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'électronique

Mémoire

Présenté pour obtenir

LE DIPLOME DE MASTER

FILIERE : ELECTRONIQUE

Spécialité : INDUSTRIES ELECTRONIQUES

Par

- **Merrouche Abd Elmoumin**
- **Guendouz Abdelouahab**

Intitulé

Etude d'un système chaotique bidimensionnel pour le cryptage audio

Devant le Jury composé de :

Nom & Prénom	***Grade***	***Qualité***	***Etablissement***
M. Abdelkarim BOUSSAHOUL	MAA	Président	Univ-BBA
M. Seif Eddine AZOUG	MCB	Encadreur	Univ-BBA
Mme. Fouzia HAMADACHE	MAA	Examinatrice	Univ-BBA

Année Universitaire 2022/2023

Résumé

À l'ère numérique, le partage des données multimédias, y compris les données audios, est devenu facilement accessible dans les contextes personnels et professionnels. Le maintien de la confidentialité des données audio peut être assuré par l'application d'algorithmes de cryptage audio. Parmi ces algorithmes, on trouve ceux qui s'appuient sur la théorie du chaos, car les systèmes chaotiques offrent un potentiel cryptographique en raison de leur sensibilité aux paramètres de contrôle.

Des progrès récents ont permis d'introduire des systèmes chaotiques bidimensionnels, qui offrent une sécurité accrue par rapport aux systèmes conventionnels. En utilisant plusieurs paramètres, ces systèmes présentent une meilleure résistance aux différents types d'attaques.

Mots clés : Audio, Cryptage, Chaos, Systèmes chaotiques bidimensionnels, clé

Abstract

In the digital era, the sharing of multimedia data, including audio data, has become easily accessible in both personal and professional settings. Maintaining the confidentiality of audio data can be achieved through the application of audio encryption methods, which involve encrypting the data using algorithms and secret keys. Among these algorithms are those that leverage chaos theory, as chaotic systems offer cryptographic potential due to their sensitivity to control parameters.

recent advancements have introduced two-dimensional chaotic systems, which provide enhanced security compared to conventional systems. By utilizing multiple parameters, these systems exhibit improved resistance against different types of attack.

Keywords: Audio, Encryption, Chaos, Two-dimensional chaotic systems, key

ملخص

في العصر الرقمي، أصبحت مشاركة البيانات المتعددة الوسائط، بما في ذلك بيانات الصوت، متاحة بسهولة على الصعيدين الشخصي والمهني على حد سواء. يمكن تحقيق سرية بيانات الصوت من خلال استخدام طرق التشفير الصوتي، والتي تشمل تشفير البيانات باستخدام خوارزميات ومفاتيح سرية. من بين هذه الخوارزميات هي تلك التي ترتكز على نظرية الفوضى، حيث توفر الأنظمة الفوضوية إمكانات تشفيرية نظرًا لحساسيتها لمعاملات التحكم.

أدت التطورات الحديثة إلى ظهور أنظمة فوضوية ثنائية الأبعاد، والتي توفر أمانًا معززا بالمقارنة مع الأنظمة التقليدية. بسبب استخدامها لعدة معاملات،حيث اظهرت هذه الأنظمة مقاومة جد كبيرة ضد مختلف أنواع الهجمات.

الكلمات المفتاحية : الصوت, التشفير ,الفوضى, أنظمة فوضوية ثنائية الأبعاد, المفتاح

Dédicaces

Nous dédions ce modeste travail en signe de respect, reconnaissance et de remerciement

A nos pères et nos mères

Qui ont été toujours dans nos esprits et dans nos cœurs, Nous vous dédions aujourd'hui notre réussite. Nous prions Dieu Tout-Puissant de les bénir d'une santé et d'un bien-être parfaits, et de partager avec nous d'autres succès et joies à venir.

Remerciements

Nous remercions tout d'abord **Allah** de m’avoir aidé et m’avoir donné le courage, la volonté et la patience de mener à terme le présent travail.

Nous tenons exprimer notre profonde gratitude au Dr. S.E. AZOUG, encadrant du mémoire, pour son soutien inestimable, ses conseils judicieux et sa bienveillance exceptionnelle tout au long de l'élaboration de ce modeste travail. Nous sommes sincèrement reconnaissants de sa présence et de son engagement à nos côtés.

Nous souhaitons également exprimer nos sincères remerciements à Monsieur Abdelkarim BOUSSAHOUL pour l'intérêt qu'il a porté à notre travail et d'avoir accepté de présider ce jury. Sa présence et son expertise ont été précieuses, et nous lui sommes profondément reconnaissants.

Nous tenons également à remercier Madame Fouzia HAMADACHE d'avoir honoré notre travail de sa présence et d'avoir accepté d'en examiner les détails. Nous lui adressons notre gratitude et notre profond respect.

Nous tenons à remercier également tous nos enseignants pour leurs bonnes orientations et pour leur aide précieuse.

Ainsi

Que tous les amis de notre promo et tous ceux qui ont collaborés de près ou de loin à l'élaboration de ce travail.

Enfin, un très grand merci à nos petites familles qui nous ont fourni les motivations qui ont permis à l'aboutissement de ce travail.

Table des matières

INTRODUCTION GENERALE..... 1

Chapitre 01 GENERALITES SUR LE CRYPTAGE & le CHAOS 3

1.1. Introduction 3

1.2. Cryptographie 3

1.3. Système cryptographique 4

1.4. Cryptanalyse 4

1.5. Types de cryptage 5

1.5.1. Cryptage symétrique (A clé privée) 5

1.5.2. Cryptage asymétrique (A clé publique) 5

1.6. Principe du cryptage 6

1.6.1. Confusion (substitution) 6

1.6.2. Diffusion (permutation) 7

1.7. Introduction du chaos en cryptographie 7

1.8. Les suites chaotiques 7

1.8.1. La suite logistique 8

1.9. Propriétés des suites chaotiques 8

1.9.1. Diagramme de bifurcation 8

1.9.2. Exposant de Lyaponov 10

1.10. Conclusion 10

Chapitre 02 Cryptage audio basée sur les suites CHAOTIQUES 2D 11

2.1. Introduction 11

2.2. Intérêt du cryptage audio 11

2.3. Les suites chaotiques bidimensionnelles 2D 12

2.4. Type de suites chaotiques bidimensionnelles 12

2.4.1. La suite de Hénon 12

2.4.2. La suite de Lozi 12

2.4.3. La suite standard 2D 13

2.4.4. La suite d'Arnold 13

2.5. Suite chaotique 2D-LNIC 13

2.6. Cryptage audio avancé AEA-NCS 14
2.7. Principe de génération des clés en AEA-NCS 15
2.8. Algorithme de cryptage audio AEA-NCS 17
2.9. Algorithme de décryptage audio 20
2.10. Conclusion 22
Chapitre 03 : RESULTATS et discussions 23
3.1. Introduction 23
3.2. Environnement de travail 23
3.3. Critères de performances 24
3.3.1 Entropie 25
3.3.2. Coefficient de corrélation 25
3.3.3. L'attaque différentielle 25
3.3.4. Espace des clés 26
3.3.5. Sensibilité de la clé 26
3.5. Résultats des simulations et analyse de sécurité 26
3.5.1. Résultats du cryptage & du décryptage 26
3.5.2 Evaluation de l'entropie 30
3.5.3. Evaluation du coefficient de corrélation 30
3.5.4 Evaluation du NPCR et UACI 32
3.5.5. Espace de la clé secrète et sa sensibilité 32
3.5.7 Immunité contre le bruit additif 34
3.5.8. Temps d'exécution 35
3.6. Comparaison 2D-LNIC vs Lozi en AEA-NCS 35
3.6.1. Résultats du AEA-LZM 35
3.6.2. Comparaison de l'entropie 37
3.6.3. Comparaison des coefficients de corrélation 37
3.6.4 : Comparaison du NPCR et UACI 38
3.6.5. Comparaison de la sensibilité des clés 39
3.6.7. Résistance au bruit additif 39
3.6.8. Comparaison de la vitesse d'exécution 40
3.7. Discussion 41
3.8. Conclusion 41
Conclusion générale 42
Reference bibliographique 43

List des figures

Figure1.1 : Système cryptographique 4
Figure 1.2: Processus du cryptage symétrique 5
Figure1.3 : Processus du cryptage asymétrique 6
Figure 1.4 diagramme de bifurcation généralisé 9
Figure 1.5 le diagramme de bifurcation pour r entre 3 et 4 9
Figure :1.6 l'exposant de Lyapunov de la suite logistique. 10
Figure2.1 : SHA-256 16
Figure 2.2 : Organigramme de génération des clés par l'AEA-NCS 16
Figure2.3 : Organigramme cryptage AEA-NCS 17
Figure 2.4 : organigramme du processus de cryptage audio 20
Figure 2.5 organigramme de l'opération de décryptage. 22
Figure3.1 : Exemple d'un signal audio 24
Figure3.2. Signaux audio originaux 27
Figure3.3. Signaux audios cryptés par AEA-NCS. 28
Figure3.4. Signaux audios décryptés par AEA-NCS 29
Figure3.5 Sensibilité de la clé secrète en AEA-NCS. 33
Figure3.6 : l'effet de AWGN sur AEA_NCS.. 34
Figure 3.7: Description des informations audio. 36
Figure3.8 : informations audio cryptées par AEA_LZM 36
Figure 3.9: les informations audios décryptées par AEA_LZM. 36
Figure 3.10 : sensibilité de clé de AEA_LZM. 39
Figure3.11 : l'effet de AWGN sur AEA_LZM. 40

List des tableaux

Tableau 3.1 : Evaluation de l'entropie 30

Tableau3.2 : Coefficients de corrélation des signaux audio originaux 31

Tableau 3.3 : Coefficients de corrélation des signaux audio cryptés par AEA_NCS 31

Tableau3.4 : Valeurs des NPCR et UACI en cryptage AEA_NCS 32

Tableau3.5 : Vitesse du cryptage de l'AEA_NCS 35

Tableau3.6 : l'entropie de l'information de AEA_NCS vs AEA_LZM 37

Tableau 3.7: coefficients de corrélation de signaux audios cryptés de AEA_NCS vs AEA_LZM 38

Tableau 3.8 : NPCR et UACI de AEA_NCS vs AEA_LZM. 38

Tableau3.9 : La vitesse de cryptage de AEA_NCS vs AEA_LZM 41

Liste des abréviations

AES	Advanced Encryption Standard
DES	Data Encryption Standard
RSA	Rivest Shamir Adleman
PWLCM	Piecewise Linear Chaotic Map
SHA-256	Secure Hash Algorithm
IBM	International Business Machines
NPCR	Number of Pixels Change Rate
UACI	Unified Average Changing Intensity
AWGN	Additive White Gaussian Noise
SNR	Signal-to-noise ratio

INTRODUCTION GENERALE

Suite au développement rapide des technologies de l'information, les documents multimédias sont devenus un élément central dans les différents domaines d'application. En effet, ils sont des outils de travail essentiel en biomédical, en imagerie satellitaire et astronomique, en production cinématographique, ou encore en informatique industrielle.

Ce développement phénoménal ne s'est pas fait sans entraîner des inquiétudes de manipulations illicites puisque n'importe quelle personne peut facilement copier, modifier et distribuer les audios sans risque de les détériorer. Ces manipulations illicites sont un problème central pour la sécurité d'un système, quel qu'il soit : l'état, une entreprise ou un particulier. D'où, l'importance de protéger ces documents multimédias contre un accès ou une distribution non autorisée.

C'est pour répondre à ce problème qu'a été inventée la cryptographie visuelle. Elle est une branche de la cryptographie qui consiste à transformer une audio en d'autres audio cryptées n'ayant aucune ressemblance ou corrélation avec l'originale.

Depuis quelques années, le domaine de cryptage d'audio connaît un extraordinaire développement et plusieurs techniques ont vu le jour, mais chacune ne peut pas garantir de ne pas avoir de faiblesses ou qu'elle est insensible aux méthodes d'attaque. C'est pourquoi, les chercheurs ne cessent de développer de nouveaux systèmes de cryptographie pour minimiser ces problèmes.

Problématique et objectif

Maintenant, il est devenu clair que nous ne pouvons pas utiliser les méthodes de cryptage classiques standard comme RSA, DES, AES, pour le chiffrement d'audio, par ce qu'ils ne sont pas atteints fin requis pour ce type de données et l'accélération en multimédias.

Ainsi les audios sont caractérisées par la redondance élevée, la forte corrélation et la taille volumineuse. Le problème posé est comment peut-on concevoir un système de cryptage pour assurer la sécurité de ce type de données ?

Organisation du mémoire

Nous avons structuré notre mémoire en trois chapitres.

- Le premier chapitre nous avons revus les notions de base sur la cryptographie, la cryptanalyse et le cryptage, y compris le cryptage symétrique et asymétrique. On a également vu l'intérêt de l'utilisation de la théorie du chaos dans les algorithmes de cryptage, en particulier l'exploitation des suites chaotiques et leurs propriétés chaotiques (confusion et diffusion)

- Dans le deuxième chapitre, nous allons revoir quelques suites chaotiques bidimensionnelles connues et particulièrement la suite 2D-LNIC Logistic Nested Infinite Collapse. Il s'agit d'un système hyper-chaotique proposé en combinant une suite d'effondrement infini (1D-ICM) et une suite logistique.

- Dans le dernier Nous avons étudié des critères de performance importants qui doivent être pris en compte pour déterminer la sécurité d'un algorithme de chiffrement Et nous avons identifié les attaques électroniques auxquelles chaque norme de chiffrement est exposée, puis nous avons étudié ces normes sur plusieurs audios, et nous avons obtenu des résultats, puis nous les avons comparés avec l'algorithme sur lequel nous avons travaillé AEA_NCS

Chapitre 1

CHAPITRE 01 GENERALITES SUR LE CRYPTAGE & LE CHAOS

1.1. Introduction

Dans le monde numérique d'aujourd'hui, la cryptographie joue un rôle essentiel dans la sécurisation des données. Ce chapitre introduit les concepts du cryptage, des systèmes cryptographiques et de la cryptanalyse. Il explique les techniques de cryptage symétrique et asymétrique, ainsi que les principes de confusion et de diffusion. De plus, il explore l'intégration de la théorie du chaos dans la cryptographie, mettant en évidence l'utilisation de suites chaotiques pour le cryptage.

1.2. Cryptographie

La cryptographie est un mot d'origine grecque composé de deux parties, : (kriptos) qui signifie caché, et (grafee) qui signifie écrit. Donc littéralement, la cryptographie est l'étude de l'écriture cachée. [1]

En réalité, la cryptographie est la science qui utilise des fonctions mathématiques pour crypter et décrypter les données afin de rendre n'importe qui capable de stocker ou transmettre des informations sensibles de sorte que personne d'autre que le destinataire prévu ne puisse les lire [2].

Les gouvernements, les armées et les industriels l'utilisent afin de protéger certaines informations, elle n'est plus limitée à cela seulement, mais s'est étendu à l'utilisation par les individus dans leur vie privée. [1]

La cryptographie a trois buts principaux :[3]

- **Confidentialité :** Empêcher que le message ne soit lu par une personne autre que le destinataire prévu.
- **Intégrité :** Garantir au récepteur que le message reçu n'a pas été modifié au cours de la transmission par rapport au message d'origine.

- **Authenticité :** La preuve de l'identité d'une personne. Un moyen de prouver que l'émetteur a réellement envoyé le message.

