REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
Université de Mohamed El-Bachir El-Ibrahimi - Bordj Bou Arreridj
Faculté *des Sciences et de la technologie*
Département d'Electronique

Mémoire

Présenté pour obtenir
LE DIPLOME DE MASTER
FILIERE : Electronique
Spécialité : Electronique des Systèmes Embarqués
Par

- **ABACHE HOUSSAM**
- **DEBBAH MOHAMMED ABDESLAM**

Intitulé :

Etude des performances de quelques fonctions chaotiques dédiées au Cryptage de la parole

Par la commission d'évaluation composée de :

Nom & Prénom	*Grade*	*Qualité*	*Etablissement*
M. Abdelhakim LATOUI	*MCA*	*Président*	*Univ-BBA*
M. Mohamed El Hossine DAACHI	*MCA*	*Encadreur*	*Univ-BBA*
M. Nacira DIFFELLAH	*MCA*	*Examinateur*	*Univ-BBA*

Année Universitaire 2021/2022

Remerciements :

Avant tout je tiens mon remerciement à Allah de nous avoir donné la foi, la force et le courage.

Je tiens à exprimer toute ma reconnaissance à mon directeur de mémoire, monsieur MOHAMED EL HOSSINE DAACHI. Je le remercie de m'avoir encadré, orienté, aidé et conseillé.

Je tiens a remercier également tous les membres de jury qui ont voulu examiner ce travail

Dédicaces :

Je dédie ce travail

A mes très chers parents, source de vie, d'amour et d'affection

A mes chers frères et leurs enfants, source de joie et de bonheur

A toute ma famille, source d'espoir et de motivation

A tous mes amis, et toute la promotion de 2éme année Master Système embarque Electronique2021-2022

A vous cher lecteur

Table des matières :

Liste des figures :

Liste des tableaux :

Liste des abréviations :

MIT **:**Massachusetts Institute of Technology

DES**:** Data EncryptionStandard

3DES**:** Triple-dataEncryptionStandard

RC4 : RivestCipher 4

RC5 : RivestCipher 5

AES :AdvencedEncryptionStandard

RSA :RivestShamirAdleman

DSA : :Digital Signature Algorithm

Résumé :

Ce mémoire de fin d'étude est réalisé dans le contexte du cryptage de la parole. En effet, nous avons étudié le cryptage d'un signal parole en utilisant plusieurs fonctions chaotiques. Pourvu que le cryptage consiste en deux phases distinctes : la phase de permutation et la phase de diffusion, nous avons étudié l'effet de l'utilisation de plusieurs fonctions chaotiques dans la phase de diffusion. Les données relatives à la séquence du signal parole sont enregistrées dans le PC moyennant une application Matlab. Concernant la phase de diffusion, les données seront divisées en trois parties. Chaque partie lui sera réservée une fonction chaotique. Pour tester les performances de cette technique, une comparaison au cryptage réalisé avec une seule fonction chaotique sera également établie. Quant à la phase de permutation, elle sera réalisée via l'emploi d'une seule fonction chaotique pour les deux méthodes de cryptage. Les résultats obtenus montrent l'intérêt de l'emploi de plusieurs chaotiques dans la phase de diffusion.

ملخص :

تم إنجاز هذه الأطروحة النهائية في سـياق تشـفير الكلام. لقد درسـنا تشـفير إشـارة الكلام باسـتخدام العديد من الوظائف الفوضوية. بشرط أن يتكون التشفير من مرحلتين متميزتين: مرحلة التبديل ومرحلة النشر ،حيث قمنا بدراسة تأثير استخدام العديد من الوظائف الفوضوية في مرحلة النشر. يتم تسجيل البيانات المتعلقة بتسلسل إشارة الكلام في الكمبيوتر الشخصي عبر تطبيق MATLAB. بالنسبة لمرحلة النشر ، سيتم تقسيم البيانات إلى ثلاثة أجزاء. سيكون لكل جزء وظيفة فوضوية. لاختبار أداء هذه التقنية، سيتم أيضًا إنشاء مقارنة مع التشفير الذي يتم إجراؤه مع وظيفة فوضوية واحدة. أما بالنسبة لمرحلة التبديل، فسـيتم تنفيذها باسـتخدام وظيفة فوضـوية واحدة لكلتا طريقتي التشـفير. وتبين النتائج التي تم الحصـول عليها فائدة استخدام العديد من الفوضى في مرحلة النشر.

Abstract:

This paper is done in the context of speech encryption. we have studied the encryption of a speech signal using several chaotic functions. Provided that encryption consists of two distinct phases: the permutation phase and the diffusion phase, we have studied the effect of using several chaotic functions in the diffusion phase. The data relating to the sequence of the speech signal is recorded in the PC by means of a MATLAB application. For the diffusion phase, the

data will be divided into three parts. Each part will be given a chaotic function. To test the performance of this technique, a comparison to the encryption performed with a single chaotic function will also be established. As for the permutation phase, it will be carried out through the use of a single chaotic function for the two encryption methods. The results obtained show the advantage of using several chaotic in the diffusion phase.

Introduction générale

L'envoi de messages sans que les autres ne puissent les intercepter est une tâche qui remonte à des dates avant jésus christ. Le plus ancien document chiffré qui a marqué l'histoire est celui daté du XVI^{ème} siècle avant jésus Christ. A titre d'exemple, la communication entre les différentes composantes d'une armée se fait souvent par messages. Donc, les gens veillent toujours et prennent garde à ce que les messages ne tombent pas entre les mains de l'ennemi soit en faisant dissimiler les messages (Stéganographie), soit ces messages subissent un traitement de sorte à les rendre incompréhensible par l'ennemi (Cryptographie).

Le développement de la technologie a permis, entre autres, la conception de nouveaux moyens de communication très avancés ce qui permet de transmettre des données et des informations de taille importante dans un délai réduit. Cependant, la protection des données transmises contre d'éventuelles attaques devient de plus en plus indispensable, ce qui a poussé les chercheurs à développer des outils de protection puissants. Le cryptage des données basé sur les fonctions chaotiques est l'une des techniques les plus utilisées pour la protection des données.

Notre projet de fin de fin d'étude est réalisé dans le contexte du cryptage de la parole. En effet, nous allons étudier le cryptage d'un signal parole en utilisant plusieurs fonctions chaotiques. Pourvu que le cryptage consiste en deux phases distinctes : la phase de permutation et la phase de diffusion, nous allons étudier l'effet de l'utilisation de plusieurs fonctions chaotiques dans la phase de diffusion. En effet, les données relatives à la séquence du signal parole sont enregistrées dans le PC moyennant une application Matlab. Concernant la phase de diffusion, les données seront divisées en trois parties. Chaque partie lui sera réservée une fonction chaotique. Pour tester les performances de cette technique, une comparaison au cryptage réalisé avec une seule fonction chaotique sera également établie. Quant à la phase de permutation, elle sera réalisée via l'emploi d'une seule fonction chaotique pour les deux méthodes de cryptage.

Nous tenons à noter que les fonctions chaotiques à utiliser dans ce mémoire s'inspirent des travaux antérieurs s'agissant du cryptage d'image. Les différents tests seront réalisés par simulation dans l'environnement Matlab.

Par ailleurs, le reste du manuscrit est organisé en trois chapitres suivis d'une conclusion générale.

Dans le premier chapitre, nous allons introduire des généralités sur le signal parole. Le deuxième chapitre est dédié au cryptage et à la présentation des caractéristiques de quelques fonctions chaotiques relevant de la littérature. Le troisième chapitre quant à lui, représentant le cœur de notre travail, est réservé à la présentation des fonctions chaotiques à employer pour le cryptage du signal parole. Aussi, les résultats de simulation seront présentés dans ce chapitre avec également une comparaison entre l'approche de cryptage proposée utilisant plusieurs trois fonctions chaotiques dans la phase de diffusion et celle employant une seule fonction chaotique. La comparaison sera basée sur trois critères d'évaluation : le PSNR, la corrélation et la sensibilité de la clé. Nous terminons notre manuscrit par une conclusion générale et nous donnons quelques perspectives.

Chapitre I : Etude des caractéristiques du son

I.1 Introduction :

Dans toutes les formes de vie, la communication est nécessaire. La forme la plus évoluée et la plus complexe est la fonction d'expression des idées et de communication entre les humains, à travers le système de signes sonores et éventuellement le système de signes picturaux qui composent le langage.

Ce chapitre présente les Caractéristiques de son pour notre projet de fin d'étude, il débute par la définition et la production de parole, est on fait une étude sur le son.

I.2 Définition de la parole :

La parole est une succession de séquences sonores et de silences, et le seul moyen qui permet de communiquer la pensée par un système de sons articulés. Les humains sont les seuls êtres vivants qui utilisent un tel type des systèmes structurés, et il est le résultat d'une variation de la pression produite par l'émission d'un son par un locuteur.[1]

I.3 La production de parole :

La production du langage est l'opération la plus complexe de l'activité biologique humaine, un système dynamique dont le comportement à un instant donné dépend de son état antérieur. Par conséquent, le système s'appuie sur des variables configurables. Par définition, le son est ce que l'oreille perçoit à partir des vibrations du corps. Cette vibration est une onde (créée par des objets, guitares, pianos, tambours, marteaux, etc.) qui parcourt le corps (air, eau, métal, bois, etc.) et le corps (air, eau, métal, bois, etc.), la parole Les propriétés acoustiques d'un son diffèrent des autres sons en raison du mécanisme par lequel il est produit.

Le signal vocal est généré par le dispositif vocal. C'est un organe d'une grande complexité mécanique. Il se compose de deux parties anatomiquement distinctes. Les poumons et le larynx, la partie supérieure de l'artère trachéale, constituent la partie principale du générateur de sons. [1] [4]

I.3.1 Architecture de l'appareil Vocal :

Un dispositif générateur de sons ou un système générateur de sons se compose de quatre éléments de base qui sont étroitement couplés pour générer un signal acoustique. Ce sont, dans leur ordre évolutif :

- Soufflerie
- Vibreur
- Corps sain
- Système occlusal

La soufflerie se compose d'un réservoir d'air, de poumons entraînés par les muscles pectoraux et abdominaux et d'artères trachéales qui transportent l'air vers les cordes vocales. Le vibreur est le larynx qui génère les ondes aériennes ; le corps sonore est constitué d'un ensemble complexe de résonateurs, principalement le pharynx et la bouche ; enfin, le système articulaire est constitué d'éléments fixes et mobiles qui modifient fortement la forme de l'onde laryngée, ces sont étroitement liés au système nerveux central, assurant leur synchronisation et leur coordination. [2]

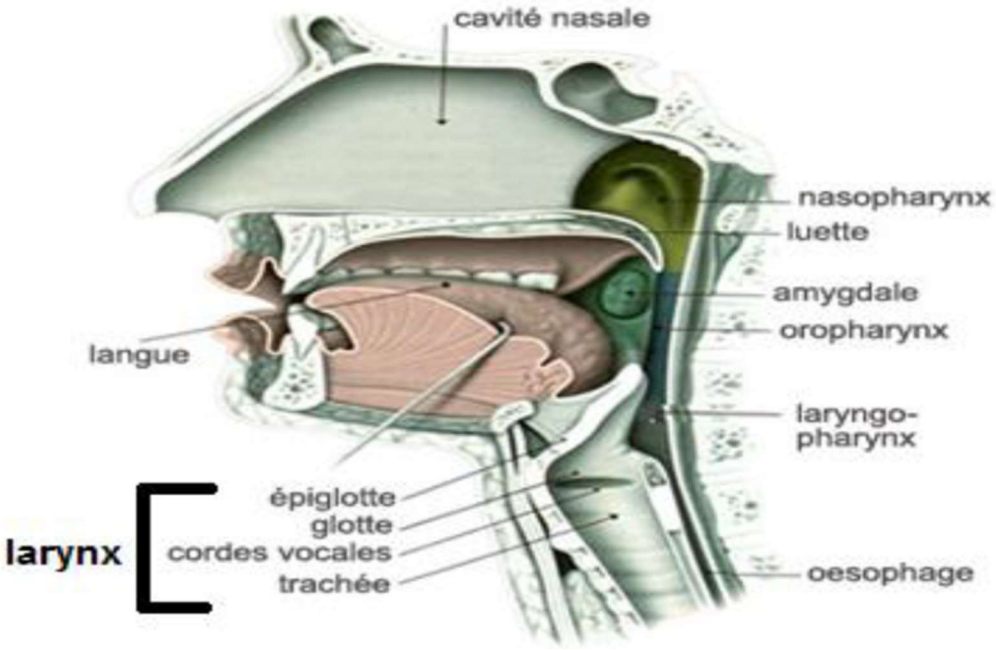

Figure I-1 Appareil vocal

I.3.1.1 Soufflerie et vibration :

L'air est la matière première du son, et si la fonction de notre organe vocal est souvent comparée à celle d'un instrument de musique, alors il convient de la décrire comme celle d'un instrument à vent. En effet, le système respiratoire est comme une soufflerie, expulsant l'air des poumons à travers la trachée. Cela se produit en abaissant la cage thoracique pour produire une "respiration vocale" ou, dans le cas de la vocalisation, par l'action des muscles abdominaux.[2]

I.3.1.2 Le larynx :

Le larynx est un ensemble de muscles et de cartilages mobiles qui entourent une cavité située à la partie supérieure de la trachée artère, se trouve au sommet supérieur de trachée-artère, où la pression de l'air est modulée avant d'être appliquée au conduit vocal. Le larynx est un ensemble de muscles et de cartilages mobiles. Les cordes vocales sont en fait deux lèvres symétriques placées en travers du larynx. Ces lèvres peuvent fermer complètement le larynx et, en s'écartant progressivement, déterminer une ouverture triangulaire appelée glotte. L'air y passe librement pendant la respiration et la voix chuchotée, ainsi que pendant la phonation de sons non-voisés. Les sons voisés résultent au contraire d'une vibration périodique des cordes vocales. Le larynx est d'abord complètement fermé, ce qui accroît la pression en amont des cordes vocales, et les force à s'ouvrir, ce qui fait tomber la pression, et permet aux cordes vocales de se refermer. [2]

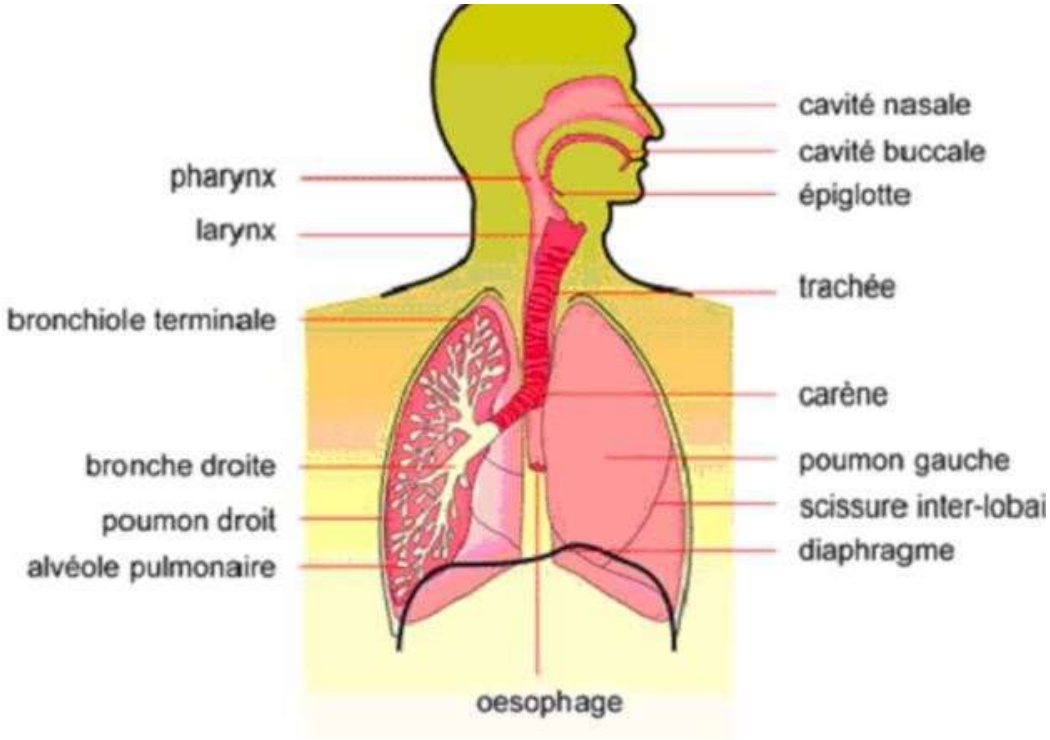

Figure I-2 Le larynx

I.3.1.3 Corps sonore :

Le résonateur du système de sonorisation est principalement responsable du timbre du son. Leur originalité par rapport aux caisses de résonance des instruments traditionnels réside dans leur capacité à varier, grâce à un réseau dense et fin de muscles, dans des proportions larges et très rapides de forme et de volume, assurant ainsi une diversité acoustique.

Il y a cinq résonateurs : le pharynx, la cavité buccale est divisée en deux, la cavité labiale et la cavité nasale. Ils communiquent tous entre eux par des ouvertures redimensionnables.

Tapissées de muqueuses, elles sont peu humides.

Contrairement à la croyance populaire, les sinus faciaux sont trop petits pour agir comme des résonateurs et n'ont aucune fonction reconnue dans la vocalisation. [2]

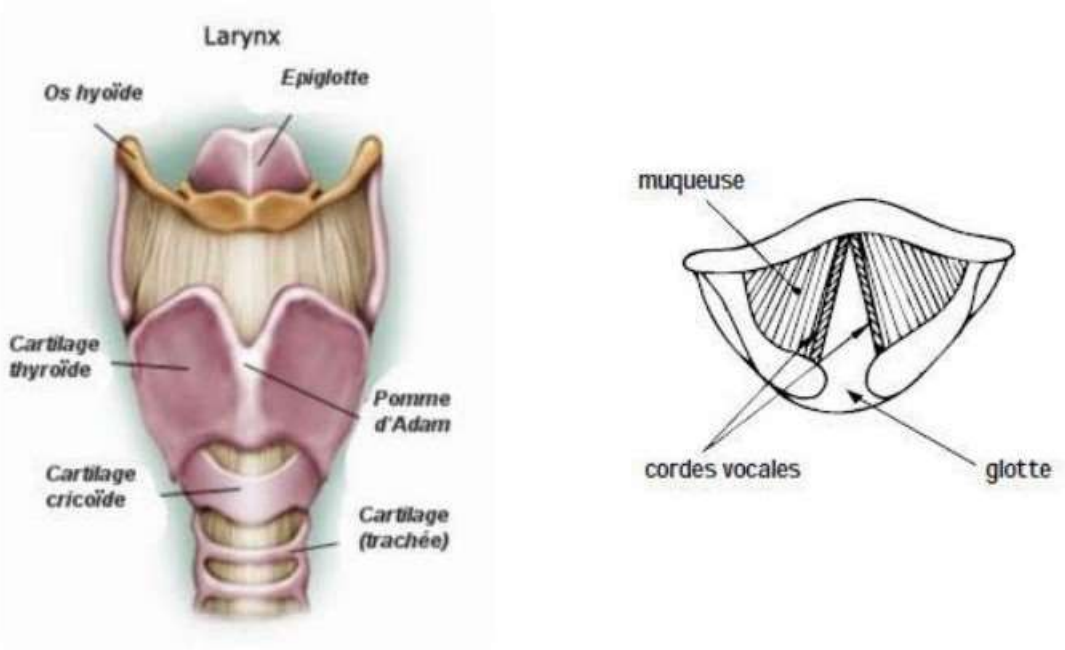

Figure I-3 vue schématique antérieure du Larynx

I.3.1.4 Système occlusal :

Il contient un ensemble d'organes mobiles, le palais mou, la mâchoire inférieure (ou mâchoire mandibule), la langue et les lèvres. Le mouvement mandibulaire est un facteur majeur de modification du volume oral. La base de la langue est attachée à l'os hyoïde et est contrôlée par dix-sept muscles (huit pairs et un impair) et est très flexible ; elle est située à divers points de la trompe d'Eustache pour relier les phonèmes. [2] Ces points de convergence sont :

- Lèvres (lèvres ou articulations des lèvres)
- Dents (articulations dentaires)
- Alvéoles 16 (articulations alvéolaires)
- Le palais dur, ou partie osseuse du fornix (articulation palatine)
- Palais mou ou « palais mou » (articulation du palais mou)
- Luette (l'articulation de la luette)
- Pharynx (articulations pharyngées)
- Glotte (articulation de la glotte)

I.3.2 Mécanisme sonore :

L'une des caractéristiques les plus importantes des signaux de parole est la nature de l'excitation. Il existe deux types d'excitation de base qui produisent des sons vocaux. [2]

- Phonation des sons voisés

  - Le son est produit par des stimuli agissant sur le tractus vocal et consiste en une série d'impulsions d'air périodiques provenant du larynx. Les cordes vocales sont initialement fermées, et sous la pression d'air constante des poumons, s'ouvrent progressivement, libérant cette énergie potentielle. Lors de cette ouverture, la vitesse de l'air et l'énergie cinétique augmentent jusqu'à ce que la tension élastique des cordes vocales soit égale à la force de séparation du flux d'air. La glotte a la plus grande ouverture à ce moment.

