{0.7}} = \frac{1.609.10^{-5}s^6 + 0.04858\, s^5 + 14.73s^4 + 492.5\, s^3 + 1834s^2 + 753.2\, s + 31.06}{0.005179s^6 + 3.37s^5 + 220.1s^4 + 1586s^3 + 1272s^2 + 112.6\, s + 1}$
$q = 0.8$	$\frac{1}{s^{0.8}} = \frac{1.642.10^{-6}s^5 + 0.0174s^4 + 9.818s^3 + 310.5s^2 + 550.3\, s + 51.94}{0.003162s^5 + 3.351s^4 + 189s^3 + 597.7s^2 + 106\, s + 1}$

$q = 0.9$	$\frac{1}{s^{0.9}} = \frac{1.776.10^{-5}s^3 + 0.4972s^2 + 82.94s + 82.45}{0.2154s^3 + 60.31s^2 + 100.6\,s\, + 1}$

Tab. La liste d'approximation des intégrateurs fractionnaires utilisant la méthode de Charef : erreur d'approximation $2dB$ et $\omega = [10^{-2}, 10^{2}]\ rad/s$.

[1] L. Ait Messouad, « *Contribution à la commande des systèmes par les régulateurs d'ordre non entier : Application à la commande de la machine asynchrone* », Mémoire de Magister, UMMTO, 2007.

[2] A. Ali-Pacha, N. Hadj-said, A. M'hamed, A. Belghoraf « *Chaos Cryptosystème basé sur l'Attracteur de Hénon-Lozi* » Université des Sciences et de la Technologie d'Oran.

[3] R. Ben Mahmoud, S.Hammami, M.Benrejeb « *Sur l'analyse et la synchronisation de systèmes chaotiques chen* » Ecole nationale d'ingénieurs de Tunisie.

[4] 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.

[5] C.Clavier, « *De la sécurité physique des cryptosystèmes embarqués* » Thèse de Doctorat en Informatique, Université de Versailles Saint-Quentin, 2007.

[6] W.Ditto and T.Munakata, « *Principles and applications of chaotic systems*». November 1995/ Vol. 38, No.

[7] T.Ebrahimi, **F.Leprevost**, **B.Warusfel,** « *Cryptographie et sécurité des systèmes et réseaux* » LAVOISIER, 2006.

[8] Ph. Fraisse, R.Protiere, D.Mary-Dessus, « *Transmission de l'information* », ellipses ,1999.

[9] C.Giraud, « *Attaque de cryptosystèmes embarqués et contre-mesure associées* » Thèse de Doctorat, Université de Versailles Saint-Quentin, 2007.

[10] H. Hammiche « *Inversion à Gauche des Systèmes Dynamiques Hybrides Chaotiques. Application à la Transmission Sécurisée de Données* » Thèse de Doctorat, UMMTO, 2011.

[11] Hartley « *Fundamental Theory and Application* ».IEEE Transactions on Circuits and Systems, Vol. 42, No. 8, August 1995.

[12] M.L'Hernault-Zangamel, « *Faisabilité d'un système d'émission-réception analogique pour les communications sécurisées par le chaos* », Thèse de Doctorat, Université Paris 6,2007. Ecole National Polytechnique de Lorraine, 2006.

[13] D. Idieu, « *Implémentation analogique de dérivateur et d'intégrateur d'ordre fractionnaire variable* », Mémoire de Magister, université Mentouri de Constantine, 2008.

[14] **G. Kaddoum** « *Contribution à l'amélioration des systèmes de communication multiutilisateurs par chaos : synchronisation et analyse des performances* » Thèse de doctorat, Université de TOULOUSE, 2008.

[15] **A. Kiani, K.Fallhi, N.Paeriz, H.Lueng**, «*A chaotic secure communication scheme using fractional chaotic systems based on a extended fractional Kalman filter*», Communication in Nonlinear Science and Numerical Simulation 14 (2009) 863-879.

[16] **M-W. Lee**, « *Etude des comportements dynamiques en modulation de cohérence appliquée à la cryptographie* », Thèse de Doctorat, université de Franche-Comté, France, 2002.

[17] **I.N'Doye**, «*Généralisation du lemme de Gronwall-Bellman pour la stabilisation des systèmes fractionnaires*», Thèse de Doctorat, université Henri Poincaré-Nancy1 et de l'université Hassen II Ain Chock- Casablanca, 2011.

[18] L.M Pecora and T.L. Carrol, « *Synchronization in Chaotic Systems*», Physicals Review Letters,vol. 64,no.8, pages. 821-824, 1990.

[19] S.Penaud « *Eude des Potentialités du Chaos pour les Systèmes de Télécommunication* » Thèse de Doctorat, Université de LIMOGE, 2001.

[20] **I.Petras**, « *Fractional order nonlinear systems* », Springer, 2011.

[21] **C. Servin**, *« Réseaux & telécoms* ». Dunod, 2003.

[22] **M. Shahiri and al**, « *Adaptive backstepping chaos synchronization of fractional order Coullet system with mismatched parameters* ». The 4th IFAC Workshop Fractional Diffrerentiation and its Applications. Spain, October, 2010.

[23] L-J. Sheu,W-C. Chen,Y-C. Chen and W.T. Weng, «A two channel secure communication using fractional chaotic systems», World Academy of Science Engineering and Technology, 2010.

[24] K. Sun, X. Wang, « *Bifurcation and chaos in fractional order simplified Lorenz system*», International Jouranl of Bifurcation and chaos, Vol.20, No. 4 (2010) 1209-1219.

[25] **W.Tan, F.Ling Jang, C.Xia Huang and L.Zhou,** «*Synchronization for class of fractional-order hyperchaotic system and its application*», Journal of applied mathematics. Volume 2012, 11pages.

[26] A.Zemouche « *Sur l'observation de l'état des systèmes dynamiques non linéaires* », Thèse de Doctorat, Université Louis Pasteur Strasbourg I, 2007.

[27] **G. Zheng, B. Bouta, J-P. Barbot**, « *Discussion sur les formes normales d'observabilité et les observateurs à mode glissants étape par étape* », Equipe Commande des Systèmes (ECS-EA), ENSEA, France.

Résumé

Ce travail a comme objectif principal l'étude de deux dispositifs de transmission sécurisée de données à base de systèmes chaotiques d'ordre entier et fractionnaire.

Le système de communication complet est composé de l'émetteur, un système chaotique d'ordre entier dit circuit de Chua (un circuit électronique simple permet de générer le chaos) et à la réception un observateur à mode glissant fonctionne étape par étape permet de reproduire les signaux chaotiques générés par l'émetteur et le message en temps fini. Le message confidentiel est crypté avec deux méthodes de cryptages : « addition » et « inclusion ».

Les mots clés : communication sécurisée, chaos, synchronisation, observateur à mode glissant, système d'ordre fractionnaire.