1.3. Système cryptographique

Pour assurer la confidentialité des données, nous devons faire appel à un système cryptographique comme le montre la figure 1.1. Un système cryptographique se compose en général de [4] :

- Un message en clair non crypté appelé texte en clair (plaintext)
- Un message crypté appelé texte crypté (ciphertext).
- La conversion du texte clair en texte crypté est appelée algorithme de cryptage
- La restauration du texte à partir du texte crypté est appelée algorithme de décryptage.
- Une clé de cryptage et une autre pour le décryptage

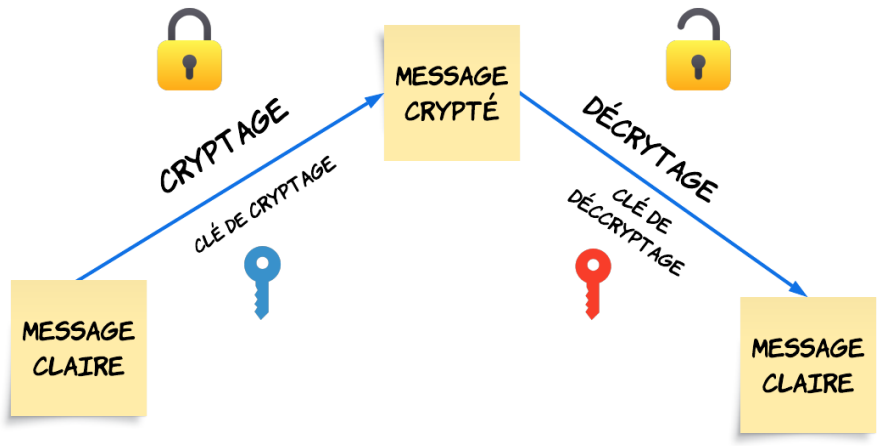


Figure1.1 : Système cryptographique

1.4. Cryptanalyse

L'ensemble de la cryptographie et de la cryptanalyse forment la science du secret ou la cryptologie. Si la cryptographie est la science du cryptage, alors la cryptanalyse est l'étude scientifique du décryptage qui intègre toutes les méthodes de décryptage visant à restaurer le texte chiffré dans sa forme originale, sans avoir connu au préalable la clé secrète où l'attaquant peut analyser l'algorithme de cryptage ou de décryptage et essayer plusieurs clés prédéfinis [5]

1.5. Types de cryptage

1.5.1. Cryptage symétrique (A clé privée)

Le cryptage symétrique est une technique de cryptographie qui utilise la même clé pour le cryptage et le décryptage [6]. Cela signifie que l'émetteur et le destinataire utilisent la même clé pour crypter et décrypter les données comme le montre la figure 1.2.

Figure 1.2: Processus du cryptage symétrique

Les fameux algorithmes de cryptage AES et DES ce sont des algorithmes de cryptage symétrique. Le cryptage symétrique est largement utilisé et plus rapide, mais il présente certains inconvénients, tels que la nécessité de garder la clé secrète et de la modifier fréquemment. [6]

1.5.2. Cryptage asymétrique (A clé publique)

Le cryptage à clé publique ou bien le cryptage asymétrique est une technique qui utilise une paire de clés pour le cryptage : une clé publique pour crypter les données et une clé privée correspondante (clé secrète) pour le décryptage.

Vous pouvez publier votre clé publique dans le monde entier tout en gardant votre clé privée secrète. Le propriétaire d'une clé publique peut crypter des informations, mais ne peut pas les décrypter. Les informations ne peuvent être décryptées que par la personne qui possède la clé privée correspondante.

L'algorithme RSA est le plus utilisé en cryptage à clé publique. L'un des principaux avantages du cryptage à clé publique est qu'il permet d'utiliser des signatures numériques. Cela permet le destinataire de vérifier l'authenticité de l'origine de l'information et de s'assurer que l'information n'a pas été modifiée au cours de la transmission [3].

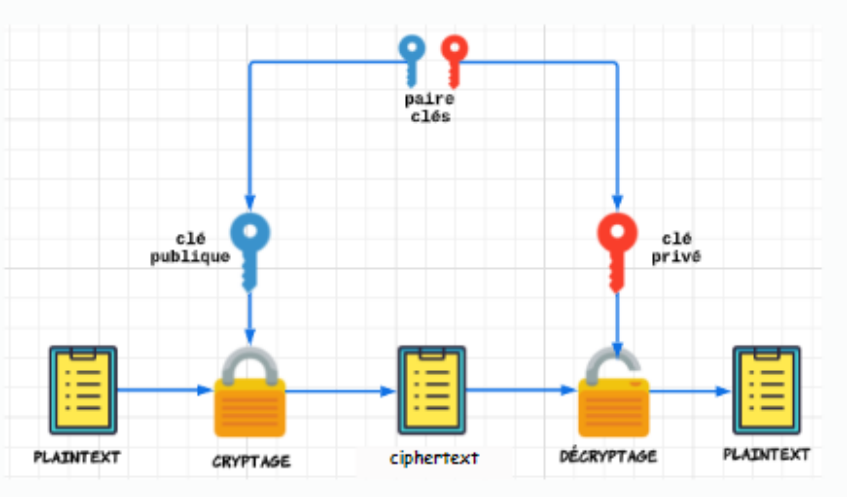


Figure1.3 : Processus du cryptage asymétrique

1.6. Principe du cryptage

Quelle est la meilleure façon de déterminer si un système cryptographique est suffisamment sécurisé ? Pour répondre à cette question, Claude Shannon a proposé le principe de la confusion et de la diffusion pour avoir des systèmes cryptographiques sécurisés. L'objectif est d'empêcher la cryptanalyse basée sur les propriétés statistiques du texte en clair.

1.6.1. Confusion (substitution)

Dans les définitions originales de Shannon, la confusion est l'une des deux composantes principales d'un cryptage sécurisé. Son objectif est de rendre la relation entre la clé et le texte chiffré aussi complexe que possible, afin qu'un attaquant ne puisse pas facilement déduire la clé ou le texte en clair.

La substitution est un moyen de créer la confusion, en remplaçant chaque lettre du texte en clair par un caractère ou un symbole différent. Cependant, une confusion efficace ne se limite pas à la substitution. Il est essentiel que chaque lettre de la clé affecte chaque lettre du bloc de texte chiffré, de sorte qu'il soit difficile pour un pirate de déterminer la clé ou le texte en clair [7].

Pour ce faire, chaque caractère du texte chiffré doit dépendre de plusieurs éléments de la clé, et la relation entre la clé et le texte chiffré doit sembler aléatoire [7]. Les cryptages qui ne présentent pas de confusion significative peuvent être cassés par un pirate disposant d'une puissance de calcul suffisante. [7]

1.6.2. Diffusion (permutation)

La diffusion est une façon de brouiller un message pour qu'il se répande partout. Elle diffère de la confusion, qui se contente de remplacer les lettres une à une. Avec la diffusion, les lettres du message sont dispersées au hasard dans le message crypté.

Il est donc beaucoup plus difficile de retrouver le message d'origine à l'aide de moyens statistiques et il faut donc beaucoup plus de messages cryptés pour y parvenir.[7]

1.7. Introduction du chaos en cryptographie

Le chaos est un comportement complexe et imprévisible qui peut survenir dans des systèmes déterministes, où de petits changements dans les conditions initiales entraînent de grands changements dans les résultats au fil du temps [8].

La théorie du chaos est une branche mathématique qui étudie le comportement des systèmes complexes et imprévisibles. Elle a été étudiée pour la première fois par Henri Poincaré et Andrey Kolmogorov au début du vingtième siècle, mais elle a gagné en popularité dans les années 1960 et 1970 à la suite de la découverte de l'effet papillon par Edward Lorenz [8]. La théorie du chaos a depuis été appliquée à plusieurs domaines dont la cryptographie.

L'utilisation du chaos en cryptage est plus efficace que le cryptage conventionnel car il génère une suite mathématique hautement aléatoire appelée suite chaotique, en anglais « chaotic map », en se basant sur la sélection appropriée d'un système déterministe chaotique [9].

1.8. Les suites chaotiques

Une suite chaotique est une fonction mathématique qui présente un comportement chaotique, ce qui signifie qu'un petit changement dans les conditions initiales ou dans les paramètres de l'équation mathématique de la suite peuvent conduire à des résultats très différents ce qui la rend plus sécurisé que les systèmes de cryptage conventionnels [10].

Ces suites sont exploitées en cryptographie pour générer des nombres aléatoires ou pseudo-aléatoires ou créer de la confusion dans les données d'origine pour les crypter [10].

Les suites chaotiques peuvent avoir différentes dimensions, allant d'une à quatre, et peuvent être continues ou discrètes. Elles peuvent être classés en trois catégories principales [9] :

- Suites chaotiques à faible dimensions (unidimensionnelles ou bidimensionnelles)
- Suites chaotiques multidimensionnels
- Suites hyper-chaotiques

Il existe plusieurs suites chaotiques en littérature où les suites chaotiques à faible dimension sont les plus utilisées car ils ont une structure simple et elles sont largement utilisés en cryptage, de ce fait, nous nous limiterons dans notre étude à seulement aux suites chaotiques à faible dimension.

Les suites chaotiques à faible dimension, c'est-à-dire les suites chaotiques unidimensionnelles ou bidimensionnelles il en existe plusieurs tels que la suite logistique, la suite Tent, la suite, la suite Chebyshev ...etc [9][11].

Afin de mieux comprendre le principe des suites chaotiques, nous prenons comme exemple à étudier la suite logistique.

1.8.1. La suite logistique

La suite logistique est une suite chaotique unidimensionnelle couramment utilisée. Il s'agit d'un système chaotique très simple mais très répandu. Elle est définie comme suit :

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

Où 'r' est le paramètre chaotique de la suite logistique et x_n est la séquence chaotique logistique.

La suite logistique a des comportements chaotiques lorsque le paramètre de contrôle ' r' se varie dans l'intervalle [3.5, 4]. [11]

1.9. Propriétés des suites chaotiques

Le comportement d'une suite chaotique peut être analysé à l'aide de diagrammes de bifurcation, d'exposants de Lyapunov et de coefficients de corrélation. [10].

1.9.1. Diagramme de bifurcation

La bifurcation est un processus observé dans les systèmes chaotiques où une petite perturbation ou un changement dans les règles directrices provoque un changement d'état ou de comportement du système. C'est un concept important pour comprendre la théorie du chaos et peut conduire à l'émergence de nouveaux modèles ou comportements qui n'étaient pas présents dans le système auparavant [9].

. La figure 1.4 montre le diagramme de bifurcation de la suite logistique lorsque $x0$=0.1 et r ∈ [0,4] et la figure 1.5 lorsque r ∈ [3,4] et $x0$ = 0.5789

On peut voir sur ces figures le phénomène de chaos et de la bifurcation ou la suite logistique devient chaotique seulement lorsque le paramètre de contrôle r ∈ [3,4].

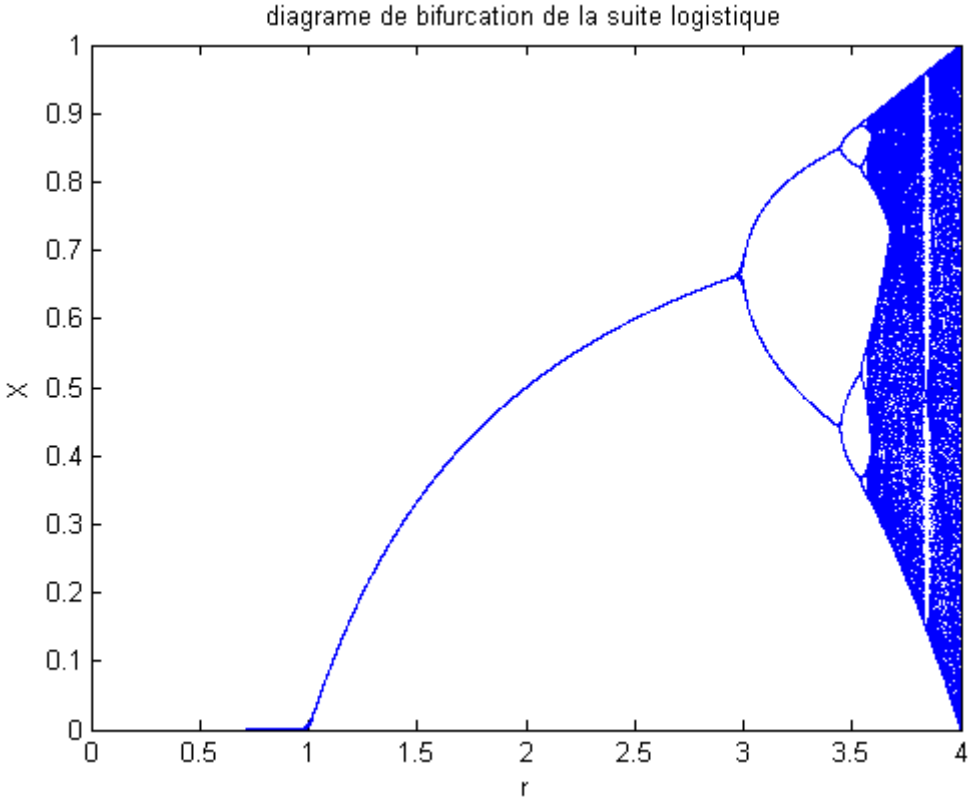


Figure 1.4 diagramme de bifurcation généralisé

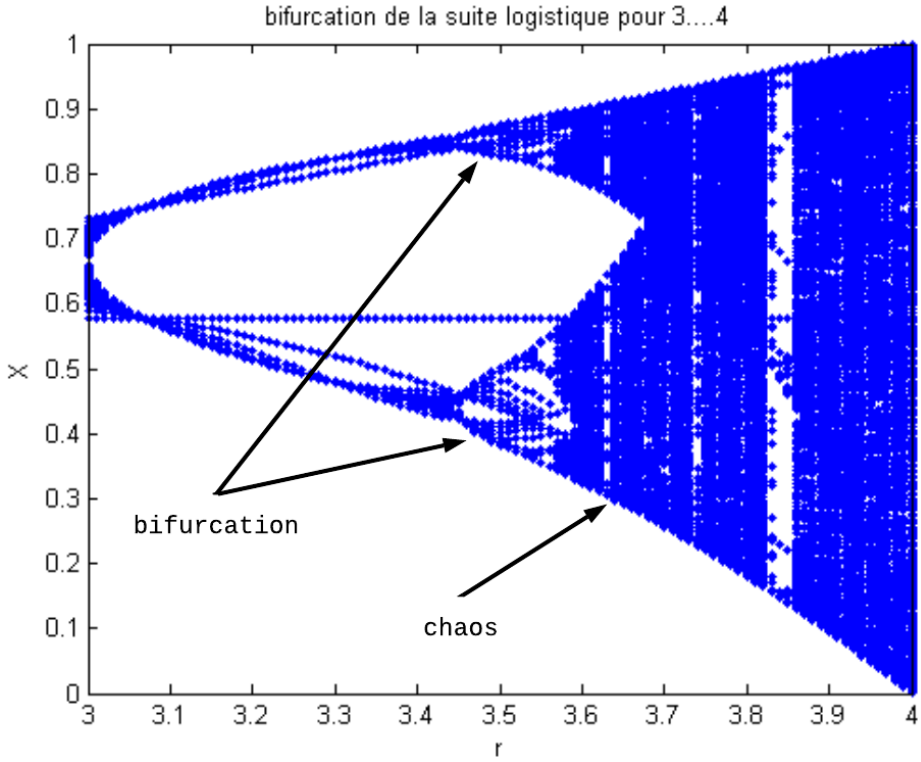


Figure 1.5 le diagramme de bifurcation pour r entre 3 et 4

1.9.2. Exposant de Lyapunov

L'exposant de Lyapunov permet de détecter le chaos dans un système dynamique et de quantifier la stabilité ou l'instabilité de ces mouvements.[12]

Markus-Lyapunov (1857-1918) a étudié le phénomène de stabilité des systèmes dynamiques en développant une quantité appelée "exposant de Lyapunov" pour mesurer le degré de sensibilité d'un système dynamique. [13]

Le comportement du système dynamique est chaotique si l'exposant de Lyapunov est positif, et non chaotique si l'exposant de Lyapunov est négatif.[12]

La figure :1.6 suivante présente le diagramme de l'exposant de Lyapunov de la suite logistique pour $x0 = 0.1$ et $r\epsilon[3.5,4]$. Nous pouvons observer le comportement chaotique de la suite logistique dans l'intervalle [3.55 ,4] où l'exposant de Lyapunov est positif.