  - La force de Bernoulli accélère encore la fermeture brutale de la glotte à partir de l'énergie cinétique qui s'accumule lorsque la tension élastique dans les cordes vocales commence à rétrécir cette ouverture. Ce processus périodique est caractérisé par le fait que chacun a une fréquence spécifique, appelée fréquence fondamentale (Fo) ou hauteur, qui donne la hauteur normale du son. Les sons non voisés

- La plage de fréquence fondamentale est de 80 à 200 Hz pour les voix masculines, de 150 à 450 Hz pour les voix féminines et de 200 à 600 Hz pour les enfants.
- Cette fréquence fondamentale variera en fonction de facteurs liés au stress, au tonus et à l'humeur. Le timbre d'un son est déterminé par les amplitudes relatives des harmoniques fondamentales.
- L'intensité du son produit est lié à la pression de l'air en amont du larynx. Tous ces aspects du son voisé

- Phonation des sons non voisés : Le son non voisé est produit par la forte contraction de l'air à travers un point du conduit vocal. Ils sont générés sans entrée de gorge et ne présentent pas de structure périodique.

I.3.3 Classification des phonèmes :

Il existe plusieurs façons de classer les phonèmes. Un phonème est statique ou continu si la configuration du canal ne change pas pendant la production sonore. Un phonème est discontinu si la configuration du conduit vocal change au cours de sa génération. Les 36 phonèmes du français peuvent être classés selon la sonorité du générateur de sons. [2]

I.3.3.1 Voyelles :

Les voyelles sont des sons continus exprimés qui ont généralement la plus grande amplitude de tous les phonèmes, et leur durée peut varier considérablement, entre 40 et 400 millisecondes.
Les voyelles orales sont produites sans l'intervention de la cavité nasale, tandis que pour les voyelles nasales, les voies nasales sont reliées à la bouche et la vocalisation est accomplie simultanément par la bouche et les narines. Les voyelles sont divisées en trois groupes selon la position de la courbure de la langue et le degré de contraction provoqué dans le conduit vocal.
Il existe trois groupes en fonction de l'endroit où la langue se plie et de la quantité de contraction qu'elle induit dans le tractus vocal.
L’analyse dans le domaine temporal et fréquentiel révèle plusieurs caractéristiques acoustiques qui aident à la classification de chaque son. L’analyse dans le domaine temporal montre que les voyelles sont de sons quasi périodiques dus à l’excitation.
Les voyelles peuvent être identifiées par les locations de leurs formants dans le domaine frèquentiel.la position des deux premiers formants est suffisants pour caractériser la majorité des voyelles, le troisième formant est nécessaire juste pour quelques-uns. La position de

formants de fréquence plus élevée reste Presque inchangée et n'apporte pas d'information utile pour l'identification. [2]

Tableau I-1 : Phonèmes de langue Française [2]

Phonèmes								
Voyelles		Semi-consonnes	Consonnes					
Orales	Nasales		Voisées	Non- Voisées	Fricatives		Occlusives	
					Voisées	Non- Voisées	Voisées	Non-Voisées
i(I) e(E) ɛ(AI) a(A) ɔ(O) u(OU) y(U) Ø(EU) œ(OE) ə(E) o(AU)	ɛ̃(IN) œ̃(UN) ã (AN) ɔ̃ (ON)	j(Y) w(W) ɥ(UI)	l(L) R(R)	m(M) n(N) ɲ(GN)	v(V) z(Z) ʒ(J)	f(F) s(S) ʃ (CH)	b(B) d(D) g(G)	p(P) t(T) k(K)

I.3.3.2 Diphtongues :

Les diphtongues comprennent d'une voyelle initiale à une autre voyelle finale. Les diphtongues sont essentiellement des sons discrets.

Une diphtongue diffère de deux voyelles distinctes en ce que sa durée de transition est supérieure à la durée de chaque voyelle, et la voyelle initiale est plus longue que la voyelle enfin. Dans le discours, les deux voyelles constitutives d'une diphtongue peuvent ne pas être pleinement réalisées, soulignant l'idée de non-stationnarité de la diphtongue. [2]

I.3.3.3 Semi-consonnes :

Les semi-consonnes sont des sons voisés discontinus avec des caractéristiques spectrales similaires aux voyelles. Les semi-consonnes peuvent être considérées comme des sons transitoires qui s'approchent puis s'éloignent de la position cible. La durée de la transition est comparable à la durée de la transition vers l'emplacement cible. [2]

I.3.3.4 Consonnes :

Comparé aux voyelles, le conduit vocal est plus étroit lors de la production de consonnes.
Les consonnes impliquent deux formes d'excitation des voies vocales, qui peuvent ou non être exprimées. [2]

- Consonnes de friction :

Les fricatives non prononcées sont produites par la turbulence de l'air dans la structure du canal, qui peut être près des lèvres, au milieu du conduit vocal sur les dents et au bas du conduit vocal sur le palais.
Dans ce cas, le point de pincement provoque une source de bruit et divise le canal en deux cavités. La première cavité agit comme une enceinte anti-résonnante qui atténue les basses fréquences, de sorte que l'énergie est concentrée aux hautes fréquences dans le domaine spectral. Pour les fricatives vocales, les stimuli sont mélangés et des chocs périodiques provenant des vibrations des cordes vocales sont ajoutés à la source de bruit.

- Consonnes occlusives :

Une consonne d'arrêt est une combinaison de sons vocaux et non vocaux et de brefs silences.
Une forte pression d'air est créée avant qu'un point du canal ne soit complètement bloqué puis soudainement relâché. Cette période d'occlusion est appelée la période de maintenance.
Pour les pauses non voisées, la phase d'entretien est une période de silence suivie d'une période de friction plus longue que pour les pauses voisées. Pour les pauses sonores, pendant la phase de maintien, les cordes vocales vibrent pour produire des sons de basse fréquence.

- Consonnes nasales :

Les consonnes nasales sont des sons vocaux continus. Les vibrations produites par les cordes vocales excitent le conduit vocal, formé cette fois par une cavité nasale ouverte et une bouche fermée. La résonance atténue certaines fréquences, selon le point auquel elle s'éteint. Les consonnes nasales ont une forme d'onde similaire aux voyelles, mais leur énergie est généralement inférieure en raison de la capacité réduite de la cavité nasale à répéter les sons par rapport à la cavité buccale.

- Consonnes liquides :

Les consonnes liquides sont des sons non continu et voisés qui possèdent des caractéristiques spectrales similaires aux voyelles. Elles sont plus faibles en énergie due au fait que le conduit vocal et plus étroit pendant leur production.

I.4 Analyse de la parole :

L'analyse et la synthèse sont deux activités duales, l'analyse fournit une description du signal sonore et la synthèse sert à le restituer. L'analyse acoustique est une partie importante du processus de traitement du signal sonore, permettant des systèmes de synthèse, de compréhension ou de reconnaissance vocale de haute qualité. L'opération consiste à extraire du signal de parole un ensemble de paramètres corrélés, distinguables et robustes pouvant le représenter Plusieurs techniques d'analyse sont utilisées dont l'une peut être analysée au moyen d'un spectrogramme **[1]**

I.5 Définition de son :

Le son est une onde qui se propage sous forme d'ondes longitudinales produites par la vibration d'un milieu fluide ou solide. Dans le cas le plus simple, l'onde est une simple sinusoïde, une vibration d'équation suivante :

$$x(t) = A.\sin(2\pi f.t - \varphi) \qquad I\text{-}1\ )$$

A est appelée l'amplitude du son, f sa est sa fréquence et φ est le déphasage de la vibration par rapport à l'origine du temps.

Ces sons sont appelés sons « purs ». Dans l'air, l'amplitude correspond au changement de pression qui caractérise l'onde.

Les sons les plus couramment rencontrés sont rarement purs. Ils sont la somme de plusieurs sons purs, c'est-à-dire de plusieurs sinusoïdes, souvent appelées « harmoniques ».

Un son est dit « riche » lorsqu'il contient de nombreuses harmoniques (comme la parole), et « pauvre » lorsqu'il contient peu d'harmoniques (comme le son d'une flûte). [3]

I.6 Transmission du son :

Le son ne voyage pas dans le vide. Si vous mettez une cloche dans une cloche et que vous faites le vide à l'intérieur petit à petit, vous constaterez que plus l'air est fin, plus le son est atténué, jusqu'à ce qu'il soit complètement éteint.

Lorsqu'une source sonore émet un son, les vibrations se propagent de particule en particule puis vers nos tympans qui vibrent à leur tour. Plus le médium est dense, plus le son se propage rapidement. Le son se propage à environ 350 m/s dans les mers, 1500 m/s dans l'eau et 5050 m/s dans l'air. La vitesse de propagation du son dépend de la température, de la pression et surtout de la densité du milieu. [3]

I.7 La perception humaine du son :

Les vibrations mécaniques de la matière et de l'air qui font vibrer nos tympans ne constituent pas en elles-mêmes un son. Le son naît et se forme dans notre cerveau.

Le son n'existe pas en dehors de notre cerveau. Entre le signal vibratoire atteignant l'oreille et la perception du son par le cerveau, se produit le phénomène de traitement du signal par le système nerveux. Cela signifie que les vibrations physiques de l'air n'atteignent pas le cerveau de manière brute. Il est converti que la gamme des vibrations perceptibles est tronquée, c'est-à-dire que même si leurs vibrations atteignent nos oreilles, nous ne pouvons pas entendre des sons qui ne sont ni trop bas (basses fréquences) ni trop hauts (hautes fréquences). Le système nerveux ne peut traiter que les vibrations dont les fréquences sont comprises entre 20 Hz et 20 kHz. Les sons avec des fréquences inférieures à 20 Hz sont appelés infrasons et les sons avec des fréquences supérieures à 20 kHz sont appelés ultrasons.

Toute créature ayant une ouïe ne peut percevoir qu'une partie du spectre sonore, selon l'espèce concernée. Par exemple, les chats peuvent percevoir des sons jusqu'à 25 kHz, les chiens jusqu'à 35 kHz et les chauves-souris et les dauphins jusqu'à 100 kHz.

De plus, l'ouïe est capable de traiter les signaux sonores afin d'en extraire uniquement les informations dont nous avons besoin pour percevoir notre environnement. Par exemple, dans un environnement bruyant, une personne est capable d'extraire automatiquement des sons significatifs pour elle, comme les mots de la personne avec qui elle parle. Les humains sont également capables de reconnaître des modèles sonores, tels que ceux produits par des instruments de musique. [3]

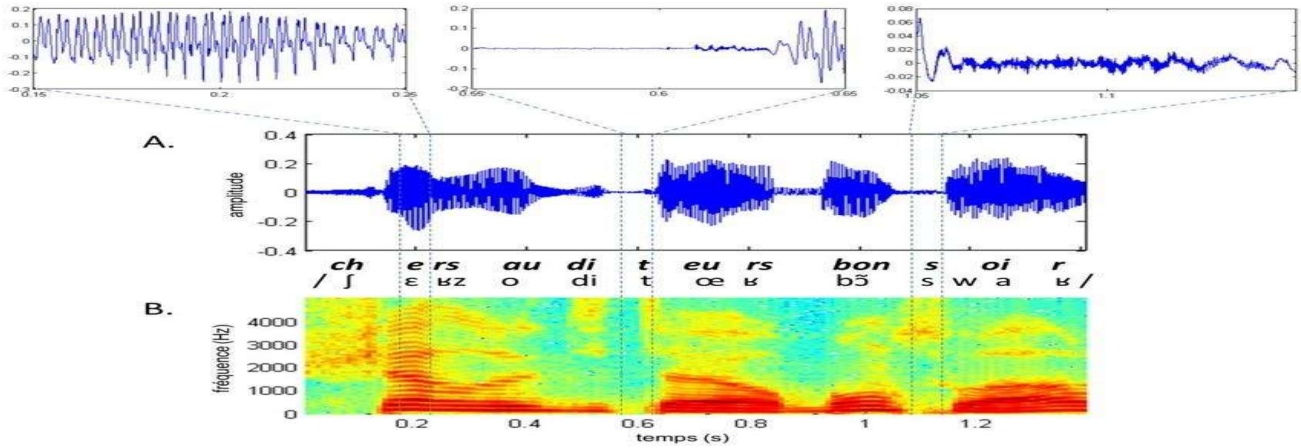

Figure I-4 Représentations de la phrase « Chers auditeurs, bonsoir. ».
A. Représentation temporelle du signal, ou forme d'onde, et agrandissements de certaines portions du signal correspondant aux phonèmes /ɛ/, /t/ et /s/.
B. Représentation temps-fréquence, ou spectrogramme, du même signal.[6]

I.8 Caractéristiques de son:

I.8.1 La durée :

La durée d'une unité est mesurée par le nombre d'images qu'elle contient. Pour calculer la durée de chaque trame, il faut fixer deux événements sur le signal de parole, et ces deux événements définissent la marque initiale et la marque finale de cette trame. Il représente le temps de prononciation d'un phonème. [1]

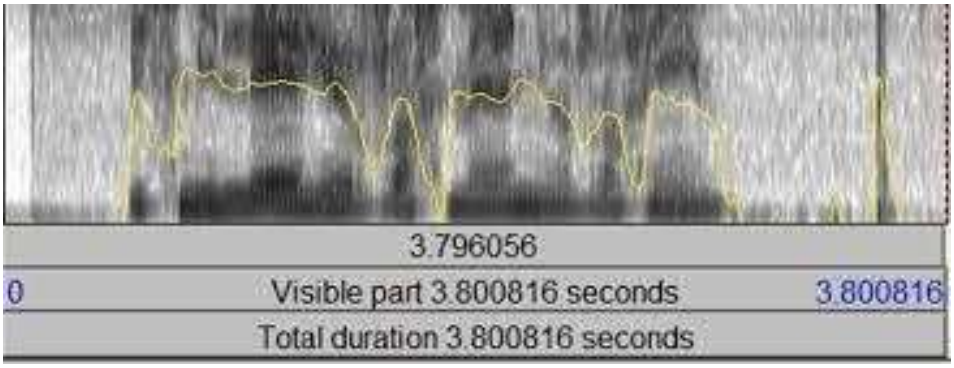

Figure I-5 vocal signal du temporelle L'évolution [1]

I.8.2 L'intensité :

L'intensité d'un son dépend directement de son amplitude. Elle caractérise ce que l'on entend par un son fort (c'est-à-dire qui tend à assourdir) ou faible (c'est-à-dire qui est presque inaudible). L'intensité I en un point donné diminue en fonction de la distance r qui sépare ce point de la source. [3] Elle est liée à la puissance P de l'émetteur par la formule :

I-2)

$$I = \frac{P}{4\pi r^2}$$

L'intensité sonore exprime en effet la puissance de la vibration sonore reçue par unité de surface à l'endroit où l'on se trouve. Son unité est donc le W/m².

En acoustique, l'intensité est cependant exprimée en décibels pour les raisons citées ci-dessous :

- Ils permettent de travailler avec des valeurs facilement manipulables (ni « trop grandes », ni « trop petites »).
- L'oreille humaine perçoit l'intensité sonore de façon logarithmique.

Dans le standard international, on a pris comme intensité de référence I0 W/m² le seuil d'audibilité de l'oreille humaine pour un son de fréquence 1000 Hz.

L'intensité acoustique (qui s'exprime en dB) est définie par :

I-3)

$$L = 10log\frac{I}{I_0}$$

Le seuil d'audition de notre oreille se situe à 0 dB et le seuil de douleur à 120 dB. [3]

I.8.3 La hauteur :

La hauteur d'un son est le paramètre qui distingue un son grave (ou bas) d'un son aigu (ou élevé). Cela dépend directement de la fréquence. Plus la fréquence est élevée, plus le son est aigu et inversement, plus la fréquence est basse, plus le son est grave. [3]

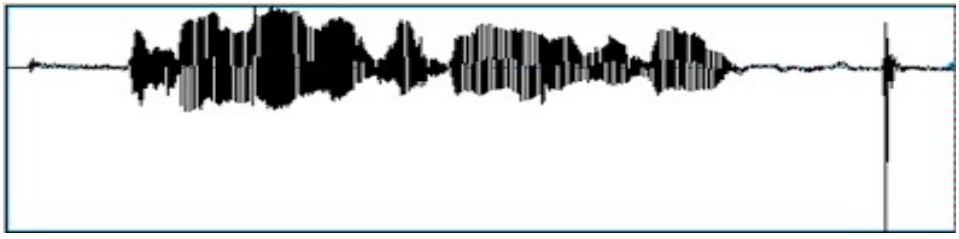

Figure I-6 Évolution de la fréquence de vibrations des cordes vocales [1]

I.8.4 Le timbre :

Le timbre est l'empreinte vocale qui permet de reconnaître la voix d'une personne, ou d'un instrument. Il est caractérisé par la fréquence des harmoniques, leur nombre, leur amplitude.[3]

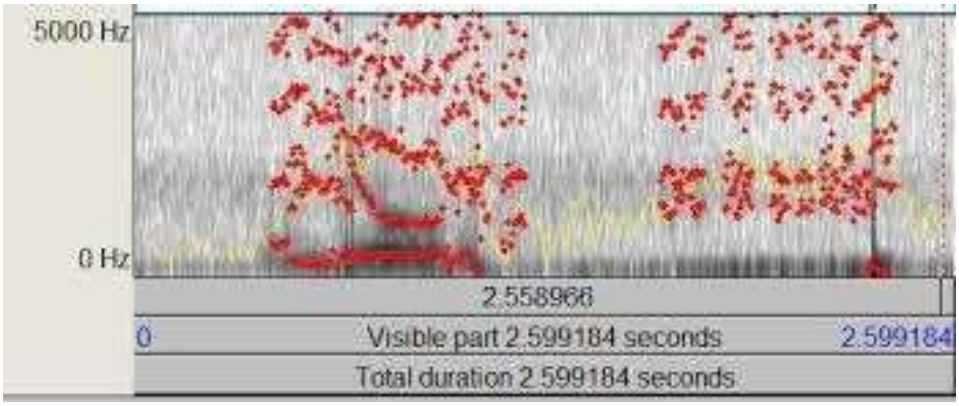

Figure I-7 L'Intensité et le timbre de parole [1]

- D'autres caractéristiques physiques dépendent du placement source-auditeur comme : La localisation dans l'espace ou l'orientation par rapport à l'auditeur ou directement de l'auditeur : la conjugaison des stimuli ou l'imprévisibilité

Tableau I-2: Liaisons entre critères d'appréciation généraux et caractéristiques physiques d'un évènement sonore [5]

Critères d'appréciations	Type de son	Caractéristiques globales	Caractéristiques physiques
Intelligibilité	Environnement	Identification de la source	Hauteur
			Timbre
			Durée
		Localisation dans l'espace	Eloignement de la source (Intensité…)
			Orientation par rapport à l'auditeur
	Parole	Compréhension du vocabulaire	Hauteur
			Timbre
			Durée
			Intensité
	Musique	Identification de l'instrument	Timbre
			Durée
			Intensité
			Hauteur
		Identification des plans sonores (mélodie/rythme/harmonie...)	Timbre
			Durée
			Intensité
			Hauteur
		Localisation dans l'espace	Eloignement de la source (Intensité)
			Orientation par rapport a l'auditeur
Gene occasionnée	Environnement Parole Musique	Son trop fort	Intensité
		Son trop long	Durée
			Répétitive
		Son désagréable	Hauteur
			Timbre
		Son agressif	Localisation dans l'espace
			Imprévisibilité
Esthétique	Environnement	Nature de l'environnement	Timbre/Durée/Intensité/Localisation des sources
		Harmonie générale	Ambiance sonore
		Relation avec les autres sens	Conjugaison des stimuli
	Parole	Nature de la voix (femme/homme)	Timbre/Durée/Intensité/Localisation des sources
		Emotion	Timbre/Durée
	Musique	Nature des instruments	Timbre/Durée/Intensité/Localisation des sources

I.9 Propriétés spécifiques des signaux de parole :

I.9.1 Continuité :

Le langage parlé est une séquence continue de sons sans séparation entre les mots. Le silence est généralement une pause aléatoire dans la respiration. Il y a très probablement un espace silencieux au milieu d'un mot et aucun espace entre deux mots consécutifs. [1]

I.9.1 Variabilité :

La parole présente une très grande variabilité due à un certain nombre de facteurs, qu'il s'agisse du même locuteur ou de plusieurs locuteurs. Ces facteurs comprennent les interférences du microphone (selon le type, la distance et l'orientation) et l'environnement (bruit, réverbération). [1]

I.10 Conclusion :

Dans ce chapitre nous avons exposé des notions de base sur la généralité et la production de la parole, des spécifications du signal vocal et quelques caractéristiques de son.

