République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Amar Telidji-Laghouat

Faculté de Technologie

Département Électronique

Thèse présentée en vue de l'obtention du diplôme de Doctorat en Sciences

Option: Génie Electrique

Spécialité : Electronique

Présenté par:

OUGUISSI HADDA

Thème

Contrôle et synchronisation des systèmes chaotiques en utilisant les méta-heuristiques : Application à la sécurité des communications numériques

Soutenue devant le jury composé de:

Pr.	**BELKHIRI MOHAMED**	**Université Amar Telidji de Laghouat**	**Président**
Pr.	**SAADI SLAMI**	**Université Zaine Achour Djelfa**	**Encadreur**
Pr.	**KIOUS MECHERI**	**Université Amar Telidji de Laghouat**	**Co-encadreur**
Pr.	**BESSISSA LAKHDAR**	**Université Zaine Achour Djelfa**	**Examinateur**
Pr.	**KHERFI MOHAMED LAMINE**	**Ministère de l'enseignement supérieur et de la recherche scientifique**	**Examinateur**
Pr.	**MERAH LAHCEN**	**Université Amar Telidji de Laghouat**	**Examinateur**
Pr.	**MESSELMI FARID**	**Université Zaine Achour Djelfa**	**Examinateur**

Dans cette thèse, nous sommes intéressés à la conception des systèmes de communication vocale à haute sécurité en utilisant deux niveaux de cryptages basés sur les systèmes chaotiques. Le premier niveau est le masquage chaotique, tandis que le deuxième niveau est le brouillage. Dans le niveau de masquage nous utilisons deux méthodes, la première méthode est le masquage mélangé entre les cartes chaotique (logistique map et tent map), tandis que la deuxième méthode est basée sur le système chaotique de Chua. Ensuite, le signal audio crypté à l'aide des systèmes chaotiques est intégré avec une image de filigrane à des fins de vérification. Au niveau de brouillage, l'utilisation de la carte d'Arnold. (Cat map) permet de diffuser des échantillons de signal au moyen d'une clé secrète, et récupérer le signal original des échantillons n'est pas possibles sans cette clé. Au niveau du récepteur et pour récupérer le signal audio masqué par le système du Chua nous utilisons la synchronisation Pecore-Carroll. Nous avons estimé les paramètres du système du Chua en utilisant des algorithmes d'optimisations (GA, PSO) pour minimiser l'erreur de synchronisation. La technique de chiffrement et déchiffrement tirent pleinement parti de l'intégration du système chaotique à faible dimension pour optimiser l'espace de la clé. Cela favorise une complexité de calcul, et un temps de calcul plus élevés, tandis que le système du Chua, l'un des systèmes avec des comportements dynamiques riches et complexes a une grande espace pour la clé. À partir des résultats obtenus, et par les valeurs du coefficient de corrélation et le SNR, notre conception est validée parmi les meilleures méthodes par rapport aux autres approches robustes existantes et publiées récemment.

Les mots clés : audio sécurisés ; cryptage ; chaos ; synchronisation ; filigrane ; algorithmes méta-heuristiques.

الملخص:

في هذه الأطروحة نحن مهتمون بتصميم نظام اتصالات صوتي عالي الأمان باستخدام مستويين من التشفير على أساس الأنظمة الفوضوية. المستوى الأول هو التقنيع الفوضوي ، بينما المستوى الثاني هو التشويش . في مستوى التقنيع، نستخدم طريقتين الأولى هو التقنيع بواسطة المزيج بين الخرائط الفوضوية(الخريطة اللوجستية و خريطة الخيمة)، بينما الطريقة الثانية تعتمد على التنقيع بواسطة نظام الفوضوي لChua. ، يتم تضمين صورة العلامة المائية في الصوت المشفر للتحقق من سلامته وعدم التعرض له عند الاسترجاع. في مستوى التخليط، نستخدم خريطة (خريطة القط) تسمح ببعثرة عينات الإشارة عن طريق المفتاح السري و لا يمكن استعادة الإشارة الأصلية من العينات بدون هذا المفتاح. قمنا باستخدام المزامنة الفوضوية على جهاز الاستقبال لاستعادة الاشارة الصوتية المحجوبة باستخدام تزامن بيكورا كاوول، و لتقليل خطا الذي اعتبرناه كمشكل تحسن غير خطي استخدمت الخوارزميتين الجينية و ذكاء سرب الطيور . تستفيد تقنيات التشفير وفك التشفير بالكامل من تكامل الأنظمة الفوضوية منخفضة الأبعاد لتحسين مساحة المفتاح ولكن هذا يعزز تعقيدا و وقتا حسابيا أعلى. في حين ان نظام شويا هو احد الأنظمة ذات السلوكيات الديناميكية الغنية و المعقدة و لديه مساحة رئيسية.

من النتائج التي تم الحصول عليها من قيم كل من معامل الارتباط و SNR. تم التحقق من صحة تصميمنا و انه من بين أفضل الطرق مقارنة بالمناهج القوية الأخرى التي كانت موجودة مؤخرا

الكلمات المفتاحية: حماية الصوت، التشفير، الفوضى، التزامن، العلامة المائية، خوارزميات التحسين.

Abstract

In this thesis, we are interested in the design of a high-security voice communication system using two levels of encryption based on chaotic systems. The first level is chaotic masking, while the second level is scrambling. In the masking level,we use two methods, the first method is masking the mixing between the chaotic map(logistic map and tentmap), while the second method is based on the chaotic system of the Chua. After usget theen crypted audio using chaotic systems, a watermark image is embedded in the encrypted signal for verification. In the scrambling level,we use the Arlond map (Cat map) allowing the transmitted signal samples by means of a secret key, and the recovery of the original signal from these samples is not possible without having this key. At the receiver level, and to recover the audio signal masked by the Chua system,we use Pecora-Carroll synchronization. We estimated the Chua system parameters using optimization algorithms(GA, PSO) to minimize the synchronization error. The encryption/decryption technique take full advantage of low dimensional chaotic system integration to optimize key space, but this promotes higher computational time, while the Chua system is one of systems with rich and complex dynamic behaviors and has a large keyspace. From the obtained results, and by the values of correlation coefficient and SNR,our design has been validated among the best methods compared to other robust approaches existing recently.

Keywords: speech security, encryption, Chaotic, Watermarking, Synchronisation, Méta-heuristics algorithms.

.

Je dédie ce modeste travail :

A l'âme de mes parents, que Dieu leur fasse isériсorde,

A mes sœurs et mes frères,

A tous ceux qui me portent l'amour dans leurs cœurs.

Cette thèse n'aurait pu voir le jour sans l'aide du Dieu et le soutien de nombreuses personnes, aussi je voudrais simplement leur exprimer ici toute ma reconnaissance et ma gratitude.

Tout d'abord, j'exprime ma profonde gratitude à Monsieur ***SAADI Slami***, Professeur à L'Université de Djelfa pour la confiance, la patience et l'aide qu'il m'a accordé au cours de ces années en tant que directeur de thèse, pour les nombreuses discussions que nous avons eues ensemble, pour la qualité scientifique de ces remarques et pour le temps qu'elle a bien voulu me consacrer.

J'exprime toutes mes profondes reconnaissances à mon Co-encadreur Monsieur ***KIOUS Mecheri***, Professeur à l'Université de Laghouat pour ces encouragements et pour tout l'effort qu'il a fournis pour munir à bien et accomplir notre travail.

J'adresse mes plus vifs remerciements et ma grande reconnaissance à Monsieur ***BELKHIRI Mohamed,*** Professeur à l'Université de Laghouat pour m'avoir fait l'honneur de présider le jury de cette thèse.

Je tiens à exprimer ma gratitude à Monsieur, ***KHERFI Mohammed Lamine***, Professeur, Direction des Réseaux et du développement numérique, Ministère de l'enseignement supérieur et de la recherche scientifique, pour l'intérêt qu'il a bien voulu porter à notre travail de recherche et pour avoir accepté la lourde tâche d'examinateur.

Je voudrais remercier très vivement Monsieur ***MESSELMI Farid***, Professeur à L'Université de Djelfa pour l'honneur qu'il m'a fait en acceptant d'examiner cette thèse.

Je remercie très chaleureusement Monsieur, ***BESSISSA Lakhdar***, Professeur à L'Université de Djelfa pour le temps qu'il a bien voulu consacrer à l'examen de mon travail en tant qu'examinateur.

Mes remerciements vont également à Monsieur, ***MERAH Lahcene***, Maitre de conférence –A- de l'université de Laghouat, pour avoir accepté de participer au jury et examiner ce travail.

Je tiens à exprimer ma gratitude à Monsieur, **AMEER KADHIM Jawad**, Maitre de conférence de l'université islamique najaf-Iraq- pour son aider et pour ses précieuse informations, qui ont été une référence pour moi.

Je ne peux pas oublier la gratitude que je dois à Monsieur ***MERRAD Ahmed***, Maitre de conférences à l'Université de Djelfa, pour sa grande contribution qui m'a aidé à accomplir mon travail.

Enfin, merci à toutes les personnes qui ont contribué, de près ou de loin, à la réussite de ce travail

DSE	Data Encryption Standard
RSE	Rivest Shamir Adleman
HD	Haut Dimension
OGY	Ott, Gerbogi et York
HZ	Hertz
KHZ	Kilo Hertz
ADC	Analog to Digital Convert
CDA	Convert Digital to Analog
MIC	Microphone
RIFF	Resource Interchange File Format
DFT	Discrete Fourier Formation
DWT	Discrete Wavelet Transform
DCT	Discrete CosineTransform.
AWGN	Additive White Gaussian Noise
Mod	Modulo
UACI	Unified Average Changing Intensity
NSCR	Number of Sample Change Rate
SNR	Signal to Noise Ratio
BER	Bit Error Rate
PSO	Particle Swarm Optimization
GA	Genetic Algorithms

Introduction générale

Introduction générale

La communication vocale est en relation étroite avec la vie quotidienne, comme l'éducation, l'apprentissage en ligne, le commerce, la politique et la diffusion de l'information. Avec le développement des technologies modernes de communication et multimédia, une énorme quantité de données vocales sensibles voyage quotidiennement sur des réseaux ouverts et partagés. Afin de maintenir la sécurité, les données sensibles doivent être protégées durant leur transmission.

Les chercheurs ont proposé un grand nombre de manières de crypter un signal vocal tels que les techniques cryptographiques conventionnelles sont efficaces pour les données textuelles [1], [2].

L'une des solutions potentielles qui a une association avec la croissance du système de communication non linéaire et les données vocales volumineuses et redondantes est le chaos. Grâce aux propriétés des systèmes chaotiques, tels que la très sensibilité des systèmes non linéaires aux conditions initiales, et le fait qu'ils évoluent dans une large bande de fréquence, ce qui fait apparaitre leurs trajectoires comme de bruit pseudo aléatoire, les systèmes chaotiques sont devenus de bons candidats pour la cryptographie afin d'augmenter le degré de la sécurité [3-6].

Les systèmes chaotiques ont été appliqués aux cryptographies afin d'augmenter le degré de la sécurité au cours de ces dernières décennies. Les systèmes restés méconnus jusqu'au 20^{eme} siècle. Henri Poincaré [7] découvrit la notion de la sensibilité aux conditions initiales à travers le problème d'interaction de trois corps célestes plus tard, en 1960, les travaux de Edward Lorenz [8], passionné de météorologie, ont chargé le cours de cette branche des mathématiques.

Les techniques de chiffrement et de déchiffrement utilisant un système chaotique de faible dimension ont un petit espace de clés, ces techniques offrent une faible résilience face aux attaques par force brute [9]. De nombreuses techniques de chiffrement aléatoires tirent pleinement parti de l'intégration de nombreux systèmes chaotiques pour optimiser l'espace de clé, mais cela favorise une complexité de calcul et un temps de calcul plus élevés [10]. Des techniques de chiffrement basées sur des systèmes chaotiques à haute dimension qui présentent des comportements très complexes ont été proposées [11-12].

Grâce à des techniques de brouillage de la parole [13], Le combinant à la fois le brouillage chaotique et le cryptage par masquage de la voix peut produire une intelligibilité très faible et une force hautement cryptanalyse. Pour supprimer avec succès le masquage chaotique, la synchronisation est une partie centrale dans tout système de communication sécurisée qui comprend un système chaotique [14].Le développement des systèmes de communication utilisant le chaos a commencé donc avec des schémas de synchronisations très simples de circuits électroniques, visant le cryptage et la reconstruction simultanée d'un signal d'information [15-17].

De plus, le signal de l'information peut être lui-même un signal chaotique, même que le signal chaotique est originalement imprédictible, il sera contrôlé de sorte qu'il ne change pas de comportement mais portant un signal bien utile. Pour obtenir une synchronisation parfaite entre l'émetteur et le récepteur et une estimation des paramètres de contrôle adéquat, plusieurs algorithmes d'optimisation : *GA* et *PSO* sont utilisés.

Nous nous intéressons, dans le cadre de cette thèse, à la conception d'un système de communication vocale à haute sécurité utilisant deux niveaux de cryptages basés sur les systèmes chaotiques. Le premier niveau est le masquage chaotique, tandis que le deuxième niveau est le brouillage. Dans le niveau de masquage utilisant deux méthodes, la première méthode est le masquage en utilisant une hybridation entre les cadres chaotique (*logistique map* et *tent map*), tandis que la deuxième méthode est basée sur le système chaotique du *Chua*. Dans le niveau de brouillage nous utilisons la carte d'Arnold. Au niveau du récepteur et pour récupérer le signal audio crypté, nous utilisons la synchronisation Pecore et Carroll. Nous avons estimé les paramètres du système du Chua en utilisant des algorithmes d'optimisations (GA, PSO) pour minimiser l'erreur de synchronisation.

Cette thèse est organisée de la façon suivante:

Le chapitre 1 est consacré à donner un aperçu sur les systèmes chaotiques, ensuite nous avons présenté quelques exemples sur les systèmes chaotiques et leurs caractéristiques.

Dans le chapitre 2, nous proposons des techniques de brouillage d'un audio (de brouillage), ici nous présentons des méthodes de masquage d'un signal, puis nous donnons brièvement une notion sur le tatouage numérique. Enfin de ce chapitre, nous présentons des tests expérimentaux pour tester les performances des méthodes proposées.

A travers le chapitre 3, nous représentons quelque méthodes de synchronisation des deux systèmes chaotiques, et ensuite nous présentons les algorithmes d'optimisation *PSO* et *GA* utilisés pour estimer les paramètres du système chaotique.

Dans le chapitre 04, nous discutons les méthodes de masquage chaotique et brouillage chaotique, et nous présentons la méthode de synchronisation des deux systèmes chaotique du *Chua* par *Pecora et Carroll*, et enfin nous présentons la méthode d'optimisation de l'erreur de synchronisation par estimation les paramètres du circuit *Chua* avec les algorithmes d'optimisation *PSO* et *Ga*.

Le chapitre 5 présente les résultats du chiffrement des méthodes proposées en plus des évaluations par des tests expérimentaux.

Enfin on termine ce modeste travail par une conclusion et perspectives.

Chapitre 1

Généralité sur les systèmes chaotiques

1.1 Introduction

L'objectif de ce chapitre est de présenter des généralités sur les systèmes chaotiques, ensuite nous donnons quelques exemples sur les systèmes chaotiques, puis nous étudions le système chaotique du *Chua* et sa méthode de contrôle.

1.2 Généralités sur les systèmes chaotiques

Le terme "chaos" définit un état particulier d'un système dont le comportement ne se répète jamais.

Il existe plusieurs définitions possibles du chaos [18-19]. Ces définitions ne sont pas toutes équivalentes, mais elles convergent vers certains points communs caractérisant ainsi le chaos :

- Non-linéarité : si le système est linéaire il ne peut pas être chaotique.
- Déterminisme : un système chaotique a des règles fondamentales déterministes (plutôt que probabilistes).
- Sensibilité aux conditions initiales : des très petits changements sur l'état initial peuvent mener à un comportement radicalement imprévisible.
- Imprévisibilité : en raison de la sensibilité aux conditions initiales, la réponse est totalement imprévisible après un certain temps d'évolution.
- Irrégularité : ordre caché comprenant un nombre infini de modèles périodiques instables (ou mouvements). Cet ordre caché forme l'infrastructure des systèmes chaotiques.

1.2.1 Caractéristique du chaos

Nous présentons, dans ce qui suit, quelques caractéristiques qui permettent de comprendre qualitativement les points marquants d'un système chaotique :

1.2.1.1 Sensibilité aux conditions initiales

Les systèmes chaotiques sont extrêmement sensibles aux perturbations. Ce concept est illustré par le fameux «effet papillon», énoncé et popularisé par le météorologue Edward Lorenz [8]. L'évolution d'un système dynamique chaotique est imprédictible en ce sens qu'elle est sensible aux conditions initiales. Ainsi, deux trajectoires de phases initialement voisines s'écartent toujours l'une de l'autre. Nous allons illustrer ce phénomène par une simulation numérique de l'équation de *logistique map*.

1.2.1.2 Attracteur étrange

Un attracteur est la zone de l'espace des phases qui attire les trajectoires d'un système dynamique. L'attracteur le plus simple est un point. Il existe deux type d'attracteurs, les attracteurs réguliers et les attracteurs étranges ou chaotiques. Dans le cas d'un système chaotique, la trajectoire converge vers une région particulière de l'espace appelée attracteur étrange qui est un signaleur du chaos [8].

1.2.1.3 Exposant de Lyapunov d'un système chaotique

L'exposant de Lyapunov sert à mesurer le degré de stabilité d'un système, un système sensible à de très petites variations des conditions initiales aura un exposant positif (système chaotique).Un attracteur étrange possédera toujours au moins un exposant de Lyapunov positif, autrement dit le plus grand exposant est positif pour un système chaotique et négatif pour les autres systèmes [20], [21].

1.3 Quelque exemples des systèmes chaotiques

Il existe plusieurs systèmes chaotiques qui sont utilisés pour générer les signaux chaotiques. Dans cette section, nous présentons deux classes : les systèmes chaotiques continus et les systèmes chaotiques discrets.

1.3.1 Systèmes chaotiques discrets :

-La carte logistique (une seule dimension):

La fonction chaotique logistique s'exprime :

$$x_{n+1} = r x_n (1 - x_n) \tag{1.1}$$

Ou $x_0$prend valeur dans l'intervalle [0,1] appelé les conditions initiales.

r est une constante positive et prend une valeur de 0 jusqu'à 4 comme montre les figures Fig.1.1 et Fig.1.2.

Pour illustrer les comportements d'un système dynamique prenons comme exemple la carte logistique décrit par l'équation (1.1).

On a choisi pour chaque valeur de $r\epsilon\,[0,4]$ une séquence de 500 échantillons avec une période de transition de 500 échantillons. Suivant la valeur de r (paramètre de bifurcation) et la valeur initiale de x_0 de la suite x_k, celle-ci présente des comportements très différents.:

- pour $r = 2{,}7$ et $x_0 = 0.15$ l'évolution de suite x_k converge rapidement vers un point fixe et stable du plan (x_k, x_{k+1}).
- pour $r = 3{,}2$ nous remarquons que la suite converge vers une solution périodique. Dans ce cas, la trajectoire converge vers un cycle d'ordre 2.
- On augmentant la valeur de r la nouvelle suite converge vers une solution périodique avec doublement de période.
- Pour $r \geq 3{,}57$ la suit x_k ne représente plus une structure ordonnée. Donc, le système devient chaotique comme montre la Fig.1.2.

On peut résumer la route vers le chaos à l'aide d'un diagramme de bifurcation donné par la Fig1.1

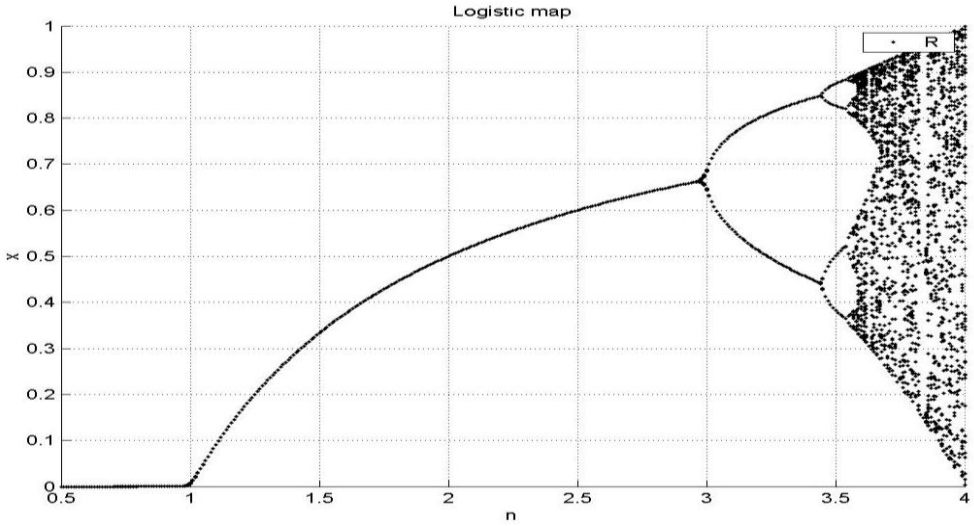


Fig.1.1 -Diagramme de bifurcation de la carte logistique

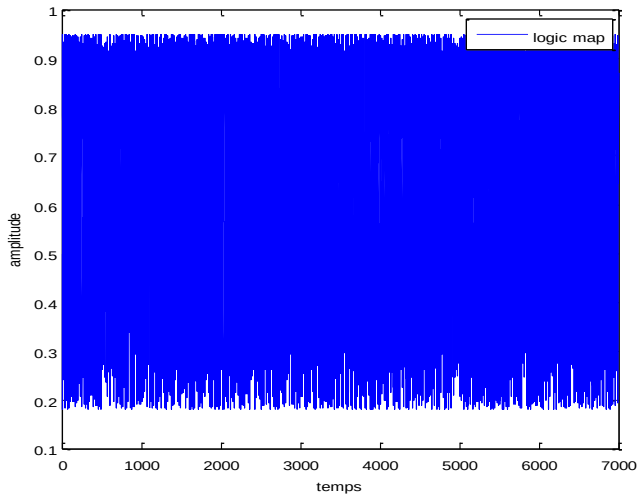


Fig.1.2–le signal chaotique de la carte logistique.

Cette carte logistique est très sensible aux conditions initiales. Nous allons fixer deux conditions initiales très proches $x_0 = 0.25$ et $y_0 = 0.251$ pour le système chaotique (1.1). Dans un premier temps, les deux systèmes évoluent de la même manière, mais très vite, leur comportement devient différent comme le montre la Fig.1.3.

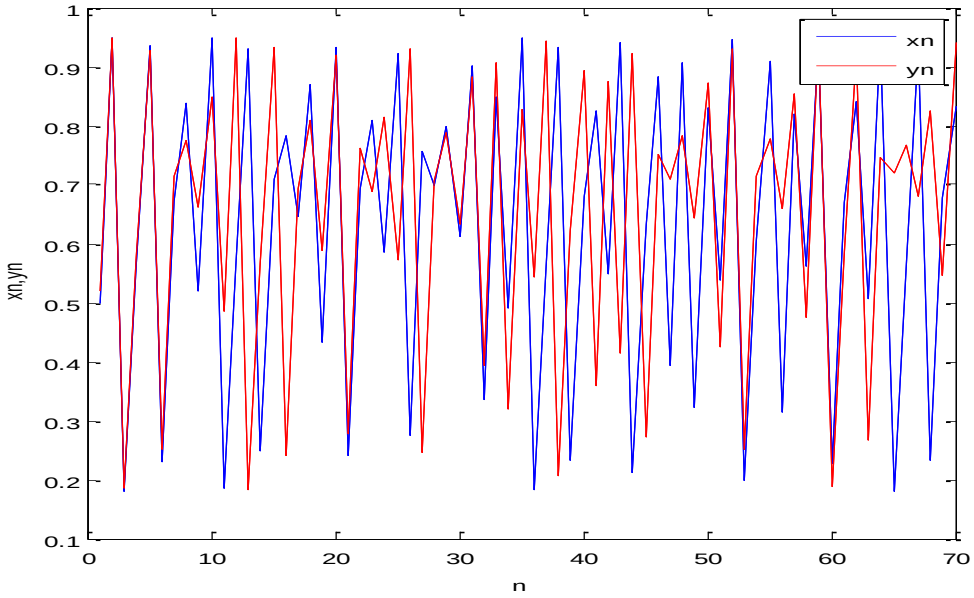


Fig.1.3 -L'évolution dans le temps pour deux conditions initiales très proches.

-La carte *tent map*

Est une carte linéaire par morceaux, décrite par l'équation suivante :

$$\begin{cases} f(x_i, u) = ux_i & si \quad x_i < 0.5 \\ f(x_i, u) = u(1 - x_i) & si\ autrement \end{cases} \tag{1.2}$$

Où $x_i \epsilon [0,1]$ pour i $\geq$0.

Et u est le paramètre de contrôle qui varie dans l'intervalle [0,2], x_0 est une initiale valeur de système.

En fonction du paramètre de contrôle u, le système illustre une variété d'actions dynamiques variant d'attendu à chaotique comme montre la figure Fig.1.4.

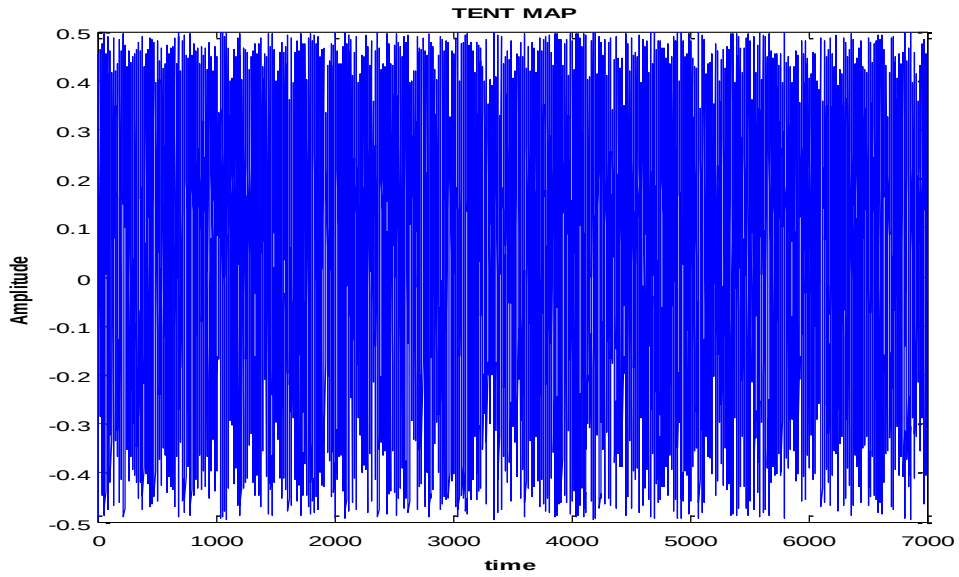


Fig.1.4–le signal chaotique de la carte tant map.

-La carte d'ARNOLD

La carte chaotique appelée la carte d'Arnold en reconnaissance de mathématicien russe Vladimir I. Arnold, qui la découverte en utilisant une image d'un chat. C'est une démonstration et une illustration simple et élégante de certains principes de chaos, une évolution apparemment aléatoire d'un système.

Si nous considérons $X = \begin{pmatrix} x \\ y \end{pmatrix}$, une matrice de taille $\times N$, la transformation d'Arnold T est :

$$\begin{pmatrix} \grave{x} \\ \grave{y} \end{pmatrix} \equiv \begin{pmatrix} 1+1 \\ 1+2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} mod\ N \qquad (1.3)$$

Ou' mod N est modulo N, (x, y) sont les coordonnées du filigrane d'origine et (x', y') sont les coordonnées du filigrane brouillé. N est la hauteur ou la taille du signal qui doit être traité.