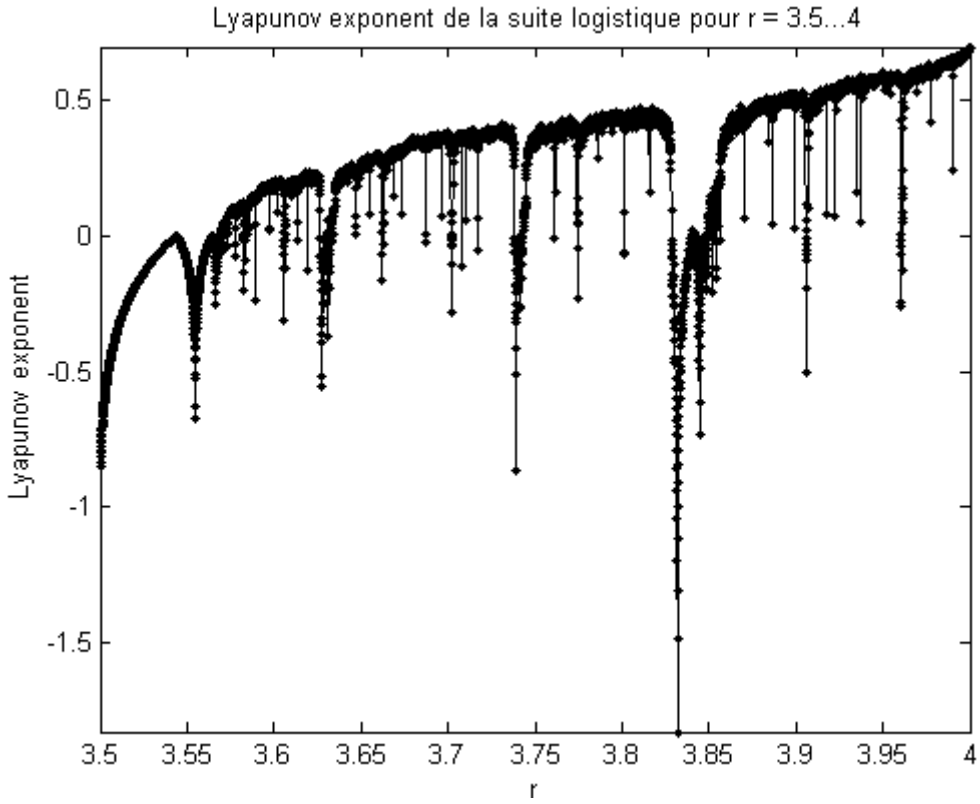


Figure :1.6 l'exposant de Lyapunov de la suite logistique.

1.10. Conclusion

Dans ce chapitre nous avons revus les notions de base sur la cryptographie, la cryptanalyse et le cryptage, y compris le cryptage symétrique et asymétrique. On a également vu l'intérêt de l'utilisation de la théorie du chaos dans les algorithmes de cryptage, en particulier l'exploitation des suites chaotiques et leurs propriétés chaotiques (confusion et diffusion). Ces notions nous serons utiles pour la suite de notre projet.

Chapitre 2

CHAPITRE 02 CRYPTAGE AUDIO BASE SUR LES SUITES CHAOTIQUES 2D

2.1. Introduction

Avec le besoin croissant de transmission et d'échange sécurisé d'informations confidentielles, le cryptage audio est devenu un outil essentiel pour protéger les fichiers audios d'un accès non autorisé.

Dans ce chapitre, nous allons revoir quelques suites chaotiques bidimensionnelles connues et particulièrement la suite 2D-LNIC Logistic Nested Infinite Collapse **[14]**. Il s'agit d'un système hyper-chaotique proposé en combinant une suite d'effondrement infini (1D-ICM) et une suite logistique. L'utilisation des suites 2D-LNIC en cryptage audio garantie la sécurité des fichiers audio.

2.2. Intérêt du cryptage audio

En raison de la croissance rapide des technologies de communication de nos jours, la confidentialité de l'échange et de la transmission d'un fichier audio secret est devenue un grand défi, et le meilleur moyen de le faire c'est par « cryptographie audio ». [15]

Le cryptage audio est la méthode qui consiste à rendre l'audio original inintelligible et inaccessible aux personnes non autorisées.[15]

La première utilisation de ce type de cryptage a été à la fin des années 1940, pendant la deuxième guerre mondiale, l'armée américaine a utilisé le cryptage audio pour empêcher les ennemis d'accéder à des informations et pour assurer une communication sécurisée entre les soldats.[16]

Alors, les principaux avantages du cryptage audio sont la transmission d'informations sécurisées et la garantie de la sécurité audio entre l'émetteur et le récepteur.[15]

2.3. Les suites chaotiques bidimensionnelles 2D

Les systèmes chaotiques 1D ont une structure simple et faciles à mettre en œuvre [17] sauf que ces suites n'ont qu'un seul paramètre de contrôle, tandis que les suites chaotiques bidimensionnelle en ont deux ou plus. Cela signifie que l'espace des paramètres des suite chaotiques 2D est plus grand que celui des suite chaotiques 1D, ce qui peut augmenter la sécurité de l'algorithme de cryptage.

Une autre différence est que les suites chaotiques 1D génèrent une séquence unidimensionnelle de nombres, alors que les suites chaotiques bidimensionnelle génèrent une séquence bidimensionnelle de nombres. Cela signifie que les suites chaotiques 2D peuvent être utilisées pour crypter des données bidimensionnelles, telles que des images ou des vidéos, alors que les suites chaotiques 1D sont généralement utilisées pour crypter des données unidimensionnelles, telles que des fichiers audios ou des textes.[14]

2.4. Type de suites chaotiques bidimensionnelles

Il existe de nombreux types de suites chaotiques bidimensionnelles ou 2D peuvent être utilisées pour le cryptage audio.

Vu qu'il existe plusieurs suites chaotiques, on se limitera ici de revoir seulement les suites chaotiques 2D les plus connues.

2.4.1. La suite de Hénon

La suite de Hénon (Hénon map) a été découverte pour la première fois en 1978, et elle est décrite comme suit :[18]

$$\begin{cases} x_{n+1} = 1 - ax_n^2 + y_n \\ y_{n+1} = bx_n \end{cases} \tag{2.1}$$

Où a et b sont les paramètres de contrôle du système.

Le système présente un comportement chaotique lorsque a=0,3 et b=1,4.

2.4.2. La suite de Lozi

La suite de Lozi (lozi map) est une suite du chaos à temps discret introduite par Lozi en 1978. Il s'agit d'un modèle mathématique décrit par l'équation (2.2) :[19]

$$\begin{cases} x_{n+1} = 1 - \alpha|x_n| + y_n \\ y_{n+1} = \beta x_n \end{cases} \quad (2.2)$$

Tel que α et β sont des paramètres de contrôle.

2.4.3. La suite standard 2D

La suite standard 2D est définie comme suit :

$$\begin{cases} x_{i+1} = \left(x_i + r_x + y_i + r_y\right) mod\ N \\ y_{i+1} = (y_i + r_y + k \sin\left(x_i + 1^N/2\pi\right)) mod\ N \end{cases} \quad (2.3)$$

Où K est un nombre entier positif et les deux paramètres r_x et r_y sont situés dans l'intervalle $[0 \ldots \ldots . N - 1]$ [20]

2.4.4. La suite d'Arnold

Cette suite porte le nom de Vladimir Arnold, qui en a démontré les effets en utilisant une image de chat dans les années 1960, il est défini par : [21]

$$\Gamma: (x, y) = (2x + y, x + y) mod\ N \quad (2.4)$$

$x, y \in \{0, 1, 2 \ldots N - 1\}$, et N est la taille de l'image.

2.5. Suite chaotique 2D-LNIC

LNIC signifie en anglais **L**ogistic **N**ested **I**nfinite **C**ollapse. Il s'agit d'un système hyper-chaotique bidimensionnel 2D proposé par Wu et al. **[14]** en combinant une suite chaotique dite à effondrement infini (1D-ICM) et une suite logistique.

2D-LNIC a deux paramètres contrairement à la suite logistique classique, ce qui augmente l'espace des paramètres des systèmes chaotiques.

L'expression mathématique de l'ICM 1D est la suivante :

$$f(u_1, x_n) = x_{n+1} = \sin\left(\frac{u_1}{x_n}\right) \quad (2.5)$$

Tel que u_1 est un paramètre de contrôle.

L'expression de la suite logistique vu sur le chapitre 1 et donnée ici comme suit :

$$g(u_2, y_n) = y_{n+1} = u_2 y_n (1 - y_n) \tag{2.6}$$

Où u_2 est un paramètre de contrôle varie de 0 à 4 [22]

L'expression mathématique de 2D-LNIC proposée par Wu et al. **[14]** est donnée par :

$$l_{2D-LNIC}(u_1, u_2, x_n, y_n) = \begin{cases} x_{n+1} = u_2 \sin\left(\frac{u_1}{y_n}\right)\left(1 - \sin\left(\frac{u_1}{x_n}\right)\right) \\ y_{n+1} = \sin\left(\frac{u_1}{u_2 x_n (1 - y_n)}\right) \end{cases} \tag{2.7}$$

2.6. Cryptage audio avancé AEA-NCS

Les algorithmes de cryptage traditionnels pour les images ne sont pas adaptés au cryptage audio car les informations audios sont fortement corrélées dans des temps adjacents et le type de données est en virgule flottante.[14]

Il existe de nombreux algorithmes de cryptage audio dans la littérature :

- Gnanajeyaraman et al Ont créé une table de recherche complexe et l'ont utilisée avec la technologie blockchain pour le cryptage audio. Cependant, l'algorithme est difficile à mettre en œuvre et présente des limites. [23]

- Dai et al ont utilisé un système chaotique de Chen Memristor pour le cryptage audio, avec de bons résultats. Cependant, l'espace des clés est restreint, ce qui le rend vulnérable aux attaques par force brute. [24]

- El et al [25], et Abdelfattah [26] ont utilisé le codage ADN pour le cryptage audio, ce qui améliore la sécurité mais réduit l'efficacité.

- Wang et Su ont utilisé le PWLCM pour générer un flux de clés et le codage et le décodage de l'ADN pour le cryptage audio, avec de bons résultats expérimentaux. Cependant, le PWLCM n'a qu'un seul paramètre de contrôle et doit être utilisé plusieurs fois pour générer le flux de clés [27]

- Algorithme de Feistel : Cet algorithme est considéré comme ayant des failles de sécurité et a été déchiffré par Solak et amélioré par Xie et al [28]

- Algorithme de codage de l'ADN et de cryptage par la suite logistique proposé par Naskar et al : cet algorithme nécessite l'utilisation multiple d'une suite logistique pour générer un flux de clés, ce qui réduit son efficacité. [29]

C'est pourquoi un algorithme de cryptage audio plus évoluée en cryptage chaotique est nécessaire.

Récemment, Wu et al [14] ont proposé un algorithme de cryptage audio basé sur 2D-LNIC appelé AEA-NCS qui signifie en anglais : Audio Encryption Algorithm based on a Nested Chaotic System.

Cet Algorithme effectue une confusion et une diffusion simultanément, ce qui augmente la sécurité de l'algorithme et le rend efficace face aux différentes attaques statistiques et de cryptanalyse. [14]

2.7. Principe de génération des clés en AEA-NCS

La clé secrète en AEA-NCS est générée par l'utilisation de fonctions de hachage [14].

La fonction de hachage est un cryptage à sens unique qui produit une sortie de longueur fixe en bits d'un message d'entrée quelle que soit sa taille. La fonction de hachage garantit qu'un petit changement, même d'un seul bit, dans l'entrée, produit une valeur de sortie entièrement différente. [2].

AEA-NCS utilise la fameuse fonction de hachage SHA-256 (Secure Hash Algorithme 256-bit en anglais). Donc l'espace de clé de AEA_NCS est de 2^{256}. Cela rend AEA_NCS plus fort et résistant aux attaques par force brute.[14]

SHA-256 est un type de fonction de hachage cryptographique qui appartient à la famille SHA, elle est à sens unique c'est-à-dire une fonction irréversible.[03]

SHA-256 produit toujours une sortie de 256 bits (32 octets), qui est toujours codé en 64 caractères alphanumériques en hexadécimal, quelle que soit la taille des données d'entrée, même si elle est vide [30] comme le montre la figure 2.1

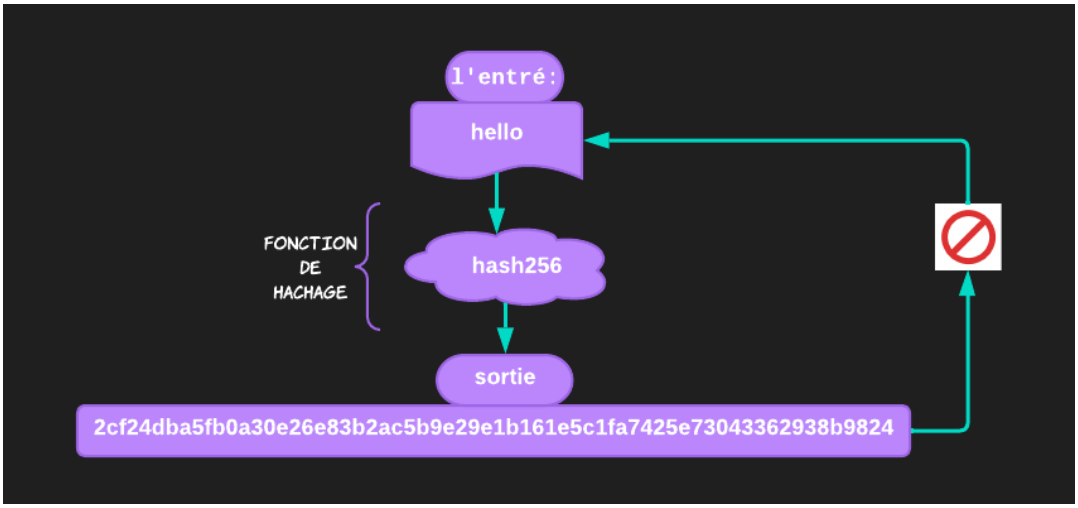


Figure2.1 : SHA-256

Le hash généré à la sortie est considéré dans le cas de l'algorithme AEA-NCS comme une clé secrète nommée « K » de taille 256 bits.

Des sous-clés $k1$, $k2$, $k3$ et $k4$ sont dérivés de la clé secrète « K » [14] comme le montre l'organigramme sur la figure 2.2.

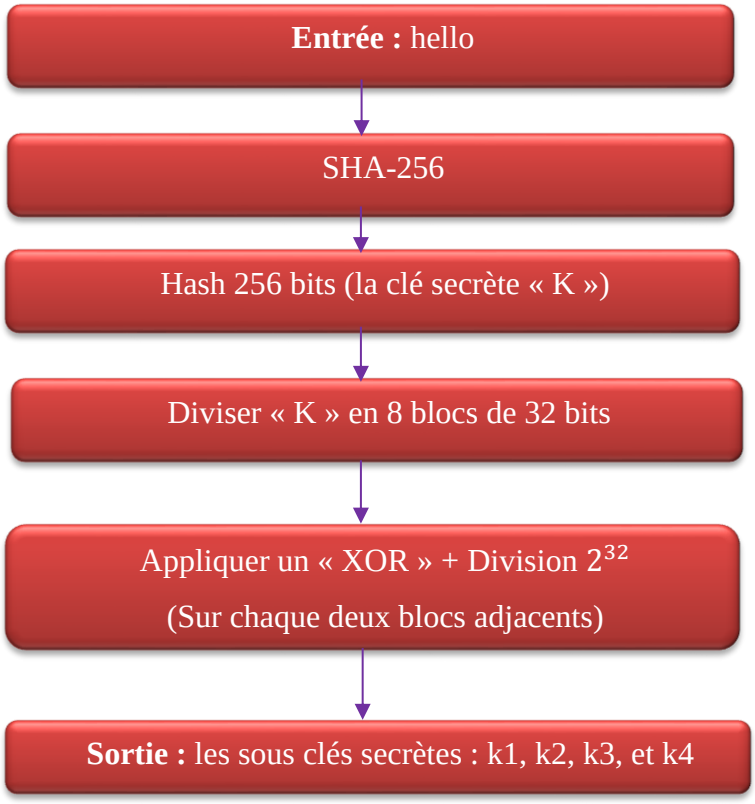


Figure 2.2 : Organigramme de génération des clés par l'AEA-NCS

Les sous-clés $k1$, $k2$, $k3$ et $k4$ sont donc obtenus en suivant ces étapes : [14]

- Le hash 256 bits qui représente la clé secrète « K » est divisée sur huit blocs de taille 32 bits.
- Chaque bloc est converti vers le format décimal
- Obtenir les sous-clés $k1$, $k2$, $k3$ et $k4$ tels que :

$$k1 = K\,(1:32) \oplus K\,(33:64) \;\; / \; 2^{32} \qquad (2.8)$$

$$k2 = K\,(65:96) \oplus K\,(97:128) \;\; / \; 2^{32} \qquad (2.9)$$

$$k3 = K\,(129:160) \oplus K\,(161:192) \,/\; 2^{32} \times 100 + 4 \qquad (2.10)$$

$$k4 = K\,(193:224) \oplus K\,(225:256) \,/\; 2^{32} \times 100 \qquad (2.11)$$

2.8. Algorithme de cryptage audio AEA-NCS

Supposons qu'on souhaite crypter une suite de données audio **A** de longueur L avec une clé secréte K générée comme décrit sur la section précédente.