Les objectifs de ce chapitre sont de définir les notions que nous utiliserons dans notre travail.

Chapitre 2 : Notions sur la cryptographie et les fonctions chaotique

II.1 Introduction :

Le chaos a fait l'objet de nombreuses recherches intensives, il peut donc être introduit dans divers domaines.

Dans ce chapitre, nous avons introduit les concepts de cryptographie, l'objective de cryptage et les types des chiffrements accompagnés avec trois tests pour mesurer le cryptage d'information (le PSNR, la corrélation et la sensibilité de la clé). Ensuite nous avons identifié au sens général le chaos accompagnés avec quelque fonction chaotique est leurs caractéristiques, nous nous intéressons aux ces systèmes dynamiques chaotiques en précisant leurs caractéristiques et notre but dans crée un algorithme de cryptage a base se ces caractéristiques.

II.2 La cryptographie :

II.2.1 Historique sur la cryptographie :

L'antiquité Vers 600 ans avant J.-C, le roi de Babylone Nabuchodonosor écrivait le message qu'il souhaitait transmettre à ses généraux, sur le crâne préalablement rasé de ses esclaves. Il attendait que leurs cheveux repoussent avant de les envoyer chez ces généraux, qui rasaient de nouveau les cheveux des messagers pour lire le texte.

Dans la Xème et VIIème siècle avant J.-C les Grecs ont utilisé le chiffrement de la scytale spartiate c'est un exemple de chiffrement par transposition. Des lettres étaient écrites sur une longue et mince bande de cuir enveloppée autour d'un cylindre, pour déchiffrer ces lettres, il devait faire un cylindre d'un diamètre identique à celui utilisé pour le chiffrement, il lui suffit d'enrouler la scytale autour de ce cylindre pour obtenir les lettres en clair. Le diamètre du cylindre était la clé.

Dans 200 avant J.-C apparait les premiers systèmes de cryptographie, ce sont les chiffrements par substitution ; il existe 4 types de substitutions : Mono-alphabétique : Remplace chaque lettre du message par une autre lettre de l'alphabet. Poly-alphabétique : Utilise une suite de chiffres mono-alphabétiques "la clé" réutilisée périodiquement. Homophonique : Fait correspondre à chaque lettre du message en clair un ensemble possible d'autres caractères. Polygrammes : Substitue un groupe de caractères dans le message par un autre groupe de caractères. Dans le1 er siècle avant J.-C lorsque Jules César envoyait des messages à ses généraux, il ne faisait pas confiance à ses messagers. Il remplaçait donc tous les A contenus dans ses messages par des D, les B par des E, et ainsi de suite pour tout l'alphabet. Seule la personne connaissant la règle du "décalage par trois" pouvait déchiffrer ses messages. Et voilà comment tout a commencé. [7]

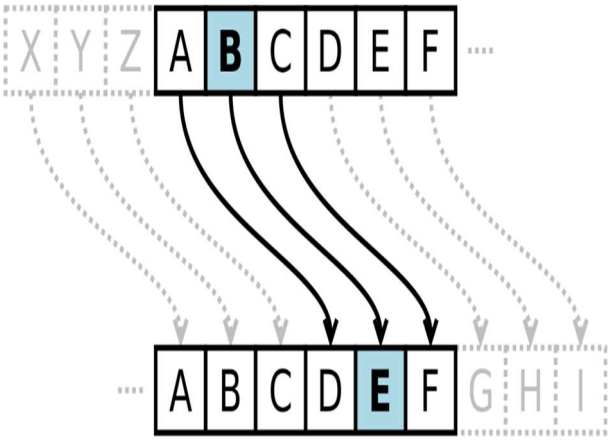

Figure II-1 Chiffrement de César

En 1918, l'Allemand Arthur Scherbius donne naissance à la célèbre machine Enigma, dont le principe est de remplacer une lettre par une autre, et les règles de remplacement de cette machine changent à chaque lettre. Avec le développement de la technologie électronique et l'émergence d'ordinateurs puissants et le développement des technologies de communication, la sécurité de l'information est devenue un nouvel enjeu, non seulement la confidentialité, mais aussi la préservation du contenu des messages et la garantie de l'identité des expéditeurs et des destinataires.

En 1970, les efforts de recherche d'IBM pour trouver de nouvelles méthodes de cryptage ont

Figure II-2 Enigma (Machine)

conduit au développement du DES (Data Encryption Standard).

En 1976, WhitField et Martin Hellman ont proposé la cryptographie à clé publique. En 1978, trois mathématiciens américains, Rivest, Shamir et Adleman, ont proposé le système de cryptage à clé publique RSA, qui a conduit à la croissance explosive des applications de cryptage civiles. Les deux derniers algorithmes de chiffrement à clé publique et à clé secrète révolutionnent aujourd'hui le monde de la cryptographie. [7]

II.2.2 Généralités sur le cryptage :

Chiffrer ou (encryptage, chiffrement, chiffrer) peut être défini comme une fonction transformation réversible des données en tenant compte de la protection des informations toute connaissance du contenu (confidentialité) ou modification inappropriée (intégrité). Le cryptage est conçu pour assurer la sécurité et l'incompréhensibilité des informations. [8]

II.2.3 Définition de la cryptographie :

La cryptographie est la science du secret, en premier lieu elle a été réservée uniquement aux relations diplomatique ou militaire, ensuite elle s'est généralisée. Son objectif est l'étude des méthodes permettant d'assurer les services d'intégrité, d'authentification, de confidentialité,

et du non répudiation dans les systèmes d'information et de communication

Cryptographie **:** science de l'écriture secrète, qui nous permet de stocker et de transmettre les données sous une forme qui est disponible uniquement pour les individus auxquels elles sont destinées.

Crypto-système : est l'ensemble des deux méthodes de chiffrement et de déchiffrement, il est le matériel ou logiciel de mise en œuvre de la cryptographie, qui transforme un texte clair en un texte chiffré et de retour au clair.

Chiffrement : C'est l'opération qui permet de transférer un texte en clair à un texte chiffré c'est-à-dire le rendre incompréhensible aux personnes qui ne possèdent pas une clé de déchiffrement.

Déchiffrement **:** C'est l'opération inverse de chiffrement, elle permet de retrouver le texte en clair à partir du texte chiffré à l'aide d'une clé de déchiffrement c'est-à-dire le texte sera compréhensible. [9]

II.2.4 Notions sur le chiffrement

Stéganographie : Contrairement à la cryptographie, la stéganographie consiste à intégrer un message dans un autre, et certains mots doivent être lus pour découvrir le texte caché.

Cryptage : comprend la conversion d'un message en clair en un message crypté en lui appliquant des fonctions de cryptage.

Déchiffrer : représente une opération de cryptage inversé, qui consiste à convertir un message codé en texte clair en possédant une clé ou une fonction de décryptage.

Décryptage : comprend la traduction d'un message codé en un message en clair sans posséder de clé ou de capacité de décryptage.

Effacer le message : spécifie le message avant le chiffrement.

Message crypté : également appelé mot de passe, fait référence à un message crypté.

Crypto-système : Il est défini comme un ensemble de clés possibles(keyspace), d'éventuels textes clairs et chiffrés associés à un algorithme donné.

Clé : représente les paramètres impliqués et autorisant des opérations de chiffrement et/ou de déchiffrement. [10]

II.3 Les types de *chiffrement:*

Ilya clé secrète symétrique, et clé secrète asymétrique.

D'une façon formelle un crypto-système est caractérisé par les éléments $(P;C;K;E;D)$ où :

• *P* est l'ensemble des textes clairs possibles,
• *C* est l'ensemble des textes chiffrés possibles.
• *K* est l'espace des clés.
• *E* est l'ensemble des fonctions de chiffrement,
• *D* est l'ensemble des fonctions de déchiffrement. [7]

II.3.1 Chiffrement symétrique :

On dit que le chiffrement est symétrique si la clé de chiffrement et la clé de déchiffrement sont identiques (la même clé est utilisée pour le chiffrement et le déchiffrement). La clé de chiffrement peut être calculée à partir de la clé de déchiffrement et inversement. Les communicants doivent donc s'accorder à l'avance sur une clé, et cette clé doit être gardée secrète car la sécurité de la communication en dépend. [7]

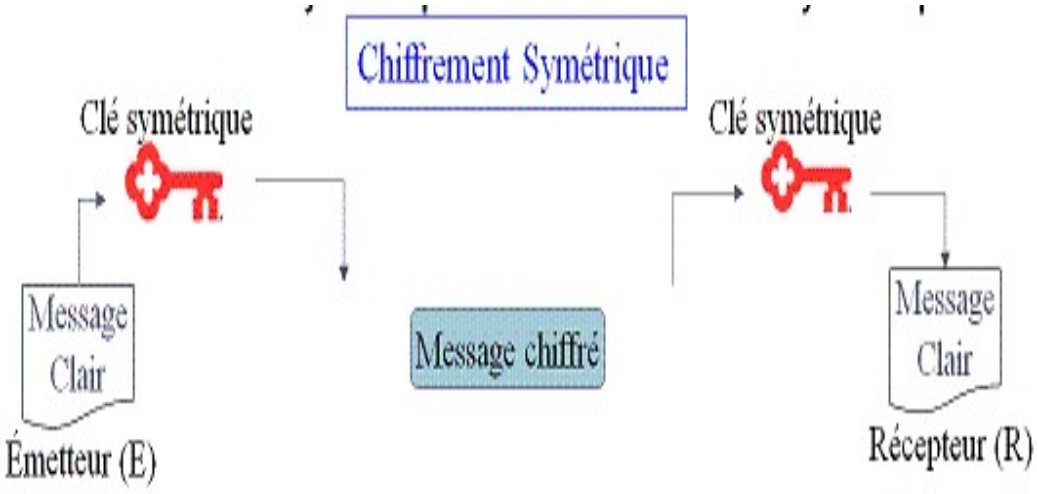

Figure II-3 Schéma explicatif de chiffrement symétrique

On distingue deux types de chiffrement dans cette famille : le chiffrement par blocs et le chiffrement par flot.

- Chiffrement par blocs : traite le message en clair par groupes de bits appelés bloc, chaque bloc est chiffré l'un après l'autre.
- Chiffrement par flot : appelé aussi chiffrement continu, traite l'information bit à bit.

Quelque exemple de systèmes cryptographiques qui utilise le chiffrement symétrique : DES (Data EncryptionStandard)[11], 3DES (Triple-dataEncryptionStandard), RC4 (RivestCipher 4)[12], RC5, AES (AdvencedEncryptionStandard), chiffre césar.

II.3.2 Chiffrement asymétrique :

Le chiffrement asymétrique utilise deux clés une clé pour le chiffrement et une deuxième clé différente pour le déchiffrement. Ce chiffrement est appelé aussi chiffrement à clé publique. La clé secrète ne peut pas être déduite facilement à partir de la clé publique, donc il faut garder la clé privée secrètement mais la clé publique on peut la diffuser même sur des canaux pas sûrs [7]

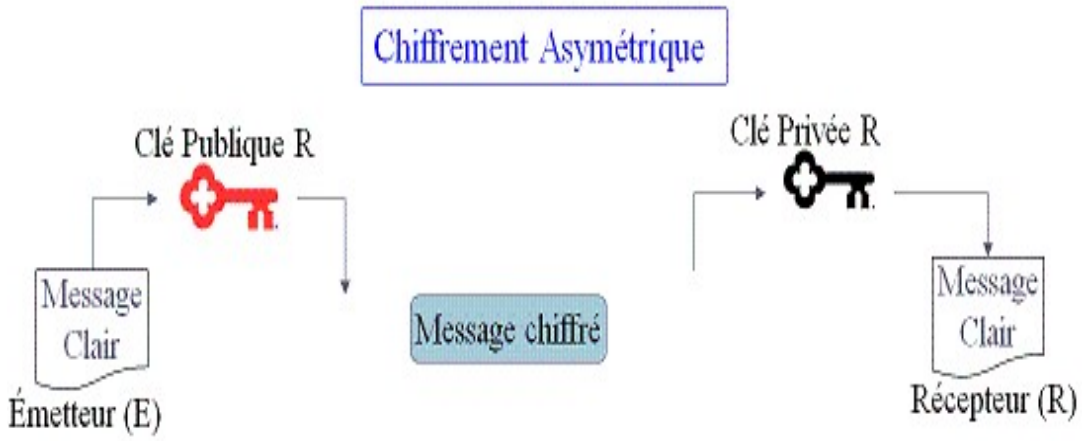

Figure II-4 Schéma explicatif de chiffrement asymétrique

Ce concept de chiffrement a été inventé par Whitfield Diffie et Martin Hellman en 1976[13]. Elle a pour but de résoudre le problème posé dans le chiffrement symétrique ce qui concerne la distribution de la clé de chiffrement. Quelque exemple de systèmes cryptographiques qui utilise le chiffrement asymétrique : RSA [14] : (RivestShamirAdleman) c'est un algorithme utilisé pour chiffrer les données ou pour les signé, Diffie-Hellman [13] : c'est un protocole d'échange des clés. DSA [15] :(Digital Signature Algorithm) c'est un algorithme de signature. ElGamal[16]: c'est un algorithme utilisé à la fois pour le chiffrement et pour la signature.[7]

II.4 Objective de la cryptographie :

La cryptographie a traditionnellement été utilisée pour masquer les messages de certains utilisateurs. Cette utilisation est d'autant plus intéressante aujourd'hui que les communications sur Internet circulent dans des infrastructures où la fiabilité et la confidentialité ne peuvent être garanties. Désormais, la cryptographie est utilisée non seulement pour protéger la confidentialité des données, mais aussi pour garantir l'intégrité et l'authenticité des données.

- **Confidentialité :** comprend le fait de rendre les informations compréhensibles pour des personnes autres que les participants à la transaction.

- **Intégrité :** la vérification de l'intégrité des données consiste à déterminer si les données n'ont pas été modifiées pendant la communication.
- **Authentification :** consiste à s'assurer de l'identité de l'utilisateur, c'est-à-dire assurer à chaque correspondant que son partenaire est bien ce qu'il croit être un partenaire dont le contrôle d'accès peut permettre (par exemple via un mot de passe qui doit être crypté) d'accéder à la ressource aux seules personnes autorisées.
- **Non-répudiation :** L'information est l'assurance qu'aucun correspondant ne peut nier la transaction. [17]

II.5 Système dynamique :

II.5.1 Définitions :

En général, un système dynamique décrit un phénomène (mécanique, physique, économique, environnemental ou tout autre domaine) son état (un ensemble de grandeurs suffisantes pour définir le système) qui évolue dans le temps, le mot « système » fait référence à un ensemble de variables d'état Par conséquent, l'étude de l'évolution d'un système nécessite donc la Connaissances :

- Son état initial, c'est-à-dire son état à l'instant t0 ;
- Ses Lois évolutives. [18]

II.5.2 Représentation mathématique :

- **En temps Continu :** Dans le cas continu, le système dynamique est régi par un système d'équations différentielles

II-1)

$$\frac{dx}{xt} \equiv \dot{x} = f(x,t,v) x_k \in U \subseteq R_n, v \in V \subseteq R_p$$

- **En temps Discret :** Un système dynamique dans le cas discret, représenté par une équation aux différences, également appelée équation de récurrence

II-2)

$$x_{k+1} = f(x_k, v) x_k \in U \subseteq R_n, v \in V \subseteq R_p, k = 1,2,\dots$$

S'appellent des systèmes dynamiques. R n est l'espace des phases, R p est l'espace des paramètres [19]

II.6 Théorie du Chaos :

II.6.1 Historique :

Henri Poincaré fut l'un des premiers à entrevoir la théorie du chaos. Il découvrit la notion de sensibilité aux conditions initiales à travers le problème d'interactions de trois corps célestes, et a écrit « Une cause très petite, qui nous échappe, détermine un effet considérable que nous ne pouvons pas ne pas voir et alors nous disons que cet effet est dû au hasard ». Plus tard, en 1961, Edward Lorenz météorologue et professeur de mathématique au MIT observa par hasard le phénomène qui s'appellera plus tard la théorie du chaos ou le chaos déterministe, à la suite des calculs visant à prévoir les phénomènes météorologiques. Ces prévisions nécessitaient un grand nombre de calculs d'équations différentielles complexes à très grand nombre de variables impossibles à faire à la main, il a utilisé alors un ordinateur, son Royal Mcbee LGP-300 qui est entrée dans l'histoire de la théorie du chaos, et qui a fait de Lorenz le père officiel de cette théorie puisque les calculs des systèmes chaotiques régissant ces phénomènes étaient difficiles à comprendre et à simuler sans ordinateur. Après plusieurs heures de calculs, Lorenz avait obtenu une série de résultats et a décidé de repasser une deuxième fois ces résultats dans l'ordinateur pour s'en assurer. Pour gagner du temps, il avait entré les variables avec trois chiffres après la virgule, au lieu de six, il pensait qu'une faible variation dans les variables à la base d'un calcul aurait une incidence du même ordre de grandeur sur le résultat final mais à sa grande surprise, les résultats étaient totalement différents de la première série. Il venait de découvrir le comportement chaotique d'un signal non linéaire ; soit, d'infimes différences des conditions initiales d'un système déterministe entraineraient des résultats complètement différents. Ce phénomène, qui traduit cette sensibilité aux conditions initiales, est connu sous le nom d'effet papillon : « Le simple battement d'aile de papillon au Brésil pourrait déclencher une tornade au Texas » [19]

II.6.2 Définition :

Le chaos est un phénomène non linéaire complexe qui repose sur plusieurs paramètres, qui se caractérisent par une extrême sensibilité aux conditions abréviation. Un système chaotique est un système dont la trajectoire évolue d'une certaine manière Les régions délimitées présentent des caractéristiques stables mais ne convergent pas vers un point Cycles fixes ou limites. Ces trajectoires qui restent denses dans la région sont très sensible aux conditions initiales. Solutions aux équations différentielles non linéaires Ne peut pas être calculé analytiquement avec précision car il n'y a pas de méthode La résolution analytique de ces équations, à l'exception de certaines catégories spécifiques. Le comportement du système est ensuite déterminé numériquement et analysé par simulation [10]

II.6.3 Propriétés des systèmes chaotiques :

Parmi les caractéristiques principales permettant d'évoquer un comportement chaotique, on peut retenir les propriétés suivantes :

II.6.3.1 Déterminisme et imprévisibilité :

Dans le cas d'un système déterministe, la connaissance de l'état initial de l'entrée et du modèle permet théoriquement de prédire l'état futur du système. Cependant, il est difficile de calculer des solutions analytiques théoriques pour certains systèmes non linéaires, ce qui est le cas des systèmes chaotiques déterministes, car ils sont caractérisés par une sensibilité aux conditions initiales, et de simples erreurs de mesure ou de simples arrondis peuvent conduire à des solutions différentes, ce qui les rend imprévisible, donc la prévisibilité n'a plus à voir avec la certitude. [10]

II.6.3.2 Aspect aléatoire :

Bien que les systèmes chaotiques soient déterministes, tous les états des systèmes chaotiques ont des aspects aléatoires. [19]

II.6.3.3 Attracteur étrange :

Lorsque Edward Lorenz entreprit graphiquement la solution de son système À l'aide de son ordinateur, tracez deux courbes avec deux ensembles de conditions initiales très proches, il s'attendait à ce que les deux courbes se séparent, mais à sa grande surprise, les deux courbes sont plus ou moins les mêmes, elles ressemblent à deux ailes Papillon.