1.3.2 Les systèmes chaotiques continus :

-Système de Lorenz

En 1963, Edward Lorenz a modalisé un système différentiel à comportement chaotique pour certaines valeurs de paramètres. Ce système est défini par les équations suivantes :

$$\begin{cases} \dot{x} = \sigma(y - x) \\ \dot{y} = -rx - y - xz \\ \dot{z} = -bz + xy \end{cases} \quad (1.4)$$

Ci-dessous l'attracteur de Lorenz pour les valeurs suivantes $\sigma = 10$, $r = \frac{3}{8}$, $b = 28$,et conditions initiales $x_0 = y_0 = z_0 = 0.01$, avec un pas de simulation 0.01.

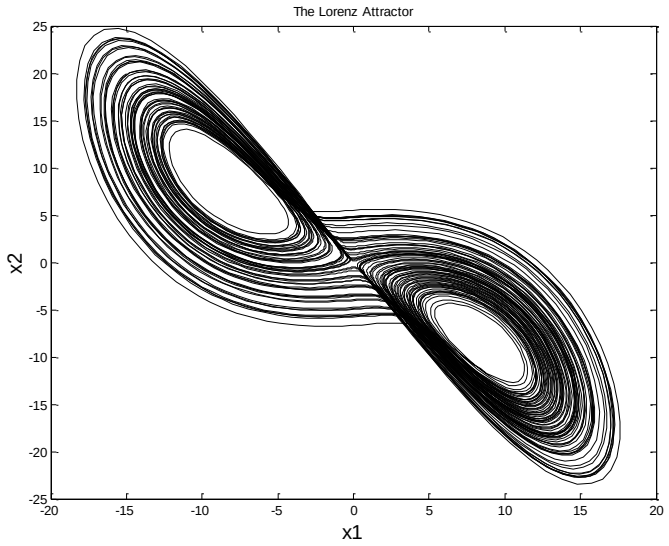


Fig.1.5 Système chaotique de Lorenz

.

- Circuit du *Chua*

Le circuit de *Chua* est un circuit électronique simple(Fig.1.6) qui montre le comportement classique de théorie de chaos [22-24]. Il a été présenté en 1983 par **Leon O. Chua**, qui était un visiteur à l'université de Waseda au Japon à ce moment.

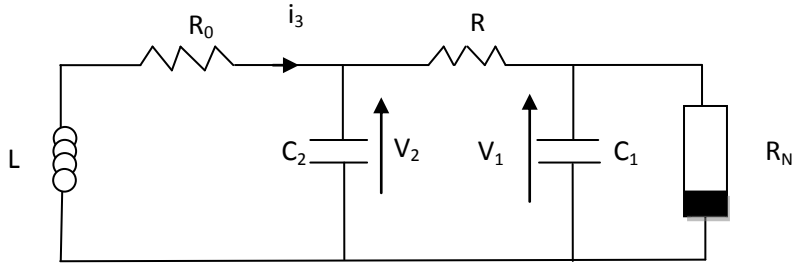


Fig.1.6 -Circuit de *Chua*.

Le système de *Chua* représenté par l'ensemble d'équations différentielles :

$$\begin{cases} \dot{x} = \alpha(y - x - f(x)) \\ \dot{y} = x - y + z \\ \dot{z} = -\beta(x - R_0 z) \end{cases} \quad (1.5)$$

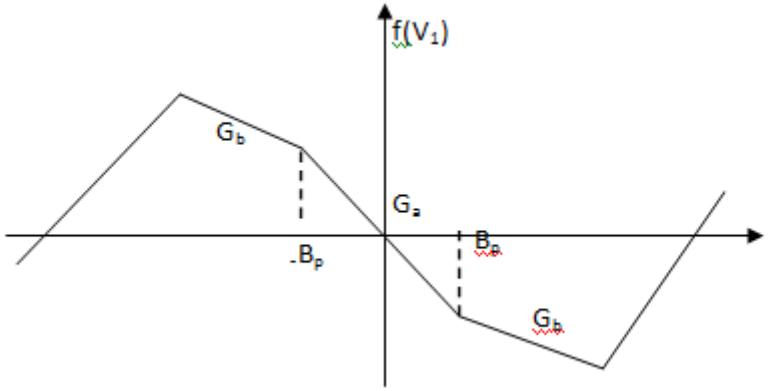


Fig.1.7 –Caractéristique tension-coutant de la résistance non-linéaire.

Ou' $f(x) = m_1 x + \frac{m_0 - m_1}{2}(|x+1| - |x-1|)$ (1.6)

Avec les paramètres de ce circuit dépendent essentiellement des valeurs de la résistance, de l'inductance ainsi que celles des condensateurs :

$$\alpha = \frac{C_2}{C_1}, \beta = \frac{R^2 C_2}{L}, m_0 = \frac{G_a}{G}, m_1 = \frac{G_b}{G} \quad (1.7)$$

Avec $G = {}^1/_R$

1.4 Contrôle du système chaotique :

Dans le but de camoufler un message confidentiel en le superposant à un système chaotique, le signal d'information doit être lui-même un signal chaotique, mais comme un signal chaotique est intrinsèquement imprévisible, il est donc nécessaire de le contrôler pour qu'il ne change pas de comportement mais il porte un signal d'information.

De ce qui est précédé, nous avons remarqué que nous pouvons atteindre le régime chaotique par la variation du paramètre de contrôle.

1.4.1 Technique de contrôle le chaos

Il est clair que le comportement dynamique d'un système non linéaire peut être changé en changeant certaines valeurs de ses paramètres. Dans le contrôle du chaos, on

est amené à travailler dans l'espace de phase, l'espace paramétrique ainsi que la carte de Poincaré. De plus, les exposants de Lyapunov et le diagramme bifurcation sont des outils typiques pour l'étude.

Le contrôle du chaos est réalisé en stabilisant les orbites périodiques instables d'un système chaotique en appliquent une petite perturbation à certains paramètres du système, où la première à évoquer cette notation Ott, Gerbogi et York (OGY) [25], et parce qu'il est devenu possible de contrôler un système chaotique qui est évalué du contrôle le chaos dans les circuits électronique [26].

1.4.2 Contrôle du système chaotique du *Chua*

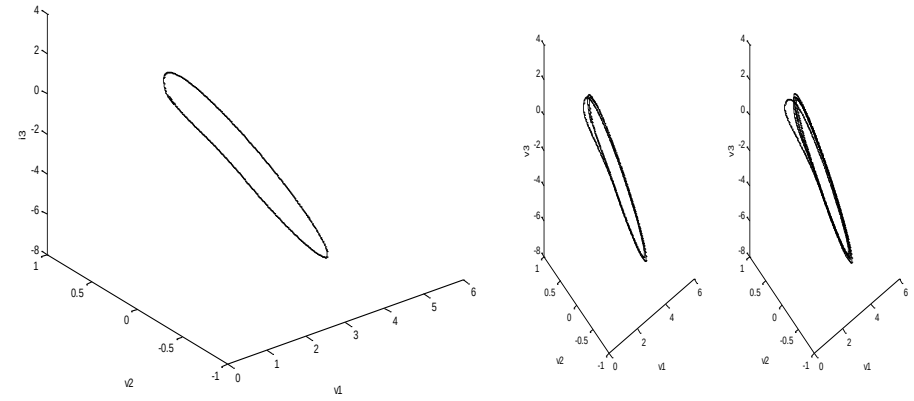
Le contrôle de système du *Chua* basé sur les exposants de Lyapunov et le diagramme bifurcation**.**

Nous avons le système du *Chua* (1.5), les points fixes de ce système sont :

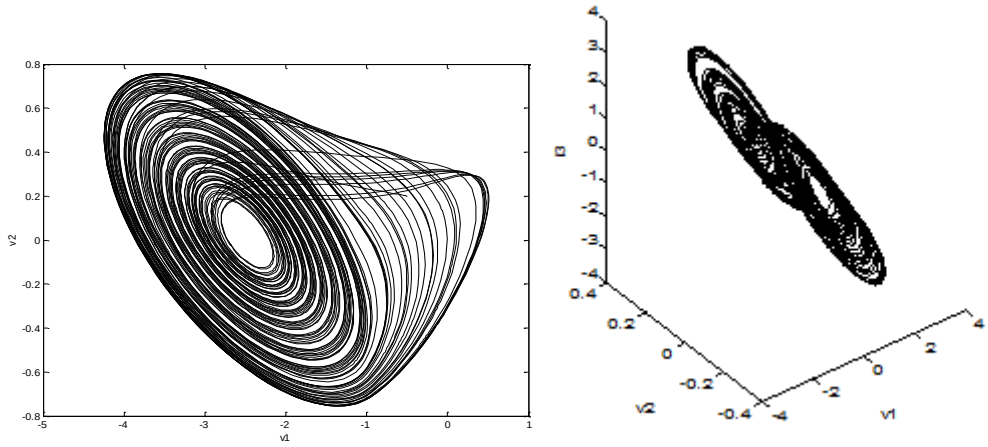
$$C_0(0,0,0), C_1\left(\frac{m_0-m_1}{m_1+1},0,\frac{m_1-m_0}{m_1+1}\right), C_2(\frac{m_1-m_0}{m_1+1},0,\frac{m_0-m_1}{m_1+1})$$

1.4.2.1 Le comportement de système chaotique du *Chua*

Il est suffisant de modifier la valeur d'un composant pour étudier les divers modes ou les différents comportement qu'il peut montrer le circuit de Chua. Dans le circuit de Chua, nous prenons la résistance α comme paramètre de bifurcation, nous avons effectué des simulations en faisant varier le paramètre α de 10 à 17avec un pas d'itération de 0.01, et $\beta = 28, m_0 = -1.27, m_1 = -0.68$.



(a)



(c) (d)

Fig.1.8-Le comportement du circuit du *Chua* pour différente valeur de α

1.4.2.2La stabilité par exposant de Lyapunov:

Nous prenons les valeurs des paramètres du système du *Chua* (1.5) comme le cas chaotique $\alpha = 15.6, \beta = 28\, m_0 = -1.27, m_1 = -0.68$, nous choisissons les valeurs initiales de l'état comme $x_0 = 1\,, y_0 = 0.5, z_0 = -1$ l'exposant de Lyapunov du système (1.5) sont :

$L_1 = 0.2, L_2 = 0, L_3 = -4.3$, le système (1.5) est chaotique car il a un exposant de Lyapunov positive L_1.

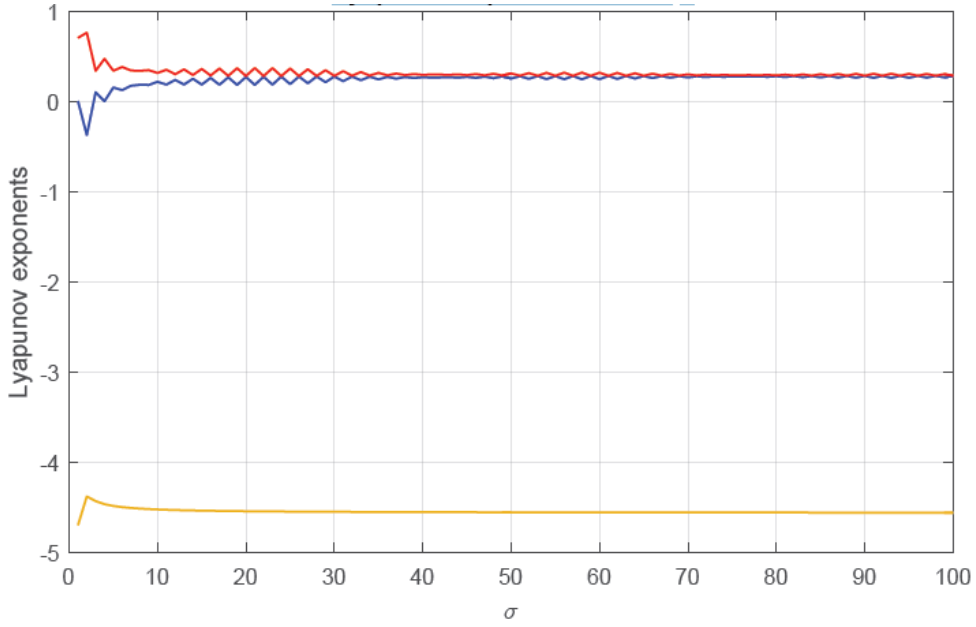


Fig.1.9.Exposant de Lyapunov de système du Chua.

1.5 Conclusion

Dans ce chapitre et après avoir présenté quelques exemples sur les systèmes chaotiques et ses caractéristiques. Nous avons trouvé qu'il est possible de contrôler le système non linéaire en contrôlant leurs paramétrés. Quelque application du contrôle du chaos, qui consiste à concevoir un contrôleur afin de permettre la transmission d'une information dans un système de communication.

Chapitre 2

La transmission sécurisée d'une audio base de chaos

2.1 Introduction

Les séquences chaotiques ont des propriétés similaires aux propriétés de cryptographie de confusion et de diffusion, ils ont donc été utilisés pour construire de bons systèmes cryptographiques. Ainsi, ces propriétés rendent les crypto système chaotiques résistants aux attaques statistiques [27]. Et aussi, l'utilisation du chaos dans le système du cryptage assurera la sécurité, la complexité, la vitesse et la puissance de calcul [28].

2.2 La cryptographie

La cryptographie est l'étude des méthodes permettant de transmettre des données de manière confidentielle. En transmission sécurisée de l'information, le message appelé le texte est transformé de manière à le rendre incompréhension, ce processus est appelé "chiffrement" ou "cryptage. Par ailleurs le destinataire doit engager un processus appelé "déchiffrement" ou "décryptage", pour reconstruire le message à partir du texte chiffré.

En cryptographie usuelle, et parmi une grande variété de mécanisme de chiffrement ; on distingue deux types de clé [29] : clé secrète et clé publique. Dans un algorithme à clé secrète, la clé de chiffrement est calculée à partir de la clé déchiffrement et vice versa. En générale, les clés de chiffrement et de déchiffrement sont identiques. Le chiffrement à clé publique ou chiffrement asymétrique, dans un tel schème, la clé de chiffrement est différente de celle de déchiffrement. N'importe qui peut utiliser la clé de chiffrement pour chiffrer un message, la clé privé est utilisé pour déchiffrement un message, les deux clés sont liées. Le chiffrement à clé publique peut être préféré pour générer de petite séquence, le chiffrement symétrique peut être préféré pour le chiffrement des grandes quantités des données.

2.3 Le cryptage chaotique d'un audio

La parole est enregistrée sous la forme d'un signal analogique qui est converti par la carte son en numérique en échantillonnant le signal afin de le stocker dans l'ordinateur.

2.3.1 Les caractéristiques d'un audio

Une définition simple du son peut être donnée à ses ondes résultant d'un changement de pression atmosphère, et bien que ce changement ne dépasse pas (±1) mais lorsqu'il entre en contact avec l'oreille interne du système auditif humain il fonction d'une manière dynamique large à des fréquences comprises entre 20Hz-20KHz. Le son est représenté par un diagramme en ligne continu connu sous le nom l'onde et la hauteur représentent l'amplitude du son (volume), et cette formule s'appelle le signal analogique comme illustré la figure Fig.2.1(a).

L'ordinateur et certains appareils électriques traitent les choses comme une série de nombres binaires (0,1), c'est-à-dire sous forme numérique, et pour cela, il était nécessaire de trouver un moyen ou une méthode de convertir le son de son état analogique au signal numérique formulaire afin que cet appareil puisse le comprendre et le traiter comme tel est voulu.

2.3.1.1 Enregistrement audio numérique :

Lorsque le son est stocké dans l'ordinateur via une prise de son connectée à la carte son de l'ordinateur, la prise de son (microphone) convertit les fluctuations de tension sous la forme d'un signal analogique. Le signal est mesuré et converti en parties appelées échantillons [30], puis il est converti en une série de nombres par un processus appelé quantification [31], puis ils sont convertis en une forme binaire puis stockés. Ces échantillons se trouvent à l'intérieur de l'ordinateur sur la mémoire secondaire (disque dur) au format numérique binaire. Un circuit électronique sur la carte son appelé ADC (convertisseur analogique à numérique) aide à ces opérations. Lorsque l'audio est lu, le processus est inversé, mais la fluctuation de la tension sera transmise aux haut-parleurs au lieu de la prise de son, puis convertie en une fluctuation de la pression atmosphérique, il existe également un circuit électronique qui restitue le son à son état analogique encore appelé DAC [32-33], comme montre la Fig.2.2, certains facteurs affectent le processus d'enregistrement sonore numérique, notamment :

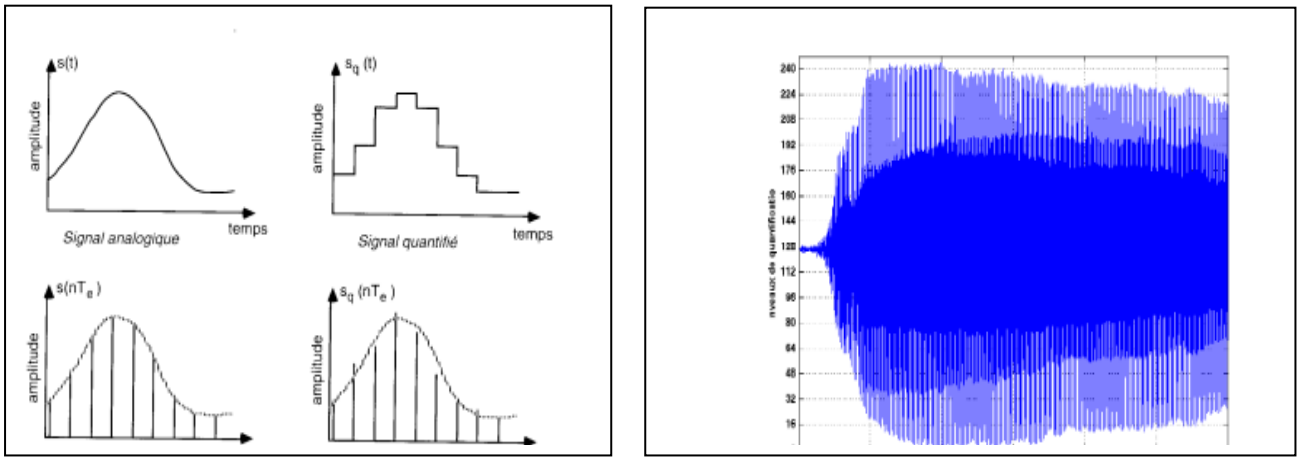


Fig.2.1 (a)-Classification morphologique des signaux (b)-signal quantifie sur 8 bits.

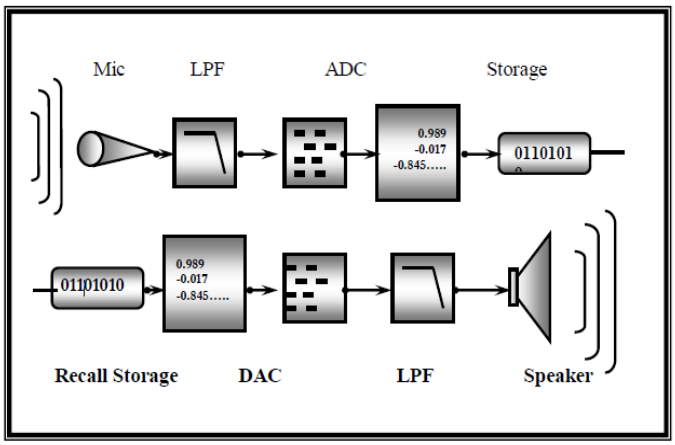


Fig.2.2 processus d'enregistrement audio numérique

Le son est stocké dans différents fichiers en fonction des différentes formats de stockage comme fichier a l'extension mp3 et extension wav.

2.3.1.2 Fichier audio avec extension (wav):

Les fichiers audio WAV sont l'un des formats audio utilisés par Microsoft dans l'environnement système Windows, ils sont l'un des formats les plus populaires et les plus utilisés de l'environnement de fichier définissant le format de fichier (commun) RIFF (Format de Fichier d'échange de Ressources). Les fichiers RIFF sont organisés en segments qui se chevauchent et sont interconnectés les uns avec les autres qui comprennent une définition du contenu du RIFF [34].

2.3.2 Les techniques de cryptage de la parole

Lorsque les communications vocales deviennent de plus en plus utilisées ou encore plus vulnérable, l'importance d'assurer un haut niveau de sécurité est un enjeu majeur. A ce jour de nombreuse technique de cryptage de la parole ont été proposées. Les techniques de cryptage de la parole peuvent être classées en quatre types à savoir : Le brouillage dans le domaine temporel, le brouillage dans le domaine fréquentiel, le brouillage d'amplitude et le brouillage mixte bidimensionnel [1], [2]. On utilise les signaux chaotiques et par une clé de permutation produite par un générateur chaotique, le signal vocal d'origine là où il est encrypté dans l'émetteur et récupérer dans le récepteur, avec les conditions initiales et les paramètres de ces cartes chaotique, il est identiques dans émetteur et le récepteur [35].

2.3.2.1 Le brouillage dans le domaine fréquentiel :

Le brouillage d'un signal dans le domaine fréquentiel est effectué par l'application d'une clé de permutation aléatoire à la transformation de Fourier discrète (DFT) du signal vocale et à la demi-gamme (symétrie conjuguée) du composante de la fréquence, le spectre du signal est divisé en sous bandes, ces sous bandes sont permutées par une clé de permutation générée par un générateur à nombre aléatoires [35].voir la Fig.2.3

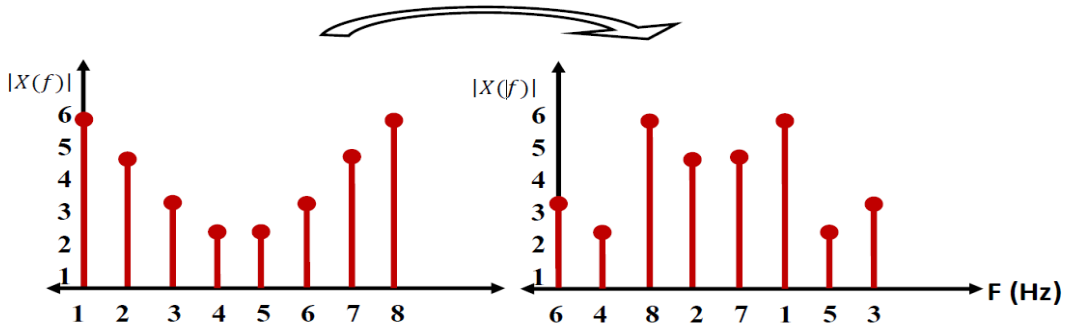


Fig.2.3. Le brouillage dans le domaine fréquentiel :

2.3.2.2 Le brouillage dans le domaine temporel :

Il divise le signal vocal en trames, et chaque trame est divisée par domaine temporel en segments (sous-trames) puis est brouillé par une clé de permutation produite par un générateur chaotique comme illustré par l'exemple suivant :

On utilise la carte chaotique logistique (1.1) définie dans le chapitre précédent, Une séquence chaotique est générée avec une longueur égale à la longueur du terme L.

Soit N=9, et avec la condition initiale $x_0 = 0.25$, et le paramètre de bifurcation $r = 3.9$ la valeur de séquence généré est :

(a)

i	1	2	3	4	5	6	7	8	9
x_i	0.5000	0.9500	0.1805	0.5621	0.9353	0.2298	0.6726	0.8369	0.5188

On a tiré les séquences chaotiques précédentes selon l'algorithme d'ordre croissant :

(b)

i'	3	6	1	9	4	7	8	5	2
x'_i	0.1805	0.2298	0.5000	0.5188	0.5621	0.6726	0.8369	0.9353	0.9500

Apres avoir tiré les vecteurs chaotique à l'étape 2, les indices des éléments sont modifiés. Ces indices représentent le nouvel indice pour brouiller dans l'émetteur et le récepteur pour crypter cette audio, pour notre séquence en étape 2, la nouvelle représentation de l'indice est :

(c)

Indice d'entrée	1	2	3	4	5	6	7	8	9
Indice de sortie	3	6	1	9	4	7	8	5	2

Table .2.1(a), (b), (c) : Permutation dans le domaine temporel d'un frame de voix.

2.3.2.3 Le brouillage bidirectionnel :

Qui combine l'embrouillage fréquentiel et temporel [35].

2.3.2.4 Le brouillage d'amplitude :

Également connu sous le nom de technique de masquage dans lequel le signal vocal est couvert par des amplitudes pseudo- aléatoires ou chaotiques.

2.4 Les méthodes de masquage chaotique

Les signaux chaotiques sont utilisés comme un porteur d'informations. Pour cela le message est crypté par l'émetteur et il est décrypté et extrait du signal chaotique par le récepteur. Dans le domaine de communication, la récupération de l'information est généralement basée sur la synchronisation entre l'émetteur et le récepteur [36]. Il existe plusieurs méthodes d'injection de l'information dans un système chaotique parmi les méthodes de transmission chaotique, on peut citer le masquage par addition [37], cryptage par inclusion [38], et le cryptage par modulation [39], etc.

2.4.1 Le masquage chaotique par addition

Cette technique développée en 1993, est appelée masquage chaotique [37]. Le principe de ce schéma est d'effectuer une simple addition entre le signal de sortie de l'émetteur $y(t)$ et le message $m(t)$. La somme de deux signaux est transmise au récepteur à travers un canal public. Le récepteur est constitué d'un système identique à celui de l'émetteur, c'est un simple soustracteur. Ainsi, après la synchronisation des deux systèmes chaotiques (émetteur et récepteur), le message est extrait à l'aide d'une opération de soustraction. Le schéma représentant cette méthode est donné par la Fig.2.4.

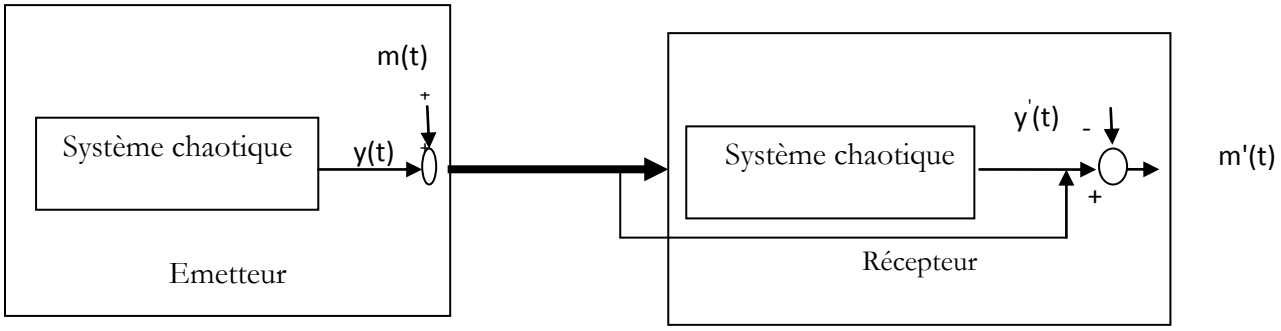


Fig.2.4-masquage chaotique par addition

2.4.2 Le masquage par les modulations paramétriques

Le principe de cette technique consiste à utiliser le message m(t) pour moduler l'un des paramètres du système chaotique de l'émetteur, un observateur à mode glissant est chargé de manière à assurer la synchronisation au niveau de récepteur.