Sachant que **A** comprend L valeurs réelles comprises dans l'intervalle [-1.0, 1.0], l'algorithme de cryptage AEA-NCS est illustré sur la figure 2.3 :

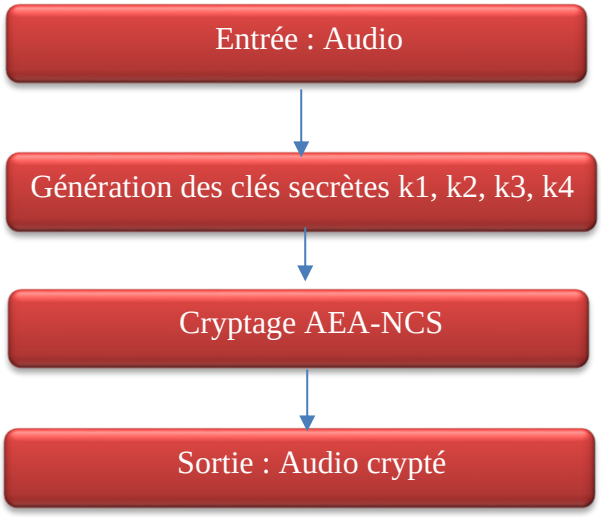


Figure2.3 : Organigramme cryptage AEA-NCS

Le flux de données audio crypté **C** en sortie de l'AEA-NCS est obtenu par les étapes décrites dans ce qui suit :[14]

- **Etape 01 :** Calculer le nouveau A (NA) :

$$NA = A \times \frac{255}{\max A - minA} + minA \times \frac{255}{minA - maxA} \qquad (2.12)$$

- A: données audio originales.
- $minA$: Valeur minimale de A.
- $maxA$: Valeur maximale de A.

Cette étape normalise l'intervalle de valeurs de A sur la plage [0, 255] au lieu [-1.0, 1.0].

- **Etape 02 :** Séparer NA en deux parties :
  - *Partie entière* $NA1 = floor(NA)$ où *floor* qui signifie l'arrondir à l'entier inférieur le plus proche
  - *Partie fractionnaire* $NA2 = NA - NA1$

- **Etape 03 :** Générer des sous clés k1, k2, k3 et k4 comme vu sur la section 2.7.

- **Etape 04 :** Générer les flux X et Y à l'aide de la suite chaotique 2D-LNIC en utilisant l'équation (2.7) en prenant comme paramètres :
  - $x0 = k1\ et\ y0 = k2$
  - $\mu 1 = k4\ et\ \mu 2 = k3$.

Les valeurs initiales $x0$ et $y0$ de la suite 2D-LNIC sont dérivées des sous-clés $k1$ et $k2$ et les paramètres de contrôle $\mu 1$ et $\mu 2$ sont dérivés des clés secrètes $k4$ et $k3$. Les deux flux X et Y ont une longueur L identique à celle de A et comprennent des valeurs réelles.

- **Etape 05 :** Calculer une matrice appelée matrice d'interférence S :

$$s = \text{mod}\ (floor\ (X \times 10^{10}), 256) \qquad (2.13)$$

Chaque valeur du flux X est multipliée par 10^{10} et arrondit par l'opération floor et modulo 256 pour obtenir des valeurs entières comprises entre 0 et 255.

- **Etape 06 :** Obtenir la matrice de tri G où Gi satisfit la condition que :$G_i < G_{i+1}$et $G_i \in Y$ (i = 1, 2, 3, ... L). Cette matrice servira comme indice de permutation des éléments de l'audio cryptée **C**.
- **Etape 07 :** Obtenir les valeurs du flux audio crypté **C** par les équations suivantes :

$$C\ [G(1)] = NA1(1) + S(1) \text{ mod } 256 \qquad (2.14)$$

$$C[G(2)] = NA1(2) + S(1) + C[G(1)] \text{ mod } 256 \qquad (2.15)$$

$$C[G(3)] = NA1(3) + S(1) + C[G(1)] + C[G(2)] \text{ mod } 256 \qquad (2.16)$$

Les trois premières valeurs du flux audio crypté $\boldsymbol{C}$ sont calculées à l'aide de la matrice de tri G, de la partie entière de l'audio $NA1$ et de la matrice d'interférence. Les valeurs restantes sont obtenues par les équations généralisées suivantes :

$$C[G(i)] = (NA1(i) + f1 + f2 + S(i)) \; mod \; 256 \qquad (2.17)$$

Où :

$f1 = floor((3.999 + k1/10^5) \times C[G(i-1)]/256 \times (1 - C[G(i-1)]/256) \times 10^{10})) \; mod \; 256$ (2.18)

$f2 = floor((3.999 + k2/10^6) \times C[G(i-1)]/256 \times (1 - C[G(i-2)]/256) \times 10^{10}) \; mod \; 256$ (2.19)

Les valeurs obtenues sont stockées dans les positions spécifiées par les indices du vecteur G. Pour chaque valeur de **C**, deux valeurs $f1$ et $f2$ sont calculées à l'aide des valeurs précédentes de **C** afin d'augmenter la non linéarité et l'effet de confusion et de diffusion.

- **Etape 08 :** Obtenir en sortie le flux audio cryptée final :

$$C \; (C = C + NA2) \qquad (2.20)$$

Il est calculé en additionnant la partie fractionnaire obtenue à l'étape 02 avec le flux audio crypté **C**.

Toutes ces étapes sont illustrées graphiquement sur la figure 2.4.

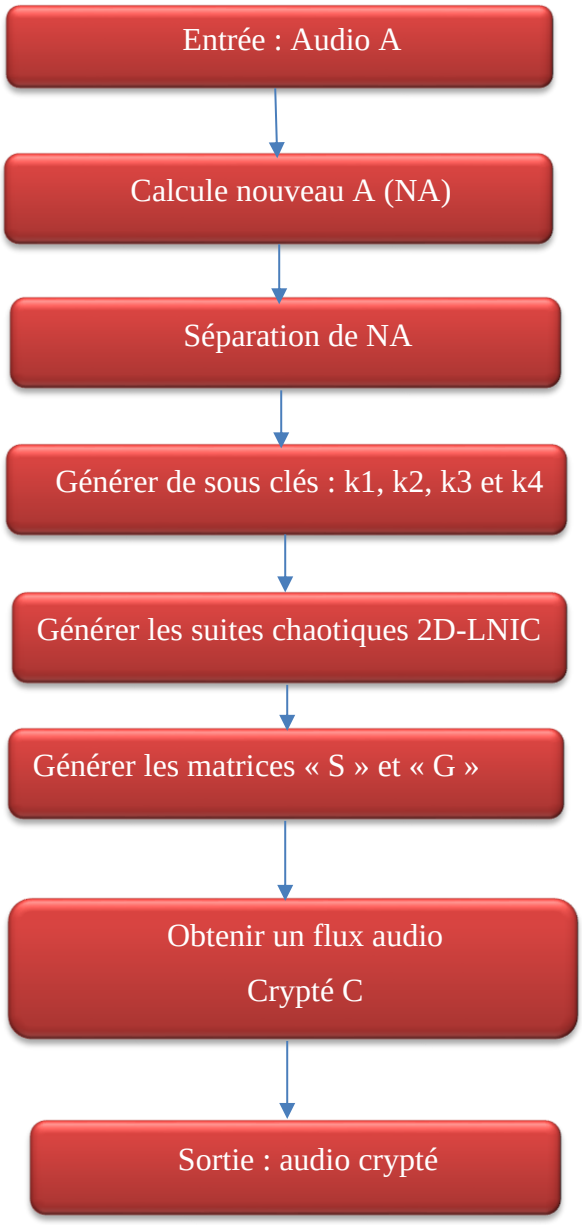


Figure 2.4 : organigramme du processus de cryptage audio

2.9. Algorithme de décryptage audio

Maintenant nous passons au processus inverse « le décryptage » [14]

- **Étape 01** : calculer la partie fractionnaire du NA :NA2

$$NA2 \leftarrow C - floor(C) \tag{2.21}$$

Chaque valeur de la partie fractionnaire est calculée en soustrayant les valeurs du flux audio crypté C, et sa partie entière, en utilisant la fonction floor.

- **Etape 02** : Générer des sous clés k1, k2, k3 et k4 comme vu sur la section 2.7

- **Etape 03** : Générer les flux X et Y à l'aide de la suite chaotique 2D-LNIC comme vu dans l'algorithme de cryptage étape 4.

- **Etape 04** : Calculer de la matrice d'interférence S comme vu dans l'algorithme de cryptage étape 5.

- **Etape 05** : Obtenir la matrice de tri G où Gi satisfit la condition que :$G_i < G_{i+1}$et $G_i \in Y$ (i = 1, 2, 3, ... L) comme vu dans l'étape 06 de l'algorithme de cryptage.

- **Etape 06** : Obtenir les valeurs du partie entière NA1 par les équations suivantes

$$NA1(1) \leftarrow C[G(1)] - S(1) \; mod \; 256 \quad (2.22)$$

$$NA1(2) \leftarrow C[G(2)] - S(1) - C[G(1)] \; mod \; 256 \quad (2.23)$$

$$NA(3) \leftarrow C[G(3)] - S(1) - C[G(1)] - C[G(2)] \; mod \; 256 \quad (2.24)$$

Les trois premières valeurs de $NA1$ sont obtenues à l'aide de valeurs du flux audios crypté C, la matrice de tri G et la matrice d'interférence S. Les valeurs restantes sont obtenues par les équations généralisées suivantes :

$$NA1(i) \leftarrow C[G(i)] - f1 - f2 - S(i) \; mod \; 256 \quad (2.25)$$

Où $f1$ et $f2$ déjà définis dans les équations (2.18) et (2.19)

- **Etape 07 :** obtenir en sortie une donnée audio originale A

$$A \leftarrow NA1 + NA2 \quad (2.26)$$

Restauration de l'audio original « A » par l'addition de partie entière NA1 obtenu dans l'étape 06 et le partie fractionnaire NA2 calculé dans l'étape 01.

Voici la figure suivante qui illustre toutes ces étapes :

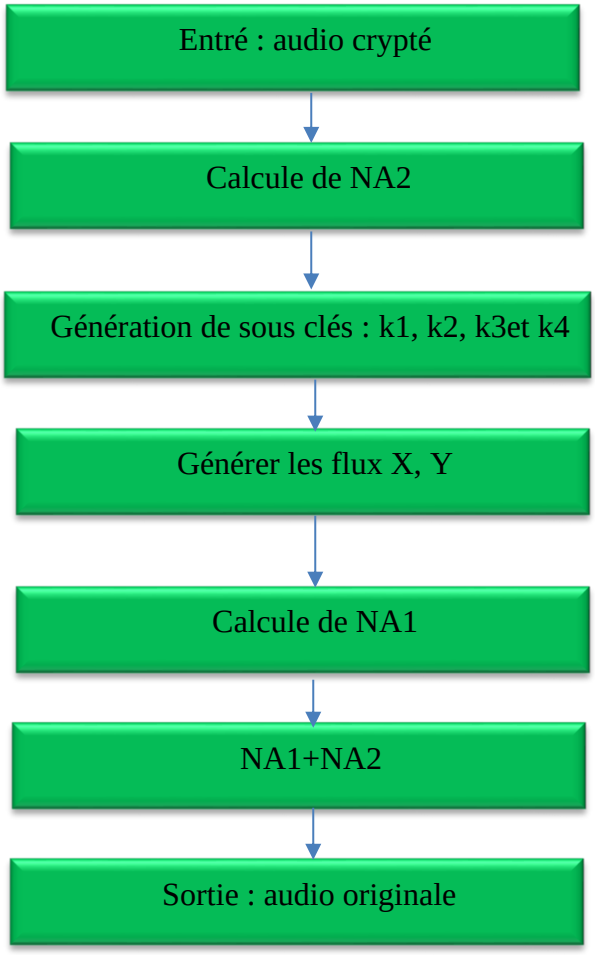


Figure 2.5 organigramme de l'opération de décryptage.

2.10. Conclusion

L'utilisation du cryptage audio est devenue de plus en plus importante dans les technologies de communication qui se développent rapidement aujourd'hui. L'inclusion de bruit dans les fichiers audio originaux par le biais du cryptage garantit qu'ils restent confidentiels et inaccessibles aux personnes non autorisées. L'utilisation de suites chaotiques bidimensionnelles pour le cryptage audio s'est avérée efficace et résistante à diverses attaques. En général, le cryptage audio offre un moyen sécurisé de transmettre des informations et de garantir la sécurité audio entre l'émetteur et le récepteur.

Chapitre 3

CHAPITRE 03 : RESULTATS ET DISCUSSIONS

3.1. Introduction

Dans ce chapitre, nous allons évaluer les performances et la sécurité de l'algorithme de cryptage proposé dans le chapitre précédent. Notre objectif est de tester en profondeur l'algorithme sur la base de critères spécifiques, afin de mieux comprendre son efficacité.

En outre, nous comparons l'algorithme proposé, connu sous le nom d'AEA_NCS, à d'autres algorithmes utilisant la suite de Lozi. Cette analyse comparative fournit des informations précieuses sur les performances de l'algorithme de cryptage proposé par rapport à un autre algorithme.

3.2. Environnement de travail

Dans le cadre de notre étude, nous utilisons :

- Un PC portable doté d'un processeur Intel® 2957u deuxième génération de fréquence 1.40 GHZ.
- MATLAB version R2010a : nous avons utilisé les fonctions et les bibliothèques fournies par MATLAB pour coder et simuler les algorithmes de cryptage audio, analyser les résultats et mesurer les performances.
- La base de données de fichiers audio ESC-50 (github.com/karolpiczak/ESC-50) qui contient une collection de 2000 enregistrements audio environnementaux de durée 5 secondes classés en 50 classes (40 exemples par classe) réparties en 5 catégories principales :
    - Sons d'animaux,
    - Paysages sonores naturels et sons d'eau
    - Sons humains non verbaux
    - Sons intérieurs/domestiques
    - Bruits extérieurs/urbains.

Les fichiers audios sont au format .wav un format de fichier audio standard pour le PC Windows, développé par Microsoft et IBM.

Pour notre étude, nous allons choisir au moins un fichier audio de chaque catégorie parmi les cinq afin de mesurer l'efficacité de l'algorithme de cryptage audio AEA-NCS.

Les fichiers audios choisis sont :

- Le son du coq dans la catégorie des animaux
- Le son de la pluie dans la catégorie des paysages sonores naturels et des sons d'eau.
- Le rire dans la catégorie des sons humains non verbaux
- L'alarme de l'horloge dans la catégorie des sons intérieurs/domestiques
- Klaxon de voiture et le train dans la catégorie des bruits extérieurs/urbains.