Le physicien David Ruelle, qui a étudié le problème, a décrit le nombre comme " d'attracteur étrange" souligne que les trajectoires ne se croisent jamais, bien qu'elles évoluant apparemment

au hasard, ils forment des personnages incontestablement identifiables.

Ainsi, lorsque l'état du système est chaotique, l'attracteur correspondant est un attracteur étrange qui a des propriétés topologiques différentes d'un attracteur simple.

Un attracteur étrange se caractérise par son pot attractif et sa dimension fractale. [10]

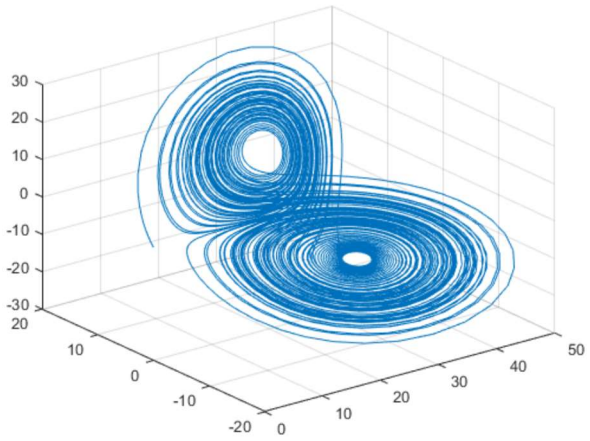

Figure II-5 Exemple d'attracteur étrange

II.6.4 Exemples de quelques fonctions chaotiques :

La combinaison de cartes chaotiques en une combinaison non linéaire de deux cartes chaotiques différentes peut être représentée comme une seule carte par l'expression :

II-3)

$$x_{n+1} = A_{FG} = \big(F(a, x_n) + G(b, x_n)\big)\ mod\ 1$$

Ou $F(a, x_n)$ et $G(b, x_n)$ sont deux textures chaotiques 1D avec les paramètres a et b, et n est le nombre d'itérations. La combinaison proposée de systèmes chaotiques est basée sur des cartes logistiques et cubiques, [18] définies comme suit :

II.6.4.1 Logistic Map :

Le diagramme logistique est l'une des fonctions chaotiques bien connues

Des recherches ont été menées pour des applications cryptographiques. [18] La fonction logistique est représentée par :

II-4)

$$x_{n+1} = r.x_n.(1 - x_n)$$

Ou X(N) prend la valeur dans l'intervalle [0, 1], le paramètre est une constante et la valeur maximale est 4. Sa valeur détermine R=3,57 Et explorez le comportement des cartes logistiques. L'itération devient désordonnée.

II.6.4.2 CUBIC MAP :

La cartographie cubique est une autre forme de cartographie chaotique qui est le plus couramment utilisée pour générer des séquences chaotiques. C'est un de Cartes les plus couramment utilisées pour les applications cryptographiques. [18] Cette carte est Formellement définie comme :

$$x_{n+1} = r.x_n.(1 - {x_n}^2) \quad \textit{II-5)}$$

Où r est son argument et X(N) est un variable système avec la valeur (0, 1) A i> 0. La méthode montre une dynamique chaotique de 2,3< r < 2,6.

II.6.4.3 Carte chaotique combinée :

Le système chaotique proposé est une combinaison d'une carte logique et d'une carte cubique, en introduisant chaque combinaison avec une fonction exponentielle, puis en appliquant Arithmétique modulo aux unités.[18] La soustraction entre la logistique et la cartographie cubique donne un nouveau système chaotique, exprimé comme suit :

$$x_{n+1} = r.e^{2x_n}.(1 - e^{x_n})\ mod\ 1 \quad \textit{II-6)}$$

II.6.5 Identification du chaos :

Comme il est difficile de calculer la solution analytique des systèmes chaotiques, des méthodes numériques sont utilisées. Dans cette section, nous présentons quelques outils qui permettent d'identifier le comportement chaotique d'un système dynamique et ses caractéristiques. [10]

II.6.5.1 Exposants de Lyapunov:

Les valeurs propres de la matrice dynamique A du système linéaire permettent Caractériser le point d'équilibre et sa stabilité. L'exposant de Lyapunov est généralisation de ces valeurs propres et permet la caractérisation des attracteurs (ou le comportement des systèmes non linéaires, en particulier leurs propriétés chaotiques ou hyper chaotique).

L'exposant de Lyapunov est la quantité qui quantifie la divergence exponentielle (ou-convergence) de la trajectoire autour d'un temps donné dans l'attracteur Systèmes dynamiques, qui peuvent également quantifier la sensibilité aux conditions Dans le cas des systèmes à temps continu et des systèmes à temps discret. [10]

II.6.5.1.1 Méthode directe de Lyapunov :

Considérons le système suivant :

$$E_{k+1} = f(E_k) \qquad \textit{II-7)}$$

Où : $\epsilon_k = \left[\epsilon_k{}^{(1)} \dots \epsilon_k{}^{(n)}\right]^T \in R^n$ et la fonction $f = [f_1 \dots f_n]^T$ et continument dérivable sur R^n

Dans la méthode directe, également connue sous le nom de seconde méthode de Lyapunov, On cherche une fonction scalaire de type "énergétique" qui admette Différence négative entre deux états consécutifs. Cette fonction s'appelle Fonction de Lyapunov.

Une fonction de Lyapunov est une fonction scalaire V:$R^n \rightarrow R$, continue en ϵ_k, telle que:

1. V (0) = 0,
2. $V(\epsilon_k) > 0, \forall \epsilon_k \neq 0$
3. $V(\epsilon_k) \rightarrow \infty$, si $\epsilon_k \rightarrow \infty$

La méthode directe est basée sur le principe de perte d'énergie d'un système. En effet, si l'énergie du système se dissipe continument, c'est-à dire décroît avec le temps, alors ce système tend à se ramener à un état d'équilibre stable.

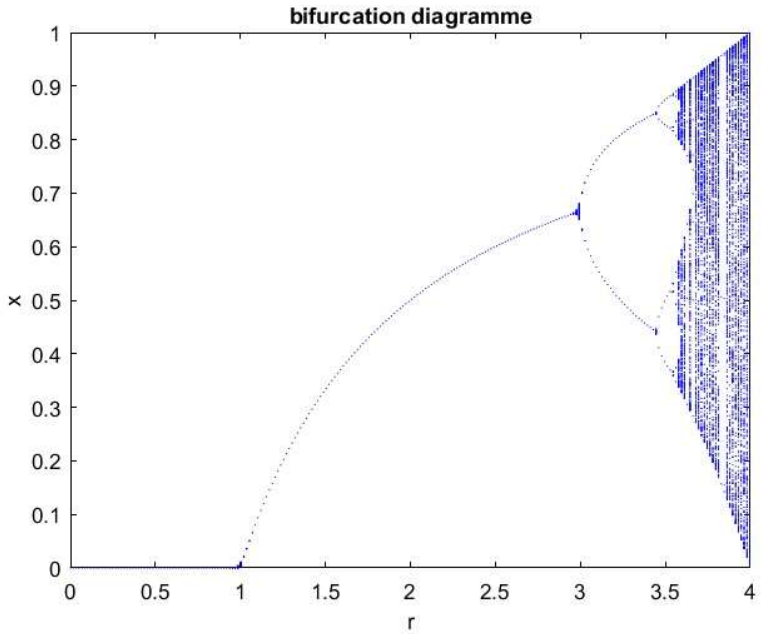

Figure II-6 Diagramme de bifurcation de la carte logistique

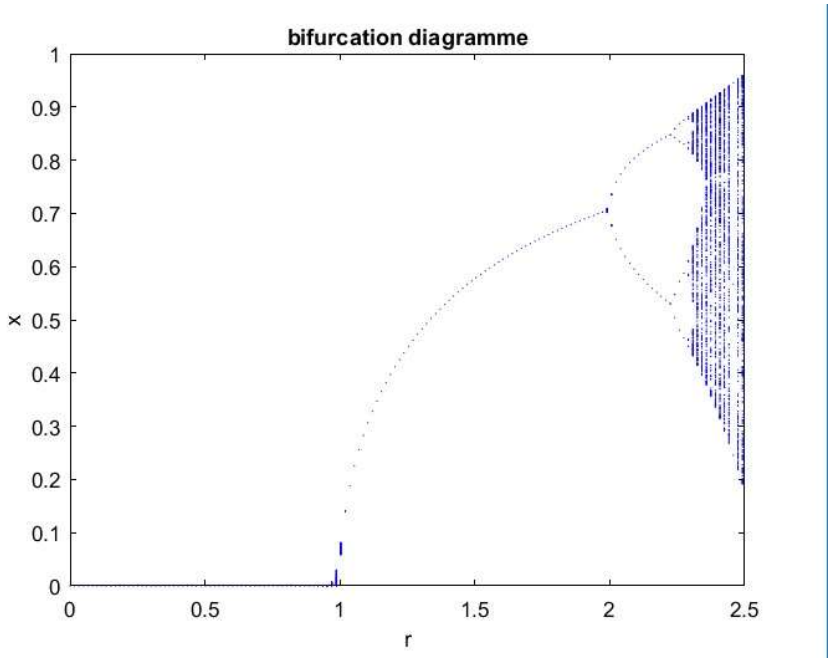

Figure II-7 Diagramme de bifurcation de la carte cubique

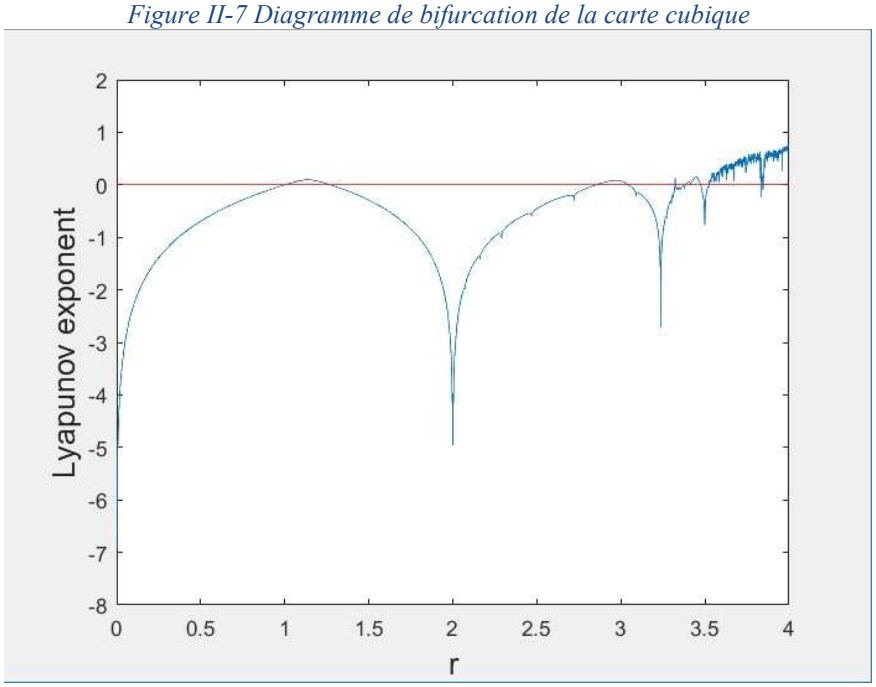

Figure II-8 Exposant de Lyapunov la carte cubique logistique

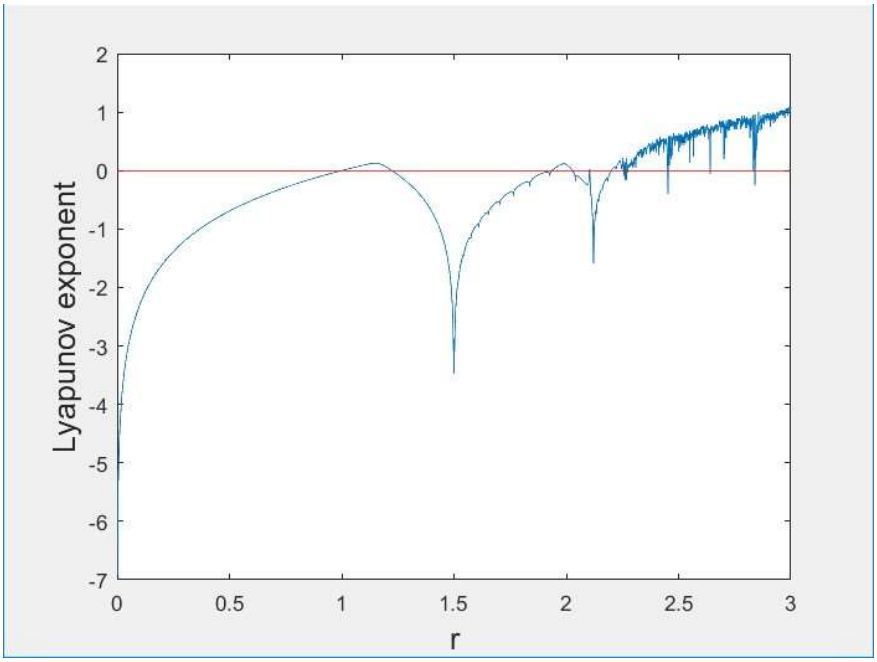

Figure II-9 Exposant de Lyapunov de la carte cubique

II.6.5.2 Bifurcation :

Une bifurcation est un changement qualitatif des propriétés d'un système non linéaire, telles que la stabilité, le nombre de points d'équilibre ou les propriétés d'un état permanent, et les paramètres dont les modifications quantitatives conduisent à des changements dans l'état dynamique du système sont appelés paramètres de bifurcation. [10]

- **Diagramme de Bifurcation**

Un diagramme de bifurcation est un dessin qui évalue rapidement toutes les solutions possibles d'un système et sa stabilité en fonction des changements dans l'un des paramètres du système. Il peut également localiser la valeur spécifique du paramètre qui a provoqué la bifurcation. Il représente l'intervalle dans lequel la solution asymptotique évolue avec les paramètres, et classe la valeur du paramètre sur l'axe des abscisses et la valeur d'une des variables d'état sur l'axe des ordonnées. [10]

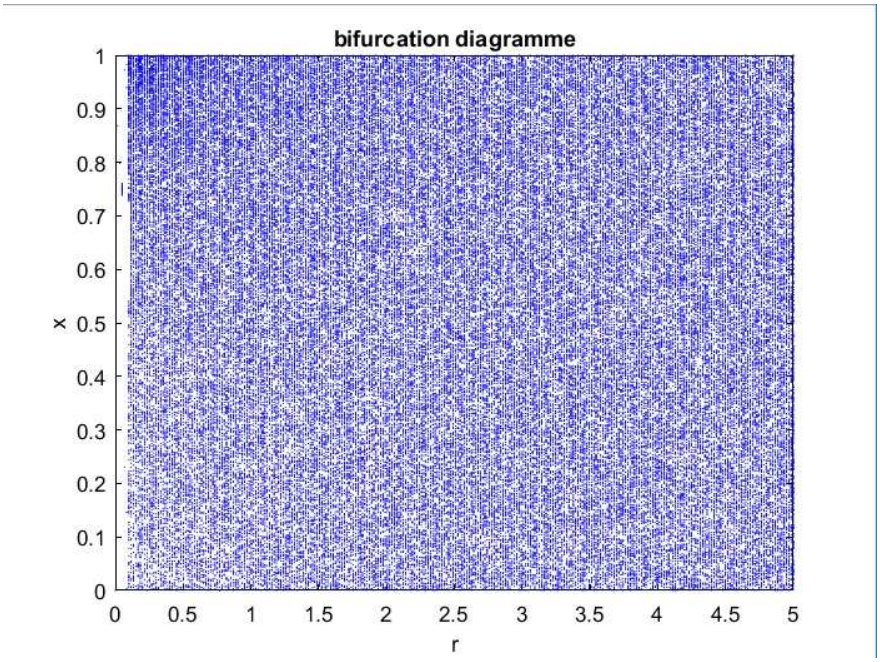

Figure II-10 Diagramme de bifurcation de Carte chaotique combinée

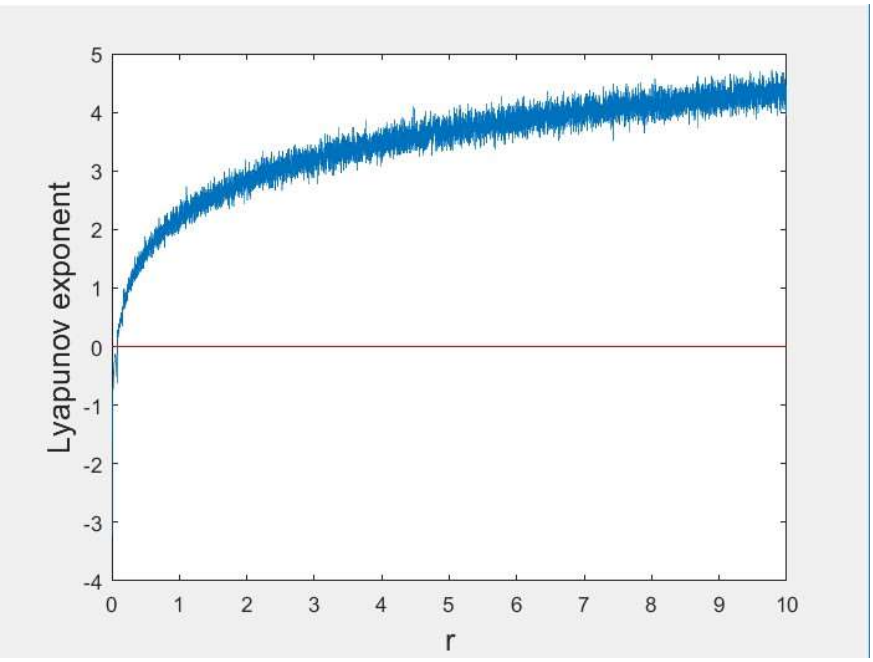

Figure II-11 Exposant de Lyapunov de la Carte chaotique combinée

II.6.5.3 Sensibilité aux conditions initiales :

La sensibilité aux conditions initiales est l'une des caractéristiques fondamentales des systèmes chaotiques que Lorenz a expliqué dans sa célèbre citation : "l'effet papillon". De petits changements dans les conditions initiales sur un système chaotique peuvent amener les deux trajectoires à se rapprocher initialement puis à diverger de manière exponentielle, après quoi les deux trajectoires sont incomparables, rendant le système chaotique imprévisible à long terme.