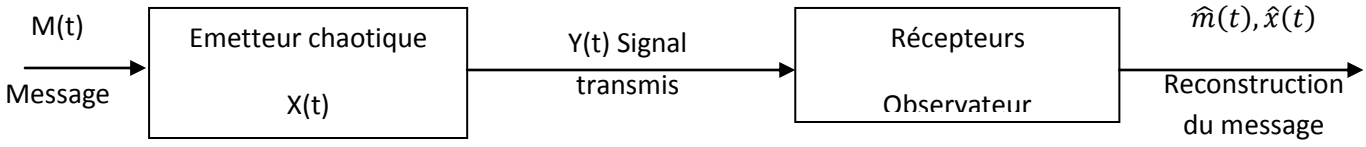


Fig.2.6. Cryptage par modulation chaotique.

2.4.3 Le masquage par inclusion

Cette technique de cryptage consiste à injecter le message dans la dynamique de l'émetteur [38] avec réalisation d'une modulation de paramètres [39] et avec un observateur à mode glissant, l'information est restaurée.

Et pour prouver le succès du système de cryptage proposé nous allons ajouter un filigrane (Watermark) au signal original pendant le processus de cryptage et extraire ce filigrane pendant le processus de décryptage. De sorte que l'extraction avec succès le filigrane lors de décryptage confirme que le signal reçu est bien authentifié et ainsi que ne souffre pas d'éventuelles attaques.

2.5 Le tatouage numérique

Le tatouage numérique est un processeur qui consiste à insérer dans un signal original dit signal hôte (une image, un document de texte, son..) une marque numérique (séquence aléatoire, un logo binaire…) de manière imperceptible et indélébile. Cette marque contient des données qui peuvent être employées dans diverses applications, y compris la protection des copyrights, la surveillance d'émission, l'authentification des données ou la transmission sécurisée. Dans le cas du tatouage audio, divers techniques ont été utilisées pour appliquer le filigrane tel que les techniques de transformation (DWT, DCT), les techniques algébriques [40-41], une nouvelle conception de filigrane aveugle pour les signaux vocaux, et ils ont utilisé la transformée en ondelettes discrètes (DWT) et la transformée cosinus discret (DCT) après segmentation du signal [42], une méthode de filigrane robuste de tatouage de l'audio à l'aveugle utilisant DCT et DWT à l'intérieur du sous échantillonnage du signal [43-44]. Pour obtenir une haute qualité d'imperceptibilité, la fusion est réalisé contre diverses attaques tels que : ré-quantification, recadrage, écho, amplification et bruit gaussien blanc additif (AWGN). Dans Annexe B des détails les techniques de tatouages DWT, DCT.

2.6 Analyse de la sécurité

2.6.1 Le cryptanalyse au système de communication base au chaos

Le cryptanalyse est l'étude de la probabilité de succès des attaques possibles [45] sur le crypto-systèmes afin de déceler leurs éventuelles faiblesses. Un crypto système doit avoir deux propriétés cryptographiques fondamentales : la confusion et la diffusion. La confusion consiste à rendre la relation entre la clé et le message chiffré la plus complexe possible. La diffusion signifie qu'un petit changement dans le message clair ou dans la clé, induit un grand changement dans le message chiffré. La cryptanalyse vise à trouver l'espace de clé et la sensibilité.

2.6.1.1 Analyse l'espace de la clé secrète

La sécurité d'un système de communication doit déprendre uniquement de sa clé secrète et c'est selon le principe de Kirchhoff [46], la taille de l'espace clé K est définie par le nombre des paires des clés au niveau du cryptage et décryptage, le nombre total de clés différentes utilisées dans le système de cryptage appelées brièvement comme clé espace [47]. De plus, le bon système de cryptage doit posséder un grand espace de clé et pour compenser la dégradation dans le PC, et empêcher ainsi les envahisseurs de décrypter les données d'origine même après avoir investi de grandes quantités de ressources et de temps [48]. Selon [49] la conception d'un crypto système qui résiste aux attaques par force brute, la taille de l'espace clé doit être supérieure à $2^{128}(\approx 3.24\times 10^{38})$.

2.6.1.2 Analyse de la sensibilité de la clé

L'analyse de la sensibilité de la clé est extrêmement importante dans la conception d'un schéma de transmission sécurisée. La modification d'un bit dans une clé génère un texte chiffré complètement différent. Calcul de l'intensité variable moyenne unifiée (UACI) et de nombre de taux de changement d'échantillon (NSCR) entre les deux signaux vocaux cryptés pour évaluer la sensibilité de la clé. Le NSCR et l'UACI des deux signaux vocaux cryptés sont calculés en utilisant l'équation ci-dessous [50].

$$\mathrm{NSCR} = \sum_{i=1}^{\mathrm{L}} \frac{\mathrm{d_i}}{\mathrm{L}} \times 100\% \qquad ou' d_i = \begin{cases} 1 & S'_{1,i} = S'_{2,i} \\ 0 & auterment \end{cases} \tag{2.1}$$

$$\mathrm{UACI} = \frac{1}{\mathrm{L}}\left[\sum_{i=1}^{L} \frac{S'_{1,i} - S'_{2,i}}{Max}\right] \tag{2.2}$$

Ou' $S'_{1,i}, S'_{2,i}$ sont les deux signaux vocaux avec une différence lente sur la clé dans I$^{\text{Ième}}$ échantillons.

L : représente la longueur du vecteur de parole.

Max : dépend de chaque échantillon de signaux vocaux et audio en supposant une valeur entière dans le range [0-65535] et dans cette situation Max=65535, donc lors de l'utilisation de l'environnement Matlab, l'audio numérique sont normalisés dans la plage

[-1,1], par la suite, le max est de 2.

2.6.1.3 La qualité de cryptage

La qualité du signal parole extrait du signal crypté est un élément essentiel, pour cela, nous discuterons la qualité du signal extrait de signal crypté, en utilisant les deux coefficients (corrélation et SNR).

2.6.1.3.1 Le coefficient de corrélation :

Le son numérique est caractérisé par des échantillons adjacents très redondants et fortement corrèles. Un schéma de transmission d'audio sécurisées robuste doit pouvoir supprimer ce type de relation.

Le coefficient de corrélation est une mesure la relation linéaire entre deux variables [51]. Si deux variables sont étroitement liés avec une plus forte association, le coefficient de corrélation est proche de la valeur 1. D'autre part, si le coefficient est proches de 0, les deux variables ne sont pas liées et ne peuvent pas être prédit.

Le coefficient de corrélation "r" peut être calculé en respectant les formules suivantes [52] :

$$r_{S_1S_2} = \frac{\frac{1}{L}\sum_i^L \left(S_{1,i} - E(S_i)\right)\left(S_{2,i} - E(S_2)\right)}{\sqrt{\left(\frac{1}{L}\sum_i^L \left(S_{1,i} - E(S_i)\right)^2\right)} \times \sqrt{\left(\frac{1}{L}\sum_i^L \left(S_{2,i} - E(S_2)\right)^2\right)}} \qquad \text{Où } E(s) = \frac{1}{L}\sum_{i=1}^L S_1 \tag{2.3}$$

Où L est la longueur des signaux vocaux (nombre d'échantillons).

S_1,S_2 sont la dualité des deux signaux (original, crypté) ou (original, décrypté).

2.6.1.3.2 Rapport du signal sur bruit(SNR) :

Pour confirmer les performances des schémas de cryptage de la parole numérique, le SNR est calculé, ou SNR mesure le bruit continu dans les signaux vocaux cryptés. Crypta analyste essaye toujours d'augmenter le continu de bruit dans le signal crypté afin de minimiser l'information dans les données cryptées. Le déchiffreur essaie également de réduire le continu sonore dans le signal déchiffré. Le rapport signal sur bruit est un facteur utilisé pour identifier la qualité de bruit sur le signal, le rapport signal sur bruit sur bruit peut être calculé par l'équation ci-dessous [53] :

$$\text{SNR} = 10 \times \log 10 \frac{\sum_{i=1}^L {S_{i,1}}^2}{\sum_{i=1}^L \left(S_{1,i} - S_{2,i}\right)^2} \tag{2.4}$$

$S_{1,i}$,$S_{2,i}$représentent les I^{ième} échantillons des signaux vocaux (original, déchiffré) ou (original, déchiffré) respectivement.

L Représente la longueur des signaux vocaux.

Pour authentifier que le signal vocal crypté reçu a été envoyé du côté de confiance, nous faisons examiner l'extraction du filigrane par le BER

2.6.2 Taux d'erreur sur les bits(BER)

Le BER est utilisé pour vérifier la similitude entre les deux filigranes, l'original et l'image de filigrane extraite. De plus, le BER est égal à zéro signifie qu'il n'y a aucun effet sur le filigrane et que l'extraction est réussie, ce que signifie que le signal vocal reçu est envoyé du côté authentifié. Le BER est exprimé par la formule suivante [42] :

$$\mathrm{BER} = \frac{B_{ERR}}{\mathrm{N}} \times 100\% \qquad (2.5)$$

Ou' B_{ERR} la qualité de bits erronés.

N : le nombre de tous les bits (taille de filigrane).

2.7 Conclusion

Dans ce chapitre, nous avons présenté les techniques de cryptage chaotique d'un audio, la principale méthode basée sur le brouillage par amplitude (masquage), et le brouillage dans le temps, et puis nous avons ajouté un filigrane où nous avons donné un bref aperçu sur le tatouage audio numérique. Enfin, nous avons donné quelques mesures d'évaluation des performances du côté de l'émetteur. Dans le côté de récepteur, et pour la reconstruction de l'audio masqué, on doit faire l'opération de synchronisation de l'émetteur et le récepteur, c'est que nous allons expliquer dans le chapitre suivant.

Chapitre 3

Synchronisation de deux systèmes chaotiques à l'aide des algorithmes méta-heuristiques PSO et GA

3.1 Introduction

La synchronisation se produit lorsque deux systèmes dynamiques évoluent de la même manière dans le temps. L'histoire de ce phénomène revient au 17eme siècle quand le Hollandais Christian Huygene (1629-1695) a apporté son observation sur deux horloges de fréquences légèrement différentes. Depuis quelconque années, la théorie des systèmes chaotiques a été appliquée dans le domaine des communications, et il est difficile de synchroniser deux systèmes chaotiques dans le cas réel. Il est extrêmement difficile de construire deux circuits identiques à cause de la tolérance sur les composants, et la sensibilité des systèmes chaotiques aux conditions initiales. Les chercheurs ont récemment découvrit des solutions pour le succès du processus de synchronisation.

3.2 La synchronisation de deux systèmes chaotiques

A cause de la sensibilité de ces systèmes chaotiques aux conditions initiales, leurs synchronisations semblent impossibles dans un premier temps. En 1983, la question de synchronisation a été abordée en utilisant des circuits électroniques linéaires par morceaux [55]. Dans les années 1990, *Pecora* et *Carroll* [56-57] ont montré que deux systèmes chaotiques identiques avec des conditions initiales différentes peuvent éventuellement être synchronisés sous certaines conditions.

3.2.1 Les méthodes de synchronisation chaotique

Les méthodes traditionnelles de synchronisation sont en général basées sur l'utilisation des circuits identiques. Supposons deux systèmes chaotiques identiques oscillants de façon totalement indépendante, si par un moyen quelconque, on leur permet d'échanger de l'énergie, action que l'on nomme "couplage", les deux systèmes finiront par céder la place à un comportement commun ils se synchronisent.

3.2.1.1Systèmes couplés :

Il est possible de coupler les systèmes chaotiques dans un sens (couplage unidirectionnelle) ou dans les deux sens (couplage bidirectionnelle) [58].

Couplage bidirectionnel : dans ce cas, l'élément de couplage permet l'échange de l'énergie dans les deux sens. L'utilisation d'une résistance, en pratique, permet d'assurer ce type de couplage.

Couplage unidirectionnel : dans le cas d'un couplage unidirectionnel, l'énergie est transférée d'un système à l'autre, à l'aide d'un élément de couplage fonctionnant dans un seul sens comme par exemple un serveur. En pratique, par exemple, un simple schéma électronique à base d'amplificateur monté en suiveur réalise cette tâche.

Pour illustrer ces deux concepts, soit les deux systèmes chaotiques identiques a et b de dimension 3 décrits par $\dot{x_a} = f(x_a)$ et $\dot{x_b} = f(x_b)$ le schéma de couplages possibles des deux systèmes est donné par la Fig.3.1.

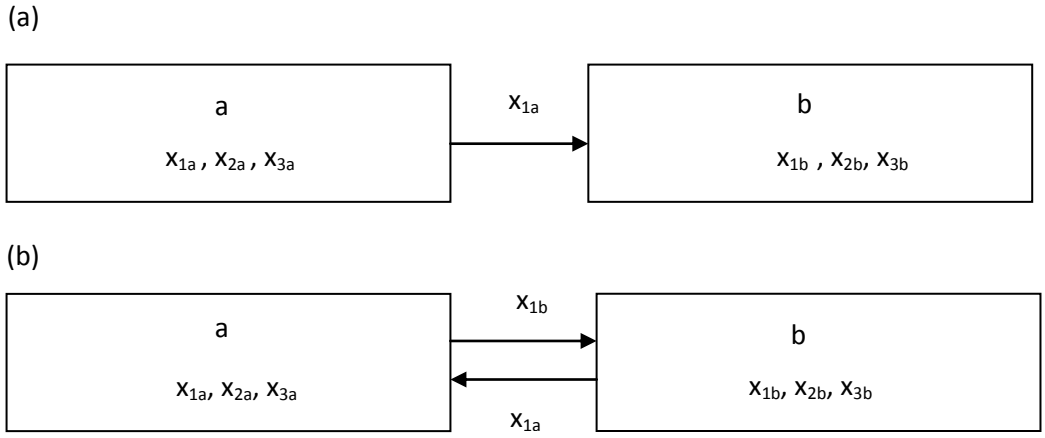


Fig.3.1 : Schéma de couplage: (a)unidirectionnel, (b) bidirectionnel.

Définition3.1 : la synchronisation peut être décrite par la définition suivante :

Considérons les deux systèmes

$$\begin{cases} \dot{x} = f_1(x) \\ \dot{y} = f_2(y) \end{cases} \tag{3.1}$$

Avec $x, y \in R^n$, $f_1 et f_2$ deux fonctions non linéaires définies de $R^n \to R^n$. Les deux systèmes sont dites synchronisés si :

$$\lim_{t\to\infty} \|y(t) - x(t)\| = 0 \tag{3.2}$$

Où $y(t) - x(t)$ représente l'erreur de synchronisation pour toutes conditions initiales $x(0)$ et $y(0)$.

3.2.2 Types de synchronisation

Il y'a plusieurs types de synchronisations proposées dans la littérature tels que la synchronisation par le couplage unidirectionnel, la synchronisation par le couplage bidirectionnel, la synchronisation identique *Pecora* et *Caroll* [57-58] et la synchronisation à l'aide d'un observateur [59].

3.2.2.1 La synchronisation à l'aide d'un observateur

La synchronisation unidirectionnelle de deux systèmes chaotiques peuvent être considérer comme un problème d'observateur non linéaire, où l'utilisation des observateurs est proposée pour estimer les états inconnus d'un système qui ne sont pas mesurable directement. Plusieurs types d'observateurs ont été rapportés dans littérateurs, observateur adaptatif [60], observateur à mode glissant [61]. La Fig.3.2 illustre ce principe de synchronisation.

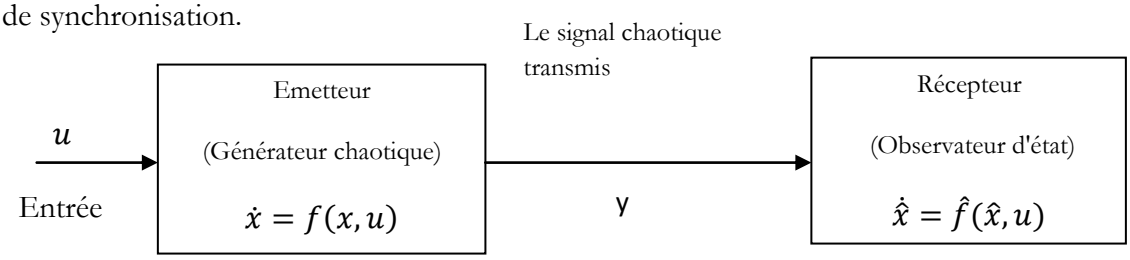


Fig.3.2-Principe de synchronisation à l'aide d'observateur.

Pour ce principe, nous disons que l'émetteur et le récepteur se synchronisent si le système observateur $\dot{\hat{x}} = \hat{f}(\hat{x},u)$ converge vers le système $\dot{x} = f(x,u)$, le probleme de synchronisation revient à déterminer une fonction $\hat{f}$ telle que :

$$\lim_{t\to\infty} \|x(t) - \hat{x}(t)\| = 0 \tag{3.3}$$

3.2.2.2 La synchronisation identique

La synchronisation identique basée sur la propriété d'accouplement de deux systèmes ou plus. La synchronisation identique développée sur la base de circuit chaotique couplé. Pour illustrer la méthode de synchronisation par couplage entre deux systèmes chaotiques on a choisi de présenter, la synchronisation identique proposée par *Pecora* et *Carroll*

3.2.2.3 La synchronisation identique Pecora et Carroll

Cette synchronisation est basée sur la notion de "Maître-Esclave". Un signal Esclave a pour but de reproduire fidèlement le signal Maître. Le système "Maître" est aussi appelé émetteur et le système "Esclave" est dit récepteur. La Fig.3.3suivante représente le processus de décomposition en sous-systèmes :

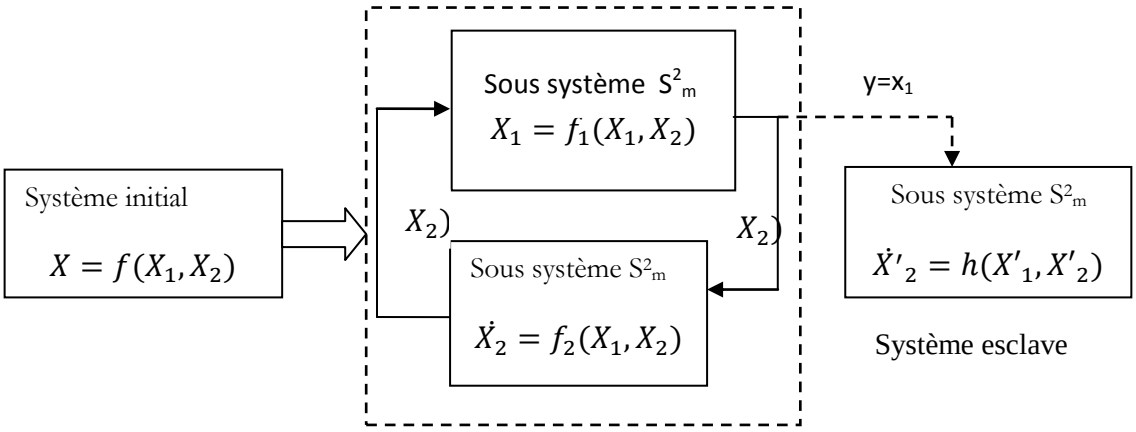


Fig.3.3- Structure de synchronisation par décomposition en sous-système.

Supposons qu'on a un système chaotique identique de dimension n $\dot{X}(t) = f(X(t))$ est décomposé en deux sous-systèmes $X = f(X_1, X_2)$ tel que

$$\begin{cases} \dot{X}_1 = f_1(X_1, X_2) \\ \dot{X}_2 = f_2(X_1, X_2) \end{cases} \quad (3.4)$$

De dimension (m et k) respectivement avec n=m+k.

En suite *Pecora* et *Carrol* ont dérivé de ce système un sous système X'_2 identique au sous-système X, tel que$\dot{X}'_2 = h(X_1, X'_2)$.

On aura donc la configuration de *Pecora* et *Carrol* pour la synchronisation identique du chaos.

$$\left.\begin{matrix} \dot{X}_1 = f_1(X_1, X_2) \\ \dot{X}_2 = f_2(X_1, X_2) \end{matrix}\right\} \text{ système maitre} \quad (3.5)$$

$$\left\{\dot{X}'_2 = f_2(X_1, X'_2)\right\} \text{ système esclave} \quad (3.6)$$

On remarque que l'accouplement entre les systèmes se produit par la variable X_1 du système maitre (3.4), qui est substituée à son analogue X'_1dans le sous système (3.6). Ainsi la synchronisation de deux sorties X_2et X'_2implique :

$$\Delta X_2 = \lim_{t\to\infty} \|X'_2 - X_2\| \to 0 \tag{3.7}$$

La vérification de ce résultat se fait comme suite :

$$\Delta X_2 = X'_2 - X_2 \to \Delta \dot{X}_2 = f_2(X_1, X'_2) - f_2(X_1, X_2) \tag{3.8}$$

Qui est égal à

$$D_{X_2} f_2(X_1, X_2) \times \Delta X_2 \tag{3.9}$$

Où

$$D_{X_2} f = \frac{\partial f_2}{\partial X_2}\Big|_{\overrightarrow{X_2}=\overrightarrow{X_2}(t)} \tag{3.10}$$

Le matrice Jacobien du sous system X_2

On déduit que l'étude de la convergence de ΔX_2 vers zéros revient à l'étude des exposants de Lyapunov du sous système X_2. En conséquence Pecora et Carrol ont énoncé le théorème suivant :

Théorème.3.1 :

Les systèmes maîtres et esclave ont synchronisés si et seulement si tous les exposants de Lyapunov du système esclave, appelés les exposants de Lyapunov conditionnels sont négatifs.

Le problème dans le principe de *Pecora Carroll* est de trouver une décomposition convenable. La réalisation de sous-système esclave dans le récepteur, dupliquer d'un sous-système du système maître de l'émetteur ne semble pas très facile à mettre en pratique à cause des disparités des paramètres, ces contraintes ont poussé les chercheurs à trouver d'autres méthodes qui cassent relativement les limites posées dans le cas de synchronisation identique. Par conséquent, l'estimation des paramètres pour les systèmes chaotiques est devenue un problème majeur de la dernière décennie, certaine études se sont concentrées sur les méthodes basées sur la synchronisation pour l'estimation des paramètres [62-66].

3.3 Les algorithmes méta-heuristiques

Le problème de synchronisation des deux systèmes chaotiques est considéré comme un problème d'optimisation. Le problème d'optimisation se définit comme la recherche du minimum ou du maximum (de optimum) d'une fonction donnée. On peut aussi trouver des problèmes d'optimisation pour lesquels les variables de la fonction sont contraintes à évoluer dans une certaine partie de l'espace de recherche [67].

3.3.1 La fonction d'objective

Un problème d'optimisation est un problème à partir duquel on peut définir une ou plusieurs fonctions objectives permettent la différenciation d'une bonne solution une mauvaise. Concrètement, ces fonctions objectives parcourent l'ensemble des solutions possibles de l'espace de recherche locale et sont à chaque itération, comparées à des optimums précédemment définis. Leur égalité (ou presque égalité dans le cas d'une garantie de performance) conduit alors à l'état final, ou à la solution.

En première approximation, on peut dire qu'une méthode déterministe est adaptée à un espace de recherche petit et complexe et qu'un espace de recherche plus vaste nécessite plutôt une méthode de recherche stochastique.

En pratique, l'objective ne pas obtenir un optimum absolu, mais seulement une bonne solution et la garantie de l'inexistence d'une solution sensiblement meilleure. Pour atteindre cet objectif au bout d'un temps de calcul raisonnable, il est nécessaire d'avoir consulté les recours à des méthodes appelées "heuristique". La plupart entre elle sont conçues spécifiquement pour un type de problème donné. D'autres, au contraire, désormais appelées "méta-heuristique", sont capable de s'adapter à différents types de problèmes. Lorsqu'une seule valeur est associée à une seule fonction objective, on parle de problème mono-objectif. Dans cette partie, nous allons donc décrire brièvement les Algorithmes (*AG*), et (*PSO*).

3.3.2 Les algorithmes génétiques

Les algorithmes génétiques sont des algorithmes d'optimisation s'appuyant sur des techniques dérivées de la génétique et d'évolution naturelle. Les algorithmes génétiques ont déjà une histoire relativement ancienne, les premiers travaux ont été mènes par Holland en 1975, puis approfondis par Goldberg en 1989.

Les algorithmes génétiques manipulent des populations (ou chromosomes) qui représentent des points de l'espace de recherche et les font évoluer au d'opérations stochastiques comme la sélection, le croisement et la mutation.

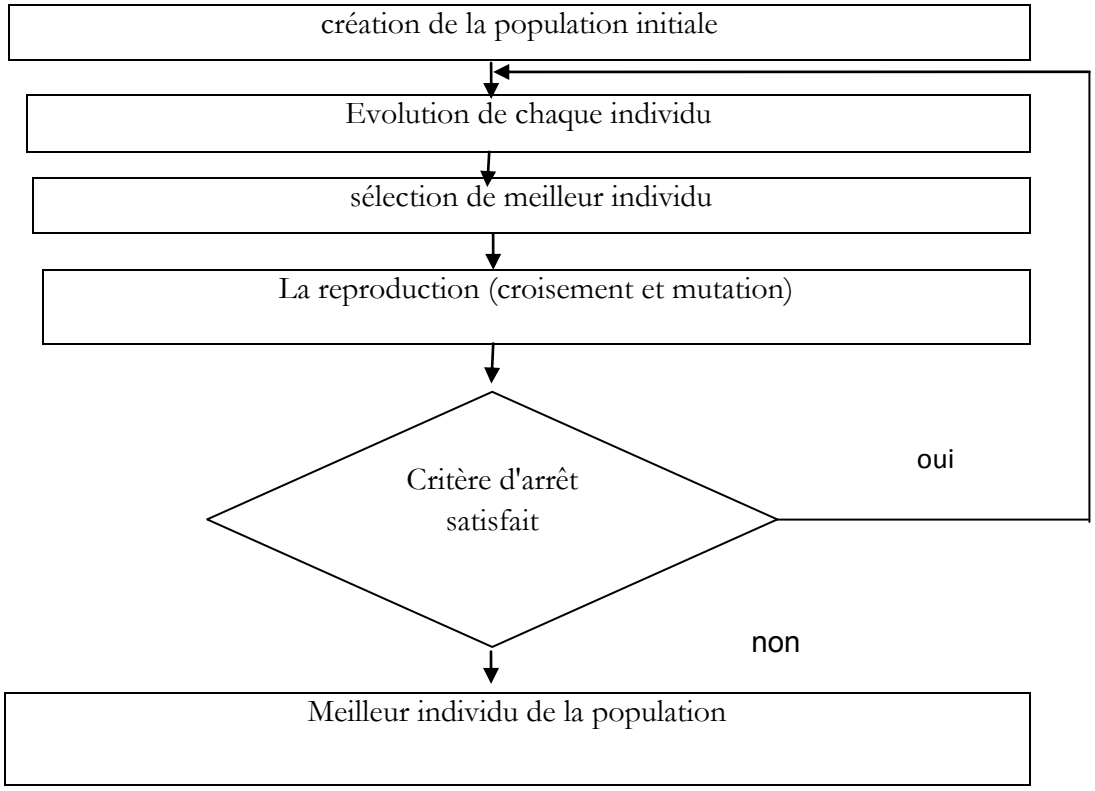


Fig.3.4. Principe de l'algorithme génétique

3.3.3 L'optimisation par Essaim Particules *PSO* :

L'algorithme d'optimisation par Essaims Particulaires(OEP) ou Particule Swarm Optimisation (*PSO*), selon la thermologie anglaise, a été proposé en 1995 par James Kennedy et Russel Eberhart [68], [69]. Il s'inspire à l'origine du monde du vivant, plus précisément du comportement social des animaux évoluant en essaim, tels que les bancs de poissons et les vols groupés d'oiseaux.