La figure 3.1 montre un exemple d'un signal audio extrait d'un des fichiers audios de l'ensemble ESC-50.

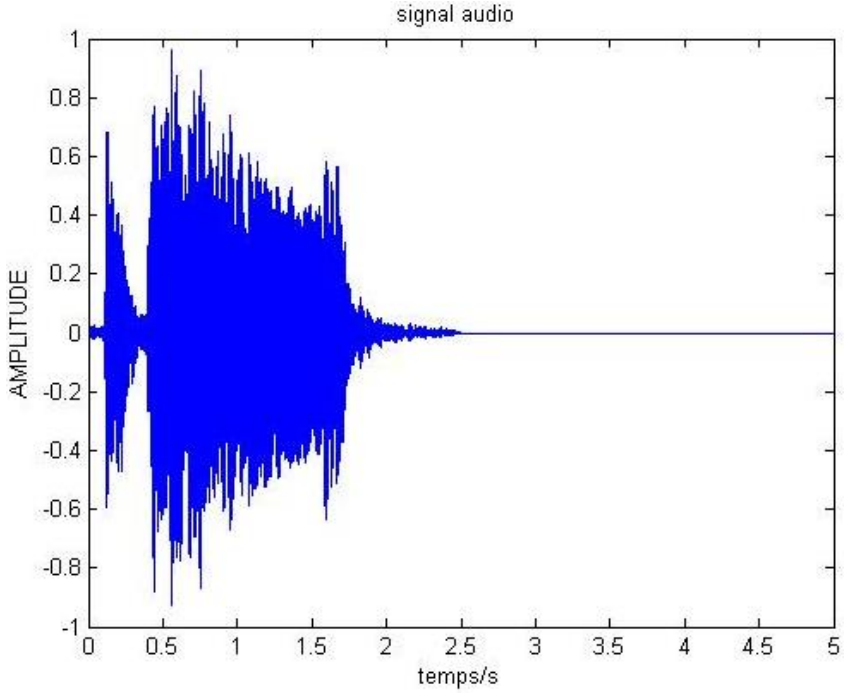


Figure3.1 : Exemple d'un signal audio

3.3. Critères de performances

Pour mesurer les performances d'un algorithme de cryptage audio, il existe de nombreux critères de performances importants qui doivent être pris en compte pour déterminer sa sécurité. Parmi les critères les plus importants on trouve :

- L'entropie

- Le coefficient de corrélation
- L'attaque différentielle
- L'espace de la clé
- La sensibilité de la clé

3.3.1 Entropie

Il s'agit d'une mesure mathématique [02] qui montre l'aléatoire et chaotique de la distribution de l'information. Plus l'entropie est élevée et proche de 8, plus l'information est imprévisible et complexe, et plus l'entropie est faible, plus l'information est prévisible. [14]

Son équation est :[31]

$$H(x)=-\sum_{i=0}^{2^n-1} p_i(x) log2(p_i(x)) \qquad (3.1)$$

x est l'échantillon étudié, Pi est la probabilité d'apparition de l'octet i.

3.3.2. Coefficient de corrélation

Le coefficient de corrélation est défini par l'équation (3.1).

$$r(p,q) = \frac{cov(p,q)}{\sigma(p)\sigma(q)} \qquad (3.2)$$

Où q est la valeur de l'élément adjacent à p.[14]

C'est une grandeur qui mesure la similarité de deux éléments adjacents [14]. Dans un système de cryptage sécurisé, la corrélation entre les éléments adjacents du texte crypté(ciphertext) obtenu doit être faible « proche de 0 » pour empêcher les attaquants de casser l'algorithme e, utilisant certains types d'attaques statistiques pour récupérer les informations d'origine(plaintext).

3.3.3. L'attaque différentielle

L'attaque différentielle est un moyen de comparer deux signaux audios pour trouver des faiblesses dans le cryptage. Un bon algorithme de cryptage devrait rendre difficile pour un attaquant de trouver ces schémas en répartissant l'effet d'un seul bit de texte en clair sur la plus grande partie possible de l'audio crypté.

Deux méthodes sont couramment utilisées pour mesurer l'effet d'un petit changement dans l'audio original : Unified Average Changing Intensity (UACI) et Number of Pixels Change Rate (NPCR). [20]

Leurs équations sont données comme suit :

$$\begin{cases} NPCR = \frac{1}{L}\sum_{i=1}^{L} |Sign(\lfloor C1(i) \rfloor - \lfloor C2(i) \rfloor) \times 100\% & (3.3) \\ UACI = \frac{1}{L}\sum_{i=1}^{L} \frac{|\lfloor C1(i) \rfloor - \lfloor C2(i) \rfloor|}{255} \times 100\% & (3.4) \end{cases}$$

Où $C1$ est le texte chiffré original, $C2$ est le nouveau texte chiffré, $\lfloor x \rfloor$ est la fonction d'arrondissement vers le zéro, $sign(x)$ est la fonction signe, et L est la longueur du signal audio.

3.3.4. Espace des clés

La clé est la partie essentielle dans chaque système de cryptage. L'espace des clés indique le nombre total de clés possibles pouvant être utilisées avec un algorithme de cryptage, plus l'espace des clés est grand, plus l'algorithme de cryptage est considéré sécurisé, et devient plus difficile pour un attaquant de déterminer la clé correcte.[20]

3.3.5. Sensibilité de la clé

La sensibilité de la clé signifie que même une petite modification de la clé secrète utilisée pour le cryptage devrait produire un résultat crypté complètement différent.

En d'autres termes, si un seul bit de la clé est modifié, l'audio en résulte doit être entièrement décrypté et par conséquent on ne doit pas connaître l'audio original. Cette caractéristique est importante pour garantir la sécurité des données audio cryptées.[20]

3.5. Résultats des simulations et analyse de sécurité

Dans le but d'évaluer la performance d'AEA-NCS, nous avons utilisé différents tests de sécurité sur des fichiers audio pour prouver la sécurité et l'efficacité d'AEA-NSC numériquement et graphiquement.

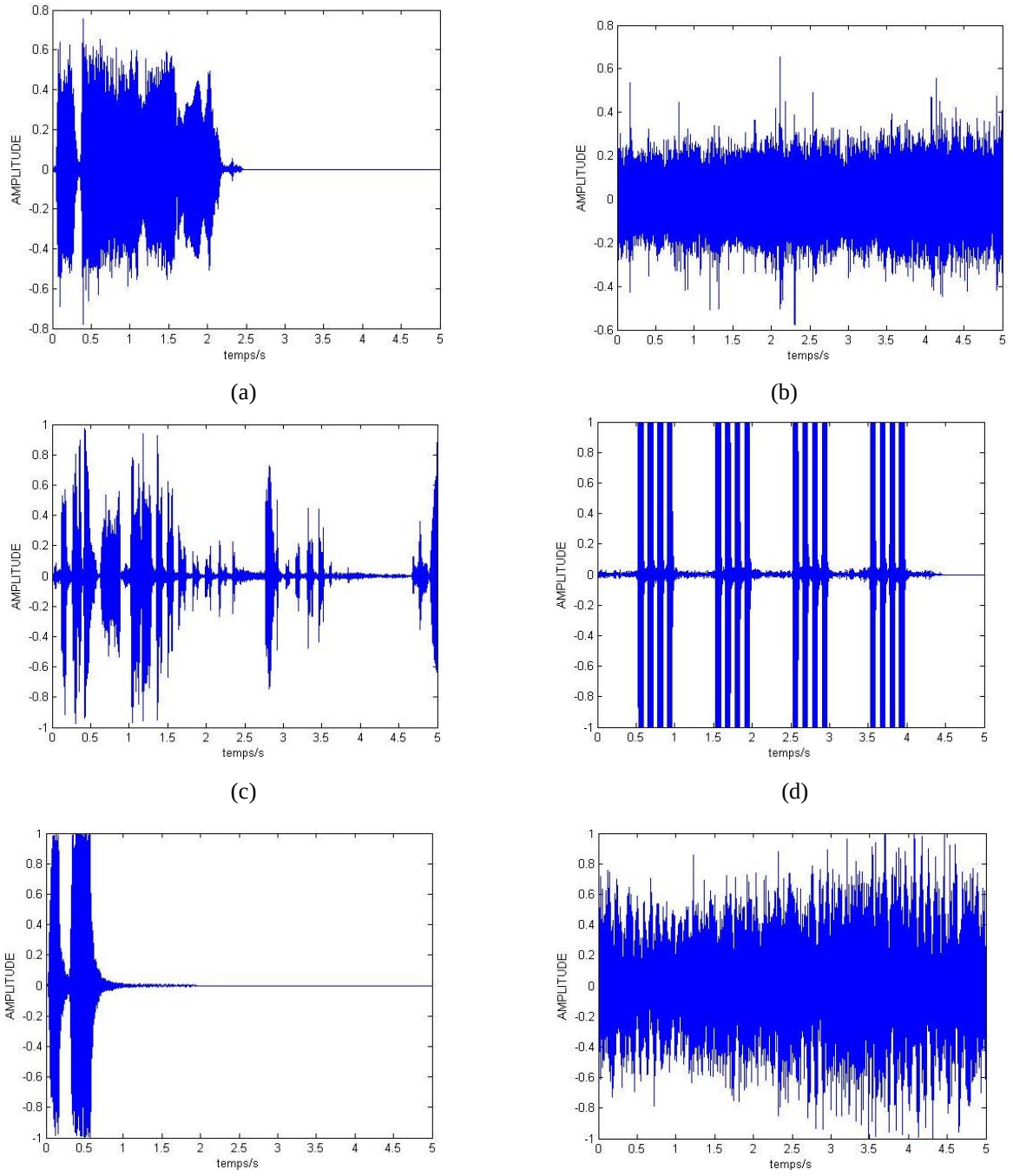
3.5.1. Résultats du cryptage & du décryptage

Nous appliquons l'algorithme AEA-NCS pour le cryptage et le décryptage des fichiers audio sélectionnés parmi les fichiers ESC-50.

La figure 3.2 montre les signaux audios qu'on souhaite crypter avec l'algorithme AEA-NCS.

La figure 3.3 montre les signaux audios après cryptage AEA-NCS en utilisant la clé de cryptage **K**={cf67be5ffc6ab758a53be70d32b2530ae46771e15feb811f93ef018f6d92ed4e}.

Nous remarquons que peu importe le type du signal audio, on obtient toujours un signal audio crypté identique dont la distribution de l'amplitude est uniforme ce qui prouve que l'AEA-NCS offre de bonne performance de cryptage et ne fuite aucune information sur l'audio original.



(a) (b)

(c) (d)

(e) (f)

Figure3.2. Signaux audio originaux (a) 1-39923-A-1.wav. (b) 1-21189-A-10.wav (c) 5-242932-A-26.wav. (d) 5-250629-A-37.wav. (e) 1-19026-A-43.wav. (f) 2-205966-A-16.wav

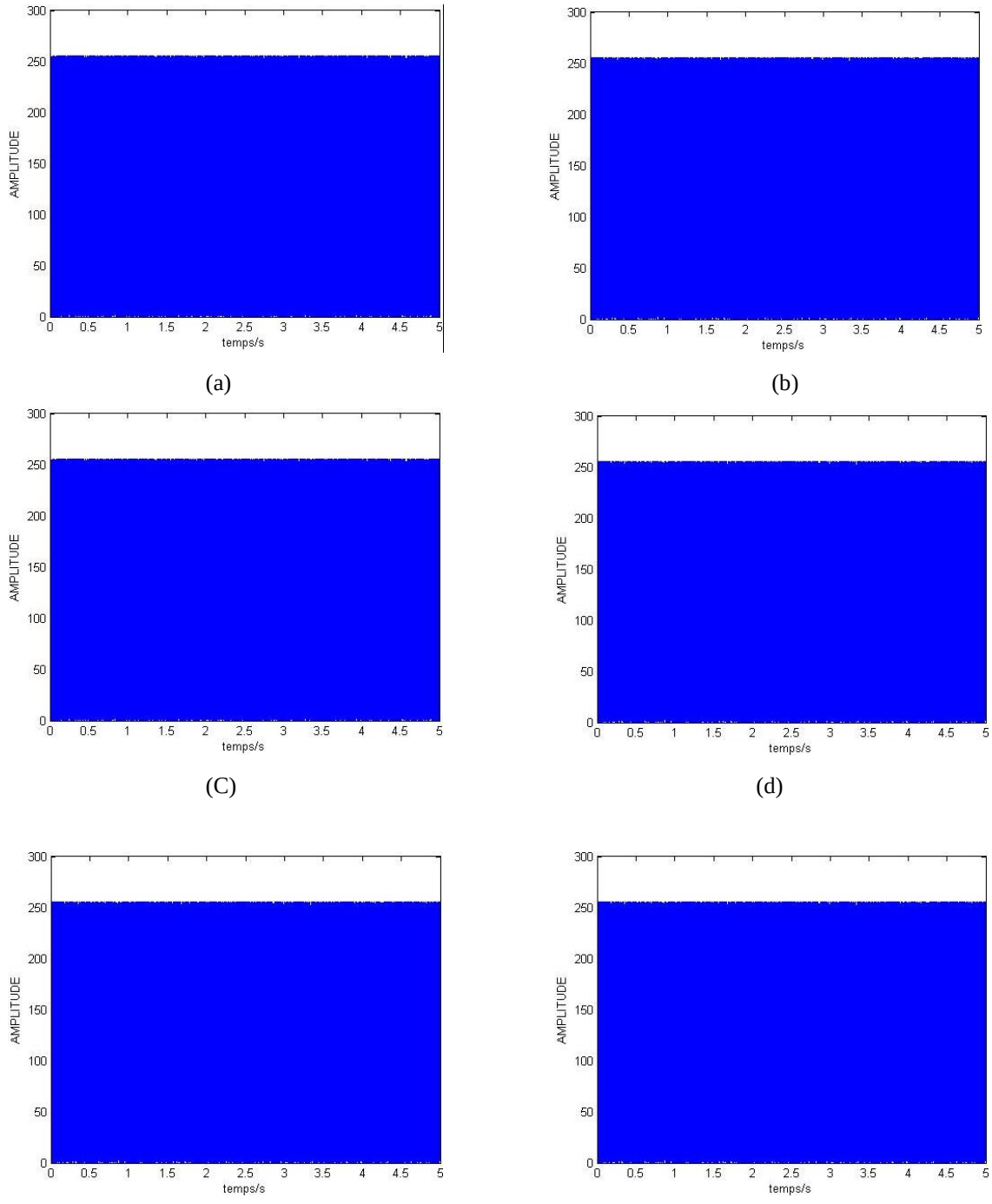


Figure3.3. Signaux audios cryptés par AEA-NCS. (a) 1-39923-A-1.wav. (b) 1-21189-A-10.wav (c) 5-242932-A-26.wav. (d) 5-250629-A-37.wav. (e) 1-19026-A-43.wav. (f) 2-205966-A-16.wav

La figure 3.4 montre qu'après le décryptage AEA-NCS par une clé **K** identique à celle utilisé en cryptage on a obtenu les signaux audios originaux.