Il est donc clair que la moindre erreur ou imprécision dans les conditions initiales ne détermine à aucun moment quelle trajectoire elle suivra réellement. [19]

x01= 0.58 and x01 = 0.58 + 10^{-16} .

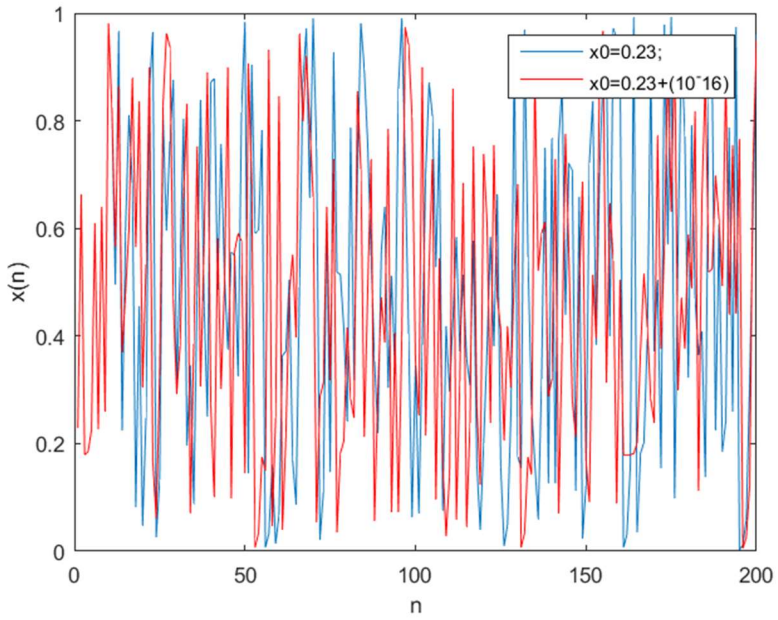

Figure II-12 Évolution de la carte combinée pour deux conditions initiales très proches

II.7 Cryptage par chaos :

II.7.1 Principe du cryptage par chaos :

Chaos chiffre les messages par superposition L'information initiale est un signal chaotique. Puis nous envoyons Messages noyés dans la confusion aux destinataires qui comprennent les caractéristiques Générateur de chaos. Il ne reste plus au destinataire qu'à soustraire l'encombrement de son message pour retrouver le message. [9]

Tableau II-1 : La correspondance entre la théorie du chaos et la cryptographie. [9]

Théorie du chaos	Cryptographie
Système chaotique	Système pseudo-chaotique
Transformation non linéaire	Transformation non linéaire
Nombre infini d'états	Nombre fini d'états
Nombre infini d'itérations	Nombre fini d'itérations
État initial	Plain text
État final	Cipher text
Condition initiale (s) et / ou paramètre (s)	Clé (s)
Indépendance asymptotique des états initiaux et finaux	Confusion
Sensibilité aux conditions initiale (s) et paramètre (s) i.e. mixage	Diffusion

II.7.2 Système de cryptage par chaos :

Le système de cryptage chaotique se compose de deux parties : Brouilleur et décrypteur. Ce sont exactement les mêmes pour s'assurer au mieux que les conditions initiales sont remplies. La synchronisation de l'appareil est établie dans le système récepteur, qui lance Le chaos est obtenu en injectant toutes les informations dans sa boucle de retard Le transport se superpose à une dynamique chaotique. Ce groupe constitue Système de cryptage symétrique à clé. Emetteur et Récepteur ont la même clé. La synchronisation représentera des étapes clés opération de déchiffrement. En raison de la complexité du comportement du signal perturbateur, la moindre déviation dans le processus de décodage peut provoquer Un parasite de l'information appelé bruit de décryptage. Des informations incorrectes peuvent rendre les informations illisibles. [9]

II.8 Mesures de performance de l'algorithme de cryptage et analyses :

II.8.1 Analyse différentielle :

Signal to Noise Ratio (SNR) :

Le test du rapport signal-bruit (RSB) est un estimateur idéal pour mesure de l'intelligibilité du signal vocal [18]. Le la métrique du domaine temporel populaire est le SNR, qui est défini moyenne des valeurs de SNR des segments courts du signal de sortie et est calculé comme suit :

II-8)

$$SNR = 10log_{10}\frac{\sum_{i=1}^{N}(x^2(i))}{\sum_{i=1}^{N}(x(i)-y(i))^2}$$

Où x(i) est la parole d'origine, y(i) est le signal de parole décrypté et Ns est le nombre d'échantillons. Lorsque le SNR diminue, La qualité du signal crypté est supérieure.

PSNR(Peak Signal-to-Noise Ratio) :

Le PSNR (Peak Signal-to-Noise Ratio) calcule le rapport signal/bruit maximal (à décibels) entre les deux informations. Ce rapport est souvent utilisé comme mesure de la qualité entre l'informations originales et cryptées.

Plus le PSNR est élevé, meilleure est la qualité de l'information Le cryptage ou la reconstruction est très bonne.

L'erreur quadratique moyenne (MSE) et le rapport signal/bruit maximum (PSNR) sont Deux mesures d'erreur utilisées pour comparer la qualité d'informations. MSE signifie l'erreur Quadratique cumulatif entre les informations cryptées (IC) et les informations d'origine (IO), tandis que le PSNR représentant l'erreur maximale. Plus la valeur MSE est petite, plus l'erreur est faible. [19]

L'erreur quadratique moyenne (MSE) est défini par l'équation suivante :

II-9)

$$MSE = \left(\sum_{n}[io_i - ic_i]^2/n\right)$$

Le PSNR (Peak Signal-to-Noise Ratio)est défini par l'équation suivante :

II-10)

$$PSNR = 10log_{10}(R^2/MSE),\text{R=255}$$

II.8.2 Coefficient de correlation:

La fonction d'autocorrélation identifie le système chaotique qui produit un fort cryptage. Une mesure utile pour évaluer la qualité de chiffrement de tout crypto-système est le coefficient de corrélation entre des segments similaires dans le signal clair et le signal de chiffrement. Il est calculé comme suit :

II-11)

$$r_{xk} = \frac{c(x,k)}{\sqrt{v(x)}\sqrt{v(k)}}$$

Où C (x, k) est la covariance entre le signal original x et le signal chiffré k. V(x) et V(k) sont les variances des signaux x et k. La variance V(x) est calculée comme suit :

II-12)

$$E(x) = \frac{1}{N_s}\sum_{i=1}^{N_s}(x(i)$$

II-13)

$$v(x) = \frac{1}{N_s}\sum_{i=1}^{N_s}(x(i) - E(x))^2$$

II-14)

$$c(x,k) = \frac{1}{N_s}\sum_{i=1}^{N_s}(x(i) - E(x))(k(i) - E(k))$$

Où Ns est le nombre d'échantillons de parole. La faible valeur du coefficient de corrélation r_{xk}montre un chiffrement de bonne qualité. [18]

II.9 Conclusion :

Dans ce chapitre nous avons introduit des notions sur la cryptographie et des tests des mesures de la performance de cryptage accompagnées avec les caractéristiques de quelques fonctions chaotiques au but de crée un algorithme de cryptage de donnés basé sur ces caractéristiques

Le cryptage et la communication sécurisée est l'un des champs d'applications prometteur des systèmes chaotiques, en effet la cryptographie chaotique peut s'effectuer sous différents schémas, il s'agit de définir la façon d'introduire le message dans l'émetteur. Dans ce chapitre nous avons introduit des notions sur la cryptographie et la transmission de données accompagnées des méthodes de chiffrement à clé privé et à clé public, ainsi que le chiffrement à base du chaos qui utilise les propriétés d'un comportement chaotique pour la transmission de données confidentielles.

Chapitre 3 :

Implémentation est résultats de simulation

III.1 Introduction :

Dans ce chapitre, nous allons étudier le cryptage d'un signal parole en utilisant plusieurs fonctions chaotiques. Nous rappelons que le cryptage se réalise en deux phases : phase de permutation et phase de diffusion. Des signaux vocaux ayant une fréquence d'échantillonnage de 8kHz est une durée de 10 secondes ont été utilisés comme fichiers de test avec le total de 80000 échantillons pour chaque fichier. Plus précisément, nous allons étudier l'effet de l'utilisation de plusieurs fonctions chaotiques dans la phase de diffusion. Pour cela, nous allons utiliser trois fonctions chaotiques relevant de la littérature dans la phase de diffusion. En effet, les données relatives à la séquence du signal parole sont enregistrées dans le PC moyennant une application Matlab. Concernant la phase de diffusion, les données seront divisées en trois parties. Chaque partie lui est réservée une fonction chaotique. Pour tester les performances de cette technique, une comparaison au cryptage réalisé avec une seule fonction chaotique est également établie. Il est à noter que la phase de permutation est réalisée via l'emploi d'une seule fonction chaotique pour les deux méthodes de cryptage.

III.2 Schéma de cryptage du signal parole Proposé :

Le schéma de cryptage proposé consiste en deux phases : phase de permutation et phase de diffusion. Chacune des phases se réalise via l'emploi de fonctions chaotiques. Notre travail de cryptage s'inspire d'un travail de recherche récemment publié dans une revue internationale.[18]

- **Processus de chiffrement**

Le processus de chiffrement est illustré à la figure (III-1) et comprend les étapes suivantes :

Le schéma présente illustre le principe de base du cryptage utilisant une seule fonction chaotique pour chaque étape. [18]

- Étape 1 : Lecture ou enregistrement du signal vocal original.
- Étape 2 : Génération d'un vecteur avec une condition initiale x_1 et un paramètre de contrôle r_1.
- Étape 3 : Disposez le vecteur chaotique dans l'ordre décroissant pour former un vecteur de permutation.
- Étape 4 : Brouiller le signal vocal en utilisant le vecteur de permutation pour modifier de manière aléatoire les positions des segments du signal vocal en fonction du vecteur chaotique généré.
- Étape 5 : Pour la phase de diffusion, trois autres vecteurs chaotiques sont générés, avec d'autres paramètres, conditions initiales x_2, x_3, x_4, et paramètres de contrôle r_2, r_3, r_4, pour augmenter la sensibilité des clés secrètes et multiplier les éléments de ces vecteurs par 255.
- Étape 6 : Exécutez l'opération XOR bit par bit entre les vecteurs chaotiques générés et le vecteur permuté.
- Étape 7 : Obtenez et extrayez la sortie de la parole chiffrée.

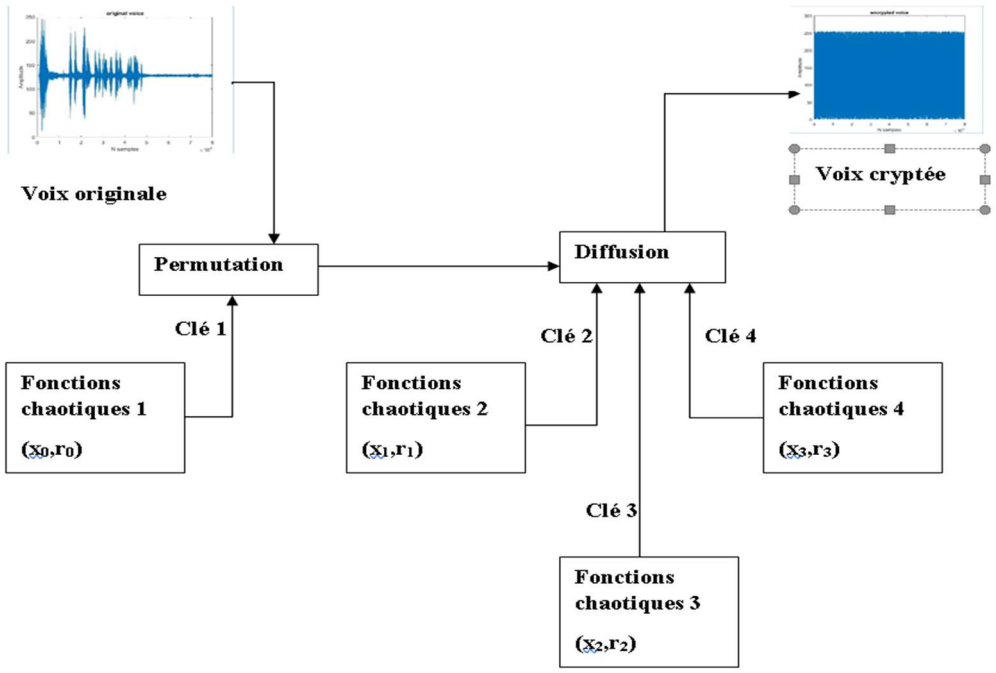

Figure III-1 Schéma modifié proposé pour le cryptage du signal de parole inspiré de la référence [18]

- **Processus de déchiffrement**

Après l'acquisition ou le chargement du signal crypté, l'opération prend le même chemin que le processus de cryptage, mais de façon inverse.

III.3 Fonctions chaotiques utilisée pour le cryptage de la parole :

Dans cette partie, nous allons décrire les deux techniques de cryptage. La première technique consiste en l'emploi de trois fonctions chaotiques pour la phase de cryptage à la différence de la première technique utilisant une seule. Quant à la permutation, les deux méthodes emploient une seule fonction chaotique.

III.3.1 Fonctions chaotiques utilisées pour la première méthode de cryptage :

(Une seule fonction pour la phase de et trois fonctions pour la phase de diffusion).

La première technique consiste en l'emploi de trois fonctions chaotiques pour la phase de diffusion

Phase de permutation :

III-1)

$$x_{n+1} = r.e^{-15.x_n}.(1 - e^{-15.x_n})$$

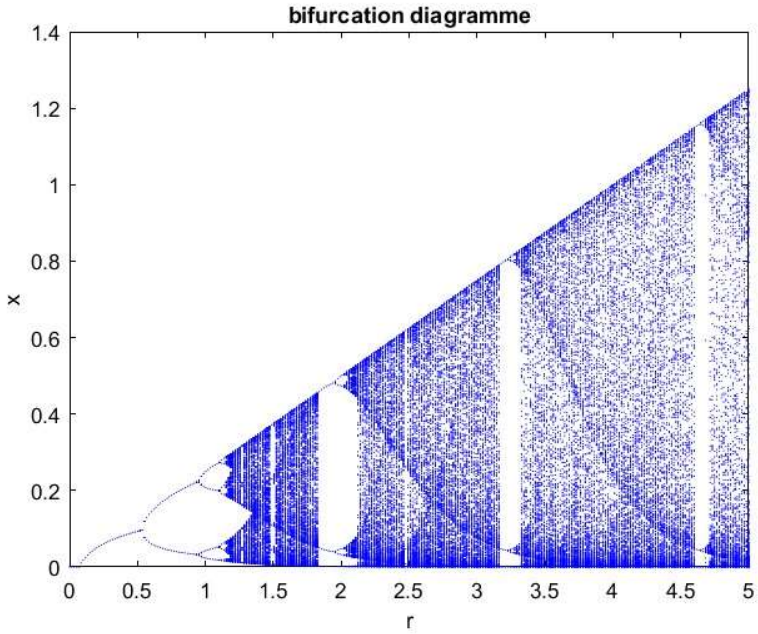

Figure III-2 Diagramme de bifurcation de la première fonction chaotique

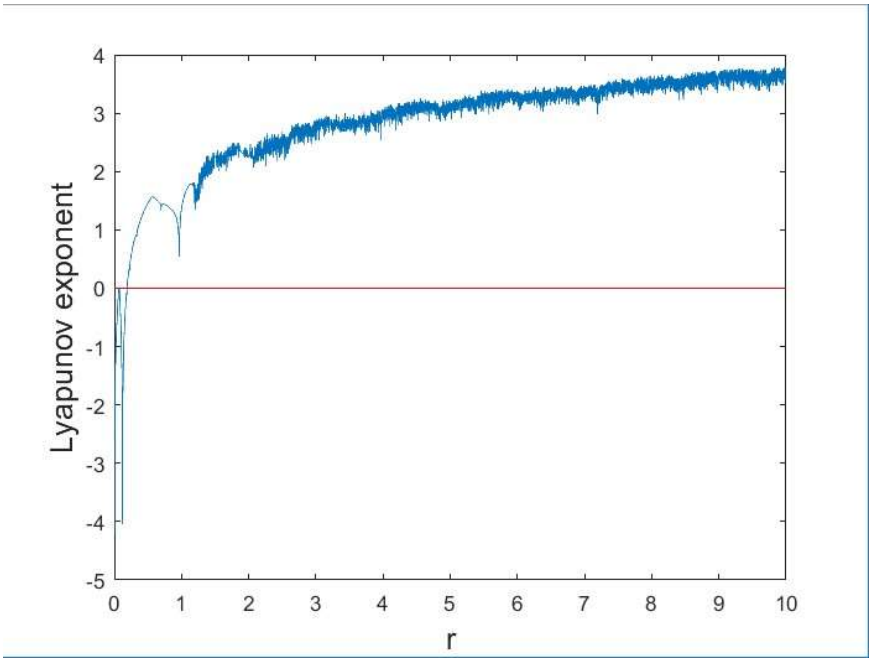

Figure III-3 Exposant de Lyapunov de la première fonction chaotique

Phase de diffusion : Les données seront divisées en trois parties. Chaque partie lui est réservée une fonction chaotique.