Le *PSO* optimise une fonction objective en réalisant une recherche basée sur la population. La population est composée de solution potentielles, appelées particules, initialisées aléatoirement et voler librement dans l'espace de recherche multidimensionnel.

Pendant le vol, les particules changent leurs propres positions et vitesse en fonction de leurs propres expériences où le cout de la fonction est optimal. Finalement toutes les particules se rassembleront autour de la solution optimale globale.

1. Initialiser La population de particules avec des positions et vitesses aléatoires

2. Evaluer Les positions des particules

3. Pour Chaque particule $i, \vec{P}_{besti} = \vec{x}_i$

4. Calculer $\vec{G}_{best}$

5. Tant que Le critère d'arrêt n'est pas satisfaire **faire**

> **6. Déplacer** Les particules
>
> **7. Evaluer** Les positions des particules
>
> **8. Mettre à jour** $\vec{P}_{besti}$ et $\vec{G}_{best}$

9. Fin

(a) (b)

Fig.3.5 Un problème multi objectif : a)-oiseaux, b)-poissons

3.4 Estimation du paramétrés

Le comportement dynamique inhérent des systèmes chaotiques, étant sensible à la fois aux conditions initiales et aux paramètres du système, rend difficile le processus d'estimation des paramètres à l'aide des méthodes d'optimisation traditionnelle. De plus l'existence de plusieurs optima locaux rendent impératif l'utilisation de méthodes qui peut atteindre une solution optima globale. Les *PSO* et se sont les deux méthodes heuristiques qui sont avérés appropriées pour trouver un optimum même en présence de multiples optimums locaux.

Soit le système dynamique de dimension n et des paramétrés m :

$$\dot{x} = f(x, x_0, \theta) \tag{3.11}$$

Avec

$x \in R^n$est le vecteur d'état de n dimension, x_0 l'état initial et $\theta \in R^m$ est le vecteur de dimension m des paramètres du système. Pour estimer les paramètres du système suivant :

$$\widehat{\dot{x}} = f(\hat{x}, x_0, \hat{\theta}) \tag{3.12}$$

Où

$\hat{x} \in R^n$est le vecteur d'estimation d'état de n dimension, x_0 l'état initial et $\hat{\theta} \in R^m$ est le vecteur de dimension m de l'estimation du paramètre du système.

Les vecteurs des erreurs pour N pas de temps entre le vecteur d'état observable de système (3.11) et le vecteur d'état du système (3.12) avec les paramètres estimés sont utilisés pour créer une fonction d'objectif J représentant la moyenne quadratique de l'erreur de synchronisation entre le système et le modèle.

$$J = \frac{1}{M}\sum_{K=1}^{M}\|x_k - \hat{x}_k\|^2 \tag{3.13}$$

Où M est le nombre des états.

x_kSont d'états du système Maitre.

Et $\hat{x}_k$ l'état du système Esclave.

L'estimation des paramètres peut être formulée comme un multidimensionnel problème d'optimisation non linéaire pour minimiser la fonction d'objective J pour le vecteur de décision de paramètre θ le schéma général est illustré par la figure Fig.3.6

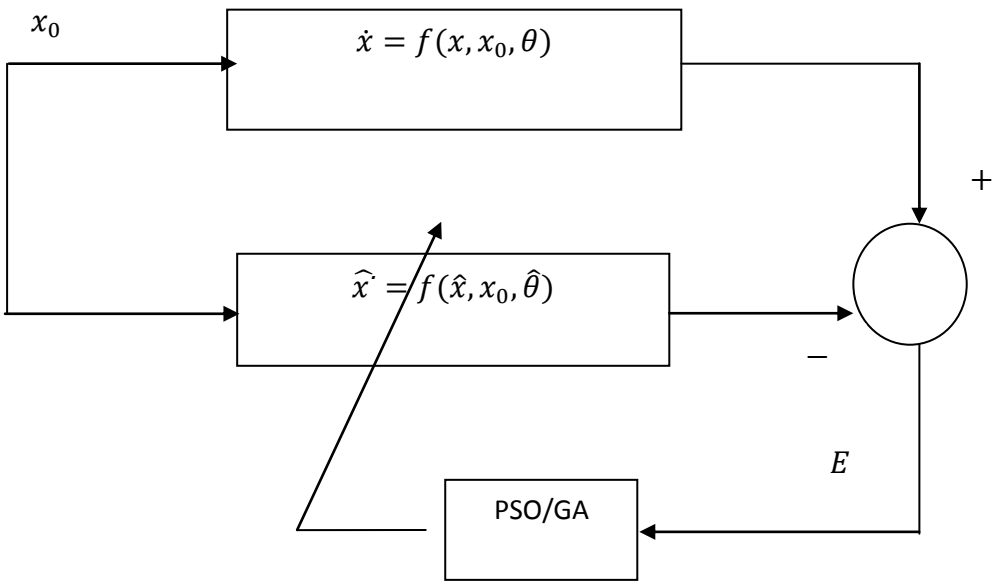


Fig.3.6. Schéma général d'estimation des paramètres dans les systèmes chaotiques.

3.5 Conclusion

Dans la première partie de ce chapitre nous avons présenté les principales méthodes de synchronisation, puis nous avons expliqué le principe de la méthode de synchronisation identique par *Pecora* et *Carroll*. La technique de synchronisation présentée par *Pecora* et *Carroll* souffre d'une forte sensibilité aux variations de paramètres. Afin d'obtenir une synchronisation parfaite entre le système maître et le système esclave. Il reste à trouver les paramètres de contrôle appropriés, c'est ce que nous allons faire en appliquant les algorithmes d'optimisation que nous les avons évoqués précédemment.

Chapitre 4

Les méthodes proposées pour la transmission sécurisé d'un audio numérique

4.1 Introduction

Nous allons présenter un projet de système de communication à haute sécurité utilisant deux niveaux de cryptage basés sur des systèmes chaotiques. Le premier niveau est le masquage chaotique tandis que le deuxième niveau est le brouillage chaotique. Le modèle du système proposé est illustré à la Fig.4.1.

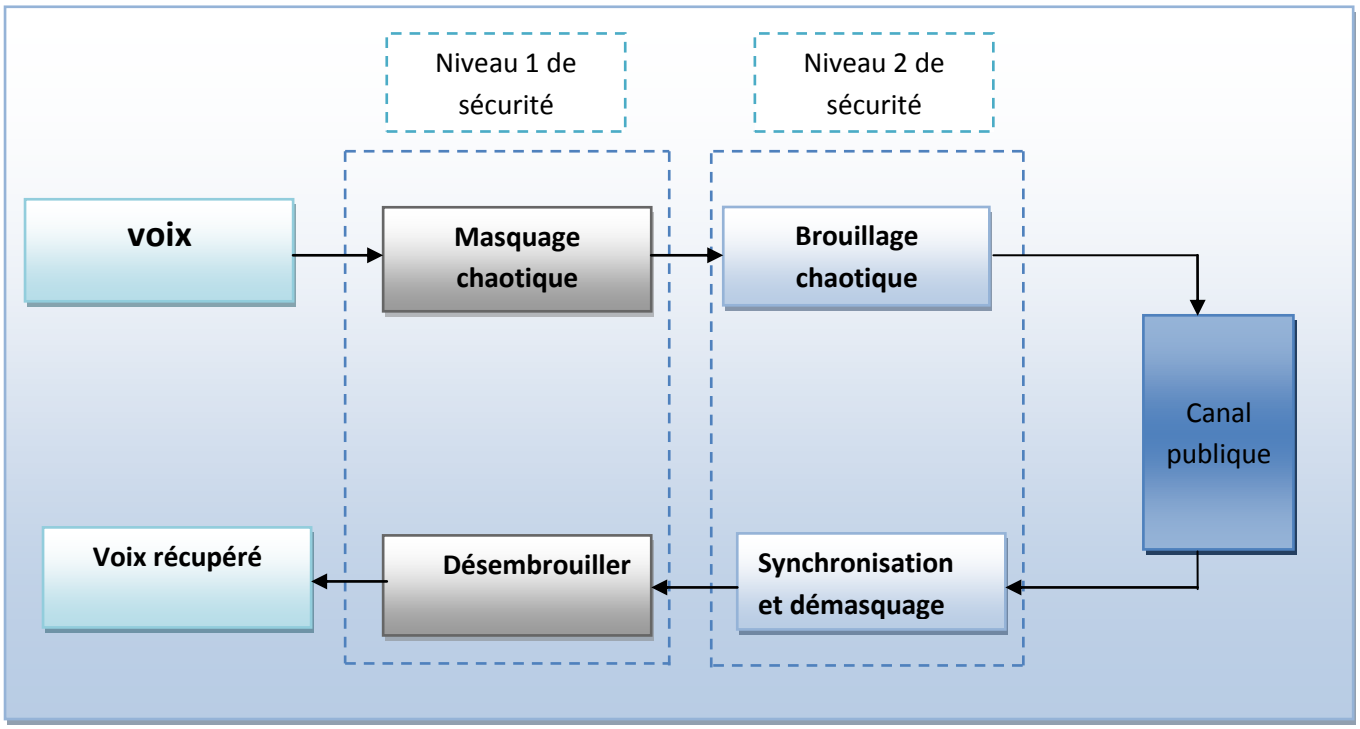


Fig.4.1 Schéma fonctionnel du système de cryptage proposé.

4.2 Les méthodes de cryptage

Au niveau de masquage, on va choisir deux générateurs chaotiques : Le premier générateur chaotique est une hybridation entre la *logistique map* et *tent map*, tandis que le deuxième générateur est le système du *Chua*.

4.2.1 Le masquage dans un générateur chaotique : hybridation entre la *logistique map* et *tent map*

4.2.1.1 Etude de l'émetteur

Dans cette méthode, nous présentons un nouveau schéma de cryptage pour améliorer la sécurité des informations vocales dans les systèmes de communication. Nous construisons une hybridation de trois approches au niveau de l'émetteur :

- Les cartes chaotique : *Logistique map* (1.1), *Tant map* (1.2) pour générer un vecteur arbitraire par certaines valeurs principalement initiées à être joindre le signal vocal d'origine.
- Une image de filigrane (*watermarking*) est intégrée dans le signal crypté afin de vérifier, l'audio filigrané est combiné avec le signal chaotique à l'aide d'une clé chaotique pour générer un fichier pendant le processus de décryptage. Le signal crypté doit être authentique et ne pas subir d'attaques à la fin.
- La troisième approche utilise une clé de brouillage par la carte d'Arnold (1.3) est utilisée pour diffuser des échantillons de signal au moyen d'une clé secrète, la récupération du signal original des échantillons n'est pas possible sans cette clé. Voir les figures Fig.4.2.

Le processus de cryptage commençant par la lecture d'un signal vocale stocké dans le disque dur à l'aide d'une fonction Matlab, où Matlab recommande de représenter le fichier vocal dans la plage [-1 ,1], et puis lisez également le fichier de filigrane*(Watermark)*. Ensuite, les étapes sont les suivantes :

1- Dans cette étape, l'utilisateur saisit une clé (clé 1) pour intégrer le filigrane en toute sécurité dans le signal de parole d'origine. Le schéma considéré pour intégrer le filigrane est représenté dans [70]. Dans cette méthode, ils ont intégrés le filigrane (*Watermark*) dans le domaine DCT et DWT et ont utilisés un-sous-échantillonnage technique. Cette méthode offre le contrôle de l'encastrement du côté transparence et robustesse du filigrane avec une valeur de décalage (Δ). Cette étape produit un signal de parole marqué par un des informations secrètes (*Watermark)* nommées Wtr_Sp.

2- La carte *logistique map* (1.1) et la carte de la*tent map* (1.2) créent deux signaux chaotiques, en fonction des valeurs initiales saisies par l'utilisateur, ces signaux chaotiques sont générés et nommés Lg_S et Tn_S, respectivement.

3- On utilisant les formules ci-dessous, les trois signaux Lg_S,Tn_S et Wtr_Sp sont mélangés pour produire un nouveau signal nommé Mx_Sg :

$$\begin{cases} Mx\_Sg_i = Tn\_S_i \times Wt\_Sp_i + (1 - Tn\_S_i)Lg\_S_i) - 1; & Wt\_Sp_i \geq 0 \\ Mx\_Sg_i = Tn\_S_i \times Wt\_Sp_i + (1 - Tn\_S_i)Lg\_S_i) + 1; & Wt\_Sp_i < 0 \end{cases} \quad (4.1)$$

Ou i: représente l'index des échantillons.

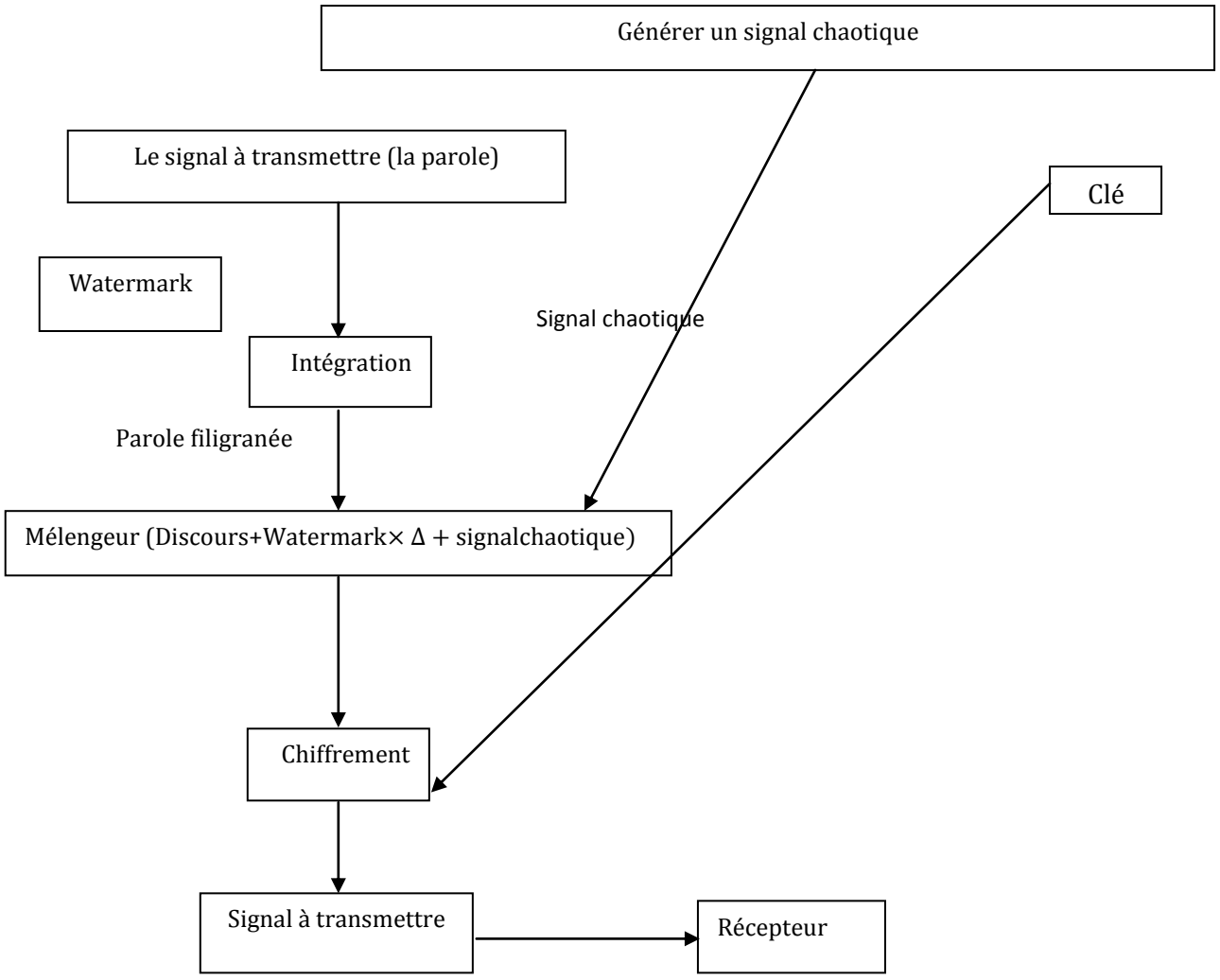


Fig.4.2.Organigramme du schéma de cryptage

4- Décomposer le Mx_Sg en segments, où chaque longueur de segments est un nombre carré.
5- Avant d'appliquer la transformation d'Arnold, chaque segment est remodelé en matrice 2D (N ×N éléments).
6- L'utilisateur insère une autre clé (clé 2), puis le processus de cryptage utilise cette clé sur chaque matrice pour brouiller ses éléments avec la transformation d'Arnold.
7- Transformez chaque matrice brouillée en un vecteur 1D de longueur N2.
8- Pour obtenir le signal vocal crypté final, le processus de cryptage collecte le segment avec d'une autre.

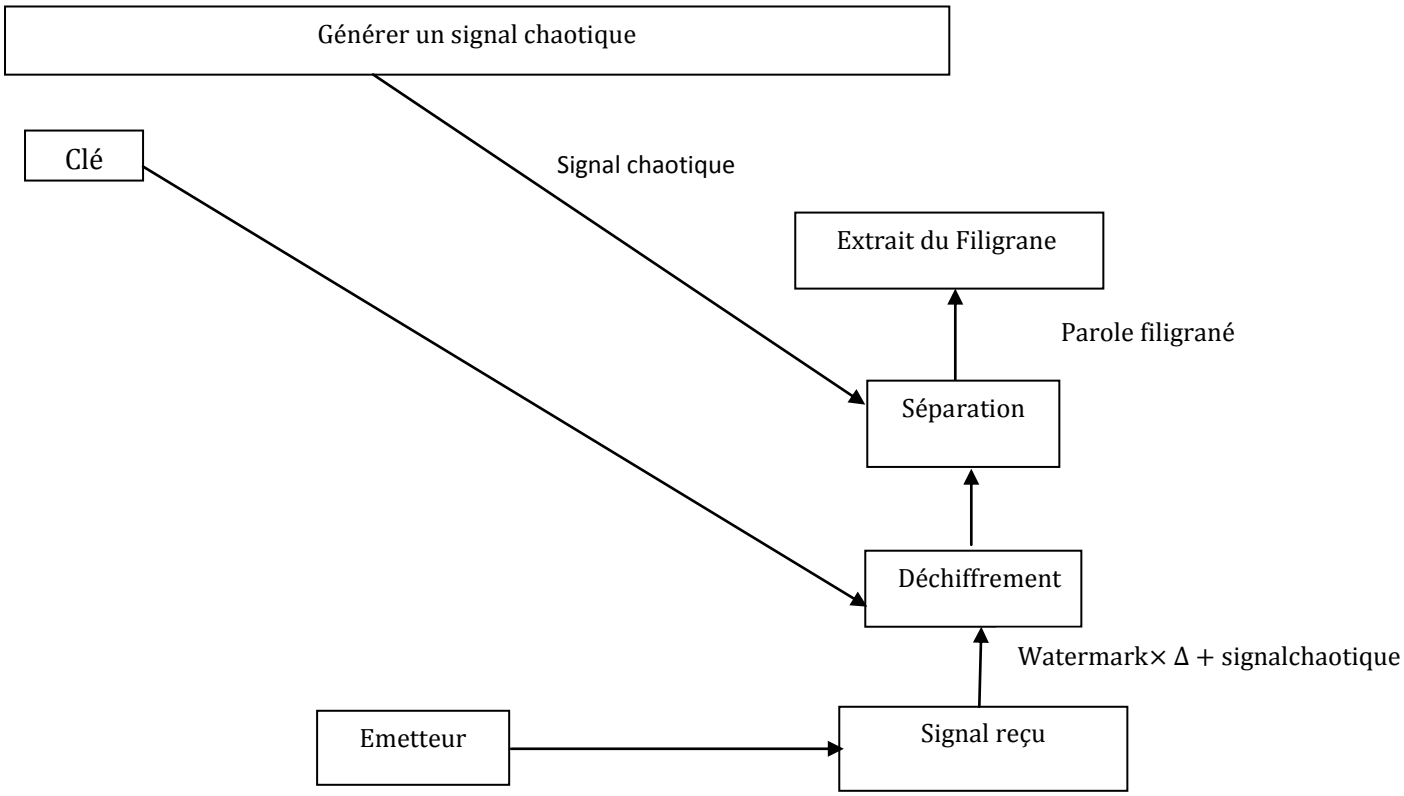


Fig.4.3.Organigramme du schéma de décryptage

4.2.1.2 Etude le récepteur

Le récepteur est utilisé pour récupérer le message (signal vocal). En utilisant la clé chaotique précédente, le signal reçu est décrypté en suppression le même signal chaotique généré du côté de l'émetteur. Nous faisons extraire le filigrane du signal déchiffré et vérifier le signal obtenu avec l'original pour assurer son originalité sans dégradation, voir la Fig.4.3 :

1- Les étapes 4 et 5 du processus de cryptage sont appliquées au signal vocal crypté

2- La transformée d'Arnold inverse est appliquée sur chaque matrice 2D en utilisant la même clé (clé 2) employé auparavant.

3-Ré-modeler chaque matrice récupérer en vecteur 1D de longueur N2.

4-Collectez les segments récupérés les uns avec les autres pour produire $Mx\_Sg_i{}'$.

5- La même deuxième étape du processus de cryptage est appliquée sans modifier la valeur initiale.

6-La séparation des échantillons de signaux vocaux déchiffrés est réalisée en respectant les éléments suivants :

$$\begin{cases} Wtr\_Sp_i' = \dfrac{Mx\_Sg_i' + 1 - (1 - Tn\_S_i)Lg\_S_i)}{Tn\_S_i} Mx\_Sg_i < 0 \\ Wtr\_Sp_i' = \dfrac{Mx\_Sg_i' - 1 + (1 - Tn\_S_i)Lg\_S_i)}{Tn\_S_i} Mx\_Sg_i \geq 0 \end{cases} \quad (4.2)$$

Ou:Wtr_Sp_i' est le signal de parole déchiffré et Mx_Sg_i' résultat de la quatrième étape.

Jusqu'à cette étape, le signal vocal est déchiffré, mais pas confirmé. Pour vérifier le signal vocal est sûr, envoyé du côté de l'authentification, le processus de décryptage est maintenu avec ces étapes :

7-Extraire le filigrane (*Watermark*) continue dans le signal vocal crypté en utilisant la même clé (clé1) dans le processus d'extraction donné dans [70].

8-L'authentification du signal vocal déchiffré est contrôlée par la vérification de la similitude entre le filigrane extrait et le filigrane d'origine. Donc, plus de similitude entre les deux moyens vocaux déchiffrés plus authentifié.

4.2.2 Le masquage par un système chaotique du *Chua*

Dans cette partie, on va présenter une proposition d'un système de communication à haute sécurité en utilisant deux niveaux de cryptage basés sur des systèmes chaotiques de dimensions supérieures (HD). A côté de l'émetteur, le premier niveau est un masquage chaotique en utilisant le système chaotique du *Chua*, tandis que le deuxième niveau est un brouillage de l'audio crypté par un *Alrond map*. Au niveau du récepteur, le masquage est retiré à l'aide d'une version de synchronisation *Pecora Carroll* du système de chaotique.

4.2.2.1 Etude l'émetteur

L'émetteur est constitué de système chaotique en temps continu de circuit de *Chua* (1.4) suivante :

$$\begin{cases} \dot{x_1} = \alpha(x_2 - x_1 - f(x_1)) \\ \dot{x_2} = x_1 - x_2 + x_3 \\ \dot{x_3} = -\beta(x_2 - x_3) \end{cases} \quad (4.3)$$

Pour masquer le signal audio original après avoir accédé aux conditions initiales et les paramètres du système du *Chua* respectivement:$x_1(0) = 1\,, x_2(0) = 0.5\,, x_3(0) = -1$ et $\alpha = 15.7$et $\beta = 28$, qui sont considérés comme une clé de cryptage (clé1), la Fig.4.5 représente le modèle du masquage chaotique. Les détails de l'algorithme de masquage chaotique et de brouillage sont donnés dans ce qui suit :

1- Le signal audio $m(t)$est ajouté à un signal de commande de générateur chaotique de chua pour obtenir un signal audio crypté $s(t)$.
2- Le signal audio crypté est divisé en trames avec longueur connue, chaque trames est divisée en sous trames (segments).
3- Avant d'appliquer la transformation d'Arnold, chaque segments est remodelé en matrice 2-D (N×N) éléments.
4- Après l'insertion d'une autre clé (clé 2), le processus utilise cette clé sur chaque matrice pour brouiller ces éléments avec l'extension de l'algorithme d'Arnold.
5- Transformez chaque matrice brouillée en un vecteur 1D de longueur N2.
6- Pour obtenir le signal vocal crypté final, le processus de cryptage collecte le sagement avec d'une autre.

Pour récupérer le signal audio crypté nous allons faire la synchronisation entre l'émetteur et le récepteur, en utilisant la synchronisation *Pecora* et *Carroll*.

4.2.2.2 La synchronisation Pecora et Carroll deux système chaotique du Chua

Nous faisons intervenir le circuit de la Fig.1.6 en tant qu'émetteur, et cela après l'ajustement de la valeur R afin d'obtenir le régime chaotique, et celui de la Fig.4.4 en tant que récepteur. Nous ajustons la commande du paramètre de récepteur R pour obtenir également le régime chaotique. Les deux circuits sont alors capables de travailler dans leur mode chaotique (double roulement). Le couplage est réalisé entre les deux circuits par l'intermédiaire de la tension électrique V_{C_1}de l'émetteur. Ce signal provenant de l'émetteur passe dans un amplificateur opérationnel suiveur avant d'être utilisé pour réaliser le couplage avec le récepteur $r(t)$.

Le récepteur est divisé en deux sous-systèmes clairement indiqués sur la Fig.4.4. Ces deux sous-systèmes sont reliés entre eux par un amplificateur opérationnel suiveur pour découpler les deux sous-systèmes. Le premier sous-système comprend la capacité C_2, la résistance R, et l'inductance L. Le deuxième est formé de la résistance R, la capacité C_1 et la résistance de *Chua* N_R.