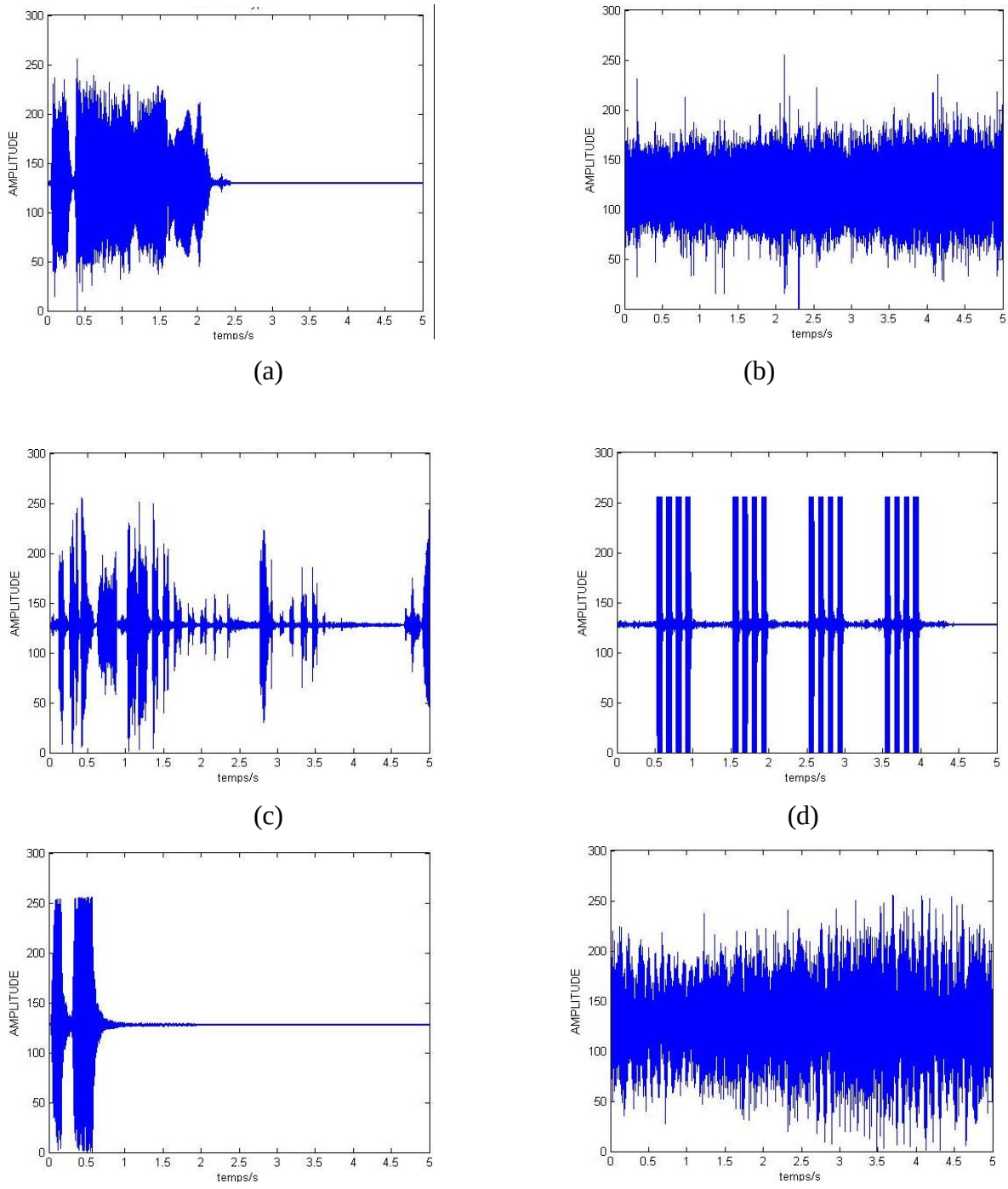


Figure3.4. Signaux audios décryptés par AEA-NCS (a) 1-39923-A-1.wav (b) 1-21189-A-10.wav (c) 5-242932-A-26.wav (d) 5-250629-A-37.wav (e) 1-19026-A-43.wav (f) 2-205966-A-16.wav

3.5.2 Evaluation de l'entropie

Comme le montre le tableau 3.1, les valeurs de l'entropie sont très proches de la valeur théorique « 8 », Il serait donc difficile pour un attaquant d'obtenir le texte en clair original (plaintext) à partir du texte crypté (ciphertext) produit par AEA_NCS.

Audio	Plaintext	Ciphertext
1-11687-A-47.wav	6.667247	7.999187
1-19026-A43.wav -	2.158945	7.999201
1-21189-A-10.wav	6.260040	7.999147
1-39923-A-1.wav	4.190523	7.999130
1-49409-A-8.wav	5.594314	7.999066
1-208757-A-2.wav	7.160551	7.999176
2-205966-A-16.wav	7.009271	7.999289
5-242932-A-26.wav	4.755275	7.999273
A5-250629-37.wav	4.302575	7.999092
Moyenne	5.344305	7.999173

Tableau 3.1 : Evaluation de l'entropie

3.5.3. Evaluation du coefficient de corrélation

Comme nous l'avons mentionné dans la section 3.3.2, le coefficient de corrélation du texte crypté doit être proche de 0 si on veut avoir un algorithme de cryptage sécurisé.

Les tableaux 3.2 et 3.3 présentent les valeurs du coefficient de corrélation de AEA_NCS pour le texte en clair(plaintext) et le texte chiffré(ciphertext) tel que : An est le n-ème élément de l'audio, An+1 est l'élément (n +1) th de l'audio, An+2 est l'élément (n + 2) th de l'audio.

D'après le tableau 3.3, nous pouvons voir que les valeurs sont proches de « 0 », ce qui montre que AEA_NCS est capable de casser la corrélation non seulement entre les éléments adjacents, mais aussi entre les éléments non adjacents ce qui lui offre une résistance aux attaques statistiques.

Audio	Plaintext		
	An, An+1	An, An+1	An, An+2
1-11687-A-47.wav	0.9076	0.7369	0.6545
1-19026-A-43.wav	0.9705	0.8994	0.8141
1-21189-A-10.wav	0.8775	0.5902	0.3008
1-39923-A-1.wav	0.9757	0.9055	0.7962
1-49409-A-8.wav	0.9475	0.8030	0.5864
1-208757-A-2.wav	0.9890	0.9584	0.9139
2-205966-A-16.wav	0.9918	0.9677	0.9289
5-242932-A-26.wav	0.9285	0.9312	0.9244
A5-250629-37.wav	0.8299	0.4121	-0.0920
Moyenne	0.9353	0.8004	0.6474

Tableau3.2 : Coefficients de corrélation des signaux audio originaux

Audio	Ciphertext		
	An, An+1	An, An+2	An, An+3
1-11687-A-47.wav	0.0009	-0.0012	-0.0005
1-19026-A-43.wav	-0.0023	-0.0016	-0.0020
1-21189-A-10.wav	0.0024	0.0002	-0.0062
1-39923-A-1.wav	-0.003	-0.0023	0.0007
1-49409-A-8.wav	0.0017	-0.0008	0.0015
1-208757-A-2.wav	-0.0006	- 0.0012	0.0001
2-205966-A-16.wav	0.0012	0.0004	-0.0019
5-242932-A-26.wav	0.0021	-0.0025	0.0030
A5-250629-37.wav	-0.0016	-0.0062	0.0016
Moyenne	0.0001	-0.0006	-0.0003

Tableau 3.3 : Coefficients de corrélation des signaux audio cryptés par AEA_NCS

3.5.4 Evaluation du NPCR et UACI

Pour qu'un algorithme soit considéré comme sécurisé contre les attaques différentielles, il faut que [32] :

- NPCR soit compris entre 99,5875 % et 100 %.
- UACI soit compris entre 33,3648 % et 33,5623 %.

Dans notre étude, les résultats obtenus lors du calcul du NPCR et UACI sont présentés dans le tableau 3.4. Les valeurs du NPCR et de l'UACI ont été calculées par les équations précédentes (3.3) et (3.4).

Audios	NPCR	Pass/fail	UACI	Pass/fail
1-11687-A-47.wav	99.6204	Pass	33.5129	Pass
1-19026-A43.wav -	99.5923	Pass	33.4574	Pass
1-21189-A-10.wav	99.6063	Pass	33.4515	Pass
1-39923-A-1.wav	99.5918	Pass	33.4659	Pass
1-49409-A-8.wav	99.6027	Pass	33.4367	Pass
1-208757-A-2.wav	99.6073	Pass	33.5042	Pass
2-205966-A-16.wav	99.6014	Pass	33.3868	Pass
5-242932-A-26.wav	99.6068	Pass	33.4571	Pass
5-250629-A-37.wav	99.6054	Pass	33.3793	Pass
Moyenne	99.6038	Pass	33.4502	Pass

Tableau3.4 : Valeurs des NPCR et UACI en cryptage AEA_NCS

Nous pouvons constater que les valeurs de NPCR et d'UACI se situent dans la gamme acceptable (pass), ce qui nous indique que AEA_NCS a la capacité de résister aux attaques différentielles.

3.5.5. Espace de la clé secrète et sa sensibilité

Comme indiqué lors du chapitre 2, la génération de la clé secrète en cryptage AEA_NCS passe par un hachage SHA256 de 256bits soit un espace de clés de 2^{256}.

Un algorithme de cryptage est considéré comme résistant aux attaques par force brute lorsque son espace de clé est supérieur à 2^{100}[33]. Dans une attaque par force brute, l'attaquant va

essayer toutes les combinaisons possibles de la clé secrète dans l'espoir de tomber sur la bonne clé.

De ce fait, l'algorithme AEA-NCS est considéré comme résistant aux attaques par force brute. Cependant, pour s'assurer de cela, nous allons tester la sensibilité de la clé de AEA_NCS sur le fichier audio 5-261464-A-23.wav

La clé secrète originale utilisée dans le processus de cryptage est K et les nouvelles clés avec des modifications mineures (un seul caractère modifié) sont $K1$, $K2$ et $K3$.

- $K = f1dcb46b68cfdd627a701a160e5553e21a1e58d72f50a4ce568d81bd7ec5db2\boldsymbol{a}$
- $K1 = f1dcb46b68cfdd627a701a160e5553e21a1e58d72f50a4ce568d81bd7ec5db2\boldsymbol{b}$
- K2 $= f1dcb46b68cfdd627a701a160e5553e21a1e58d72f50a4ce568d81bd7ec5db2\boldsymbol{c}$
- $K3 = f1dcb46b68cfdd627a701a160e5553e21a1e58d72f50a4ce568d81bd7ec5db2\boldsymbol{d}$

Les résultats de la sensibilité des clés sont présentés dans la figure 3.5.

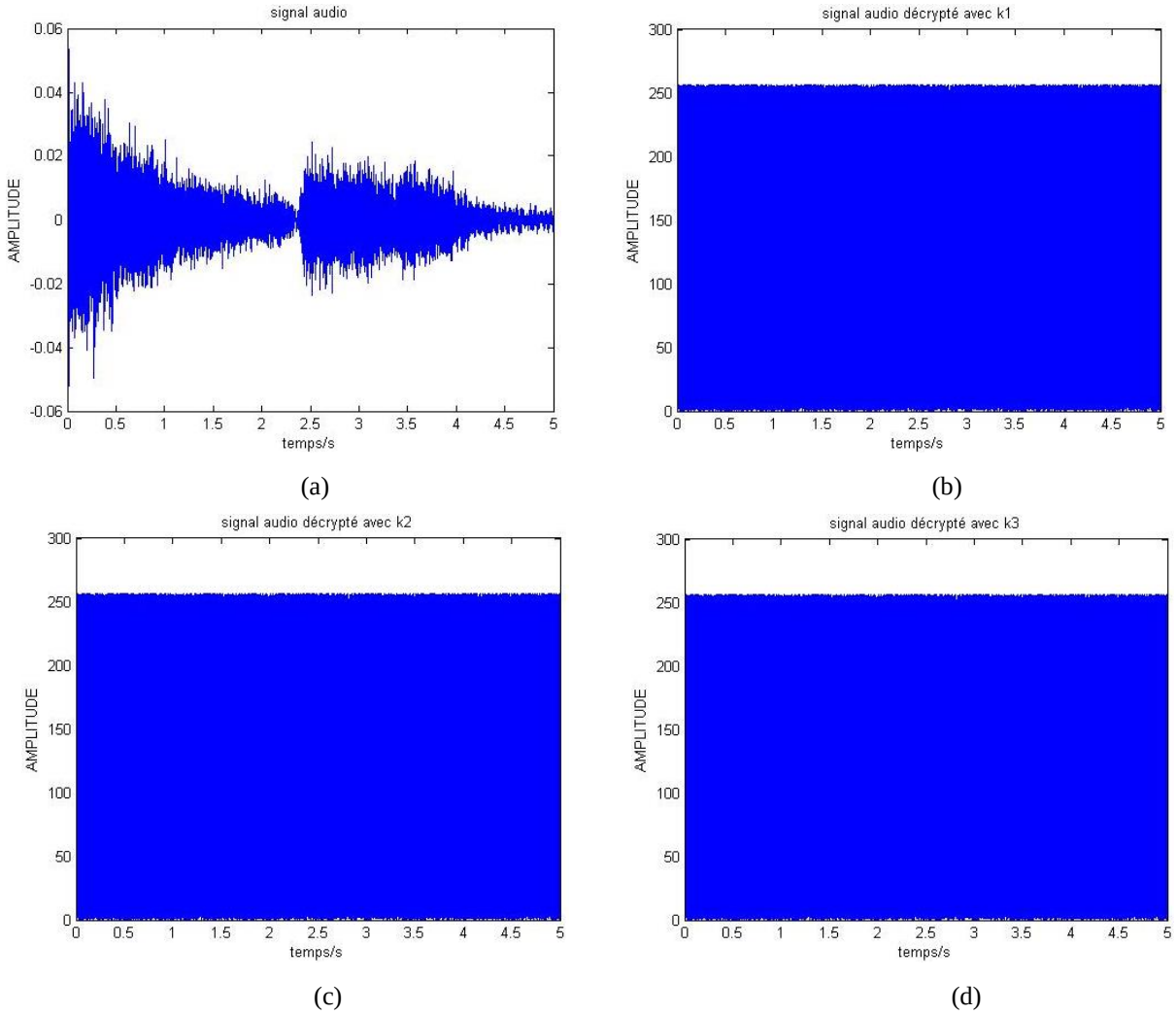


Figure3.5 Sensibilité de la clé secrète en AEA-NCS. (a) Audio décrypté par K. (b) Audio décrypté par $K1$. (c) Audio décrypté par $K2$. (d) Audio décrypté par $K3$.

Comme nous pouvons le voir, l'audio décrypté est brouillé lorsque nous utilisons une clé autre que la clé d'origine " K ", ce qui rend difficile pour un attaquant de trouver les informations utiles. De ce fait, la clé secrète en AEA_NCS est très sensible aux changements.

3.5.7 Immunité contre le bruit additif

Dans cette section, nous allons tester l'immunité de l'algorithme AEA-NCS contre le bruit blanc gaussien additif AWGN qui signifie en anglais « Additive White Gaussian Noise ».

Nous voulons ajouter du bruit blanc à un fichier audio avec un rapport signal/bruit (SNR) spécifique et essayer ensuite de récupérer le signal original de l'audio par décryptage pour voir si AEA_NCS résiste à ces perturbations en décryptage.

Les résultats de simulation sont illustrés dans la figure 3.6 avec un SNR = 0.5dB, ce qui signifie que le bruit est relativement grand par rapport au signal audio.