- **Partie 1 : à partir de l'échantillon 1 jusqu'à l'échantillon 20000**

III-2)

$$x_{n+1} = r.e^{x_n}.(1 - e^{x_n}) \; mod \; 1$$

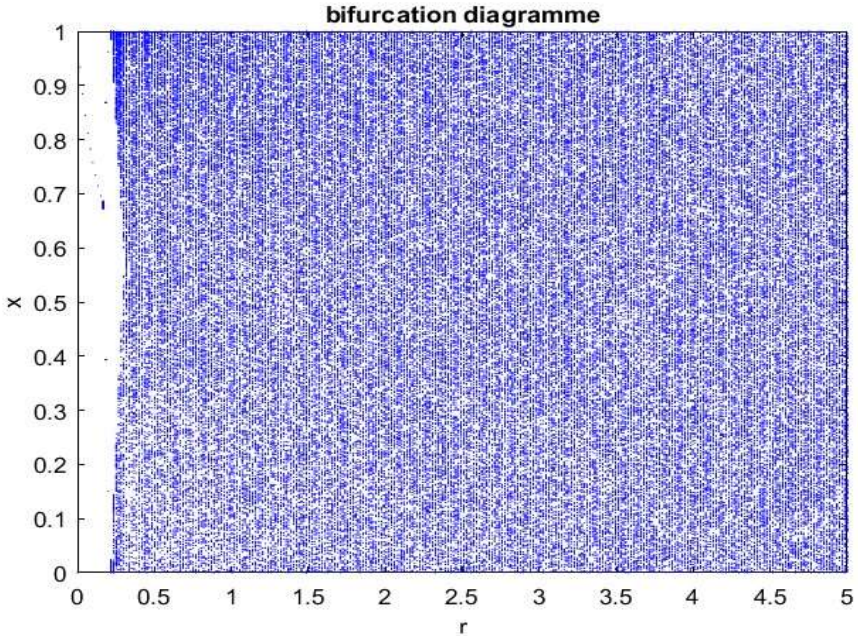

Figure III-4 Diagramme de bifurcation de la deuxième fonction chaotique

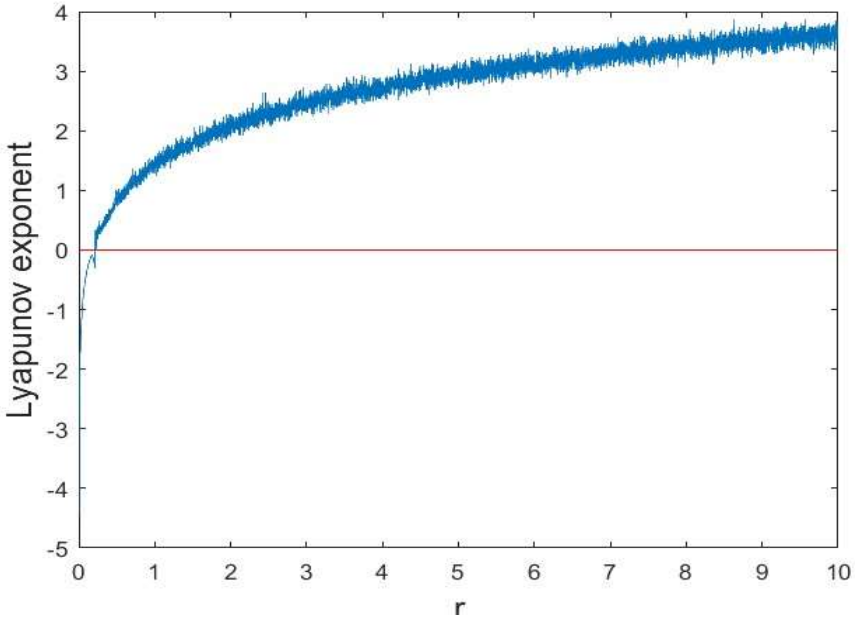

Figure III-5 Exposant de Lyapunov de la deuxième fonction chaotique

- **Partie 2 : à partir de l'échantillon 20001 jusqu'à l'échantillon 40000**

III-3)

$$x_{n+1} = r.e^{2x_n}.(1 - e^{x_n}) \; mod \; 1$$

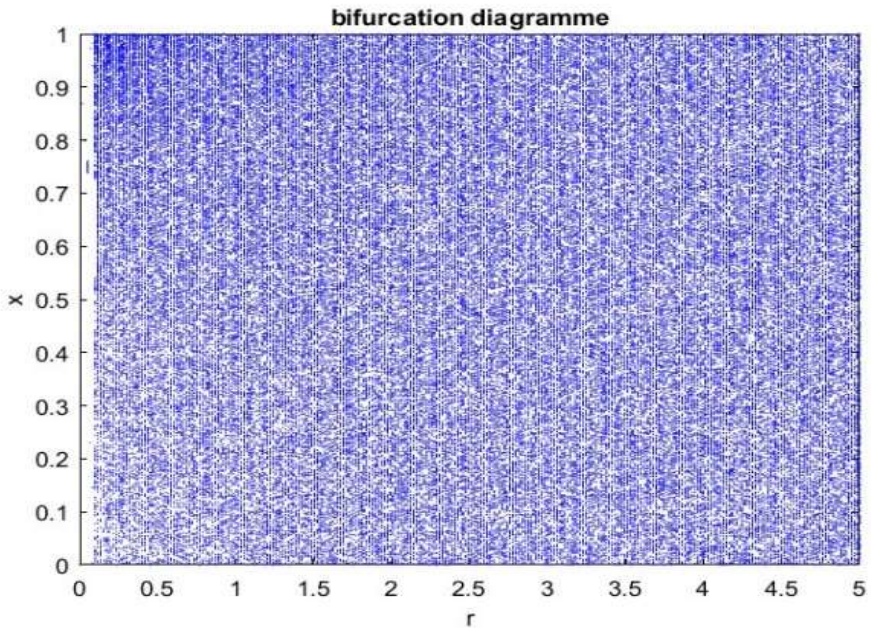

Figure III-6 Diagramme de bifurcation de la troisième fonction chaotique

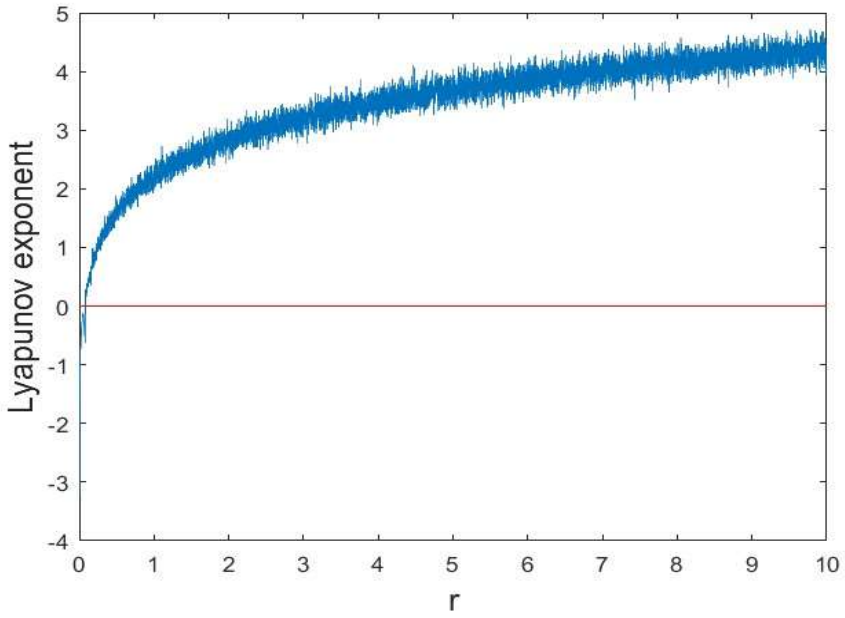

Figure III-7 Exposant de Lyapunov de la troisième fonction chaotique

- **Partie 3 : à partir de l'échantillon 40001 jusqu'à l'échantillon 80000**

III-4)

$$x_{n+1} = r.(e^{x_n})^3.(1-r).(e^{x_n})\ mod\ 1$$

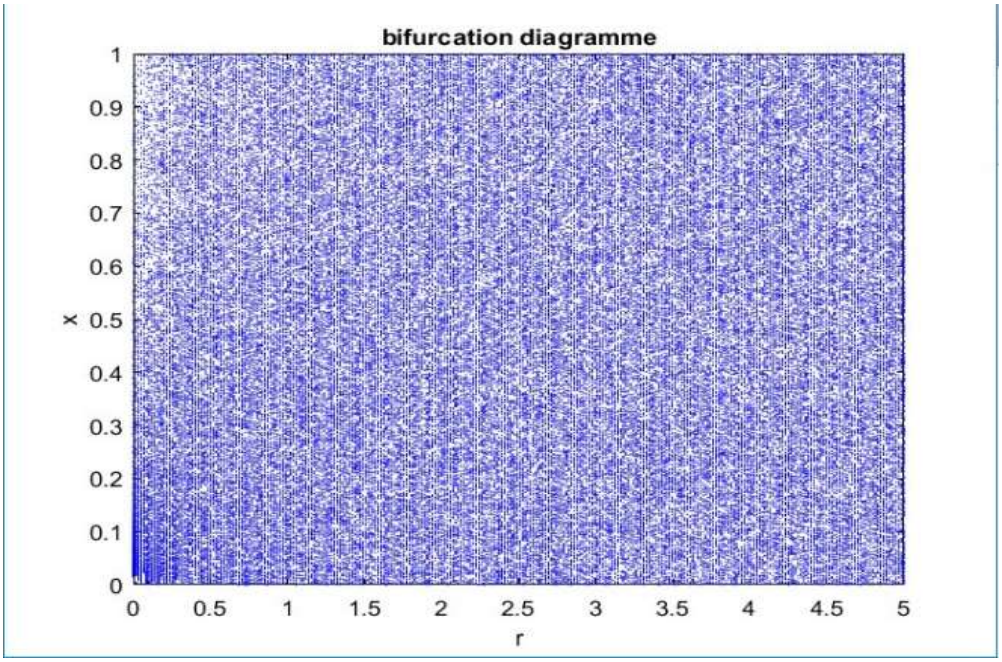

Figure III-8 Diagramme de bifurcation de la quatrième fonction chaotique

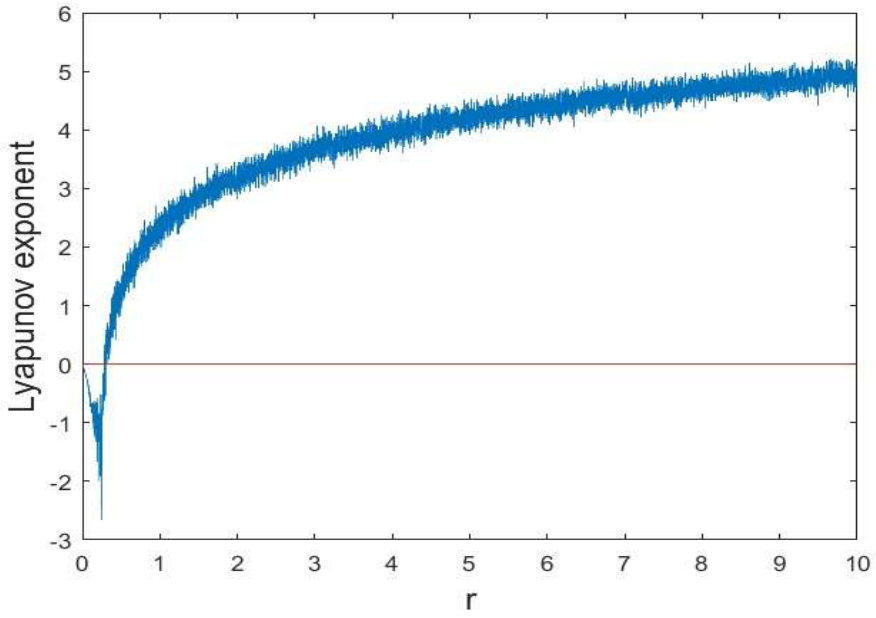

Figure III-9 Exposant de Lyapunov de la quatrième fonction chaotique

III.3.2 Fonctions chaotiques utilisées pour la deuxième méthode de cryptage :

(Une seule fonction pour la phase de permutation (même fonction utilisée dans première méthode) et une seule fonction pour la phase de diffusion)

Pour la phase de permutation nous avons utilisé la même fonction chaotique dans la première méthode (la première fonction chaotique).

Dans la phase de diffusion nous avons utilisé Une seule fonction qui est la fonction utilisée pour la deuxième partie de diffusion dans la première méthode (la troisième fonction chaotique).

III.4 Résultats de simulation :

Notre simulation est réalisée dans l'environnement Matlab. La séquence du signal parole sur laquelle s'est basée notre étude est obtenue via un enregistrement vocal moyennant une application de Matlab.

Dans cette partie, nous présentons les résultats de simulation obtenus par les deux techniques de cryptage. Nous présentons tout d'abord les résultats issus de la première méthode puis ceux issus de la deuxième méthode.

III.4.1 Résultats de simulation issus de l'application de la première méthode :

Pour la deuxième méthode de chiffrement, la clé est composée des paramètres suivants :

(x0, r0, x1, r1, x2, r2, x3, r3) ou :

x0=0.33 ; r0=3.35 ; x1=0.39 ; r1=2.68 ; x2=0.58 ; r2=1.64 ; x3= 0.23 ; r3=1.91 ;

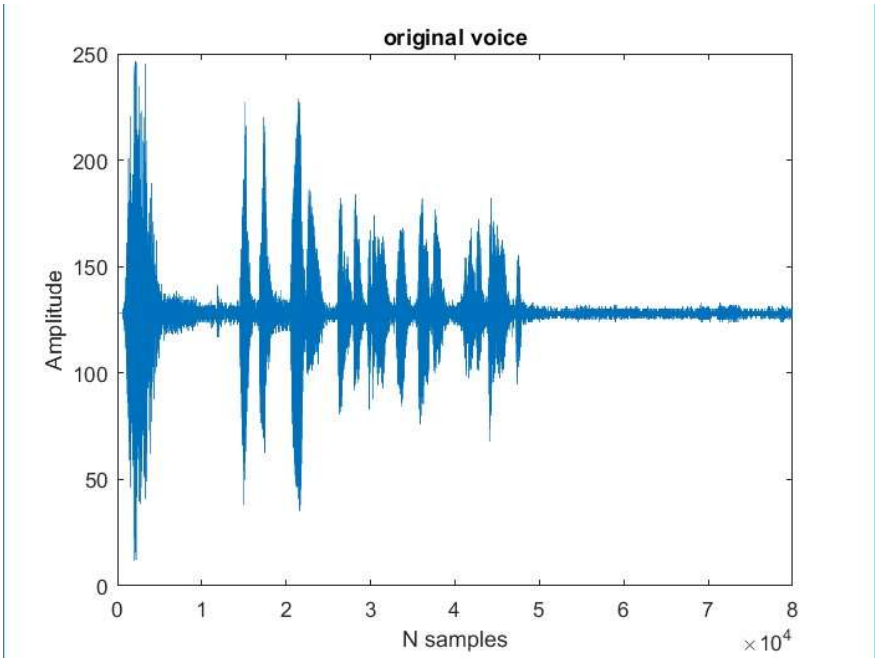

Figure III-10 Courbe de forme d'onde de la voix originale de l'application de la première méthode

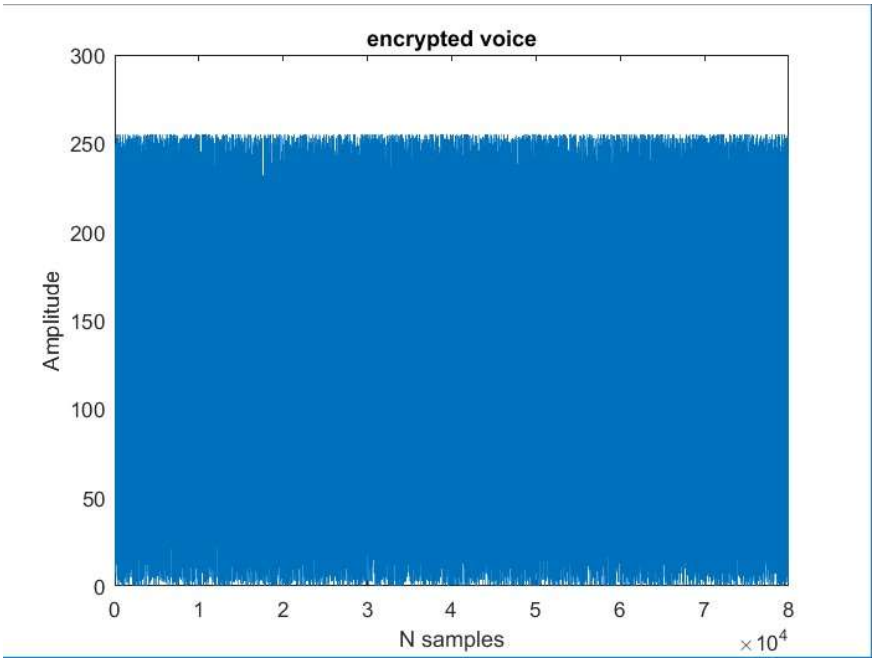

Figure III-11 Courbe de forme d'onde de la voix cryptée de l'application de la première méthode

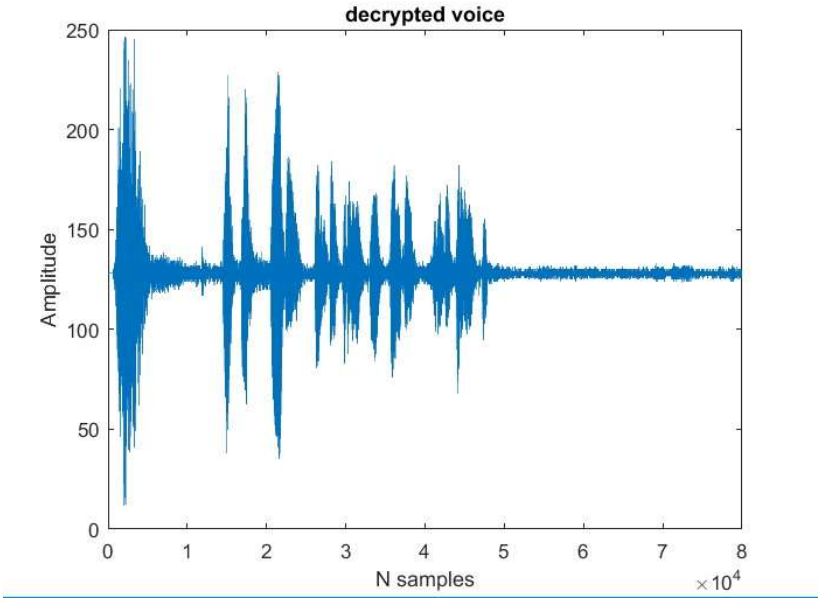

Figure III-12 Courbe de forme d'onde de la voix décryptée de l'application de la première méthode

III.4.1.1 Evaluations des performances de la première méthode de cryptage :

L'évaluation de la qualité d'un tel cryptage se fait au moyen de trois critères : le PSNR (Peak Signal-to-Noise Ratio), la corrélation et la sensibilité de clé.

Les résultats d'Analyse de corrélation et le PSNR :

Plus le PSNR diminue, plus la qualité du signal crypté est élevée. Plus le PSNR est élevé, meilleure est la qualité de l'information ou la reconstruction est très bonne, et La faible valeur du coefficient de corrélation r_{xk}montre un chiffrement de bonne qualité

Tableau III-1 : Résultats d'Analyse de corrélation et le PSNR de la première méthode :

Fichiers de test	**PSNR (en dB)**	**Corrélation (r_{xy})**
Signal 1	**10.6649**	**2.8957e-05**
Signal 2	**10.6972**	**0.0026**
Signal 3	**10. 7308**	**6.9531e-04**
Signal 4	**10. 6630**	**5.8551e-04**

III.4.1.2 Analyse de sensibilité clé :

Une approche de cryptage fiable du signal de parole doit être sensible au moindre changement de la clé secrète, c'est-à-dire que le changement d'une seule valeur de la clé secrète doit produire un signal crypté totalement différent. Les clés de chiffrement (x0, r0,x1, r1, x2, r2, x3, r3) ont été examinées pour démontrer la sensibilité de l'approche proposée. Les résultats dans les figures (17, … , 25) indiquent que si les clés de l'émetteur sont identiques à celles du récepteur, le signal décrypté est identique à l'original, mais si un changement mineur des paramètres se produit, l'image décryptée dans chaque cas est encore totalement inconnue, bien que le changement apporté aux paramètres soit très faible.