Le comportement du premier sous-système RL du récepteur est donné par le système d'équations suivant :

$$\begin{cases} C_2 \dfrac{dV_2}{dt} = \dfrac{1}{R}(r(t) - i_L) \\ \mathrm{L}\dfrac{di_L}{dt} = -V_2 \end{cases} \tag{4.4}$$

La tension V_1 pilote le deuxième sous-système RC. Son comportement est donné par l'équation suivante :

$$C_1 \frac{dV_1}{dt} = \frac{1}{R}(V_2 - V_1) - f(V_2) \tag{4.5}$$

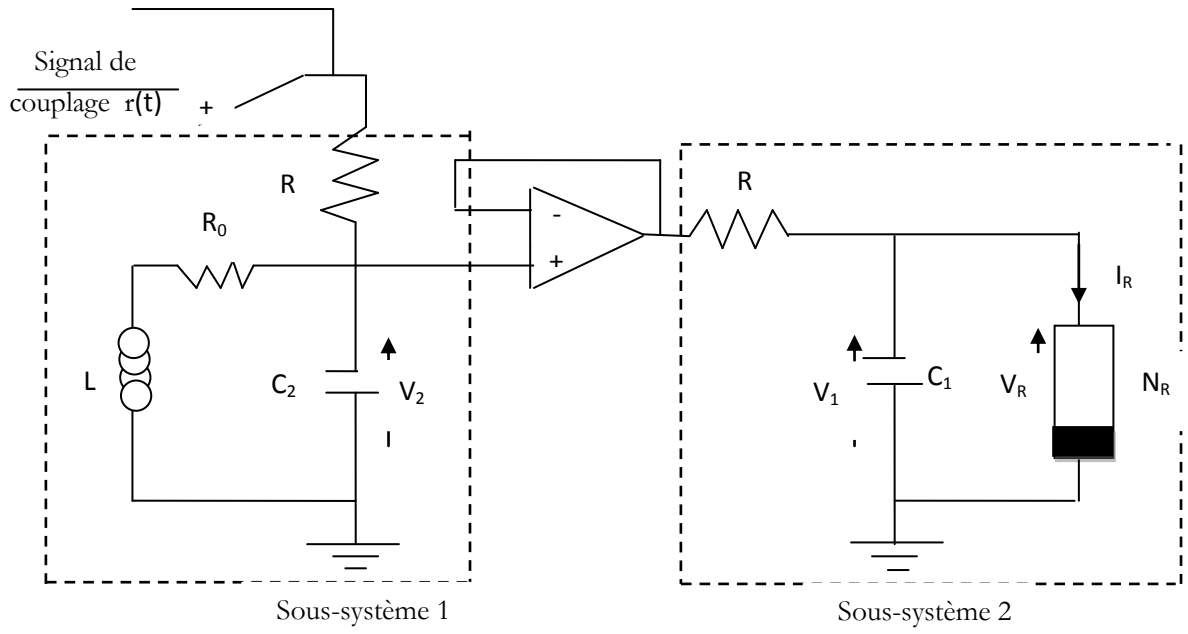


Fig.4.4 Récepteur de Chua décomposé en sous-système.

Lorsque les valeurs des composants électronique de la résistance de Chua sont les mêmes, nous observons un phénomène de synchronisation entre l'émetteur et le récepteur. En effet, la tension V_1 de récepteur se synchronise avec la tension V_1 de l'émetteur. Elles présentent les mêmes variations temporelles.

4.2.2.3 Etude de récepteur

Le récepteur est un système identique à l'émetteur en plus d'un simple soustracteur pour réussir à retirer le masquage chaotique, d'après le schéma de synchronisation de *Pecora* et *Carroll* comme a été expliqué précédent. Ce schéma est basé sur l'envoi d'un signal de conduite X_m, qui est une simple addition entre le signal de sortie de l'émetteur $y(t)$ et le message$m(t)$. Le signal s(t) est transmis au récepteur à travers le canal de transmission, supposant qu'uniquement ce canal est idéal, voir la Fig.4.5.

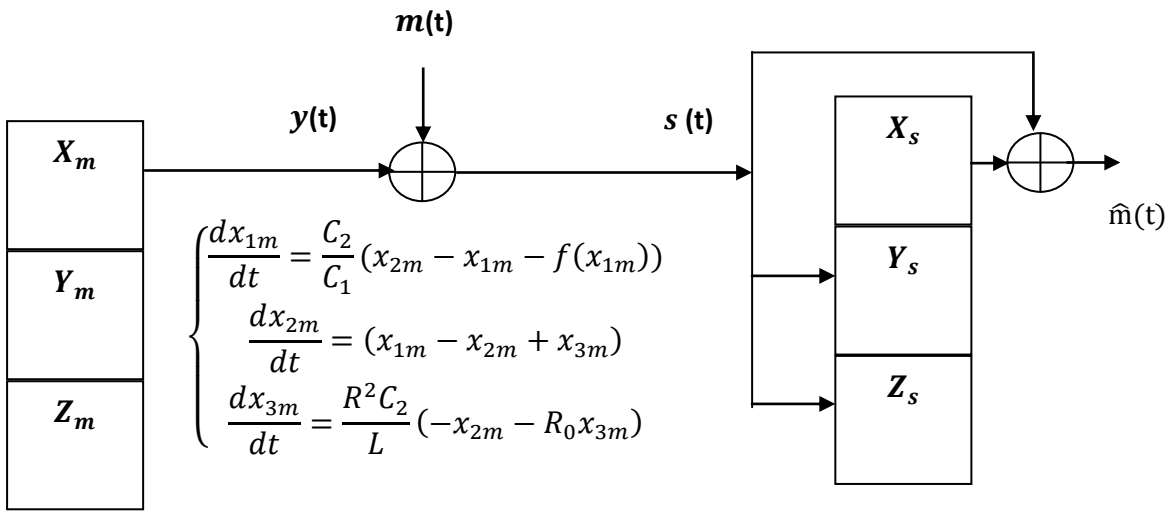


Fig.4.5 Masquage chaotique et démasquage du système *Chua*.

4.2.2.4 Le signal de commande pour la synchronisation

Soit le système Maitre du *Chua* suivant :

$$\begin{cases} \frac{dx_{1m}}{dt} = \alpha(x_{2m} - x_{1m} - f(x_{1m})) \\ \frac{dx_{2m}}{dt} = (x_{1m} - x_{2m} + x_{3m}) \\ \frac{dx_{3m}}{dt} = \beta(-x_{2m} - R_0 x_{3m}) \end{cases} \quad (4.6)$$

Pour le choix du sous-système esclave trois configurations de deux variables sont possibles

$$\begin{cases} \frac{dx_{1s}}{dt} = \alpha\left(x_{2s} - x_{1s} - f(x_{1s})\right) \\ \frac{dx_{2s}}{dt} = (x_{1s} - x_{2s} + x_{3s}) \end{cases} \quad (4.7)$$

configuration (x_{1m},x_{2m}) avec x_{3m} entrée d'accouplement

$$\begin{cases} \frac{dx_{1s}}{dt} = \alpha\left(x_{2s} - x_{1s} - f(x_{1s})\right) \\ \frac{dx_{3s}}{dt} = \beta(-x_{2s} - R_0 x_{3m}) \end{cases} \quad (4.8)$$

configuration (x_{1m},x_{3m}) avec x_{2m}entrée d'accouplement

$$\begin{cases} \frac{dx_{2s}}{dt} = (x_{1s} - x_{2m} + x_{3s}) \\ \frac{dx_{3s}}{dt} = \beta(-x_{2m} - R_0 x_{3s}) \end{cases} \quad (4.9)$$

Configuration (x_{2m},x_{3m}) avec x_{1m} entrée d'accouplement

Dans notre travail on propose le système Maître (4.6) avec le système esclave (4.9) comme le montre la figure Fig.4.6.

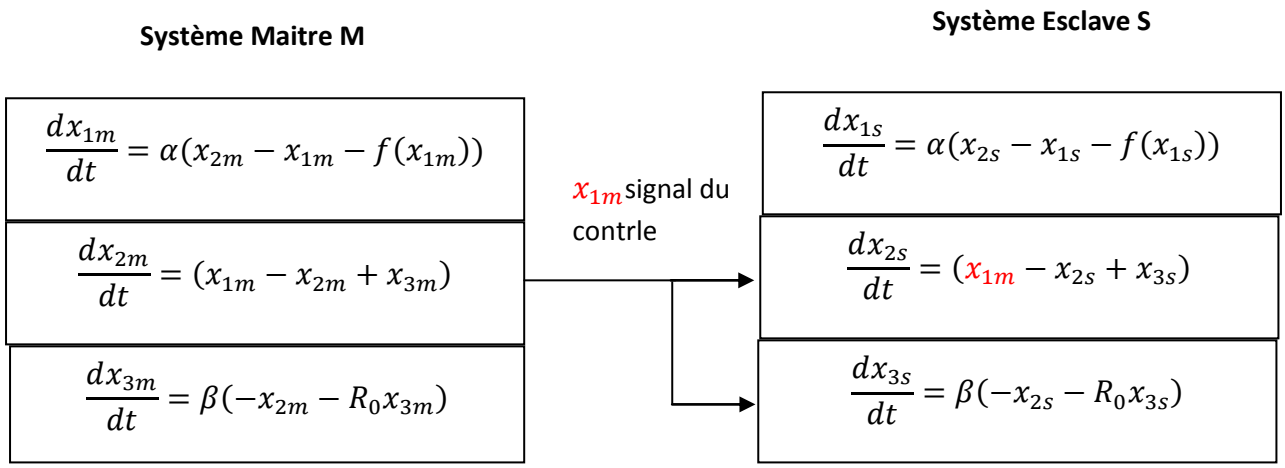


Fig.4.6. Méthode de synchronisation par *Pecora et Caroll*.

Pour ce faire, un ensemble de vecteurs appelés les vecteurs des erreurs d'état, représentant la différence entre l'état maitre et esclave est définit.

Les états d'erreurs e_{x1}, e_{x2} et e_{x3} sont donnés par

$$\begin{aligned} e_{x1} &= x_{1m} - x_{1s} \\ e_{x2} &= x_{2m} - x_{2s} \\ e_{x3} &= x_{3m} - x_{3s} \end{aligned} \tag{4.10}$$

La soustraction du système maître du système esclave donne :

$$\begin{aligned} \dot{e_{x1}} &= \dot{x_{1m}} - \dot{x_{1s}} \\ &= (\alpha(x_{2m} - x_{1m} - f(x_{1m}))) - (\alpha(x_{2s} - x_{1s} - f(x_{1s}))) \\ &= \alpha(x_{2m} - x_{2s} - f(x_{1s})) - (x_{1m} - x_{1s}) - f(x_{1m})) \\ &= \alpha(e_{x2} - e_{x1}) \end{aligned} \tag{4.11}$$

Et on obtient aussi :

$$\dot{e_{x2}} = e_{x1} - e_{x3} \tag{4.12}$$

$$\dot{e_{x3}} = -\beta(e_{x1} + R_0 e_{x3}) \tag{4.13}$$

Qui peut être décrit sous la forme :

$$\dot{e} = A(t)e \tag{4.14}$$

On peut montrer que la vérité de complète de synchronisation est globalement asymptotiquement stable à l'origine pour tout choix du signal de commande pour ces conditions.

En considérant :

$$E(e) = 1/2(1/\alpha {e_{x1}}^2 + {e_{x2}}^2 + 1/\beta {e_{x3}}^2) \tag{4.15}$$

$$\begin{aligned} \dot{E}(e) &= (1/\alpha \dot{e_{x1}} e_{x1} + \dot{e_{x2}} e_{x2} + \frac{1}{\beta} \dot{e_{x3}} e_{x3}) \\ &= ((e_{x2} - e_{x1})e_{x1} + (e_{x2} - e_{x3})e_{x2} - (e_{x2} + R_0 e_{x3})e_{x3})) \\ &= -{e_{x1}}^2 + e_{x1} * e_{x2} + e_{x2} * e_{x2} - {e_{x2}}^2 - e_{x3} * e_{x2} - R_0 {e_{x3}}^2 \\ &= -\left(e_{x1} - \frac{1}{2} e_{x2}\right)^2 - \frac{3}{4} {e_{x2}}^2 - R_0 {e_{x3}}^2 \end{aligned} \tag{4.16}$$

Nous savons que $R_0 > 0$, et à partir de là $\dot{E} < 0$, donc et selon la méthode directe de exposant de lyapunov le système est asymptotiquement stable.

Par conséquent, quelque soient les conditions initiales imposées entre les systèmes émetteur et le récepteur, la synchronisation se produit lorsque $t \to \infty$:

$$\lim_{t\to\infty} e_{x1}(t) = \lim_{t\to\infty} e_{x2}(t) = \lim_{t\to\infty} e_{x3}(t) = 0 \qquad (4.17)$$

La récupération de message (audio) dépend selon l'erreur de synchronisation, plus l'erreur de synchronisations est petite, plus la récupération est forte.

De retour à la Fig.4.5, le signal reçu est donné :

$$\boldsymbol{s}(t) = X_m(t) + m(t) \qquad (4.18)$$

et le signal de parole récupéré est :

$$\widehat{m}_{\mathrm{s}}(\mathrm{t}) = \boldsymbol{s}(t) - X_s(t) = [X_m(t) + m(t)] - X_s(t) = e(t) + m(t) \qquad (4.19)$$
$$\widehat{m}_{\mathrm{s}}(\mathrm{t}) = e(t) + m(t)$$

Avec $X_m(t) - X_s(t) = e_{x1}(t)$

L'effet de la présence de signal de l'information pendant la synchronisation au niveau du récepteur est pris en compte [71]. Ameer. K, Jawad et autre ont montré que pour neutraliser cet effet, le signal d'information est renvoyé dans l'émetteur chaotique [17]. Dans d'autres cas l'erreur de synchronisation est causée par les variations des paramètres de l'émetteur et de récepteur car il n'est pas très facile de mettre les deux systèmes similaires.

4.3 Méthodes de la synchronisation de deux systèmes chaotiques à l'aide de l'algorithme d'optimisation méta-heuristique *GA* et *PSO*

Le *GA* et le *PSO* sont proposés dans ce travail pour optimiser les paramètres du système chaotique du *Chua* pour la synchronisation des systèmes chaotiques maître-esclave. Chaque algorithme commence par la création de la population initiale et se termine par la convergence vers le meilleur individu de la population correspondant à la solution du problème d'optimisation, dans ce cas minimisé l'erreur de synchronisation.

La fonction objective est définie par l'équation (3.13). C'est la somme des carrés des erreurs entre le système maître et l'esclave. La synchronisation est atteinte lorsque l'erreur (4.10) converge vers zéros au fur et à mesure que le temps passe à l'infini. Dans ce cas, (*GA*) et (*PSO*) sont utilisé pour optimiser cette erreur.

Nous allons prendre les mêmes systèmes maîtres et esclave, le même principe de synchronisation par *Pecora* et *Carroll* avec les mêmes conditions initiales, avec les jeux de paramètres sélectionnés$\theta = (\alpha, \beta)^T = (15.6,28)^T$ et pour chaque pas de temps il faut sélectionner des paramètres précis. Après cela nous prenons le vecteur d'état comme état initial de l'algorithme d'optimisation (*PSO* et *GA*), nous prenons alors un modèle qui est régi par les mêmes équations et avec un ensemble différent de paramètres $\hat{\theta}$ limité et lié dans la plage des paramètres initiaux. Temps de réponse$x_i(1,3)$ pour les états successifs de 500(N) après que les transitoires initiaux ont été utilisés pour le processus d'estimations des paramètres. Des comparaisons sont présentées pour les trois versions de (*PSO* et *GA*) pour un certains nombres d'exécutions de ces algorithmes. Et après le choix des paramètres de simulation des deux algorithmes (*GA*) et (*PSO*) qui est donné dans la section (Chapitre 4). Dans notre exemple nous avons deux paramètres pour estimer unidimensionnelle des paramètres est considérée, cela signifie que les paramètres sont connus à l'avance avec la valeur d'origine, un des paramètres est inconnu et doit être estimé.

Dans le présent travail, le *PSO* et *GA* ont été utilisés pour estimer les paramètres $\theta = (\alpha, \beta)^T$ dans une plage autour des valeurs réelles des paramètres dans un régime chaotique, les plages de recherche des paramètres sont définies comme suit :

$$14 \leq \alpha \leq 17 \text{ et } 26 \leq \beta \leq 30$$

Pour chaque position de particule (x) consiste en m nombre réels dans la plage correspondante, chaque individu de la population représente la solution possible du problème de la minimisation de la fonction objective J.

Le choix des paramètres de simulation des deux algorithmes (*GA*) et (*PSO*) sont donnés dans le tableau table 4.1.

Nous allons exécuter chaque algorithme 20 fois et notons les résultats obtenus avec la plus petit taille de population, et nous comparons les valeurs des paramètres estimésα et β avec les valeurs réelles en minimisant l'erreur de synchronisation, et nous comparons pour discerner l'algorithme le plus efficace.

Table.4.1. Les paramètres de simulation des algorithmes *GA* et *PSO*.

GA	Longueur des chromosomes	32
	Taille de la population (N)	100
	Nombre des variables (2)	$\alpha et \beta$
	Pc, Pm , M	0.7 , 0.5, 2
PSO	Nombre de particule (n)	100
	Coefficients de l'accélération (C1, C2)	C1=C2=2
	Coefficient de l'inertie (Wf)	0.4

4.4 Evaluation des méthodes proposées dans notre travail :

Dans le processus de cryptage, trois types de test sont effectués pour vérifier les performances des systèmes proposés. Ces tests sont :

- la vérification de la cryptanalyse et la vérification de l'intelligibilité de la parole sécurisée ou tester la qualité de cryptage, ainsi que le contrôle et authentification des filigranes(*Watermark*):

4.4.1 Évaluation de la Méthode de cryptage par les cartes chaotiques (*logistique*, *tent*, *Arnold*)

4.4.1. 1 Cryptanalyse chaotique :

La cryptanalyse vise à trouver d'espace de clé et de la sensibilité

-Espace de clé :

Les clés dans cette méthode sont composées des conditions initiales et des paramètres $(a_0, r), (b_0, u)$ de logistique map et tant map respectivement comme montre le tab 5.2, et la clé de brouillage par *Arnold map*, nous allons calculer l'espace de clé à partir de ces clés.

-Analyse de la sensibilité des clés

Nous avons donc essayé de tester et d'examiner la sensibilité de l'algorithme de chiffrement en changeant une ou plusieurs clés. Cela par le calcul du NSCR et de l'UACI.

4.4.1.2 La vérification de l'inintelligibilité de la parole

C'est un facteur important dans le processus de masquage et le brouillage de la parole.

- Effet de processus de cryptage et décryptage :

Nous allons mesurer les valeurs de SNR et la valeur du coefficient de corrélation dans le cas de cryptage et décryptage.

4.4.1.3 Contrôle et authentification des filigranes (*Watermark*) :

Le but de cette opération renforce davantage la sécurité et la crédibilité et la résistance par certains AWGN qui ajoutent des bruits blancs gaussiens à travers les valeurs de BER.

4.4.2 Évaluation de la Méthode de cryptage par le système chaotique du *Chua* et *Arnold map*

Nous allons évaluer l'efficacité de cette méthode à partir des mêmes coefficients précédents qui ont les valeurs initiales et les paramètres $(\boldsymbol{x_{1m0}}, \boldsymbol{x_{2m0}}, \boldsymbol{x_{3m0}}, \alpha, \beta, K)$

du circuit du *Chua* et *d'Arnold* respectivement.

4.5 Conclusion

Dans ce chapitre, nous avons proposé un nouveau schéma pour la transmission sécurisée d'un signal vocal basé sur les systèmes chaotiques. Le schéma proposé utilise deux niveaux de cryptage basés sur les systèmes chaotiques : le premier niveau est le masquage tandis que le deuxième niveau est le brouillage. Dans le niveau de masquage nous utilisons deux types de systèmes : dans le premier, nous avons masqué l'audio par une hybridation entre les cartes logistiques (*map* et *tent*), tandis que dans la deuxième méthode nous avons masqué le signal audio par le système chaotique du *Chua*. Dans ce dernier cas, le message sera récupéré dans le récepteur après la synchronisation *Pecora* et *Carroll*.

Pour minimiser l'erreur de synchronisation, nous avons estimé les paramètres du système chaotique qui est formulé comme un problème d'optimisation en utilisant les algorithmes d'optimisation méta-heuristiques *PSO* et *GA*. À la fin de ce chapitre, nous avons présenté les coefficients de test de l'efficacité de ces méthodes proposées. Le chapitre suivant sera consacré à la présentation des résultats de simulation.

Chapitre 5

Résultats de simulation

5.1 Introduction

Dans ce chapitre, les performances des méthodes proposées dans le chapitre précédent seront évaluées par des tests expérimentaux à l'aide d'un computer PC avec Windows 7, 32 bits et le logiciel de calcul Matlab-13. Toutes les expériences sont faites en utilisant 20 fichiers vocaux comprenant des voix masculines et féminines avec des périodes différentes. Les échantillons de cette mono voix sont sélectionnés au hasard avec 16 bits pour chaque échantillon. La Table.5.1 montre les signaux vocaux utilisés avec une durée tirés de base de données vocale TIMI avec la détermination du sexe et une image de filigrane (16*16bit) utilisée et donnée en Fig.5.1.

Ce chapitre est subdivisé comme suit : la section (5.2) est consacrée à évaluer des résultats de simulation pour la transmission sécurisée d'un audio numérique qui est masqué et brouillé par des cartes chaotiques ayant les dimensions du *logistique map*, *tent map* et *Alrond map* respectivement. Les résultats de simulation d'un filigrane ajouté au signal audio pendant le processus de cryptage pour tester les avantages de la méthode proposée sont évalués dans la section (5.2.4).Dans la section (5.3) nous évaluons les résultats des simulations de la transmission sécurisée des signaux audio numériques masqués par des systèmes chaotiques à des systèmes multidimensionnels de *Chua* et brouiller par *Arlond map*. Ensuite, dans la section (5.3.1) nous allons présenter quelques résultats des simulations sur les synchronisations des systèmes chaotiques.

Dans la section (5.4) nous allons présenter les résultats des simulations pour optimiser l'erreur de synchronisation après estimation des paramètres du système *Chua* par des algorithmes *GA* et *PSO*. Dans les sections précédentes, nous évaluons le processus de chiffrement par des tests. Enfin, une comparaison des performances du système proposé avec les systèmes de chiffrement classiques existants est illustrée.

5.2 Résultats de simulation de la transmission sécurisée d'un audio numérique crypté par l'intégration des cartes chaotiques

Dans cette section, nous évaluons les résultats de simulation dans le cas d'une transmission sécurisée d'un signal audio numérique par deux niveau de sécurité : le masquage par la multiplication des cartes chaotiques (*logique map* et *tant map*) et le brouillage par la carte chaotique *d'Alrond map*.

Dans la Table.5.2, nous présentons les valeurs initiales des données statiques des deux cartes chaotiques sur laquelle tous les résultats sont obtenus.

Table.5.1.Les signaux vocaux utilisés avec une durée extraite de la célèbre base de données des voix TIMIT

Signal vocale	Durées (seconde)	Sexe (homme et femme)	Signal vocale	Durées (seconde)	Sexe (homme et femme)
SI560	**4.378**	**M**	SI1303	**4.294**	M
SI734	**4.525**	**M**	SI1308	**5.779**	F
SI770	**4.762**	**F**	SI1390	**5.094**	F
SI839	**4.653**	**M**	SI1460	**5.069**	M
SI860	**4.365**	**F**	SI1715	**4.512**	M
SI863	**4.474**	**F**	SI1992	**3.974**	M
SI943	**3.757**	**F**	SI2194	**4.723**	F
SI1103	**6.086**	**M**	SI2303	**4.058**	F
SI1109	**4.544**	**F**	SX29	**7.571**	**M**
SI1217	**5.197**	**M**	SX364	**4.339**	M

Table.5.2 Les valeurs initiales des données statiques des deux cartes chaotiques

Δ	**Logistique map**		**Tant map**		**Max_val**
	a_0	r	b_0	u	
0.002	0.5	3.85	0.5	1.8	1

Fig.5.1.Image utilisée en filigrane.

Pour évaluer le processus de cryptage proposé, nous vérifions les éléments suivants :

5.2.1. Cryptanalyse chaotique :

La cryptanalyse vise à trouver d'espace de clé et de la sensibilité.

5.2.1.1 Espace de clé :

Les clés dans cette méthode sont composées des conditions initiales et des paramètres(a_0, r), (b_0, u) de logistique map et tent map respectivement comme montre le Table.5.1, et la clé de brouillage par Arnold map.

Avec l'omission des cartes *logistique map* et *tent map*, seul le brouillage Arnold peut donner un large espace clé .Nous pouvons conclure que notre crypto système proposé peut résister à une attaque par force brute suffisante pour une pratique fiable employée.

5.2.1.2 Analyse de sensibilité des clés

Le Table.5.3 montre les valeurs des coefficients de corrélation, NSCR et UACI pour tester et examiner la sensibilité des clés (les valeurs initiales (a_0, r) de la carte *logistique map*(b_0, r)de la carte de la *Tent map* et K *d'Arnold*).

D'après les résultats obtenus, nous pouvons conclure que même les changements sur les clés de chiffrements au cours de processus de déchiffrements conduisent à de mauvais résultats de décryptage.

Table.5.3. Sensibilité des Clés des systèmes (*Logistique map*, *Tante map*, *Arlond*).

Nom de discours	**Les clés (a_0, r, b_0, r, k)**	**(3.87, 0.48, 1.82, 0.54, 205)**			**(3.85, 0.5, 1.8, 0.5, 387)**		
		NSCR (%)	**UACI (%)**	**Corr_Coef**	**NSCR (%)**	**UACI (%)**	**Corr_Coef**
SI770	(3.85, 0.5, 1.8, 0.5, 205)	99.9974	19.2024	-0.0921	99.9934	23.3060	0.0041
SI1390		99.9939	19.2098	-0.0767	99.9816	23.3290	-1.2662×10^{-4}
SI863		99.9930	19.2134	-0.0909	98.6923	29.4809	0.0023
SI1715		99.9931	19.1898	-0.0369	99.9848	18.6973	0.0053
SI1217		99.9988	19.2191	-0.0838	99.9964	23.3279	6.8499×10^{-4}

5.2.2 La vérification de l'intelligibilité de la parole

5.2.2.1 La qualité de processus de cryptage :

Le cryptage est considéré comme plus acceptable lorsque la valeur du coefficient de corrélation est proche à zéros. De plus, le processus de cryptage est meilleur lorsque la valeur SNR diminue. À partir des données recueillies dans le tableau Table.5.4, nous observons que les valeurs SNR semblent trop petites et que les valeurs des coefficients de corrélation sont proche à zéros, et deviennent négatives, ce qui montre que le signal crypté est très éloigné du signal vocal original, ce qui indique que les caractéristiques du signal d'origine sont complètent séparées.

Table.5.4.SNR et Coefficient de Corrélation entre les signaux d'origine et crypté.

signav ocale	SNR (origine, encrypté)	Coef_Corr(origine , encrypté)	Signal vocale	SNR (origine, encrypté)	Coef_Corr(origine , encrypté)
SI560	**-29.0691**	**-0.0019**	SI1303	**-35.4358**	**0.0073**
SI734	**-39.5201**	**0.0017**	SI1308	**-35.2122**	**0.0020**
SI770	**-42.6570**	**1.3989×10^{-4}**	SI1390	**-36.4082**	**0.0047**
SI839	**-32.5074**	**0.0038**	SI1460	**-37.8784**	**-5.5553×10^{-4}**
SI860	**-34.9999**	**0.0078**	SI1715	**-31.4766**	**0.0029**
SI863	**-39.7264**	**8.9170×10^{-4}**	SI1992	**-31.3417**	**-0.0047**
SI943	**-31.5172**	**-0.0030**	SI2194	**-29.6634**	**-0.0028**
SI1103	**-42.3124**	**0.0056**	SI2303	**-40.4777**	**-0.0015**
SI1109	**-37.1985**	**-0.0061**	SX29	**-35.2280**	**-7.4206×10^{-4}**
SI1217	**-36.9070**	**-0.0068**	SX364	**-30.7479**	**0.0043**

5.2.2.2 La qualité de processus de décryptage

La Table.5.5 donne toutes les données statistiques pour ces coefficients pour tous les signaux utilisés. A partir de ces valeurs, on peut facilement observer que les valeurs obtenues sont excellentes. Les coefficients de corrélation atteindront la plus petite valeur de 0.99943 qui est proche de 1.Ce qui signifie qu'il n'y a pas de différence entre les signaux vocaux originaux et déchiffrés et le processus de cryptage est très bon. Les valeurs du SNR sont également presque significatives. Les variations des valeurs SNR sont dues à l'intervalle et à l'énergie du signal vocal. De toutes ces discussions, nous pouvons conclure que le schéma proposé conserve grandement la qualité du signal de parole lorsqu'il déchiffre.