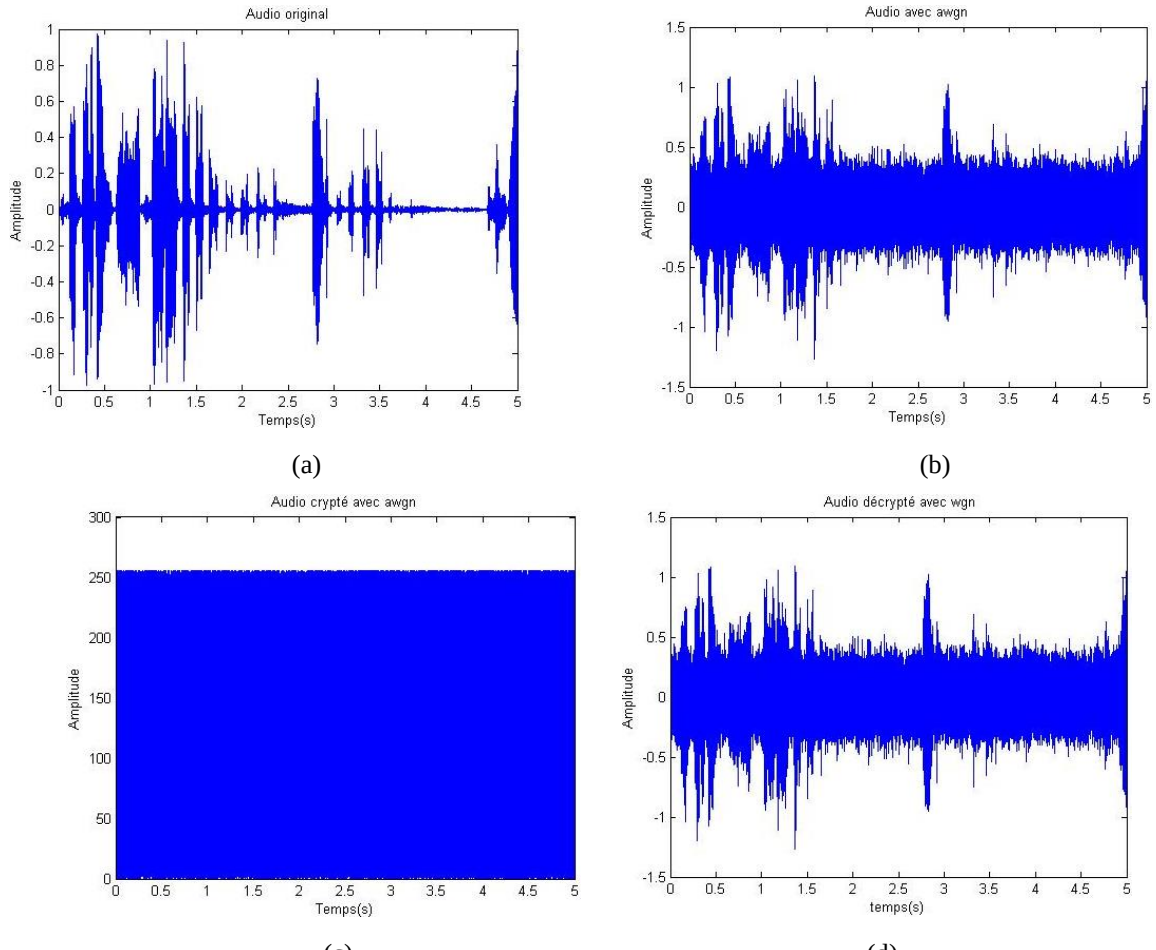


Figure3.6 : l'effet de AWGN sur AEA_NCS. (a) audio 5-242932-A-26.wav. (b) 5-242932-A-26.wav. avec WGN. (c) audio crypté avec AWGN. (d) audio décrypté avec AWGN.

Après simulation, nous pouvons distinguer l'audio original de l'audio décrypté malgré l'existence du bruit, ce qui rend AEA_NCS immunisé et non affecté par le bruit additif.

3.5.8. Temps d'exécution

La vitesse de cryptage de l'AEA_NCS est indiquée dans le tableau 3.5.

Audio	La taille (kb)	Le temps d'exécution (s)	La Vitesse (s/kb)
1-19026-A-43.wav	430	0.385857	0.000897
1-11687-A-47.wav	430	0.394889	0.000918
1-21189-A-10.wav	430	0.369530	0.000859
1-39923-A-1.wav	430	0.368775	0.000857
1-49409-A-8.wav	430	0.392129	0.000911
1-208757-A-2.wav	430	0.378529	0.000880
2-205966-A-16.wav	430	0.367158	0.000853
5-242932-A-26.wav	430	0.377600	0.000878
5-250629-A-37.wav	430	0.381238	0.000886
Moyenne	430	0.379523	0.000882

Tableau3.5 : Vitesse du cryptage de l'AEA_NCS

3.6. Comparaison 2D-LNIC vs Lozi en AEA-NCS

Dans cette section, nous proposons de remplacer 2D-LNIC en cryptage AEA-NCS par la suite Lozi vu sur le chapitre 2 qui est une suite chaotique bidimensionnelle.

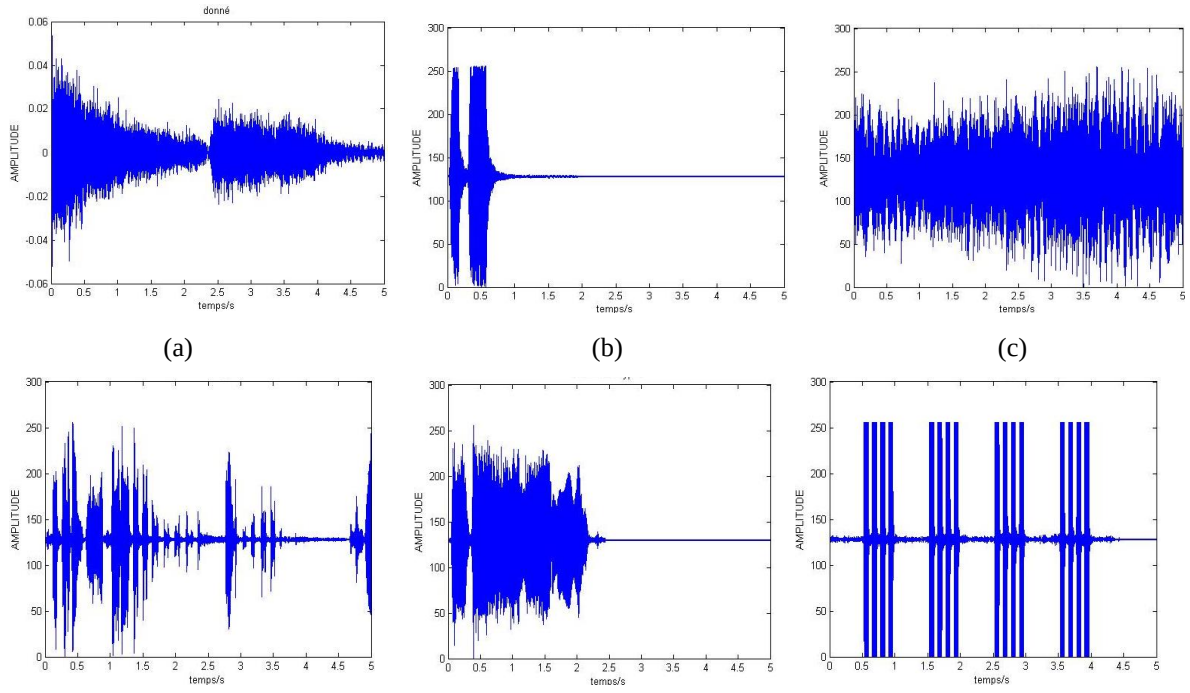
Pour des fins de comparaisons, nous appellerons ici ce cryptage AEA-NCS modifié AEA-LZM où LZM signifie Lozi map en anglais.

Ensuite, nous ferons une comparaison entre le AEA-LZM proposé et AEA _NCS pour voir celui qui présente les meilleures performances.

3.6.1. Résultats du AEA-LZM

Les figures de cryptage et décryptage par AEA_LZM sont présentés ci-dessus.

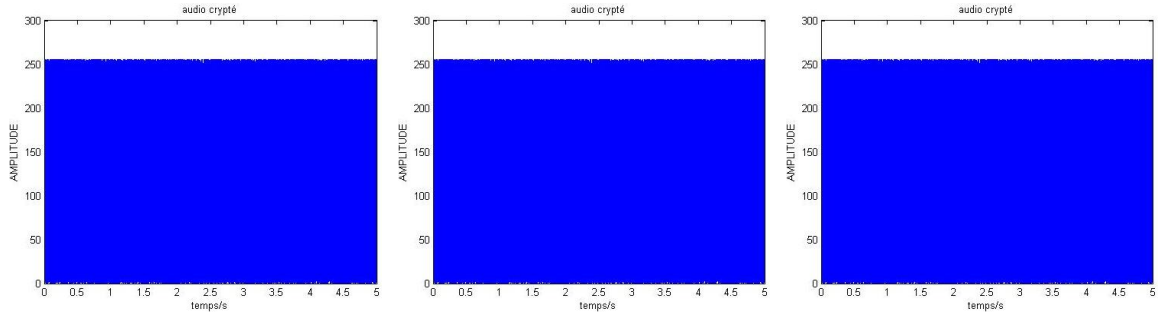
A partir de ces figures et visuellement, AEA_LZM a une bonne performance comme AEA_NCS.



(a) (b) (c)

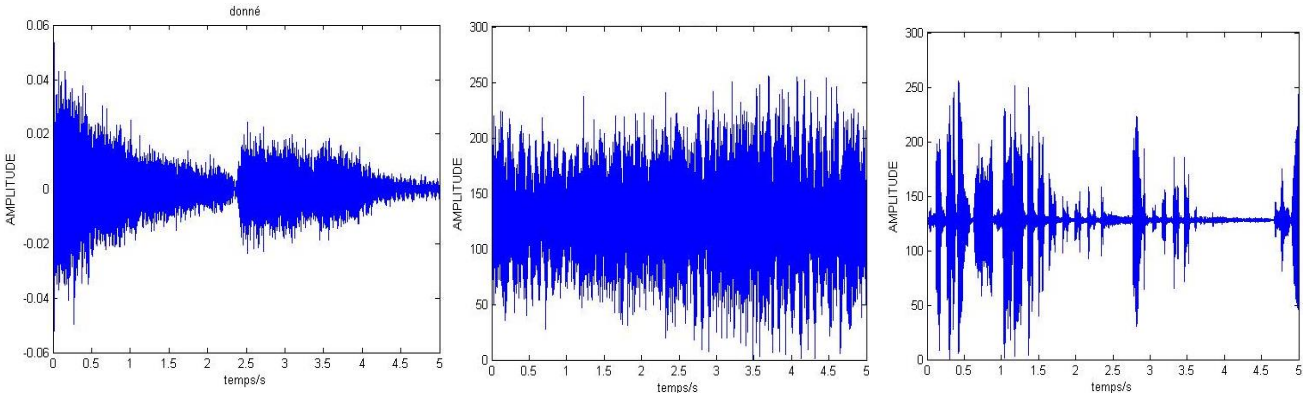
(d) (e) (f)

Figure 3.7: Description des informations audio. (a) 5-261464-A-23.wav. (b) 1-19026-A-43.wav. (c) 2-205966-A-16.wav. (d) 5-242932-A-26.wav. (e) 1-39923-A-1.wav. (f) 5-250629-A-37.wav



(a) (b) (c)

Figure3.8 : informations audio cryptées par AEA_LZM. (a) 5-261464-A-23.wav crypté. (b) 2-205966-A-16.wav. (c) 5-242932-A-26.wav



(a) (b) (c)

Figure 3.9: les informations audios décryptées par AEA_LZM. (a) 5-261464-A-23.wav. (b) 2-205966-A-16.wav. (c) 5-242932-A-26.wav

3.6.2. Comparaison de l'entropie

D'après le tableau 3.6, les valeurs d'entropie de AEA_NCS sont mieux et proches de la valeur théorique "8" que celles de AEA_LZM. La valeur d'entropie moyenne de AEA_NCS est de 7.999165 ,tandis que la valeur d'entropie moyenne de AEA_LZM est de 7.941525, ce qui rend difficile pour un attaquant d'obtenir le texte crypté (ciphertext) à partir du texte en clair (plaintext) pour AEA_NCS plus que pour AEA_LZM.

Algorithme	Audio	Plaintext	Ciphertext
AEA-NCS	**1-39923-A-1.wav**	4.190523	7.999130
	1-49409-A-8.wav	5.594314	7.999066
	1-208757-A-2.wav	7.160551	7.999176
	2-205966-A-16.wav	7.009271	7.999289
	Moyenne	**5.988665**	**7.999165**
AEA-LZM	**1-39923-A-1.wav**	4.190523	7.768610
	1-49409-A-8.wav	5.594314	7.999108
	1-208757-A-2.wav	7.160551	7.999216
	2-205966-A-16.wav	7.009271	7.999166
	Moyenne	**5.988665**	**7.941525**

Tableau3.6 : l'entropie de l'information de AEA_NCS vs AEA_LZM

3.6.3. Comparaison des coefficients de corrélation

Les coefficients de corrélation de AEA_LZM pour le texte crypté sont indiqués dans le tableau 3.7

La valeur moyenne du coefficient de corrélation pour le texte crypté de AEA_NCS entre les éléments adjacents et non adjacents (voir tableau 3.7) est meilleure et proches de "0" : que la valeur moyenne calculées par AEA_LZM, cela indique que AEA_NCS a une plus grande capacité que AEA_LZM à résister les attaques statistiques.

Algorithme	Audios	Ciphertext		
		A_n, A_{n+1}	A_n, A_{n+2}	A_n, A_{n+3}
AEA_NCS	**1-39923-A-1.wav**	-0.003	-0.0023	0.0007
	1-49409-A-8.wav	0.0017	-0.0008	0.0015
	1-208757-A-2.wav	-0.0006	- 0.0012	0.0001
	2-205966-A-16.wav	0.0012	0.0004	-0.0019
	Moyenne	**-0.0002**	**-0.0010**	**0.0001**
AEA-LZM	**1-39923-A-1.wav**	-0.0015	0.0408	-0.0028
	1-49409-A-8.wav	-0.0005	-0.0034	0.0016
	1-208757-A-2.wav	-0.0002	-0.0008	-0.0022
	2-205966-A-16.wav	-0.0006	0.0023	0.0028
	Moyenne	**- 0.0007**	**0.0097**	**-0.0002**

Tableau 3.7: coefficients de corrélation de signaux audios cryptés de AEA_NCS vs AEA_LZM

3.6.4 : Comparaison du NPCR et UACI

D'après le tableau 3.8, AEA_LZM a réussi de passer les tests NPCR et UACI avec un seul audio « 1-39923-A-1.wav », et a échoué avec les autres. Les valeurs obtenues sont très loin de 33% et 100%, ce qui rend AEA_LZM cassable devant les attaques différentielles contrairement à AEA_NCS qui a réussi dans les tests de NPCR et UACI pour tous les audios.

Algorithme	Audios	NPCR	Pass/Fail	UACI	Pass/Fail
AEA_NCS	**1-39923-A-1.wav**	99.5918	Pass	33.4659	Pass
	1-49409-A-8.wav	99.6027	Pass	33.4367	Pass
	1-208757-A-2.wav	99.6073	Pass	33.5042	Pass
	2-205966-A-16.wav	99.6014	Pass	33.3868	Pass
	Moyenne	99.6008	Pass	33.4484	Pass
AEA_LZM	**1-39923-A-1.wav**	99.8218	Pass	33.3821	Pass
	1-49409-A-8.wav	5.0163	Fail	1.6688	Fail
	1-208757-A-2.wav	11.2086	Fail	3.7482	Fail
	2-205966-A-16.wav	25.0454	Fail	8.4948	Fail
	Moyenne	35.273	Fail	11.8235	Fail

Tableau 3.8 : NPCR et UACI de AEA_NCS vs AEA_LZM.

3.6.5. Comparaison de la sensibilité des clés

L'espace de clés de AEA_LZM est 2^{256} comme AEA_NCS, car la clé secrète des deux est générée par sha-256, ce permet pour les deux de résister les attaques par force brute.

Nous allons répéter le même processus appliqué dans la section (3.5.6) sur AEA_LZM. Les résultats de test de la sensibilité des clés sont présentés dans la figure 3.10. On peut voir que la clé de AEA_LZM est sensible comme celle de AEA_NCS.