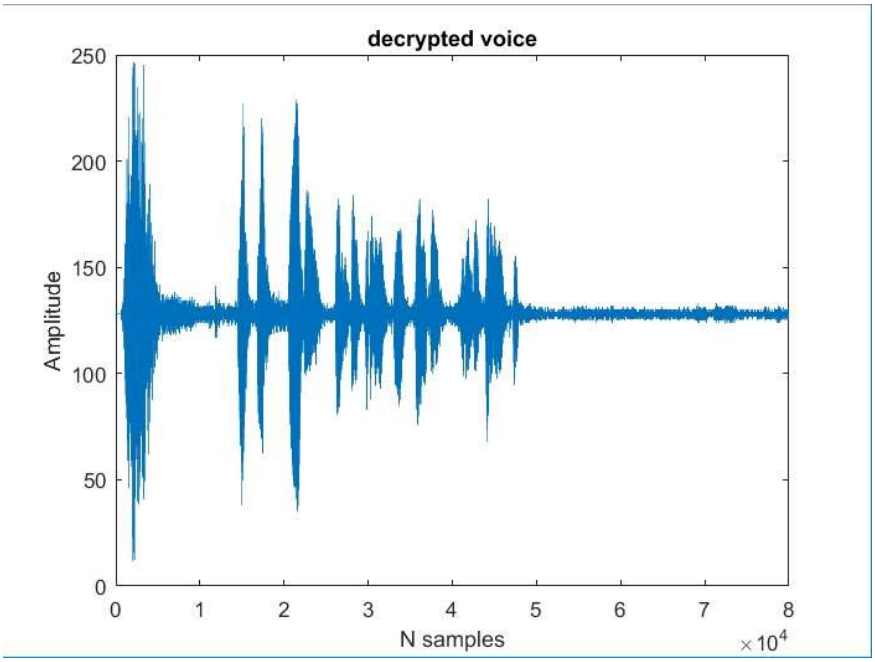

Figure III-13 Sensibilité de la clé (Paramètres identiques)

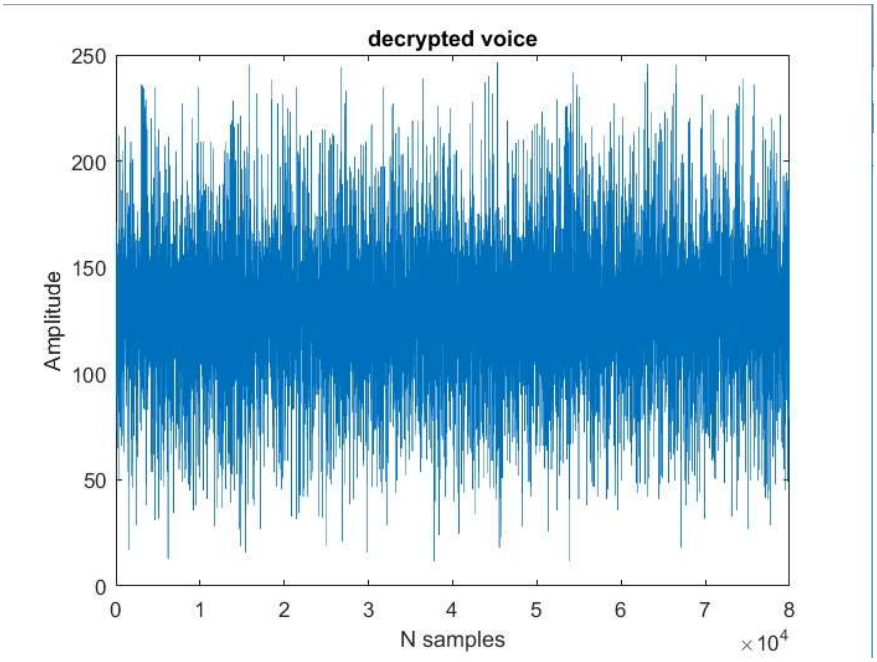

Figure III-14 Sensibilité de la clé (variation du paramètre x0)

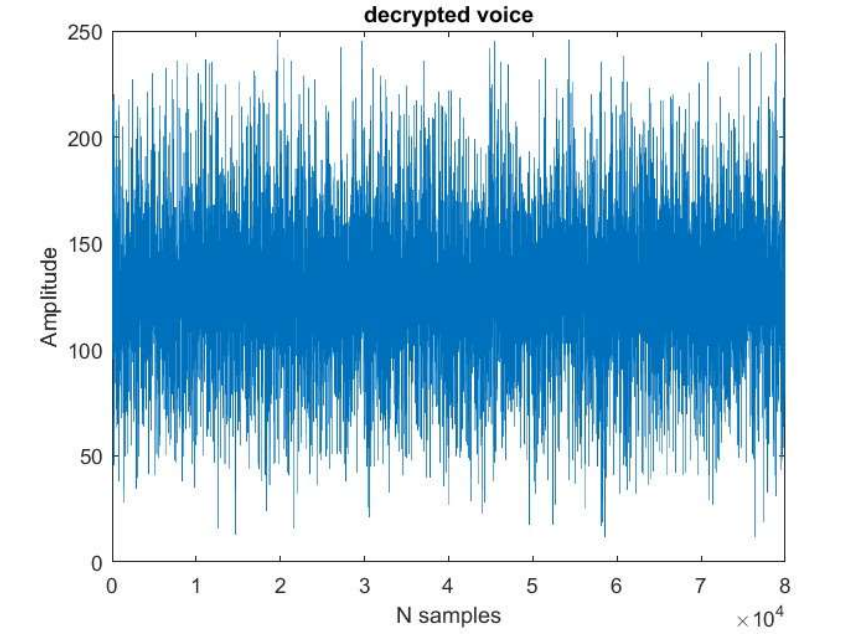

Figure III-15 Sensibilité de la clé (variation du paramètrer0)

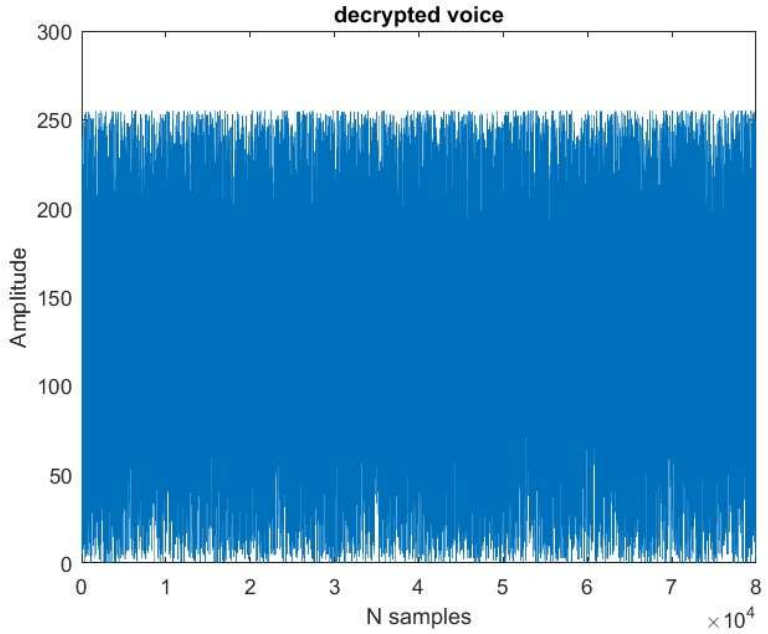

Figure III-16 Sensibilité de la clé (variation du paramètre x1)

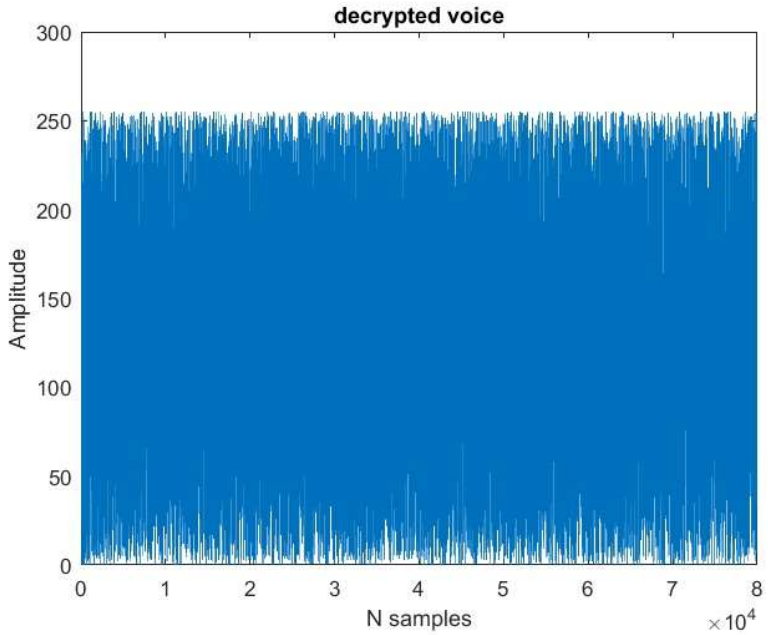

Figure III-17 Sensibilité de la clé (variation du paramètre r1)

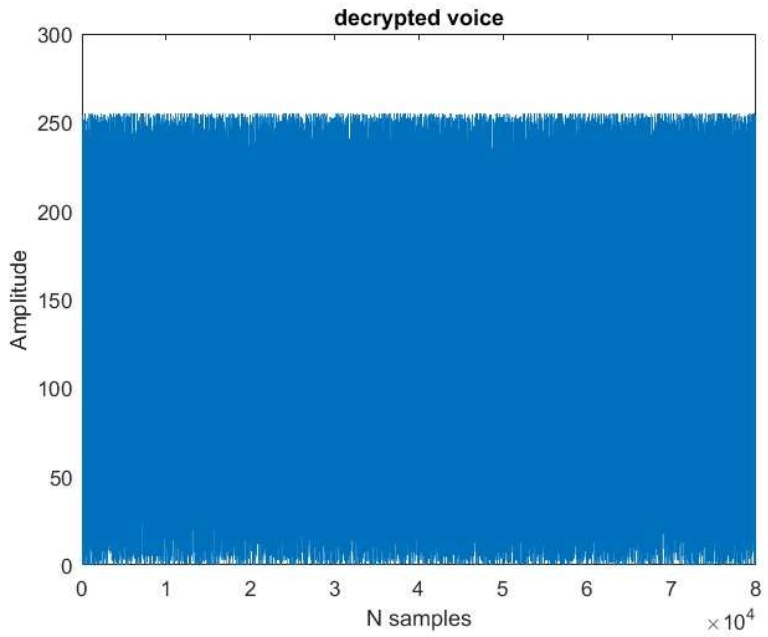

Figure III-18 Sensibilité de la clé (variation du paramètre x2)

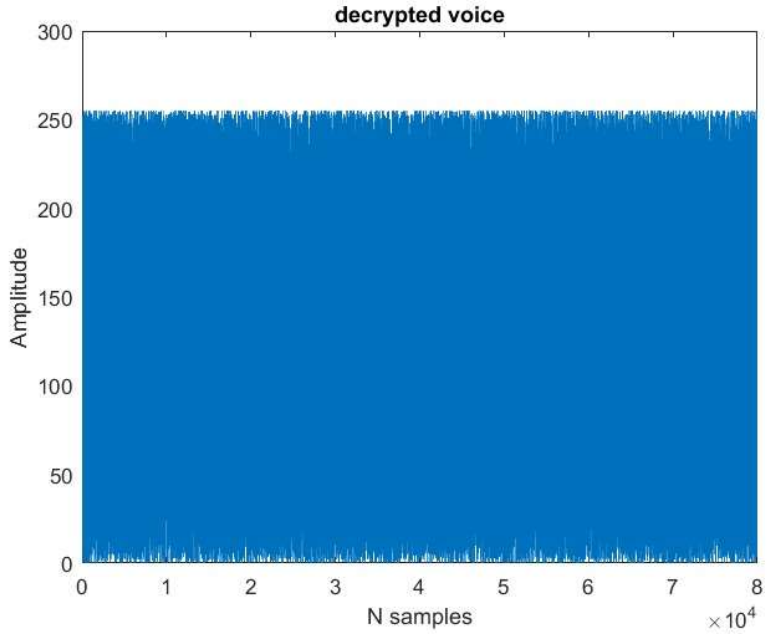

Figure III-19 Sensibilité de la clé (variation du paramètre r2)

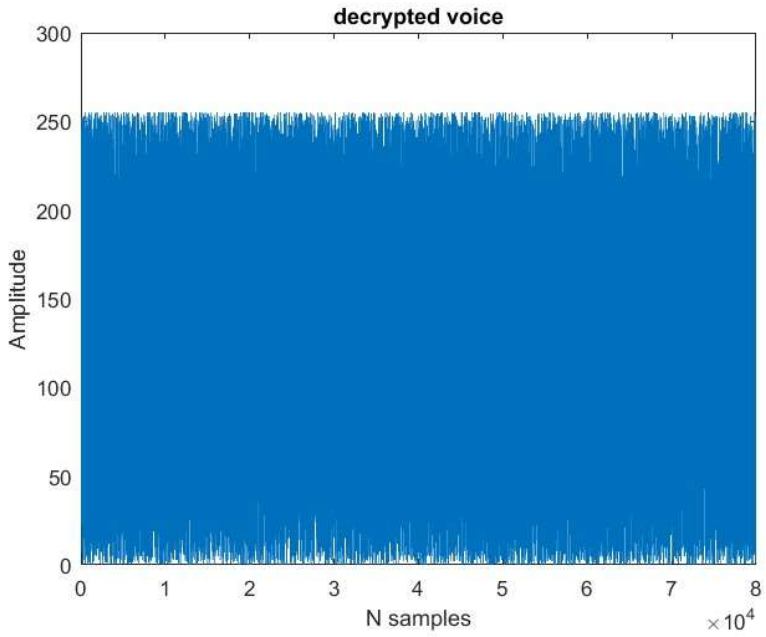

Figure III-20 Sensibilité de la clé (variation du paramètre x3)

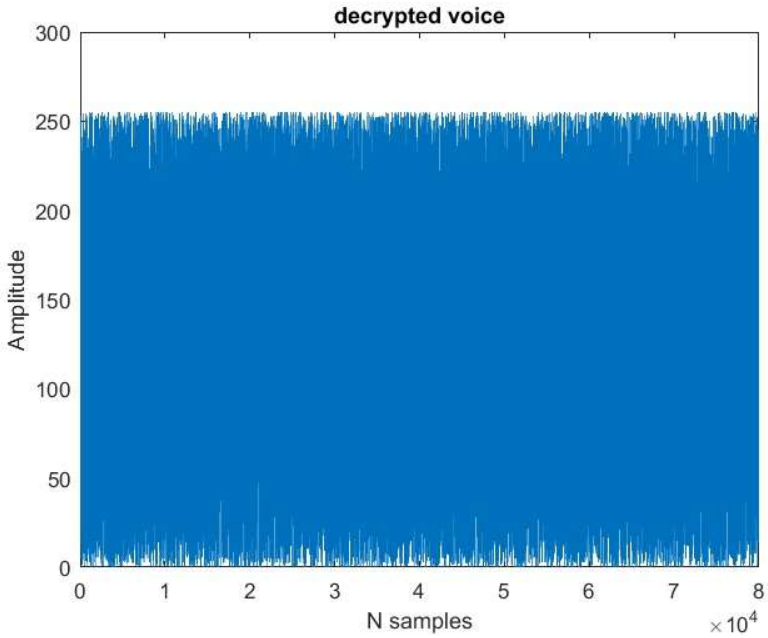

Figure III-21 Sensibilité de la clé (variation du paramètre r3)

III.4.2 Résultats de simulation issus de l'application de la deuxième méthode :

Pour la deuxième méthode de chiffrement, la clé est composée des paramètres suivants :

(x0, r0, x2, r2) ou :

x0=0.33 ; r0=3.35 ; x2=0.58 ; r2=1.64;

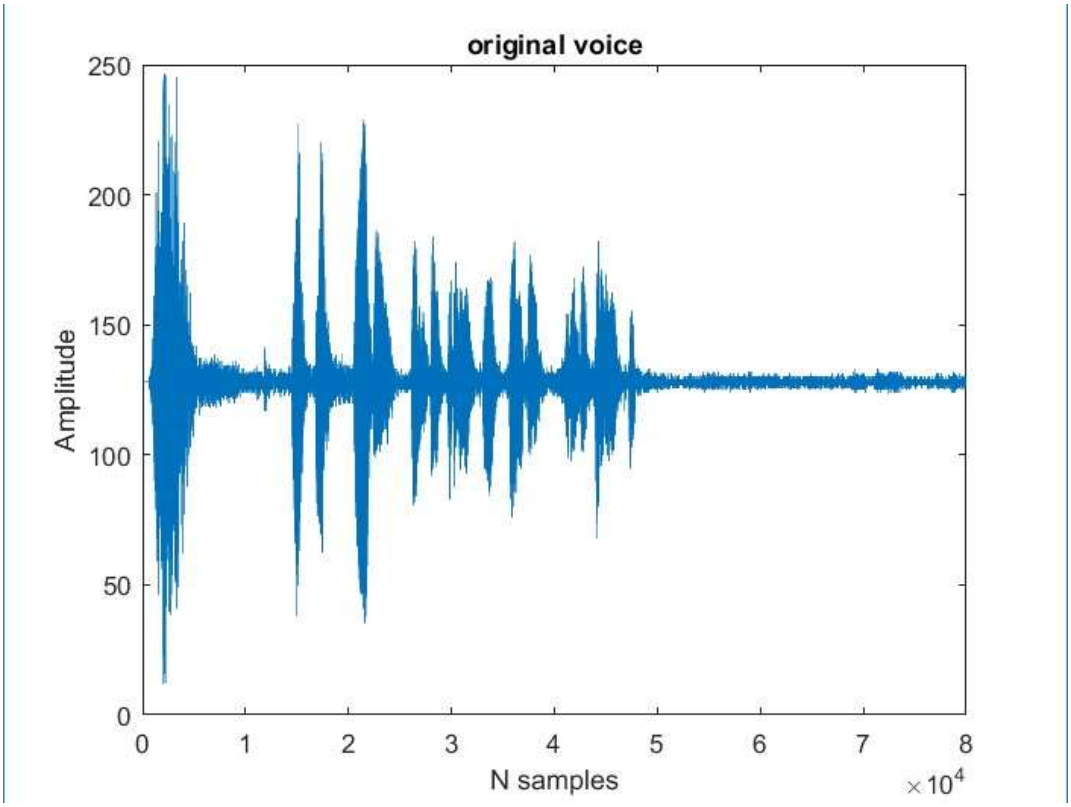

Figure III-22 Courbe de forme d'onde de la voix originale de l'application de la deuxième méthode

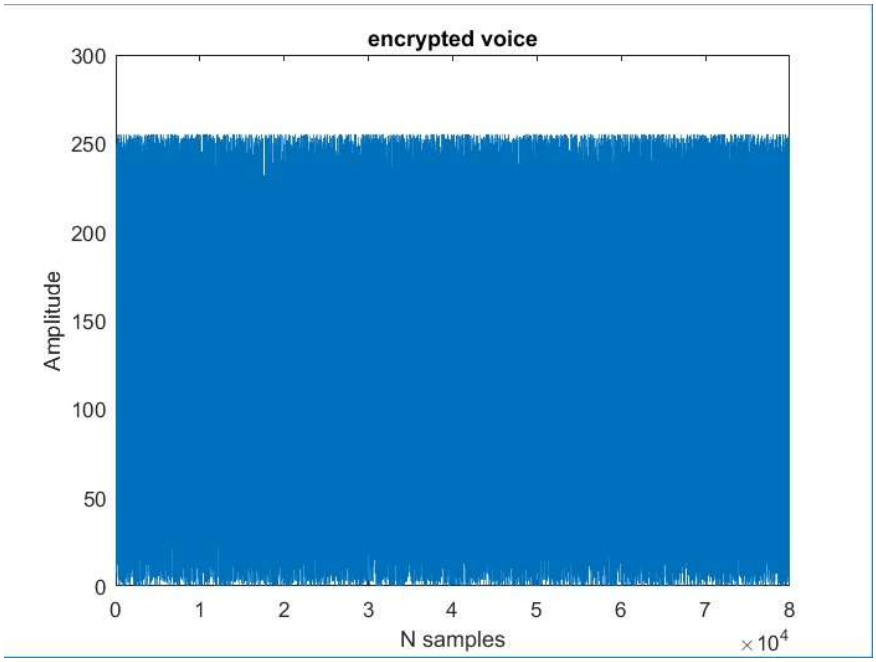

Figure III-23 Courbe de forme d'onde de la voix cryptée de l'application de la deuxième méthode