Table.5.5.SNR et Coefficient de Corrélation entre les signaux d'origine et décrypté.

signav ocale	SNR (origine, décrypté)	Coef_Corr(origine, décrypté)	Signal vocale	SNR (origine, décrypté)	Coef_Corr (origine, décrypté)
SI560	**35.3820**	**0.99985**	SI1303	**34.6068**	**0.99982**
SI734	**32.5493**	**0.9997**	SI1308	**35.8761**	**0.99987**
SI770	**27.0283**	**0.9990**	SI1390	**32.8723**	**0.99974**
SI839	**35.8473**	**0.99985**	SI1460	**33.4023**	**0.99992**
SI860	**31.2040**	**0.9996**	SI1715	**38.4230**	**0.99992**
SI863	**31.5794**	**0.9997**	SI1992	**36.1811**	**0.99987**
SI943	**34.67.54**	**0.9998**	SI2194	**40.1429**	**1.0000**
SI1103	**31.0270**	**0.9996**	SI2303	**29.4997**	**0.99943**
SI1109	**32.0621**	**0.99968**	SX29	**39.0748**	**0.99993**
SI1217	**32.5694**	**0.99972**	SX364	**37.0662**	**0.99990**

5.2.3 Examen des formes d'ondes

5.2.3.1 Signaux vocaux et signaux cryptés

La forme d'onde A des figures : Fig.5.2, Fig.5.3 montre le signal vocal original de :SI1715, SX29 respectivement. La forme d'onde C montre le signal crypté, et pour plus de clarification, la dernière forme d'onde C est illustrée en deux parties. A partir de ces figures, nous pouvons clairement mentionner qu'il n'y a pas de similitude entre le signal de parole original (A) et son version cryptée (C) qui est régulièrement uniforme et n'a aucun rapport avec les variations de la forme d'onde d'origine (A).

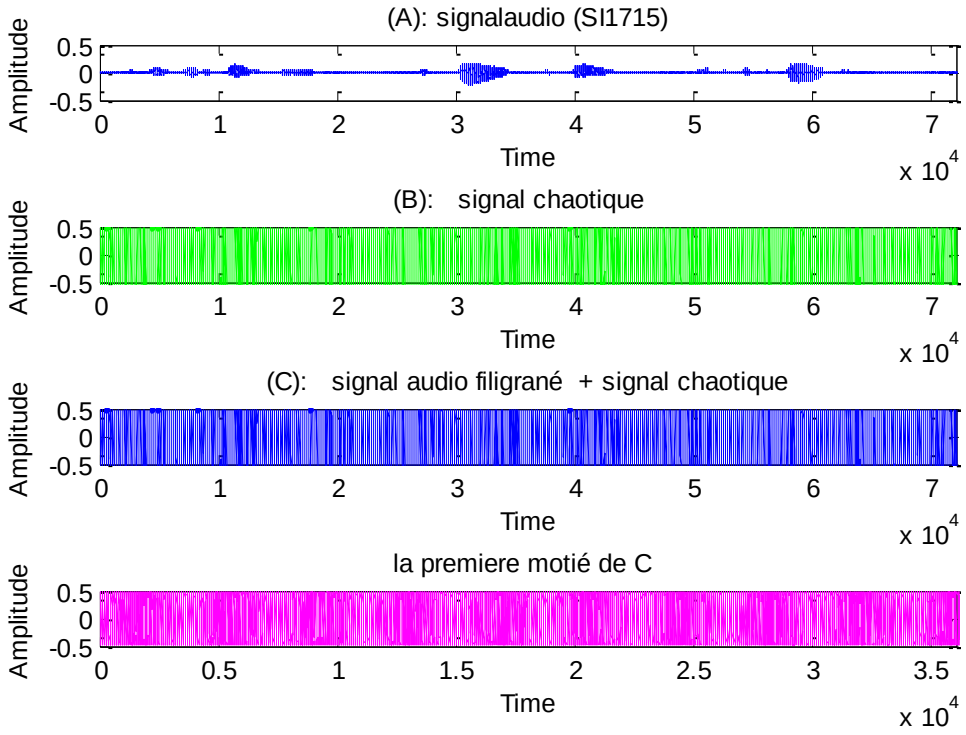


Fig.5.2. Frome d'onde SI715 (A: original, B: signal chaotique C: signal audio filigrané+signal chaotique et la première moitié du crypté(C).

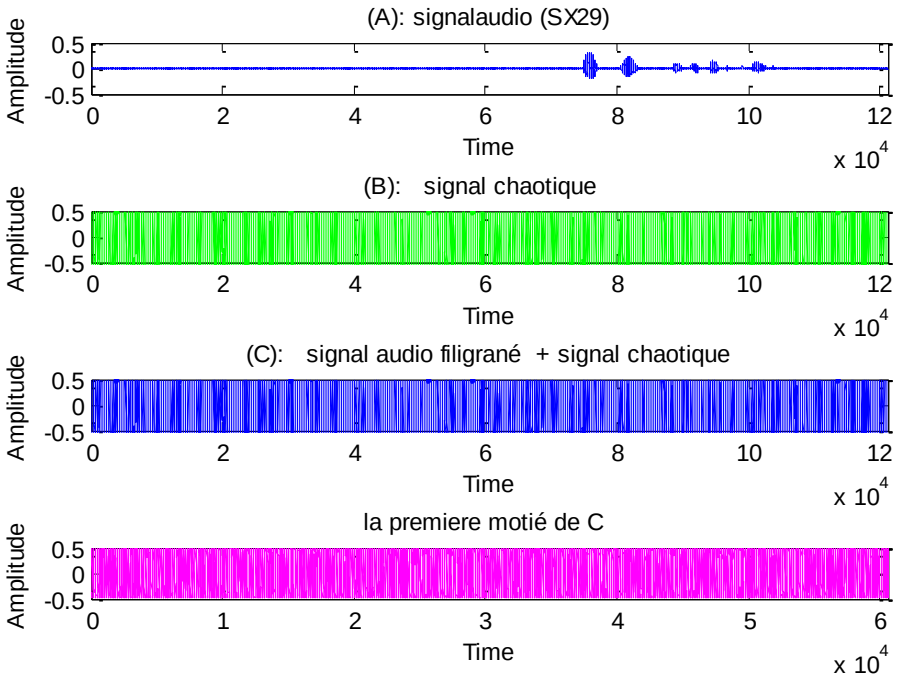


Fig.5.3. Frome d'onde SIX29 (A: original, B: signal chaotique C: signal audio filigrané+signal chaotique et la première moitié du crypté(C).

5.2.3.2 Signaux vocaux originaux et décryptés

Les signaux vocaux SI1715et SX29 sont représentés dans la première forme d'onde de : Fig.5.4, Fig.5.5 respectivement, et des signaux vocaux déchiffrés sont présentés dans la deuxième forme d'ondes des mêmes figures. La troisième forme d'onde illustre la différence entre le signal vocal d'origine et le signal décrypté. Même si nous nous concentrons bien sur les formes d'ondes, nous ne pouvons pas faire la distinction entre le signal vocal d'origine et le signal déchiffré extrait, et nous ne pouvons pas voir la différence que lorsque nous faisons la différence de forme d'onde. Cette erreur est montrée avec une très petite amplitude (0.01-0.01). Nous pouvons conclure que les deux signaux de parole : l'original et déchiffré sont similaires et trop proches les uns des autres.

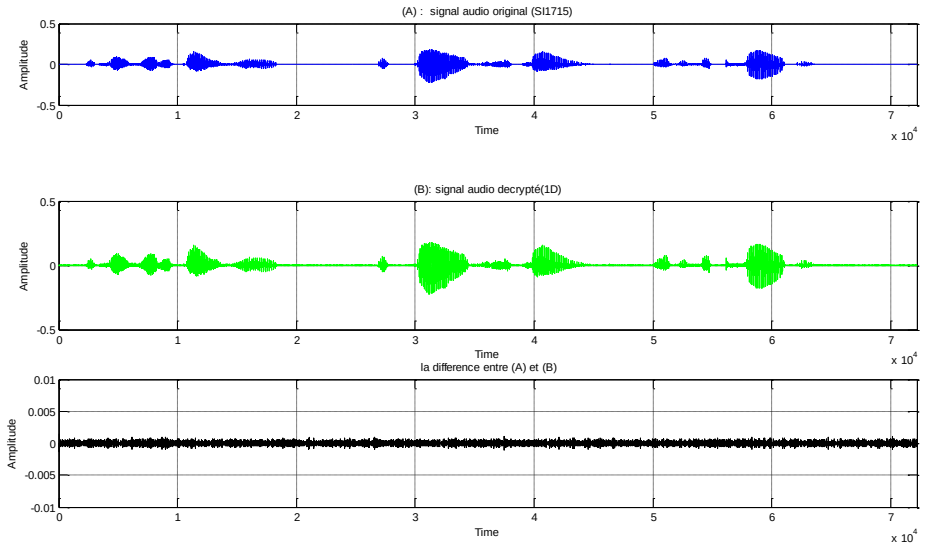


Fig.5.4 .Formes d'onde SI1715 (A : original, B : décrypté, la différence entre l'original et discours décrypté).

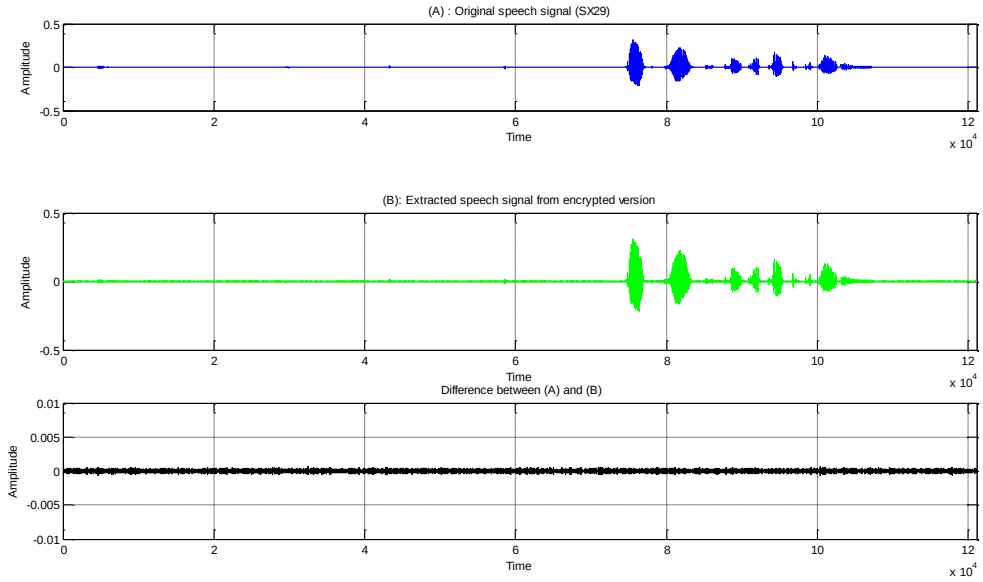


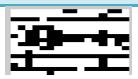
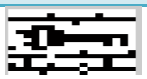
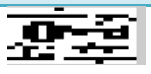
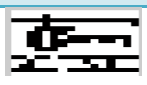
Fig.5.5 Formes d'onde SI1715 (A : original, B : décrypté, la différence entre l'original et discours décrypté).

5.2.4 Contrôle et authentification des filigranes (*Watermark*) :

Le tableau Table.5.6 fournit des résultats lorsque le signal vocal est attaqué par certains AWGN ajoutant des bruits blancs gaussiens. Dans les donnes présentées dans ce tableau, nous mentionnons que le filigrane est extrait avec succès en présence d'un petit bruit. Mais lorsque le bruit augmente considérablement, cela affecte le filigrane. Cela indique que le signal vocal est affecté. Nous pouvons observer cela dans les valeurs du BER impliquant que la transmission de signal crypté souffre de certaines attaques. Nous mentionnons que nous pouvons contrôler la force du filigrane afin que la sensibilité du filigrane puisse être augmentée ou diminuée pendant l'attaque en changeant simplement les valeurs**Δ**.

Table.5.6. Variation des valeurs de BER âpres attaques AWGN sur les signaux vocaux.

Signal vocal	AWGN (db)	BER	Filigrane (watermark) extrait	Signal vocal	AWGN (db)	BER	Filigrane (watermark) extrait
SI560	70	**0**		SI1303	70	**0**	
	60	**0.0430**			60	**0.0352**	

SI734	70	**0**		SI1308	70	**0**	
	60	**0.0781**			60	**0.0547**	
SI770	70	**0**		SI1390	70	**0**	
	60	**0.0508**			60	**0.0430**	
SI839	70	**0**		SI1460	70	**0**	
	60	**0.0430**			60	**0.0625**	
SI860	70	**0**		SI1715	70	**0**	
	60	**0.0234**			60	**0.0352**	
SI863	70	**0**		SI1992	70	**0**	
	60	**0.0742**			60	**0.0664**	
SI943	70	**0**		SI2194	70	**0**	
	60	**0.0547**			60	**0.0391**	
SI1103	70	**0**		SI2303	70	**0**	
	60	**0.0508**			60	**0.0547**	
SI1109	70	**0**		SX29	70	**0**	
	60	**0.0938**			60	**0.0547**	
SI1217	70	**0**		SX364	70	**0**	
	60	**0.0938**			60	**0.0508**	

5.3 Résultats de simulation de transmission sécurisée d'un audio crypté par un système chaotique du *Chua*

Dans cette section, nous présentons et nous évaluons les résultats de simulation dans le cas d'une transmission sécurisée d'un audio numérique par deux niveaux de sécurité : le premier niveau est le masquage par un système chaotique de trois dimensions de *Chua* avec la synchronisation par *Pecora et Carroll*, et le deuxième niveau est le brouillage par la carte chaotique *d'Alrond map*.

5.3.1 La synchronisation de deux systèmes chaotiques avec les paramètres originaux

Avec les valeurs des conditions initiales et les paramètres des systemes chaotiques maître (4.6) et le système chaotique esclave (4.9) qui sont données dans la Table.5.7et pour présenter les résultats de cette méthode, nous prenons le signal vocalSX29 de fréquence d'échantillonnage 8000 Hz et de longueur 0.45 seconde.

Table.5.7 Les valeurs initiales et les paramètres des systèmes chaotiques (4.6) et (4.9)

	Les conditions initiales	**Les paramètres**	**Max_val**
Système maitre du Chua	$(x_{1m0}, x_{2m0}, x_{3m0})$ **(1, 0.5, -1)**	(α, β) **(15.7, 28)**	**1**
Système esclave du Chua	$(x_{1s0}, x_{2s0}, x_{3s0})$ **(0.7, -1, 1)**		

Les figures Fig.5.8 et Fig.5.9 montrent respectivement les résultats de la synchronisation des états des systèmes chaotiques et les erreurs de synchronisation. On remarque que les états du système esclave convergent asymptotiquement vers les états correspondants au système maître à partir de l'instant t=0.2 sec correspondant au temps de synchronisation des systèmes (4.6) et (4.9). Nous notons qu'après cet instant, le message audio est récupéré.

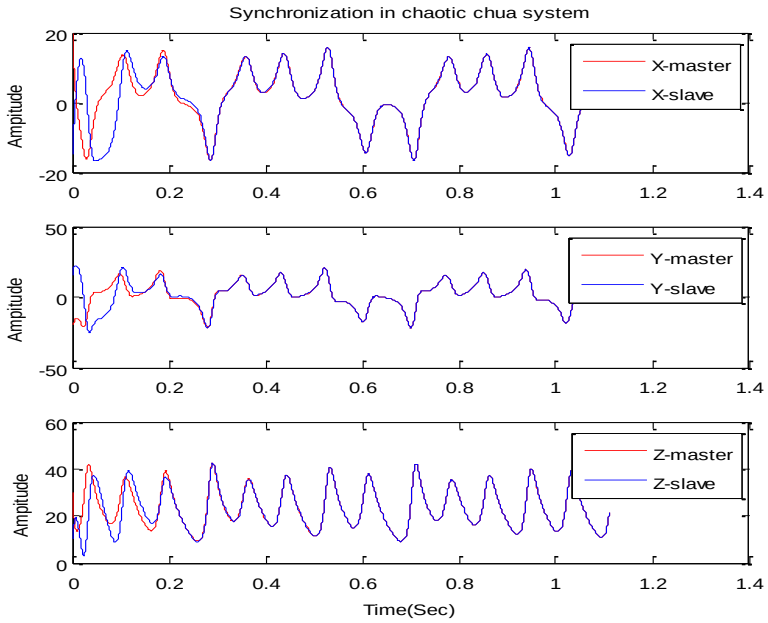


Fig.5.6. L'évaluation des états de système maître et esclave du Chua.

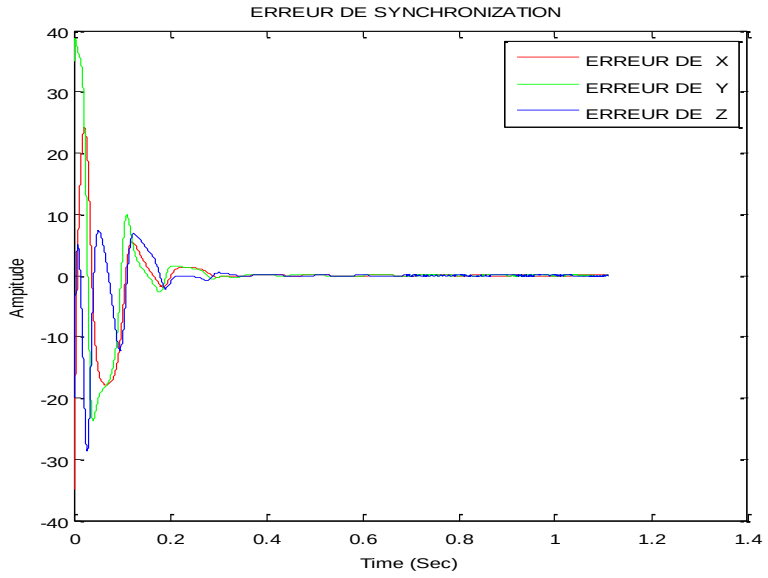


Fig.5.7 L'évaluation des erreurs de synchronisation des systèmes maitre et esclave du Chua.

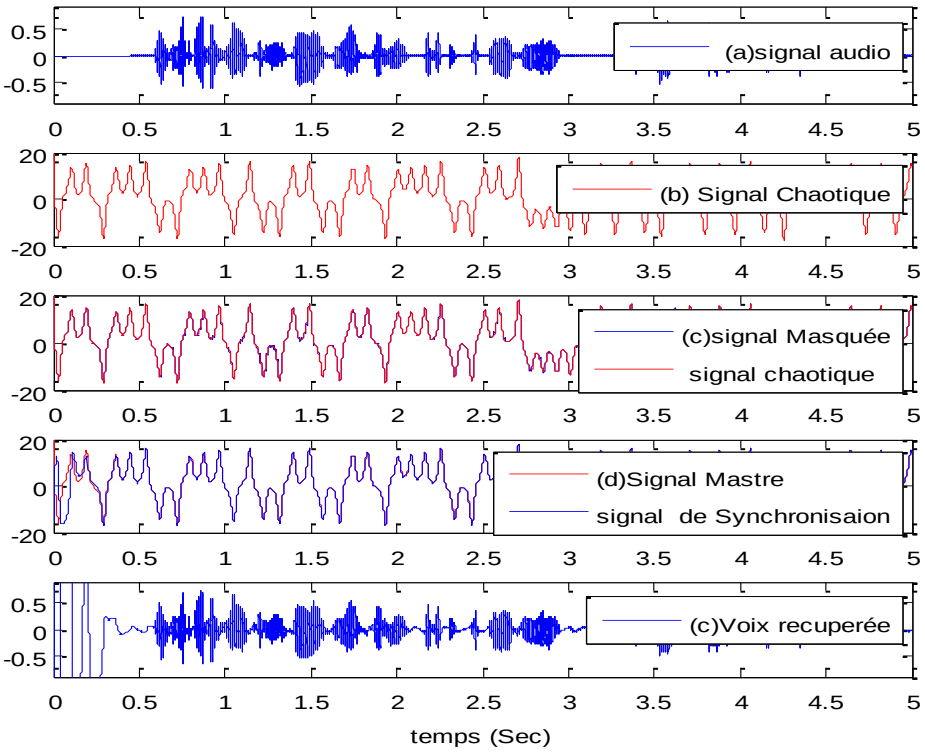


Fig.5.8. Masquage par le chaos : (a) signal audio brouillé, (b) signal chaotique signal audio masqué, (c) la synchronisation entre système maître et système esclave, (d) le signal audio récupérée.

La Fig.5.8 illustre les formes audio à partir de l'original jusqu'à la récupération passant par le cryptage. On remarque que l'audio est bien récupérer après des moments de synchronisation. Nous testons l'efficacité de ce processus de cryptage pour les signaux vocaux qui sont indiqués dans le Table.5.1.

5.3.1.1 Vérification de la cryptanalyse :

Comme mentionné précédemment, la cryptanalyse est effectuée en termes d'espace de clé et de sensibilité.

- L'espace de clé :

Les valeurs initiales du système du *Chua* et leur paramètres utilisées comme des clés et chacun de ces paramètres peut faire partie de l'espace de clé. Pour les conditions initiales si la précision est de 10^{-12}, tous les paramètres de clés prouvent prendre 10^{12}, par conséquence l'espace de clé sous la forme 10^{12*8}, ce qui est grande pour résister les attaques par force brute.

- **La sensibilité de la clé :**

Pour cela, nous avons modifié un seul paramètre des clés à la fois d'une petite quantité, tout en gardant tous les autres paramètres des clés inchangées.

Après le processus de déchiffrement avec la nouvelle clé et puis le comparé avec le signal original, nous avons remarqué que tout changement même léger dans la clé de chiffrement, affecte le processus de récupération d'un audio original, comme indiqué dans les tableaux suivants.

Table.5.8 La sensibilité des clés des (système du *Chua* , *Arlond*).

Nom de discours	**Les clés** $(x_{1m0}, x_{2m0}, x_{3m0}$ $(x_{1s0}, x_{2s0}, x_{3s0},$ $\alpha, \beta, k)$	**(1.1, 0.55, -1.02, 0.75, 1.002, 1, 15.7, 28, 205)**			**(1, 0.58, -1.2, 0.7, 1.2, 1, 15.6, 28.5, 387)**		
		NSCR (%)	**UACI (%)**	**Corr_Coef**	**NSCR (%)**	**UACI (%)**	**Corr_Coef**
SI770	**(1, 0.5, -1, 0.7, -1, 1, 15.7, 28, 205)**	**99.9986**	**29.4025**	**-0.0932**	**99.9964**	**31.3260**	**0.0051**
SI1390		**99.9952**	**29.3499**	**-0.0776**	**99.9868**	**31.3480**	**-1.2962×10^{-4}**
SI863		**99.9944**	**29.3235**	**-0.0908**	**98.7053**	**31.5000**	**0.0012**
SI1715		**99.9946**	**29.2999**	**-0.0409**	**99.9768**	**30.7403**	**0.0039**
SI1217		**99.9988**	**29.4091**	**-0.0845**	**99.9894**	**31.3979**	**6.9495×10^{-4}**

5.3.2 Résultats d'estimation les paramètres du système chaotique *Chua* pour minimiser l'erreur de synchronisation

Dans cette partie les simulations et la Table.5.7, et avec un pas de temps de 0.02 pour 1000 pas et le choix des paramètres de simulations des deux algorithmes d'optimisation (*PSO* et *GA*) qui sont donnés dans le chapitre précédent dans la Table.4.1.

A partir de la section précédente nous avons les valeurs des paramètres $\theta = (\alpha, \beta)^T = (15.6,28)^T$ comme des paramètres originaux.

- Pour estimer le paramètre∂, on considère que le paramètre β est connu à l'avance avec la valeur originale. Les suppositions initiales pour le paramètre de contrôle α sont dans la gamme [14 ,17].
- Comme pour précédemment, et pour estimer le paramètre β, on va considérer uniquement que la variation sur le paramètre β et on suppose α constants. Les suppositions initiales pour le paramètre β de contrôle sont dans la gamme [26,30].

Les tableaux Table 5.9 et Table.5.10 montrent les valeurs statistiques (meilleur, maximum et minimum) des paramètres estimés α et β pour chaque modèle des algorithmes PSO et GA.

Table.5.9 Les valeurs statistiques de paramètre α

Type d'algorithme	**Paramètre α**		
	Meilleur	Max	Min
PSO1/GA1	**15.352**	**16.830**	**14.590**
PSO2/GA2	**15.800**	**16.530**	**14.550**
PSO3/GA3	**15.400**	**16.641**	**15.020**

Table.5.10 Les valeurs statistiques de paramètre β

Type d'algorithme	**paramètre β**		
	Meilleur	Max	Min
PSO1/GA1	**27.820**	**29.513**	**26.950**
PSO2/GA2	**28.230**	**30.000**	**27.670**
PSO3/GA3	**27.950**	**28.130**	**26.653**

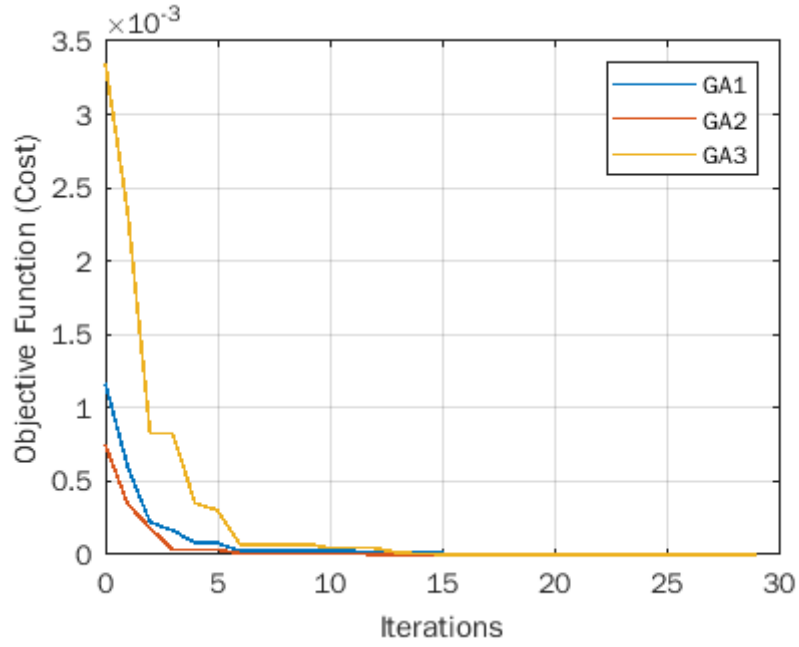


Fig.5.9 évaluation de J pour α en modèles GA (1-3).

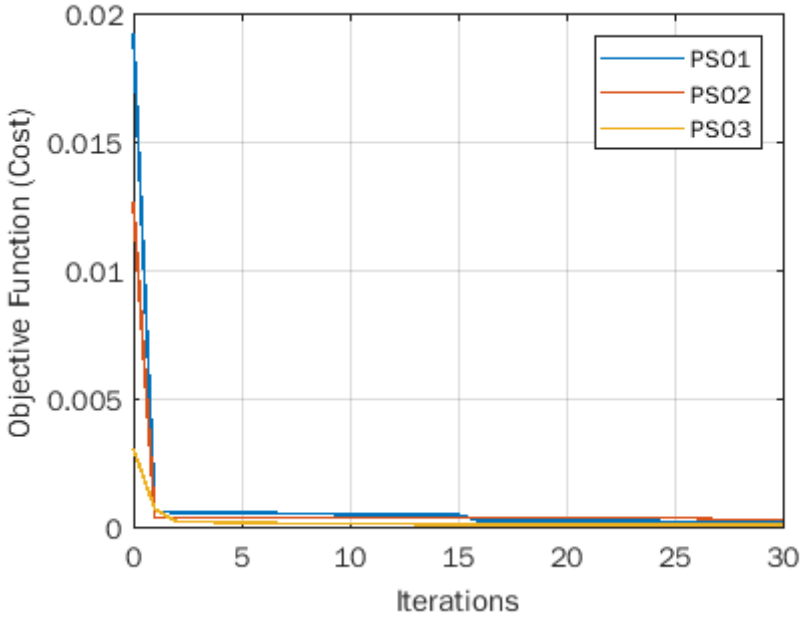


Fig.5.10 évaluation de J pour α en modèles PSO (1-3).