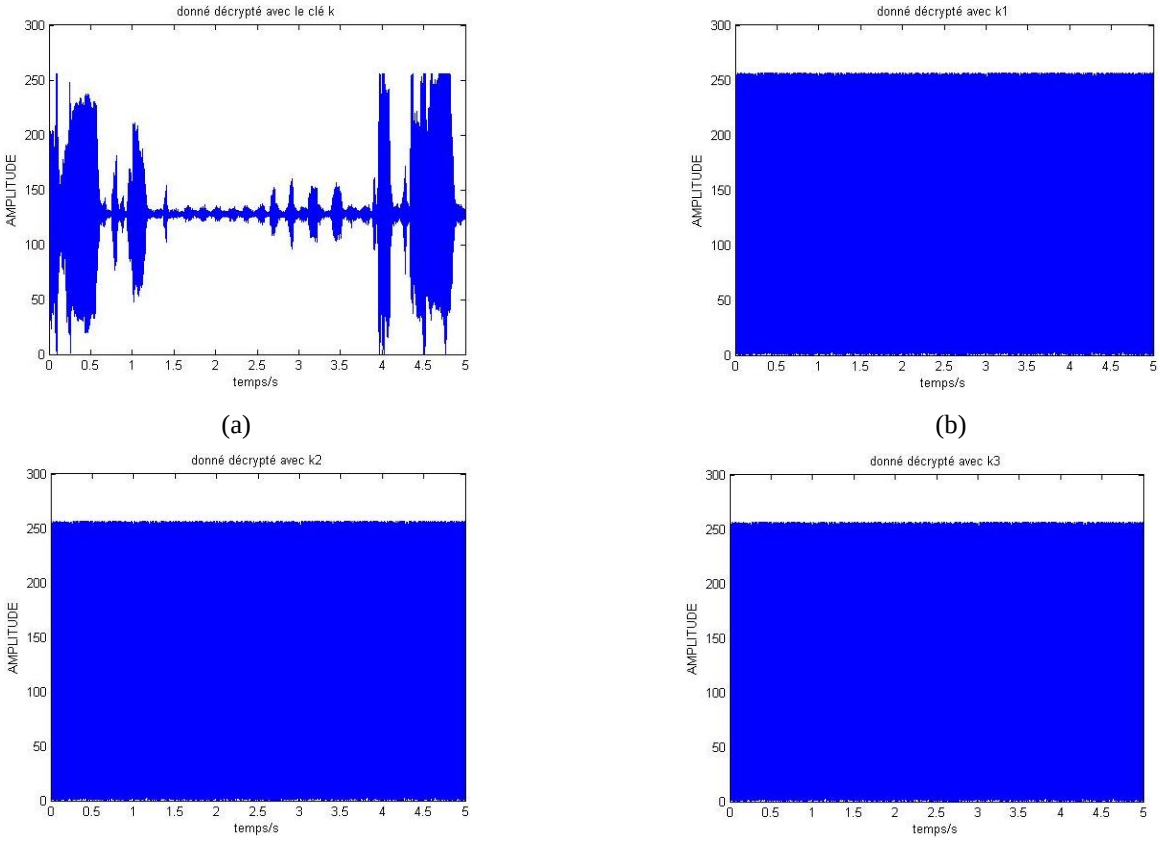
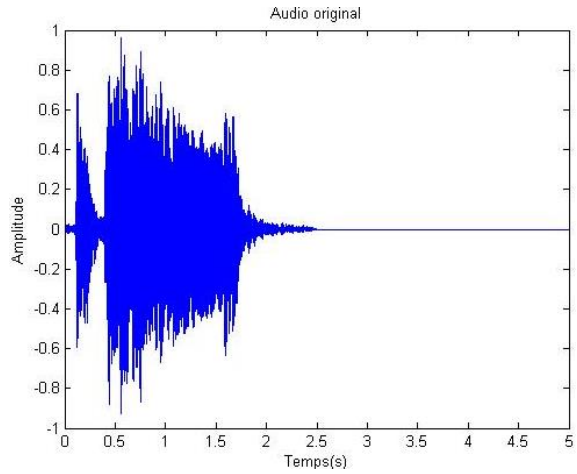


Figure 3.10 : sensibilité de clé de AEA_LZM. (a) 1-5996-A-6.wav décrypté par ’k’. (b) décrypté par ’k1’. (c) décrypté par ’k2’. (d) décrypté par ’k3’.

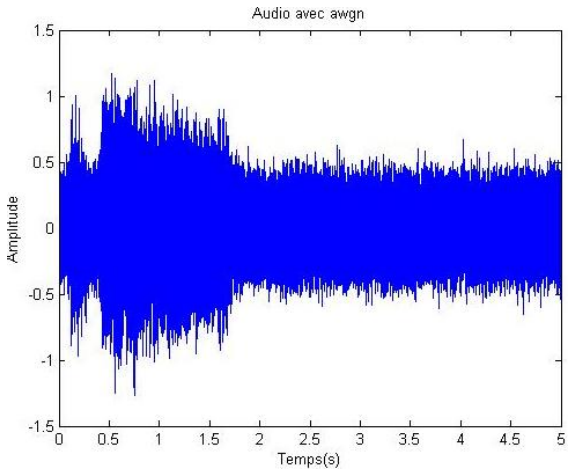
3.6.7. Résistance au bruit additif

Nous utilisons la même valeur SNR=0.5db que celle utilisée dans AEA_NCS

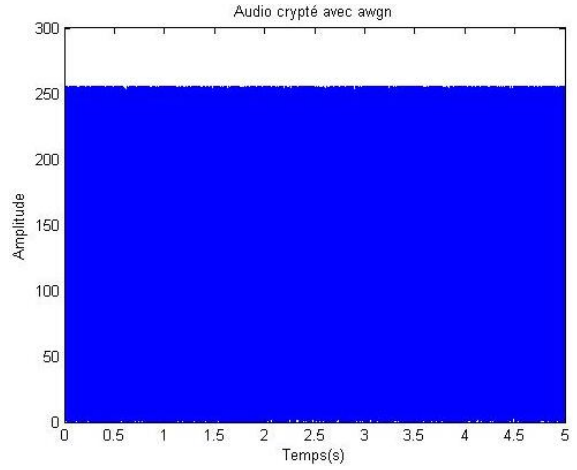
Les résultats présentés dans la figure 3.11 montrent que AEA_LZM est aussi imperméable aux hauts niveaux de bruit comme AEA_NCS.



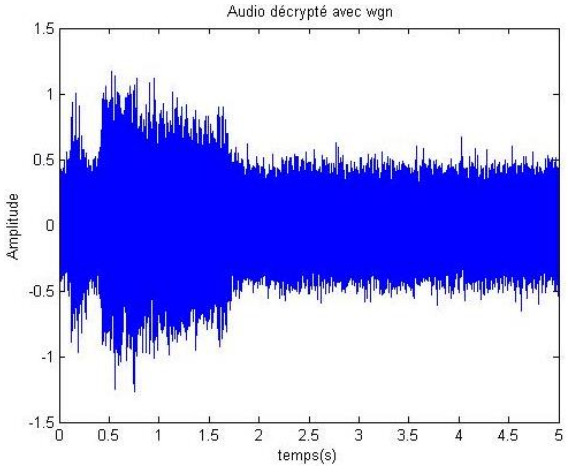
(a)



(b)



(c)



(d)

Figure3.11 : l'effet de AWGN sur AEA_LZM. (a) audio 1-26806-A-1.wav. (b) 1-26806-A-1.wav avec 'wgn'. (c) . 1-26806-A-1.wav crypté avec 'wgn'. (d) 1-26806-A-1.wav décrypté avec 'wgn'.

3.6.8. Comparaison de la vitesse d'exécution

Comme le montre le tableau 3.9, le temps d'exécution moyen de cryptage pour AEA_LZM est : 0.253244 (s), tandis que pour AEA_NCS il est : 0.376648 (s). Donc AEA_LZM surpasse AEA_NCS en termes de rapidité.

Algorithme	Audio	La taille (kb)	Le temps d'exécution (s)	La Vitesse (s/kb)
AEA_NCS	1-39923-A-1.wav	430	0.368775	0.000857
	1-49409-A-8.wav	430	0.392129	0.000911
	1-208757-A-2.wav	430	0.378529	0.000880
	2-205966-A-16.wav	430	0.367158	0.000853
	Moyenne	430	0.376648	0.000875
AEA_LZM	1-39923-A-1.wav	430	0.261324	0.000608
	1-49409-A-8.wav	430	0.241016	0.00056
	1-208757-A-2.wav	430	0.275663	0.000641
	2-205966-A-16.wav	430	0.234971	0.000546
	Moyenne	430	0.253244	0.000589

Tableau3.9 : La vitesse de cryptage de AEA_NCS vs AEA_LZM

3.7. Discussion

Après avoir soumis AEA_NCS et AEA_LZM à des tests de performance pour faire une comparaison entre les deux algorithmes de cryptage dans le but de déterminer celui qui présente les meilleures performances, nous pouvons voir malgré que AEA_LZM présente un temps de cryptage plus rapide que AEA_NCS, mais il échoue à atteindre le même niveau d'efficacité comme lui. En revanche, AEA_NCS surpasse AEA_LZM dans tous les aspects de performance, y compris l'entropie de l'information, la corrélation des coefficients, NPCR et UACI. Cette supériorité fait d'AEA_NCS un algorithme de cryptage robuste, capable de résister à différents types d'attaques et un choix fiable pour sécuriser les fichiers audios.

3.8. Conclusion

Dans ce chapitre on présente les résultats et l'analyse de notre étude sur l'utilisation d'AEA_NCS pour le cryptage audio. Nous avons effectué des tests de performance et les avons comparés avec AEA_LZM pour évaluer la sécurité et l'efficacité d'AEA_NCS. Les résultats ont été analysés numériquement et graphiquement.

CONCLUSION GENERALE

En conclusion, dans ce travail nous avons étudier l'algorithme AEA-NCS, un algorithme de cryptage audio basé sur un système chaotique bidimensionnel 2D-LNIC pour générer un flux audio crypté et sécurisé.

L'utilisation de la suite chaotique bidimensionnelle 2D-LNIC a contribué fortement à la capacité de l'algorithme AEA-NCS à fournir un cryptage amélioré et une résistance aux attaques, garantissant ainsi la confidentialité et l'intégrité des données audio cryptée.

Pour démontrer cela, nous avons effectué une analyse comparative en remplaçant la suite 2D-LNIC de l'algorithme AEA-NCS par une autre suite chaotique bidimensionnelle connue qui est la suite de Lozi. Les résultats ont mis en évidence l'efficacité et la fiabilité de l'algorithme de cryptage audio AEA-NCS basé sur la suite chaotique bidimensionnelle 2D-LNIC contrairement à l'utilisation de la suite de Lozi.

L'analyse des performances a révélé aussi que l'AEA-NCS présente d'excellentes performances et une sécurité robuste face aux différents types d'attaques par force brute, face aux attaques différentielles NPCR et UACI ainsi que contre les attaques statistiques. AEA-NCS a prouvé également sa résistance face au bruit blanc additif gaussien et sa facilité d'implémentation grâce à sa vitesse d'exécution.

Références bibliographiques

[1]: B. Furht, E. Muharemagic, D. Socek," Multimedia Encryption and Watermarking,", Springer Science+Business Media, 2005.

[2]: PGP corporation," an introduction to cryptography,", Octobre 2002

[3]: Gray C. Kissler, "an overview of cryptography," Auerbach, September 1998.

[4]: W. Stalling, L. Brown, "Cryptography and network security principles and practice", Pearson edition, 2010.

[5]: U. Maurer, Ronald L. Rivest," Information Security and Cryptography Texts and Monographs," Springer. 2002.

[6]: Q. M. ShallaA, M.U. Bokhari," Review on Symmetric Key Encryption Techniques in Cryptography," International Journal of Computer Applications (0975 – 8887) Volume 147 – No.10, August 2016.

[7]: V.K JAIN," Cryptography and Network Security, Khanna Publishers, 2017.

[8]: H. R. Biswas, Md. M. Hasan and S. K. Bala, "Chaos theory and its applications in our real life", Barishal University Journal Part 1, 5(1&2): 123-140 (2018).

[9]: A. Arshad, S.Shaukat, A. Ali , A. Eleyan ,S. A. Shah and J. Ahmad, « Chaos Theory and its Application: An Essential Framework for Image Encryption », Chaos Theory and Applications, vol.2, no.1, pp.15-20, 2020

[10]: R. B. Naik, U.Singh , « A Review on Applications of Chaotic Maps in Pseudo-Random Number Generators and Encryption », Annals of Data Science ,2022.

[11]: Y. Tang, M. Zhao and L. Li," Secure and Efficient Image Compression-Encryption Scheme Using New Chaotic Structure and Compressive Sensing article," Security and Communication Network, 2020.

[12]: S. Vaidyanathan, A. T. Azar, « Backstepping Control of Nonlinear Dynamical Systems », Academic Press, Year: 2020

[13]: P.S. SHCHERBAKOV, « Alexander Mikhailovitch Lyapunov: On the Centenary of his Doctoral Dissertation on Stability of Motion, », Automatica, Vol. 28, No. 5, pp. 865-871. 1992.

[14]: R. Wu, S. Gao, X. Wang, S. Liu, Q. Li, U. Erkan, X. Tang, « AEA-NCS: An audio encryption algorithm based on a nested chaotic system Chaos », Solitons and Fractals: the interdisciplinary journal of Nonlinear Science, and Nonequilibrium and Complex Phenomena 165, 2022.

[15]: K. R. Raghunandhan, R. Dodmane, K. B. Sudeepa, G, « Aithal Efficient Audio Encryption Algorithm for Online Applications Using Transposition and Multiplicative Non-Binary System» International Journal of Engineering Research & Technology Vol. 2 Issue 6, June – 2013

[16]: V. B. Pawar, P. A. Tijare, S.N. Sawalkar, « A Review Paper on Audio Encryption," International Journal of Research in Advent Technology », Vol.2, No.12, December2014.

[17]: N. MEKKI, M. HAMDI, T. AGUILI, T. h. kim, a real-time chaotic encryption for multimedia data and application to secure surveillance framework for IOT system », 978-1-5386-4609-0/18,2018.

[18] K. Singh, K. Kaur, « Image Encryption using Chaotic Maps and DNA Addition Operation and Noise Effects on it », International Journal of Computer Applications, Volume 23, June 2011.

[19]: S. Çiçek, « Microcontroller-based random number generator implementation by using discrete chaotic maps », Sakarya Üniversitesi Fen Bilimleri Enstitüsü Dergisi 24(5):832–844,2020.

[20]: E.A. Albahrani, et al., « A Review on Audio Encryption Algorithms Using Chaos Maps-Based Techniques », Journal of Cyber Security and Mobility, Vol. 11 1, 53–82, 2021

[21]: E. M. Elshamy et al., « Efficient audio cryptosystem based on chaotic maps and double random phase encoding », Int J Speech Technol,2015

[22]: P. Sathiyamurthi and S. Ramakrishnan, « Speech encryption algorithm using FFT and 3D-Lorenz–logistic chaotic map », Multimedia Tools and Applications, 2020

[23]: R. gnanajeyaraman, K. Prasadh, « Audio encryption using higher dimensional chaotic map », International Journal of Recent Trends in Engineering, Vol. 1, No. 2, May 2009

[24]: W. dai, X. Xu, X. Song, et al, « Audio encryption algorithm based on chen memristor chaotic system », Symmetry ,14(1):17,2021

[25] I. El Hanouti, H. El Fadili, « Security analysis of an audio data encryption scheme based on key chaining and DNA encoding », Multimedia Tools Appl 2021;80(8):12077–99, 2019.

[26] R. Abdelfatah, « Audio encryption scheme using self-adaptive bit scrambling and two multi chaotic-based dynamic DNA computations », IEEE Access 2020, 8:69894–907.

[27] X. wang, Y. Su. « An audio encryption algorithm based on DNA coding and chaotic System », IEEE Access 2019, 8:9260–70,2019.

[28] H. Feistel, « Cryptography and computer privacy », Scientific American, 228, 15-23,1973

[29] P. Naskar, S. Paul, D. Nandy, et al, « DNA encoding and channel shuffling for secured encryption of audio data », Multimedia Tools Appl 2019,78(17):25019–42,2019

[30]: D. WONG, Real-World Cryptography. “Manning Publications Co. 20 Baldwin Road PO Box 761 Shelter Island, NY 11964.

[31] Amina Yahi, Développement d’Algorithmes de Cryptage d’Images à Base des Suites Chaotiques, thèse de doctorat.

[32] Y. Wu, JP. Noonan, S. Agaian. « NPCR and UACI randomness tests for image Encryption », Cyber journals: multidisciplinary journals in science and technology,2011

[33] K. Hosny, S. Kamal, M. Darwish. « A color image encryption technique using block scrambling and chaos », Multimedia Tools Appl ,81(1):505–25, 2022.