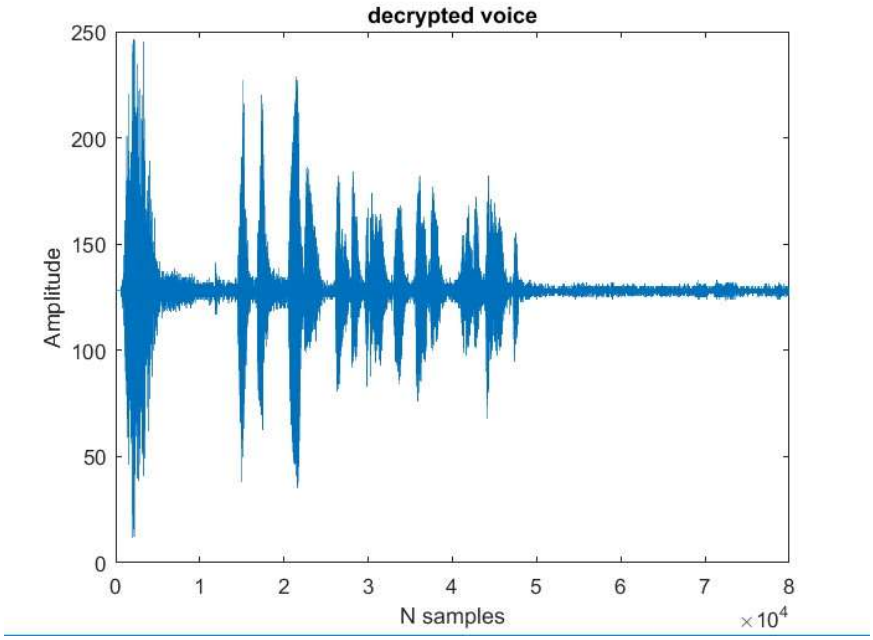

Figure III-24 Courbe de forme d'onde de la voix décryptée de l'application de la deuxième méthode

III.4.2.1 Evaluations des performances de la deuxième méthode de cryptage :

Les résultats d'Analyse de corrélation et le PSNR :

Tableau III-2 : Résultats d'Analyse de corrélation et le PSNR de la deuxième méthode :

Fichiers de test	**PSNR (en dB)**	**Corrélation (r_{xy})**
Signal 1	**11.0758**	**6.0085e-04**
Signal 2	**11.0982**	**0.0034**
Signal 3	**11.1505**	**0.0012**
Signal 4	**11.0842**	**0.0087**

III.4.2.2 Analyse de sensibilité de la clé :

Les clés de chiffrement (x0, r0, x1, r1) ont été examinées pour démontrer la sensibilité de l'approche proposée. Les résultats dans les figures (29, … , 34) indiquent que si les clés de l'émetteur sont identiques à celles du récepteur, le signal décrypté est identique à l'original, mais si un changement mineur des paramètres se produit, l'image décryptée dans chaque cas est encore totalement inconnue, bien que le changement apporté aux paramètres soit très faible.

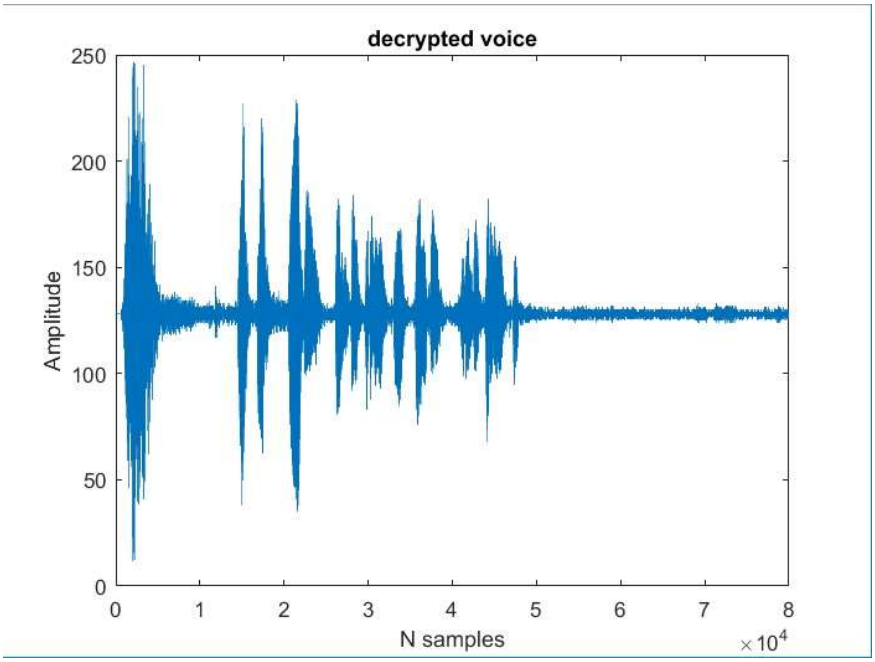

Figure III-25 Sensibilité de la clé (Paramètres identiques)

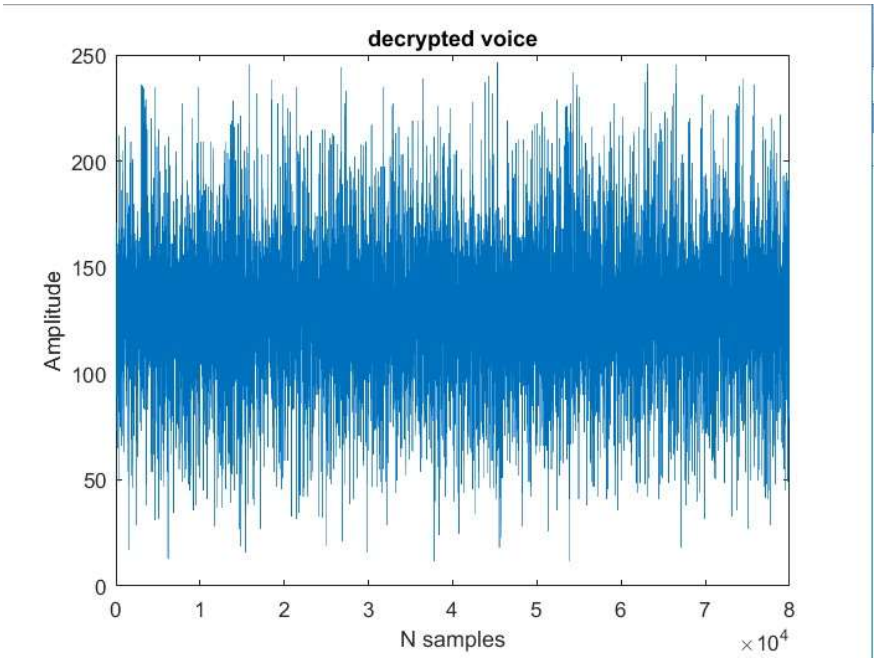

Figure III-26 Sensibilité de la clé (variation du paramètre x0)

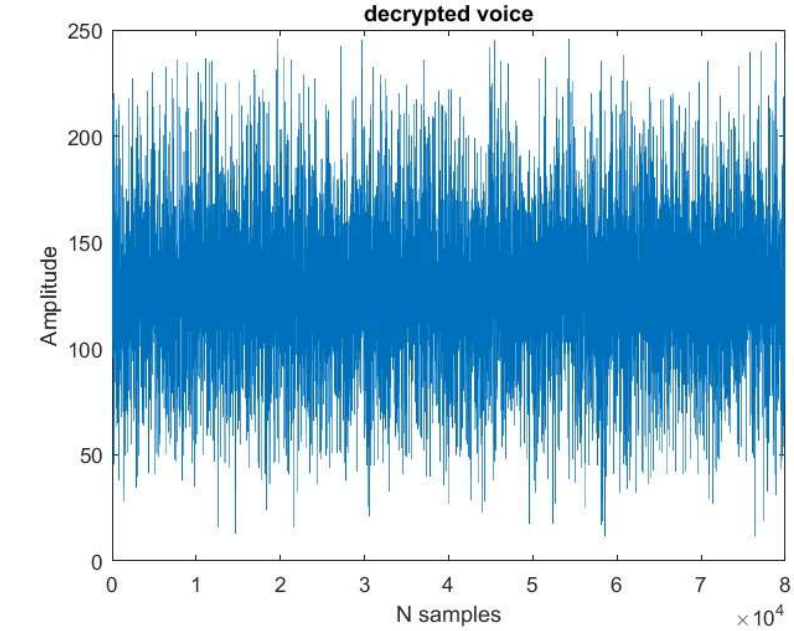

Figure III-27 Sensibilité de la clé (variation du paramètre r0)

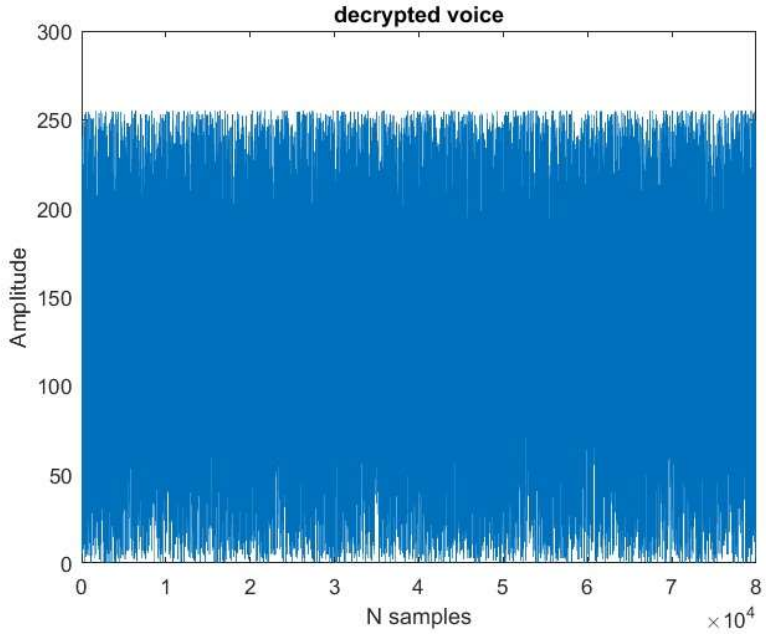

Figure III-28 Sensibilité de la clé (variation du paramètre x2)

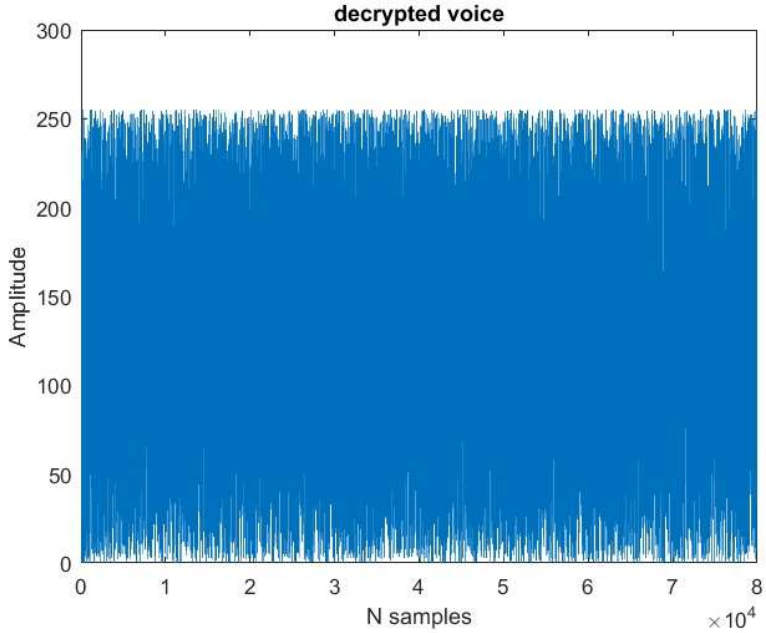

Figure III-29 Sensibilité de la clé (variation du paramètre r2)

III.5 Comparaison des performances des deux méthodes de cryptage utilisées :

Le tableau (III 3) présente une récapitulation en ce qui concerne les trois critères d'évaluation pour les deux techniques de cryptage utilisées. En effet, d'après les valeurs des différents critères données dans le tableau (III 3), nous constatons bien que le cryptage est meilleur en utilisant la première technique et ce pour les trois séquences du signal parole utilisés. Or, le PSNR, la corrélation et la sensibilité de la clé sont bien améliorés en utilisant la première méthode comparativement à la seconde méthode, d'où l'intérêt de l'emploi de plusieurs fonctions chaotique dans la phase de cryptage.

Tableau III-3 : résultats de la comparaison entre les deux méthodes.

Fichiers de test	**Méthode 1**			**Méthode 2**		
	PSNR (en dB)	**Corrélation (r_{xy})**	**L'espace clé**	**PSNR (en dB)**	**Corrélation (r_{xy})**	**L'espace clé**
Signal 1	**10.6649**	**2.8957e-05**	2^{410}	**11.0758**	**6.0085e-04**	2^{203}
Signal 2	**10.6972**	**0.0026**		**11.0982**	**0.0034**	
Signal 3	**10. 7308**	**6.9531e-04**		**11.1505**	**0.0012**	
Signal 4	**10. 6630**	**5.8551e-04**		**11.0842**	**0.0087**	

III.6 Conclusion :

Dans ce chapitre, nous avons étudié l'intérêt de l'emploi de plusieurs fonctions chaotiques dans le cryptage de la parole. En effet, il s'avère que l'utilisation de plusieurs fonctions chaotiques dans la phase de diffusion augmente davantage les performances de la technique de cryptage. Cette façon de faire permet d'améliorer une telle technique de protection des données transmises.

Conclusion générale

Le travail réalisé dans ce mémoire de fin d'étude concerne l'une des techniques de protection des données et des informations les plus répandues dans la littérature. Il s'agit du cryptage basé sur les fonctions chaotiques. En effet, le cryptage est utilisé depuis l'antiquité et ne cesse de se développer au fil du temps passant par un simple cryptage en associant un simple code au message jusqu'à l'emploi d'outils très performants.

Pour la réalisation de notre mémoire, nous avons commencé par introduire des notions générales sur la parole étant donné qu'il s'agit du cryptage de cette dernière. Nous avons ensuite présenté la notion du cryptage des données avec également les fonctions chaotiques utilisées. Aussi, nous avons présenté quelques fonctions chaotiques relevant de littérature avec également une étude de leurs performances en se basant sur des critères d'évaluation du chaos : la bifurcation ayant pour but de connaitre l'intervalle où la fonction est chaotique et le test de Lyapunov servant à déterminer l'intervalle où la fonction est supérieure à zéro, contrairement à ce qui est considéré pour la stabilité des systèmes en automatique.

L'étape importante dans la réalisation de notre mémoire est le cryptage de la parole en exploitant les caractéristiques des fonctions chaotiques. Par ailleurs, le cryptage dont nous avons réalisé consiste en le choix de diviser les données relatives à la séquence du signal parole, après la phase de permutation, en trois parties dans la phase de diffusion et d'employer une fonction chaotique pour chaque partie. Cette façon de faire a permis d'améliorer nettement la qualité du cryptage. Ceci est vérifié en faisant une comparaison avec le cryptage réalisé en utilisant une seule fonction chaotique dans la phase de diffusion. Nous rappelons que la phase de permutation est réalisée par l'emploi d'une seule fonction chaotique pour les deux techniques de cryptage. La comparaison des résultats issus des deux méthodes testées est établie moyennant un ensemble de critères d'évaluation : PSNR, corrélation et sensibilité de la clé.

Comme perspective à ce présent travail, nous envisageons revoir cette technique de cryptage proposée en utilisant autant de fonctions chaotiques dans la phase de permutation que dans la phase de diffusion. Aussi, l'emploi des techniques de l'intelligence artificielle pour la conception des fonctions chaotiques est envisagé.

Bibliographie :

[1] C. DEBILOU, S. BOUDAOUD, « Amélioration d'un synthétiseur de la parole par concaténation », MASTER ACADEMIQUE Université Echahid Hamma Lakhdar El-Oued Faculté de Technologie.

[2] I. OUNNOUGHI, A. HADDAD, « Classification des sons pathologique utilisant l'ELM », Université SAAD DAHLAB de BLIDA, Faculté de Technologie.

[3] A.V. TOLOTRA, « LA CRYPTOGRAPHIE APPLIQUEE AU TRAITEMENT DU SON », Université D'ANTANANARIVO ECOLE SUPERIEURE POLYTECHNIQUE D'ANTANANARIVO, DEPARTEMENT ELECTRONIQUE.

[4] H. TEBBI, « Transcription orthographique phonétique en vue de la synthèse de la parole a partir du texte de l'arabe standard », thèse de magister, Université SAAD DAHLAB de BLIDA

[5] https://www.editions-ellipses.fr/PDF/9782340029477_extrait.pdf

[6]https://www.researchgate.net/figure/Representations-de-la-phrase-Chers-auditeurs-bonsoir-A-Representation-temporelle_fig3_292831962

[7] A.Merzoug , «Neuronal crypto-système basé sur un attracteur chaotique », Thèse doctorat,Université de Batna 2 Faculté de mathématiques et D'informatique,2019.

[8] M.A. BIR, L. DAHMOUNI, « Etude et implémentation d'algorithmes de chiffrement à clé secrète et à clé publique : Application au cryptage de la parole», MASTER ACADEMIQUE, Université Mouloud Mammeri De Tizi-Ouzou.

[9] Fekhr El Islam Khelil, « Les systèmes chaotiques pour le chiffrement», MASTER ACADEMIQUE, Université Larbi Ben M'hidi - Oum El Bouaghi

[10] D. ARBANE, K. ARAB, « Conception de crypto-systèmes à base de systèmes chaotiques d'ordre fractionnaire : Application au cryptage de la parole», MASTER ACADEMIQUE, Université Mouloud Mammeri De Tizi-Ouzou.

[11] FIPS, Data Encryption. Standard (DES) (FIPS 46-3). csrc.nist.gov/publications/fips/fips463/fips46-3.pdf.

[12] M. Allam, A. Hamad, Evaluation of the RC4 Algorithm for Data Encryption, International Journal of Computer Science & Applications Vol. 3, No.2, June 2006.

[13] W. Diffie and M. E. Hellman. "New directions in cryptography". IEEE Trans. Inform. Theory, IT-22 :644-654, Nov 1976.

[14] R. L. Rivest, A. Shamir, and L. M. Adleman. "A method for obtaining digital signatures

and public-key cryptosystems". Communications of the ACM, 21(2) :120-126, 1978.

[15] A. Arazi, "Inegrating a key cryptosystem into the digital signature standard", Electron. Lett.,vol. 29, pp. 966-967, Nov. 1993.

[16] T. E. Gamal. "A public key cryptosystem and a signature scheme based on discrete logarithms". IEEE Trans. Inform. Theory, 31 :469-472, 1985.

[17] T. BEKKOUCHE, « Développement et implémentation des techniques de cryptage des données basées sur les transformées discrètes», Thèse doctorat, Université FERHAT ABBAS SETIF-1.

[18] S.Mokhnache, M.E.H.Daachi, T.Bekkouche et N.Diffellah ,«A Combined Chaotic System for Speech Encryption», Engineering, Technology & Applied Science Research Vol. 12, No. 3, 2022, 8578-8583 8578

[19] A.E. BENZERROUKI, Z.GUEMIDI, « Application des systèmes chaotiques à la cryptographie», MEMOIRE DE MASTER, Université TAHAR MOULAY SAIDA.