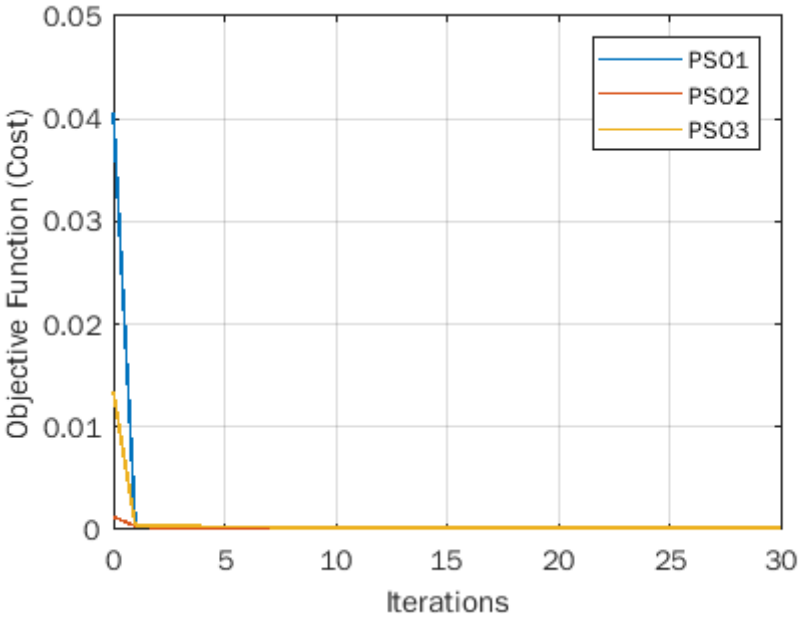


Fig.5.11 évaluation de J pour β en modèles PSO (1-3).

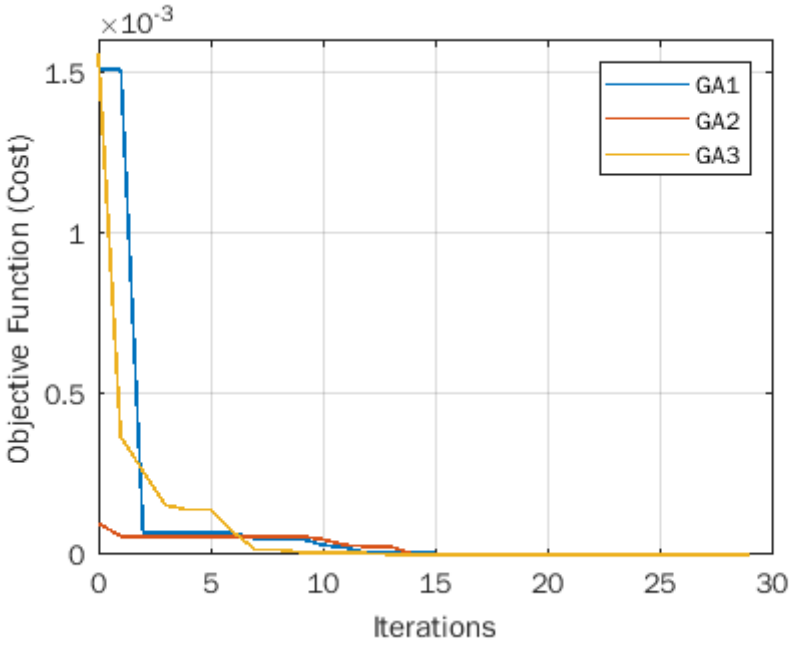


Fig.5.12 évaluation de J pour β en modèles GA (1-3).

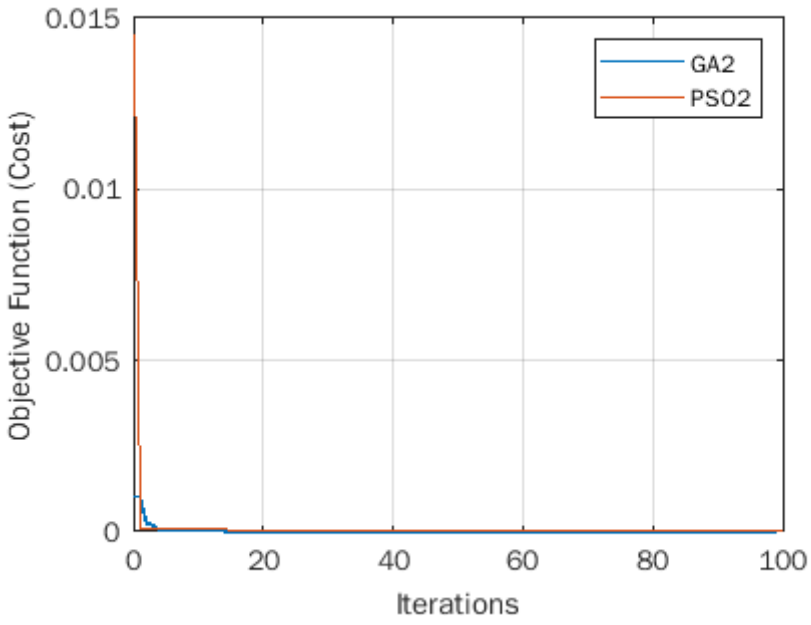


Fig.5.13. Evaluation de fonction objective J pour $\alpha = 15.8, \beta = 28.23$

Les figures: Fig.5.9, Fig.5.10, Fig.5.11, Fig.5.12 et Fig.5.13 montrent l'évaluation de la fonction objective J pour l'exécution typiques des modèles PSO(1-3) et GA(1-3) avec les valeurs des contrôles α et β respectivement.On note qu'après quelques itérations, les meilleurs résultats (valeurs estimées) sont presque les mêmes mais les modèles PSO-2 et GA-2 ont donnés la meilleure estimation des paramètres, qui sont très proches des valeurs réelles, ou les meilleurs valeurs de la fonction objective se rapprochement rapidement de la valeur la plus basse qui tend vers le zéro.

5.3.3 La synchronisation de deux systèmes chaotique avec des paramètres d'estimés

Dans cette partie, on garde le même système de communication qui est utilisé précédemment, mais avec des paramètres $\hat{\theta} = (15.80, 28.23)$ qui sont estimés par l'algorithme PSO-2.

A partir des figures Fig.5.14 et Fig.5.15, on montre que les états du système esclave converge vers les états du système maître plus rapidement et l'erreur de synchronisation converge plus vite vers les zéros à partie de t=0.08 sec en comparaison l'erreur de synchronisation appliquée avec les valeurs des paramètres initiales grâce à la méthode d'optimisation paramétrique

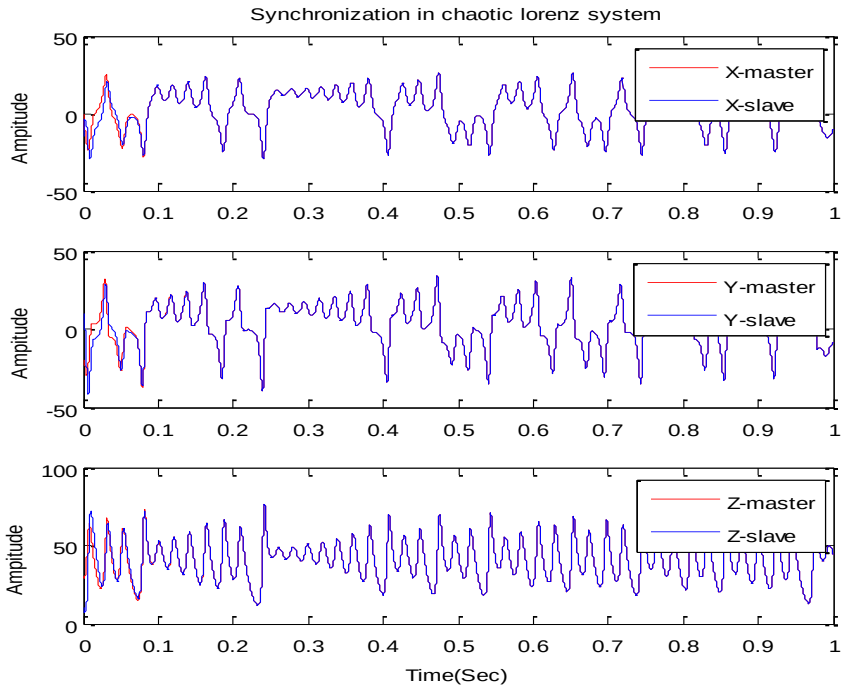


Fig.5.14. Evaluation des états du système maître et du système esclave avec des paramètres d'estimés $\hat{\theta} = (15.80,28.23)$

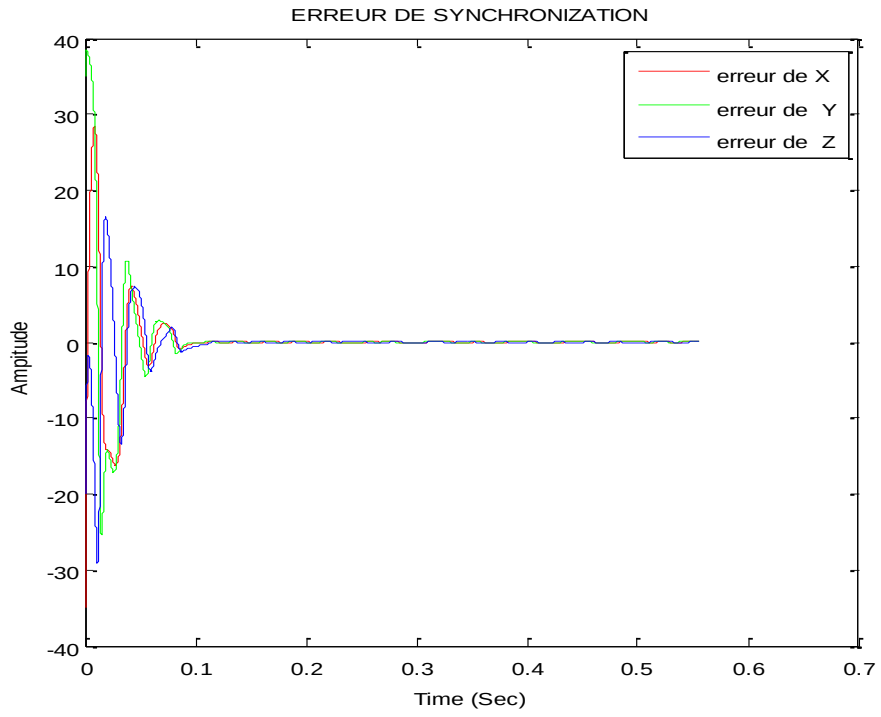


Fig.5.15. Evaluation des erreurs de synchronisation avec les paramètres d'estimées $\hat{\theta} = (15.80,28.23)$

5.3.4 Evaluer la qualité de cryptage et décryptage avec les valeurs des paramètres (originaux, estimées)

- La qualité d'un audio crypté :

D' après le tableau Table.5.11, la mesure de coefficient de corrélation a une faible valeur près de 0, c'est ainsi que les mesures du SNR sont très faibles (valeur négative) dans les deux cas de cryptage avec les paramètres (originaux, estimées).Dans le deuxième cas de cryptage avec des paramètres estimés, la corrélation est très faible entre les signaux originaux et cryptés. Il n'y a pas d'intelligibilité dans les signaux cryptés.

Table.5.11.SNR et Coefficient de Corrélation entre les signaux d'origine et crypté pour la deuxième méthode de cryptage.

Les voix	SNR (origine, encrypté) avec des paramètres originaux	Coef_Corr(origine, encrypté) avec des paramètres originaux	SNR (origine, encrypté) avec des paramètres estimés	Coef_Corr (origine, encrypté) avec des paramètres estimés
SI560	**-39.0063**	**0.0093**	**-43.1549**	**0.0008**
SI734	**-40.2001**	**0.00027**	**-44.8730**	**0.000153**
SI770	**-41.5020**	**0.0002**	**-45.4102**	**0.00012**
SI839	**-45.7030**	**0.00015**	**-42.9483**	**0.00018**
SI860	**-39.8710**	**0.0086**	**-45.6743**	**0.00017**
SI863	**-44.1590**	**0.000161**	**-44.7350**	**-0.00015**
SI943	**-45.1756**	**0.00019**	**-47.9137**	**-0.00011**
SI1103	**-40.1470**	**0.00026**	**-45.5663**	**-0.00019**
SI1109	**-40.1735**	**0.00017**	**-43.1970**	**0.00028**
SI1217	**-40.6430**	**0.00013**	**-45.4761**	**0.00018**

-La qualité d'un audio décrypté :

Pour mesurer la qualité du signal décrypté, les mêmes métriques précédentes de qualité sont utilisées. A partir du tableau Table.5.12 on peut remarquer que le SNR est très élevé (valeur positive), et le coefficient de corrélation est proche de 1, ce qui implique une corrélation significative entre la voix originale et la voix décryptée.

Table.5.12.SNR et Coefficient de Corrélation entre les signaux d'origine et décryptés pour la deuxième méthode de décryptage.

Les voix	SNR (origine, décrypté) avec des paramètres originaux	Coef_Corr(origine, décrypté) avec des paramètres originaux	SNR (origine, décrypté) avec des paramètres estimés	Coef_Corr(origine, décrypté) avec des paramètres estimés
SI560	**37.6013**	**0.99970**	**35.4179**	**0.99950**
SI734	**33.3509**	**0.99929**	**38.3200**	**0.99980**
SI770	**30.7918**	**0.0002**	**35.0810**	**0.99949**
SI839	**38.1503**	**0.99979**	**35.1910**	**0.99953**
SI860	**34.7203**	**0.99935**	**40.2738**	**0.99989**
SI863	**33.9457**	**0.99931**	**38.5301**	**-0.99981**
SI943	**36.5607**	**0.99963**	**43.9351**	**1.0000**
SI1103	**34.3510**	**0.99932**	**32.3406**	**-0.9993**
SI1109	**35.0276**	**0.99940**	**43.3761**	**1.0000**
SI1217	**34.9780**	**0.99939**	**40.3671**	**0.9998**

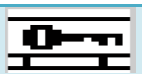
A partir des figures et tableaux précédents, on constate que le cryptage avec les paramètres estimés donne les meilleurs résultats. Plus les paramètres chez le récepteur ont une valeur proche des paramètres chez l'émetteur, plus la synchronisation sera rapide, et vice –versa.

5.3.5 Contrôle et authentification des filigranes (*Watermark*) :

Comme la section 5.2.4, Le Table.5.13 fournit des résultats lorsque le signal vocal est attaqué par certains AWGN ajoutant des bruits blancs gaussiens. Dans les donnes présentées dans ce tableau, nous mentionnons que le filigrane est extrait avec succès en présence d'un petit bruit.

Table.5.13. Variation des valeurs de BER âpres attaques AWGN sur les signaux vocaux.

Signal vocal	AWGN (db)	BER	Filigrane (watermark) extrait	Signal vocal	AWGN (db)	BER	Filigrane (watermark) extrait
SI560	70	**0**		SI1303	70	**0**	
	60	**0.0390**			60	**0.0352**	

SI734	70	**0**		SI1308	70	**0**	
	60	**0.0392**			60	**0.0356**	
SI770	70	**0**		SI1390	70	**0**	
	60	**0.0228**			60	**0.0380**	
SI839	70	**0**		SI1460	70	**0**	
	60	**0.0430**			60	**0.0225**	
SI860	70	**0**		SI1715	70	**0**	
	60	**0.0234**			60	**0.0342**	
SI863	70	**0**		SI1992	70	**0**	
	60	**0.0302**			60	**0.0264**	
SI943	70	**0**		SI2194	70	**0**	
	60	**0.0397**			60	**0.0391**	
SI1103	70	**0**		SI2303	70	**0**	
	60	**0.0409**			60	**0.0407**	
SI1109	70	**0**		SX29	70	**0**	
	60	**0.0938**			60	**0.0417**	
SI1217	70	**0**		SX364	70	**0**	
	60	**0.0338**			60	**0.0208**	

5.4 Comparaison des performances des méthodes de cryptage proposée avec les méthodes de cryptages traditionnelles

D'après les résultats obtenus précédents et afin d'évaluer les performances de la méthode proposées, il convient de la comparer aux autres systèmes de cryptage récemment publiés. En se basant sur les résultats illustrés sur la Table.5.14, nous avons confirmé que le schéma proposé offre des résultats excellents.

A travers ce qui précède, nous notons que les méthodes de cryptages basées en chaos sont efficaces pour la transmission sécurisée des voix. Dans les deux méthodes proposées le coefficient de corrélation entre le signal de parole original et le signal décrypté extrait au niveau de récepteur dans la premier méthode est 0.9999 et dans la deuxième prend la valeur un(1), ce qui signifie qu'il n'y a pas de différence entre le signal de parole original et le signal de parole décrypté. D'autre part le SNR =-35.514entre le signal original et le signal crypté est le plus petit dans notre schéma. Le SNR devient -47.9137, ce qui montre que le signal crypté est très éloigné du signal vocal original par rapport aux autres méthodes.

Par conséquent, en utilisant le système chaotique de processus de brouillage et le masquage pour améliorer la sécurité cryptographique est la meilleure solution adoptée.

Table.5.14.Comparaison entre notre approche et les cinq méthodes publiées.

Les schémas de sécurité	**Coef_Corr**		**SNR 'db' (moyen)**	
	original, encrypté)	(original, décrypté)	Original, encryptions	Original, décryptions
Brouillage (carte chaotique) [17]		**0.6087**	**-4.2272**	
Brouillage (carte+système chaotique) [16]		**0.963**	**-25.32**	
Masquage+brouillage (carte chaotique) [13]	**0,0073**	**0.9990**	**-35,514**	**34,081**
Masquage (système chaotique) +brouillage (carte)[17]	**0.0000**	**0.9998**	**-20.7803**	**312.9828**
Masquage (système chaotique+estimer les paramètres) [Notre méthode proposée]	**0.00010**	**0.9999**	**-45.7030**	**43.3761**
Masquage (système chaotique +estimer les paramètres) + brouillage [Notre méthode proposée]	**0.000153**	**1.000**	**-47.9137**	**42.9351**

5.5 Conclusion

Ce chapitre comprend les résultats de simulation à l'aide du logiciel Matlab des méthodes proposées, qui sont détaillées dans le chapitre précédent où nous avons proposés un système de communication plus sécurisée par deux niveaux de sécurités (masquage et brouillage) basée sur des systèmes chaotiques. Les résultats des simulations de la transmission sécurisée d'un audio ont été subdivisés en trois parties.

Dans la première partie nous avons présenté les résultats de simulation de la méthode de cryptage utilisant le masquage par hybridation entre les deux cartes chaotiques : *logistique map* et *tent map*. Dans la deuxième partie, nous avons masqué le signal audio par les systèmes chaotiques à trois dimensions (système du *Chua*).Dans les deux cas, nous avons fait le brouillage du signal résultant à l'aide *d'Arlond map*, et nous avons ajouté le filigrane pour tester l'efficacité de la méthode.

Les résultats obtenus indiquent que le système proposé a prouvé son efficacité pour la transmission sécurisée d'un audio. La technique de chiffrement et déchiffrement tirent pleinement parti de l'intégration du système chaotique faible dimension pour optimiser l'espace de clé, mais cela favorise une complexité de calcul, et un temps de calcul plus élevé, tandis que le système du *Chua* est un système complexe et a un grande espace de clé.

Dans la troisième partie, et pour récupérer l'audio qui est masqué par le système *Chua* dans l'émetteur, la synchronisation par *Pecora et Caroll* est utilisée. A partir des résultats de simulation, nous avons trouvé que la récupération de l'audio dépend de l'erreur de synchronisation, et pour une bonne récupération, nous avons minimisé l'erreur de synchronisation et nous avons optimisé les paramètres du système du *Chua* par les algorithmes méta-heuristiques : *PSO* et *GA*. Les résultats de simulation ont montré l'efficacité de cette étape.

Conclusion générale

Conclusion générale

Avec le développement des communications modernes et des technologies multimédias, et en raison de la sensibilité des données vocales, il est devenu très important de protéger ces données sur les communications numériques avec des systèmes de cryptage rapides et sécurisées avant la transmission ou la distribution sans se soucier de l'interception et de ses capteurs. Pour cela, nous avons conçu deux systèmes de communisation vocaux à haute sécurité en utilisant deux niveaux de cryptages basées sur les systèmes chaotique qui sont décrits dans le chapitre 1. Le premier niveau est le masquage chaotique qui est basé sur deux types des systèmes chaotiques, tandis que dans le niveau de brouillage on utilise la carte *d'Arlond (Cat map*).

Dans la première méthode, on utilise une hybridation des cartes chaotiques (*logistique map et tent map*) avec le signal audio original. Les résultats de simulation montrent bien que l'intégration du système chaotique à basse dimension consiste à optimiser l'espace de clé, et à obtenir un système complexe pour intégrer les valeurs originales du signal vocal, mais cela favorise une complexité de calcul et un temps de calcul plus élevés.

Dans la deuxième approche, nous avons masqué un audio en utilisant un système chaotique du *Chua* qui est l'un des systèmes avec des comportements dynamiques riches et complexes et à une large espace de clé. La récupération de l'audio confidentiel passe d'abord par la synchronisation des deux systèmes chaotiques et par *Pecora et Caroll* qui est détaillé dans le chapitre 3. Les résultats de simulation montrent que le masquage par le système chaotique de *Chua* donne une haute sécurité avec plus grande espace de clé et avec un fonctionnement en temps réel, à cause de la sensibilité des clés à un léger changement dans l'un des paramètres ou dans l'état initiales du système du *Chua* des valeurs d'état de signal inattendues. Mais la technique de synchronisation présentée par *Pecora* et *Carroll* souffre d'une forte sensibilité aux variations de paramètres, de plus, le signal de l'information peut être lui-même un signal chaotique pour contrôler la porteuse de l'information afin qu'elle ne change pas son comportement et préserve l'information, l'estimation des paramètres du système du *Chua* en utilisant l'algorithme d'optimisation *PSO* et *GA* est importante qui est détaillé dans le chapitre 3.

Dans cette étude, nous avons montré que dans la première partie et à partir des résultats d'un filigrane intégré dans le signal crypté dans le but de vérifier le processus de

décryptage que le signal crypté est authentifie et non soumis à des attaques externes dans le cas l'intégration du système chaotique à basse dimension est efficace pour crypté un signal vocal, mais cela favorise une complexité de calcul, et un temps de calcul plus élevés.

Par contre dans le deuxième cas, le système du *Chua* avec ses propriétés des comportements dynamiques riches et complexes avec une large espace de clé est utile pour crypter une voix. L'optimisation d'estimation des paramètres du système de *Chua* est efficace pour minimiser l'erreur de synchronisation. Les résultats confirment que l'algorithme proposé a atteint un niveau de sécurité plus élevé avec un temps de retard moyen le plus bas

Ces quelques perspectives proposées ici, peuvent faire l'Object d'une continuation possible de ce travail:

-Développer le système proposé dans la photo et la vidéo et dans l'application pratique sur l'internet.

-Pour l'augmentation de la taille de la clé secrète, on peut intégrer pleureurs systèmes chaotiques hauts dimension.

-Utiliser d'autres techniques de masquage : la modulation paramétrique et inclusion.

-Adapter une nouvelle méthode de synchronisation avec des algorithmes de réseaux de neurones.

A.1 Systèmes dynamiques

D'un point de vue mathématique la notation générale d'un système dynamique est définie par l'ensemble de variables qui forment le vecteur d'état$X = \{x_i \epsilon R\}, i = 1 \dots n$, où n représente la dimension du vecteur. L'état d'un système désigne l'ensemble des variables qui étant connus à l'instant initial, permettent de décrire l'évolution de ce système au cours du temps. L'ensemble de tous les états pouvant être pris par le système s'appelle ***l'espace des phases***. Conjointement, un système dynamique est défini par une loi d'évolution, généralement, désignée par ***dynamique*** pour décrire l'évolution du système d'un état initial à un état final.

A.1.1 Représentation mathématiques des systèmes dynamiques

Un système dynamique est une structure qui évolue au cours du temps

-Un système à temps continu

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

$$\dot{x}(t) = F(x(t), t) \tag{A.1}$$

Où et $F : R^n \times R^+ \rightarrow R^n$définit la dynamique du système en temps continu. A chaque couple choisi $(x(0), t_0)$, nous pouvons associer une solution unique du système défini à l'aide de l'équation (A.1).

-Un système à temps discret

Un système à temps discret est représenté par l'équation d'état suivant :

$$x(k+1) = G(x(k), k) \tag{A.2}$$

Où $G : R^n \times R^+ \rightarrow R^n$ est une fonction au moins continue ou continue par morceaux qui définit la dynamique du système en temps discret. De la même manière si nous associons à cette dynamique un état initial $x_0 = x(0)$ nous pourrons avoir une solution unique de G.

A.2 Comportement des systèmes dynamiques

Si dans le cas d'un système linéaire, la solution asymptotique est unique et indépendante de la condition initiale. En présence de non-linéarités, il existe une variété de régimes permanents, tel que le point d'équilibre, solution périodique, solution quasi-périodique ou chaos [23].

Point d'équilibre (Fig.A.1a):un point d'équilibre x^* est un point qui vérifie, en temps continu

$$f(x^*) = 0 \tag{A.3}$$

et en temps discret

$$f(x^*) = x^* \tag{A.4}$$

Pour un système non linéaire il y a une infinité de points d'équilibres. De plus ces points peuvent être stables ou instables suivant que les trajectoires voisines convergent ou divergent entre-elles (sensibilité aux conditions initiales).

Solution périodique (Fig.A.1b) : Le régime asymptotique permanent périodique correspond à une trajectoire dont les répliques d'une portion élémentaire sont espacées à des intervalles $n\,T, n \in N^+$ et T la période de la solution. Dans l'espace de phase, l'ensemble limite correspondant à cette solution est une courbe fermée.

Solution chaotique (Fig.A.1c) : le régime chaotique est par définition tout régime permanent qui n'appartient à aucune des classes présentées antérieurement. Une telle solution a une trajectoire asymptotique bornée avec une extrême sensibilité aux conditions initiales. Ainsi deux trajectoires générées à partir de conditions initiales très proches, vont diverger l'une par rapport à l'autre.

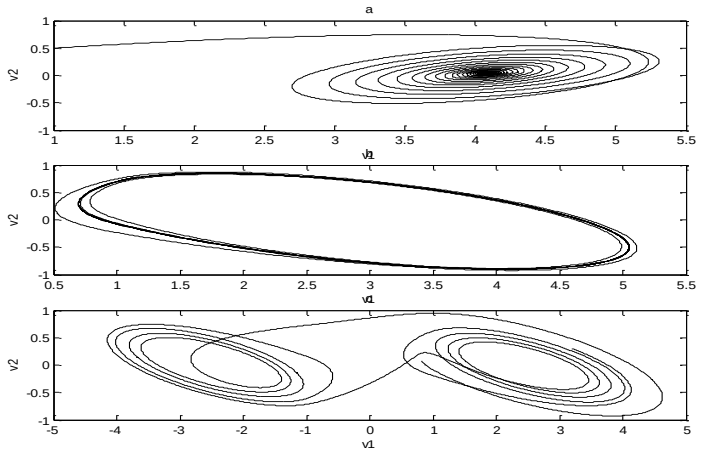


Fig.A.1 –Quelques comportements d'un système dynamique : a) point fixe, b) orbite périodique, c) chaos.

A.3 La stabilité

L'étude du comportement d'un système dynamique, correspondant à l'étude de la stabilité des points fixes. Soit le système dynamique non linéaire suivant :

$$\frac{dx}{dt} = f(x,t) \tag{A.5}$$

1-Le système est dit stable au sens de Lyapunov par rapport au point fixe si pour des conditions initiales x(0) suffisant proche de point fixe soit:

$$\forall \varepsilon > 0, \exists\, \gamma: \|x(0) - x^*\| \leq \gamma \Rightarrow \|x(t) - x^*\| \leq \varepsilon, \forall t > t_0 \tag{A.6}$$

2-Asymptotiquement stable si:

$$\exists\, \gamma > 0 \|x(0) - x^*\| \leq \gamma \Rightarrow \lim x(t) = x^*, \text{pour t } \to \infty \tag{A.7}$$

3-Exponentiellement stable si:

$$\forall \alpha > 0 \; et \; \lambda > 0 \; tels \; que : \forall\, t > 0, \exists\, B_r(x^*, r), \forall x(0) \in B_r,$$
$$\|x(t) - x^*\| < \alpha \|x(0) - x^*\| \exp(-\lambda t) \tag{A.8}$$

.

Dans lequel B_r=$\{x \in R^n / \|x(t) \leq r\|\}$ et $\|.\|$ est une norme sur R^n. Dans ce cas λ est appelé "taux de convergence".

La déférence entre la stabilité asymptotiquement et la stabilité au sens de Lyapunov réside dans le fait qu'une petite perturbation sur l'état initial d'un système autour d'un point fixe stable peut engendrer des petites oscillations entretenues, alors que ces dernières s'amortissent au cours de temps.

4- Stabilité globale si:

Le système asymptotiquement (exponentiellement) stable quelle que soit $\boldsymbol{x(0)}$

A.3.1 Linéarisation d'un système dynamique :

Considère le système dynamique non linéaire défini par:

$$\dot{x} = f(x) \tag{A.9}$$

Ou' $x = (x_1, x_2, , \dots, x_n)$ et $f = (f_1, f_2\, , \dots, f_n)$ et x^* un point d'équilibre de ce système.

Supposons qu'une petite perturbation $\varepsilon(t)$ soit appliquée au voisinage du point d'équilibre x^*. La fonction f peut être développée en série de Taylor au voisinage de point x^* comme suit:

$$\varepsilon(t) + x^* = f(x^* + \varepsilon(t)) \cong f(x^*) + J_f(x^*).\varepsilon(t) \tag{A.10}$$

Ou' $J_f(x^*)$ est la matrice jacobéenne de la fonction f définie par:

$$J_f(x^*) = \left(\begin{bmatrix} \frac{\partial f_1}{\partial x_1} & \frac{\partial f_1}{\partial x_2} \cdots & \frac{\partial f_1}{\partial x_n} \\ \vdots & \cdots & \vdots \\ \frac{\partial f_n}{\partial x_1} & \frac{\partial f_n}{\partial x_2} \cdots & \frac{\partial f_n}{\partial x_n} \end{bmatrix} \right)_{x=x^*} \quad \text{(A.11)}$$

Comme $f(x^*) = x^*$ alors l'équation (1.7) devient :

$$\varepsilon(t) + x^* = J_f(x^*).\varepsilon(t) \quad \text{(A.12)}$$

L'écriture (A.12) veut dire que le système (A.11) est linéarisée.

A.3.2 Première méthode de Lyapunov (méthode indirect):

La première méthode de Lyapunov est basée sur l'examen de la linéarisation autour du point d'équilibre x^* du système (1.3). Plus précisément, on examine les valeurs propres λ_i de la matrice jacobéenne évaluée au point d'équilibre. Selon cette méthode, les propriétés de stabilité de x^* exprime comme suivant :

- ✓ si toutes les valeurs propres de la matrice jacobéenne ont une partie réelle strictement négative, x^* est exponentiellement stable.
- ✓ si la matrice jacobéenne possède au moins une valeur propre à partie réelle strictement positive, x^* est instable.

A.3.3 Deuxième méthode de Lyapunov (méthode directe)

La seconde méthode est plus difficile à mettre en œuvre mais en contrepartie, elle est d'une portée beaucoup plus générale. Elle est basée sur la définition particulière, notée $V(x)$ appelée fonction de Lyapunov, qui est décroissante le long des trajectoires du système à l'intérieur du bassin d'attraction. Cette méthode est résumée parce théorème.

Theoreme.A.1: le point d'équilibre x^*du système (A.9) est stable s'il existe une fonction $V(x): U \to R$ Continue sur voisinage U dex^* différentiable telle que :

- $V(x^*) = 0\ et\ V(x) > 0\ , \nabla x \neq x^*$.
- Si de plus, la fonction V est telle que : $\dot{V} < 0\ V\ , \forall x \in Ux^*$.
- Alors est asymptotiquement stable
- $\dot{V} = \sum_{j=1}^{n} \frac{\partial V}{\partial x_j} x_j \leq 0 = \sum_{j=1}^{n} \frac{\partial V}{\partial x_j} f_j \leq 0, \forall x \in U$ alors x^*est un point d'équilibre stable.

B.1 Les techniques de tatouage

Le tatouage numérique est un processeur qui consiste à insérer dans un signal original dit signal hôte (une image, un document de texte, son..) une signature ou une marque numérique (séquence aléatoire, un logo binaire…) de manière imperceptible et indélébile. Cette marque contient des données qui peuvent être employées dans diverses applications, y a compris la protection des copyrights, la surveillance d'émission, l'authentification des données ou la transmission sécurisée. Dans le contexte de tatouage audio numérique, un système efficace doit satisfaire un ensemble de conditions essentielles imperceptibilité, robustesse, sécurité et la capacité [40], [41].

B.2 Algorithmes de tatouage

Les algorithmes de tatouage audio sont liés essentiellement au choix du domaine d'insertion, on distingue deux domaines principaux d'insertion temporale et fréquentielle

B.2.1 Le domaine fréquentiel

Dans ce cas le signal audio est converti en ses coefficients de transformation, et la marque est insérer à ces coefficients pour obtenir des coefficients modifiés. Parmi les transformées utilisées on peut citer: la Transformée de Fourier Discret (Discret Fourier Transform), la transformée en cosinus discrète (Discret Cosinus Transform) et la transforme en ondelette discrète (Discrete Wavelet Transform).

B.2.1.1 La transformation en cosinus discrète

La DCT (Discret Cosinus Transform) est l'une des techniques de transformation fréquentielles. C'est une transformation linéaire qui transforme une matrice de **n** éléments à une autre matrice à n coefficients comme de différente fréquence de la fonction cosinus. La technique DCT peut diviser la matrice en trois bandes de fréquence : basse fréquence (low-frequency) LF, fréquence moyenne (middel-frequency) MF et haute fréquence (high-frequency) HF [40], [41].

Les transformations du DCT unidirectionnelle et de son inverse sont définies respectivement comme de suit :

$$f(\mathrm{x}) = \sum_{x=0}^{\mathrm{N}-1} \mathrm{a(u)c(u)cos}\left[\frac{(2\mathrm{x}+1)\mathrm{u}\pi}{2\mathrm{N}}\right] \quad \text{(B.1)}$$

$$c(\mathrm{u}) = \mathrm{a(u)} \sum_{x=0}^{\mathrm{N}-1} f(\mathrm{x})\mathrm{cos}\left[\frac{(2\mathrm{x}+1)\mathrm{u}\pi}{2\mathrm{N}}\right] \quad \text{(B.2)}$$

Pour u=0,1,2,……N-1

$f(\mathrm{u})$ est la série audio dans la demain temporel,

N est le nombre d'échantillons.

$\mathrm{a(u)}$ dans l'équation (B.1) et (B.2) est définie comme suit:

$$\mathrm{a(u)} = \begin{cases} \frac{1}{\sqrt{N}}, & u = 0 \\ \sqrt{\frac{2}{N}}, & u \neq 0 \end{cases} \quad \text{(B.3)}$$

$$F(0) = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} f(x)$$

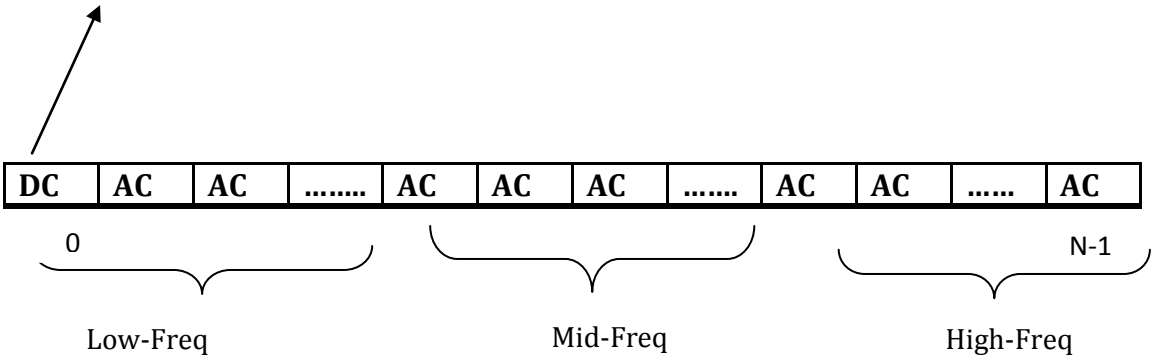


Fig.B.1. Bandes de fréquences de signale basé sur l'énergie

B.2.1.2 Transformée en ondelettes discrète

La transformation discrète des ondelettes est une technique d'analyse des signaux. C'est une nouvelle transformation qui donne une représentation temps-fréquence d'un signal.

L'une des fonctions de base DWT les plus courantes est l'ensemble d'ondelettes Haar. DWT de Haar est très utile dans la représentation du signal car il devise le signal en plusieurs sub- bandes dans un demain de fréquence.

Dans le DWT unidimensionnel (1D DWT), les filtres passe-bas et passe-haut décomposent le signal en deux sous-bandes [40] ,[41].

A partir d'un signal x(n), deux ensembles de coefficients sont calculés : coefficients de l'approximation A(n), et coefficients de détail D(n). Ces coefficients sont obtenus en convolant x(n) avec le filtre passe bas $h_0(n)$pour l'approximation et avec le filtre passe haut $h_1(n)$pour le détail, suivie d'une opération de décimation (sous échantillonnage par 2, typiquement note par$\downarrow 2$) comme montre dans la figure Fig.B.2.

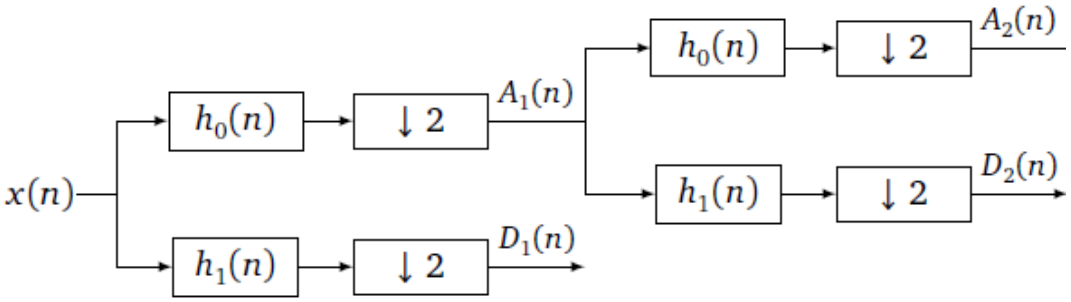


Fig.B.2.Décomposition en ondelette en deux niveaux de résolutions.

Selon l'objectif et la longueur du signal, les coefficients des approximations pourraient être aussi décomposés en deux ensembles de coefficients de haut et de passe fréquence

A partir des coefficients obtenus A(n) et D(n), le signal original peut être reconstruit en utilisant des filtres inverses$g_0(n)$ et $g_1(n)$ précédé par une opération d'interpolation (sur échantillonnage par ↑2) comme montre dans la figure Fig. B.3

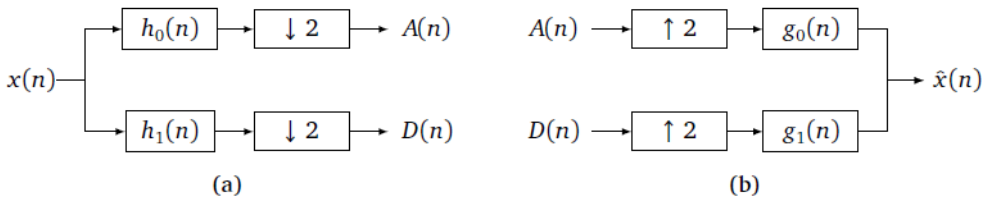


Fig.B.3. Décomposition /reconstruction à un niveau par transformée en ondelette.

Les références

[1] D. Ambika. And V. Radha, "Secure Speech communication – A Review", International Journal of Engineering Research and Applications (IJERA), Vol. 2 Issue 5 PP. 1044-1049 (2012).

[2] B. Sadkhan SattarandA. Abbas Nidaa, "Performance Evaluation of Speech Scrambling Methods Based on Statistical Approach" ATTI DELLA "Fonazione Giorgio Ronchi" AnnoLxvi, No. 5 PP. 601-6014 (2011).

[3] R. Gnanajeyaraman, K. Prasadh and Dr. Ramar, "Audio encryption using higher dimensional chaotic map", International Journal of Recent Trendsin Engineering, Vol. 1, No. 2, pp. 103-107, May 2009

[4] M. Ahmad, B. Alam and O. Farooq, "Chaos based mixed key stream generation for Voice data encryptions", International Journal on Cryptography and Informaton Security (IJCIS), Vol. 2, No. 1, March 2012.

[5] A. V. Prabu, S. Srinivasarao, T. Apparao, M. J. Rao and K. B. Rao, "Audio encryption in handsets", International Journal of Computer Applications, Vol. 40 ,No. 6, pp. 40-45, Feb. 2012

[6] M. Ashtiyani, P. M. Birgani and S. K. Madahi, " Speech Signal Encryption Using Chaotic Symmetric Cryptography", Journal of Basic and Applied Scienctific Research, Vol. 2, No. 2, pp. 1668-1674, 2012

[7] F. Anstett, "Les systemes dynamiques chaotiques pour le chiffrement: synthese et cryptanalyse", These, Université de Hanri Poincaré, Nancy1, 2006

[8] E. Cherrier, "Estimation de l'état et des entrées inconnues pour une classe de système non linéaires", Thèse, Institut National Polytechnique de Lorraine, 2006.

[9] S.Najim Al Saad, E. Hato,"A Speech Encryption based on Chaotic Map", International Journal of Computer Application (0975-8887), Vol. 93, No. 4, May 2014.

[10] M. Ammar Raheema, B. Sattar, S. SMIEE, M Sinan Majid , "Performance Enhancement of Speech Scramling Technique Based on Many Chaotic Signal", International Conference on Computer Science and Engineering (CSASE), Duhok, Kurdistan Region-Iraq,2020. October 2015.

[11] E. Hato, S. Dayla, "Lorenz and Rossler Chaotic System for Speech Signal Encryption", International Journal of Computer Application (0975-8887), Vol. 128, No. 11,

[12] F. Mahmode, M. Shalaby, Y. Kamal, S. El Ramly, "A Speech Cryptosystem Based on Chaotic Modulation Technique", Egyption Journal of Language Engineering, Vol. 4,No,1,2007.

[13] N. Hikmat Abdullah, S. Saad. Hreshee, and K. Ameer "Design of Efficient Noise Reduction Scheme For Secure Voice Masked By Chaotic Signals", Journal of American Science 2015; Vol. 11, No.7, pp. 49-55.

[14] K. Ameer, N. Abdullah, S. Saad ,"Secure Speech Comminication System Based on Scrambling and Masking by Chaotic Map", International Conference on Advance in Sustainable Engineering and Application (ICASEA), Wasit University, kut, Iraq, 2018.

[15] U. Parlitz, L.O. Chua, L. Kocarev, K.S. Halle and A. Shang, ″Transmission of digital signals by chaotic synchronization″, International Journal of Bifurcation and Choas, Vol. 2,No. 4, pp. 973-977, 1992.

[16] L.M. Pecora and T.L. Carroll, ″Synchronization in Chaotic Systems″, Physicals Review and Letters, pp. 821-824, 1990.

[17] L.M. Pecora and T.L. Carroll, ″Synchronization Chaotic Systems″, *IEEE Trans. Circuit and Systems*, vol. 38, pp. 453-456, 1991

[18] M. Lakshmanan, S.Rajaseekar, "Nonlinear Dynamics Integrability, Chaos and Patterns". Advanced Texts in Physics, Publisher Springer-Verlag Berlin Heidelberg, 2003.

[19] S. Wiggins, "Introduction to Applied Nonlinear Dynamical Systems and Chaos", Texts in Applied Mathematics, Springer-Verlag New York, 2003.

[20] A. Wolf, J.B. Swift,H.L.Swinneyand J.A.Vastano, "Determining Lyapunov exponents from a time series", Physica D, Vol. 16, pp. 285-317, 1985.

[21] M. L'Hernault, "Feasabilité d'un Système d'Emission-Reception Analogique pour les Communications Sécurisées par le Chaos", Tese, Université de Cergy Pontoise, 2007.

[22] L.O. Chua, C.W. Wu, A. Huang and G.-O. Zhong, ″A universal Circuit for Studying and Generating Chaos-Part I: Routes to Chaos″, *IEEE Trans. Circuits and Systems-I: Fundamental Theory and Application*, Vol. 40, No. 10, October, 1993.

[23] L*.O. Chua, ″Global Unfolding of Chua's Circuit″, *IEEE Trans. Fundamental*, Vol. 76, No. 5, pp.704-733, 1993.

[24] L.O. Chua, L. Kovarev, K. Eckert, and M. Itoh, *″Experimentalchoas synchronization in Chua's circuit″*, International Journal of Bifurcation and Choas, Vol. 2,pp. 705-708, 1992.

[25] E. Ott, C. Grebogi,&Yorke, J. A. [1990] "Controlling chaos," PhysicalReviewLetters64, pp. 1196—1199.

[26] L.O. Chua, & G.N. Lin, [1990] "Canonical realization of Chua's circuit family," IEEE Transaction on Circuits and Systems-I 37, pp. 885—902.

[27] A. V. Prabu, S. Srinivasarao, T. Apparao, M. Jaganmohan, and K. Babu Rao, "Audio encryption in handsets," *International Journal of Computer Applications*, vol. 40, no. 6, February 2012

[28] B. Boulebtateche, M. M. Lafifi, and S. Bensaoula. A multi media chaos-based encryption algorithm. [Online]. vailable:https://www.researchgate.net/publication/228437181.

[29] G. Djamal Eddine ,"Fonction logistique et standard chaotique pour le chiffrement des images

satellitaires",these majistere,2011, Université Mentouri de Constantine

[30] R. James Drummond, "**Analogue-to-Digital Conversion**",Microprocessor Interfacing Techniques, PP.89-108, September 1997.

[31] http://www.tsp.ecemcgil.ca/mmsp/documents/AudioFormats/

[32] Brooks,W. David ; Carr, Adam and Edkins, Keith; et al, (2004), "Data Compression", Wikipedia the Free Encyclopedia, GNU Free Documen -tation License, Boston, U.S.A.

[33] A. Chan Carusone, "Digital Algorithms for Analog Adaptive Filters", Ph.D. Thesis, University of Toronto, 2002.yption. IEEE Trans. Image Process. 15, 2061–2075 (2006).

[34] M..tahon," traitement du signal",laboratoire d'Acoustique. Conservatoire National des Arts et Métiers,2014-2015.

[35] A. kadhim Jawad,"Design and Simulation of Secure Communication System based on Chaos over AWGN Channel",Al-Mustansiriya University,2015

[36] U. Parlitz, L.O. Chua, L. Kocarev, K.S. Halle and A. Shang, *"Transmission of digital signals by chaotic synchronization"*, International Journal of Bifurcation and Choas, Vol. 2,No. 4, pp. 973-977, 1992.

[37] T. Yang, C. Wah-Wu and L. Chua, "Cryptography Based on Chaotic Systems", *IEEE Trans, Circuit and Systems-I: FundamentalTheory and Application*, Vol. 44, No. 5, pp. 469-472, May 1997.

[38] F. Anstett, "Les systèmes dynamiques chaotiques pour le chiffrement: synthèse et cryptanalyse", Thèse de doctorat, Université de Henri Poincaré, Nancy1, 2006.

[39] T. Yang and L. Chua ,"Secure Communication via Chaotic Parameter Modulation", *IEEE Trans. Circuits and Systems-I: Fundamental Theory and Applications*, Vol. 43, No. 9, pp. 817-819, September 1996.

[40] R. Channapragada Seshagiri Rao, Munaga V.N.K. Prasad "Digital WatermarkingTechniques in Curvelet and Ridgelet Domain", Springer Briefs in Computer Science (2016), DOI 10.1007/978-3-319-32951-2.

[41] M. Hemis ,"Système de Tatouage pour la Sécurité des Données audio ", Thèse de Doctorat , Université des sciences et technologies de houari Boumediene ,2017.

[42] S. Slami, A. Merrad, A. Benziane, Novel secured scheme for blind audio/speechnorm-spacewatermarking by Arnold algorithm, *Signal Processing*154 (2019) 74–86, www.elsevier.com/locate/sigpro. https://doi.org/10.1016/j.sigpro.2018.08.011

[43] A. Merrad, S. Slami, "Blind speech watermarking using hybrid scheme based on DWT/DCT and sub-sampling", *Multimed Tools Appl*(2018) 77:27589–27615, https://doi.org/10.1007/s11042-018-5939-z

[44] A. Merrad, S. Slami, A.Benziane, A. Hafaifa, Robust Blind Approach for Digital Speech Watermarking, 2018 2nd International Conference on Natural Language and Speech Processing (ICNLSP), 978-1-5386-4543-7/18IEEE. DOI: 10.1109/ICNLSP.2018.8374366.

[45] H. Delfs, H.Knebl," introduction to cryptography", Springer verlag, Berlin, 2002.

[46] A. Kerckhoffs, " La Cryptographie Militaire". Journal Des Sciences Militaires. Vol.9, pp .2-38.161-191, 1883

[47] H. Khanzadi, M.Eshghi and Shahram EtemadiBorujeni "Image Encryption Using Random Bit Sequence Based on Chaotic Maps", Arab J SciEng (2014) 39:1039–1047, DOI 10.1007/s13369-013-0713-z

[48] C.K. Huang, H.H. Nien "Multi chaotic systems based pixel shuffle for image encryption", Optics Communications 282 (2009) 2123–2127, doi:10.1016/j.optcom.2009.02.044.

[49] H. Liu, B. Zhao and Linquan Huang "Quantum Image Encryption Scheme Using Arnold Transform and S-box Scrambling", Entropy 2019, 21, 343; doi:10.3390/e21040343.

[50] P. Sathiyamurthi and Ramakrishnan ,"Speech encryption algorithm using FFT and 3DLorenz–logistic chaoticmap", Multimedia Tools and Applications(2020),https://doi.org/10.1007/s11042-020-08729-5.

[51] B. Ratner 'The correlation coefficient: Its values range between + 1 / − 1, or do they ?', Journal of Targeting, Measurement and Analysis for Marketing (2009) 17,139 – 142. doi: 10.1057/jt.2009.5

[52] F J.Farsana , K. Gopakumar "A NovelApproach for Speech Encryption: Zaslavsky Map as Pseudo Random Number Generator", 6th International Conference on Advances In Computing& Communications, ICACC 2016, 6-8 September 2016, Cochin, India (Procedia Computer Science 93 (2016) 816 – 823).

[53] K. Gopakumar, F.J. Farsana and V.R. Devi "An audio encryption scheme based on Fast Walsh Hadamard Transform and mixed chaotic key streams" Applied Computing and Informatics (Published by Emerald Publishing Limited 2019), DOI:10.1016/j.aci.2019.10.001

[54]]Y.S. Tang, A.I. Mess and L.O. Chua, "Synchronization and chaos", *IEEE Trans, Circuit and Systems*, Vol. 30, pp. 1-2, 1983.

[55] L.M. Pecora, and T.L. Carroll, "chaotic circuits," IEEEtrans Circuits yst. vol. 38, pp. 453-456, 1990.

[56] L.M. Pecora, and T.L. Carroll, "Driving systems with chaotic signals," Phys. Rev. A44, pp. 2374-2383, 1991.

[57] H. Hamiche,"Inversion a gauche des systems dynamiques: Application à la transmission securisée des données" ,These de doctorat, Université moumoudmammeri de tizi ouzou,2011.

[58] H. Nijmeijer and Iven M.Y Mareels, "An observer Looks at synchronization", *IEEE Trans. Circuit*

systems: Fundamental Theory and Application, vol. 44, October 1997.

[59] G. Kreisselmeier, Adaptative observer with exponential rate of convergence, IEEE, Transactions on Automatic and Control, vol, 22.pp. 2-8 ,1977.

[60] Y. Xiong and M. Saif, "Sliding Mode Observer for Nonlinear Uncertain Systems" ,*IEEETrans. Automatic Control*, Vol. 46, pp. 2012-2017, No. 12, December 2001.

[61] A. Maybhate and R.E. Amritkar, "Use of synchronization and adaptive control in parameter estimation from a time series," *PhysicalReview E*, Vol. 59, 1999 pp. 284–293.

[62] LQ. Shen, M. Wang, "Robust synchronization and parameter identification on a class ofuncertainchaoticsystems". *Chaos, Solitons& Fractals*, 38, 106–111, 2008.

[63] I. Zelinka," SOMA- Self-Organizing Migrating Algorithm", [Online].[01.11.2010], URL:<http://www.ft.utb.cz/people/zelinka/soma/>.

[64] B." Samanta, C.Hataraj,"Paricleswarmoptimisatin for chaotic system parameter estimation", 978-1-4244-2762-8/09/$25.00 ©2009 IEEE.

[65] E. David Goldberg. *Genetic Algorithms in Search, Optimization and Machine Learning.* Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 1st edition, 1989.

[66] I. Boussaid," Perfectionnement de methahuristiques pour l'optimisation continue", Université Paris-est Créteil, 2013.

[67] J. Kennedy , RC. Eberhart,Y. Shi."*Swarm Intelligence*". San Francisco: Morgan Kaufmann Publishers, 2001.

[68] R. Poli, J. Kennedy, T. Blackwell."Particle swarm optimization an overview". *Swarm Intelligence* 2007; 1:33-57.

[69] S. Slami, A.Merrad, A. Benziane, "Novel secured scheme for blind audio/speechnorm-space watermarking by Arnold algorithm", *Signal Processing*154 (2019) 74 86,www.elsevier.com/locate/sigpro. https://doi.org/10.1016/j.sigpro.2018.08.011.

[70] M. Kevin Cuomo, "Analysis and Synthesis of Self-Synchronizing Chaotic Systems", Ph.D. Thesis, Research Laboratory of Electronics Massachusetts Institute of Technology Cambridge, February 1994.