REPUBLIQUE ALGÉRIENNE DEMOCRATIQUEET POPULAIRE

MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR

ET DE LA RECHERCHE SCIENTIFIQUE

Université YAHIA FARES DE MÉDÉA

Faculté de Technologie

Département : GénieÉlectrique

Mémoire de fin d'études de Master

Filière : Génie électrique

Spécialité : Système de Télécommunications

Amélioration de la sécurité du système de vérification du locuteur dans un environnement mobile

Encadré par :

- Dr. KROBBA Ahmed

Présenté par :

- BOUCHENAFA Linda
- HAROUN Fetma Zohra Amira

Année universitaire 2020/2021

DÉDICACES

Je dédie ce travail. Tout d'abord je tiens à remercier Dieu le tout puissant de m'avoir donné la santé, la volonté et le courage.

Ensuite, à mes parents pour leur soutien et leurs encouragements et qu'aucune dédicace ne pourra compenser leur sacrifice pour mon bien être

A mes amis *qui m'ont toujours aidé et encouragé, qui étaient toujours à mes côtés, et qui m'ont accompagnaient durant mon Chemin d'études supérieures* et
en particulier *A mon cher binôme* ***Amira .***

A notre encadreur Dr.KROBA AHMED Et à tous ceux qui nous ont soutenus pour l'achèvement de ce projet avec réussite.

Linda

Dédicaces

Je dédie ce travail. Tout d'abord je tiens à remercier Dieu le tout puissant de m'avoir donné la santé, la volonté et le courage.

Ensuite, à mon père et ma mère pour leur soutien et leurs encouragements et qu'aucune dédicace ne pourra compenser leur sacrifice pour mon bien être et mon bonheur.

A mon petit cher frère WALID, pour lequel j'ai beaucoup d'estimes.

A ma seule sœur SARA que je lui souhaite une longue vie pleine de joie et de réussite.

A mes oncles, mes tantes et toute ma famille.

A mes amis *qui m'ont toujours aidé et encouragé, qui étaient Toujours à mes côtés, et qui m'ont accompagnaient durant mon Chemin d'études supérieures, mes aimables amis « SAKINA , CHAIMA et MUSTAPHA* , en particulier ma collègue du présent projet LINDA qui n'a jamais manqué de travailler et ceux de la promotion de la 2ème année master systèmes de télécommunications.

A notre encadreur Dr.KROBA AHMED Et à tous ceux qui nous ont soutenus pour l'achèvement de ce projet avec réussite.

Amira

Remerciements

Nous tenons à remercier le dieu de nous avoir donné la patience de terminer ce travail.

Au terme de cette étude, nous souhaitons remercier chaleureusement.

notre encadrant de mémoire ***Dr. KROBBA AHMED*** *pour leur suivi et ses encouragement, ses orientations et ses précieux conseils.*

Nous remercions également tous les professeurs et les enseignants du département d'électrique pour leurs conseils constructifs et encouragements qui ont été à la fois un complément et supplément indispensable dans notre projet de fin d'étude.

Enfin, nous exprimons nos reconnaissances à tous les membres de jury d'avoir acceptés de lire ce manuscrit et d'apporter les critiques nécessaires à la mise en forme finale de cet travail.

Liste d'Abréviations

ADN	Acide Désoxyribonucléique
AES	Advanced Encryption Standard
AMR-WB	Adaptative Multi-Rate – Wide Band
AWGN	Additive White Gaussian Noise
ASCI	Application Specific Integrated Circuit
CBC	Cipher Block Chaining
CFB	Cipher Feedback
CCM	Counter with CBC-MAC
CTR	CounTeR
DES	Data Encryption Standard
DTW	Dynamic Time Warping
ECB	Electronic Code Book
ECC	Elliptic curve cryptography
FIPS	Federal Information Processing Standard
GCM	Galois /Counter Mode.
GMM	Gaussian Mixture Model
GMM-UBM	Gaussian Mixture Model -Universal Background Model
G-PLDA	Gaussian Probabilistic Linear Discriminant Analysis
IAL	Identification Automatique du Locuteur
IBM	International Business Machines

JFA	Joint Factor Analysis
LPCC	Linear Prediction Cepstral Coefficient
MAP	Maximum A Posteriori
MFCC	Mel Frequency Cepstral Coefficient
NIST	National Institute of Standards and Technology
OFB	Output Feedback
OCB	Offset Codebook Mode
PF	Permutation finale
PI	Permutation initiale
PLD	Problème du logarithme discret
PLDA	Probabilistic Linear Discriminant Analysis
PLDCE	Problème du logarithme discret sur les courbes elliptiques
RAL	Reconnaissance Automatique du Locuteur
RAP	Reconnaissance Automatique de la Parole
S-BOX	Substitution-Box
SNR	Rapport Signal sur Bruit
SRE	Speaker Recognition Evaluation
SVM	Support Vector Machine
TC	TeleCommand
TDES	Triple DES
TM	TeleMetry
UBM	Universal Background Model
VAL	Vérification Automatique du Locuteur

Liste des figures

Figure I 1: Les principales modalités biométriques. 4
Figure I 2 : Différentes tâches du traitement de la parole [2]. 5
Figure I.3:Principe de base de l'identification du locuteur [4]. 6
Figure I 4:Vérification Automatique du locuteur [5]. 7
Figure I 5:Structure générale d'un système RAL [6] 9
Figure I 6 : Extraction des paramètres MFCCs [8]. 10
Figure I 7:L'extraction des paramètres LPCCs [9] 11
Figure I 8:Architecture GMM-UBM d'un système de vérification du locuteur [13]. 13
Figure I 9:concept du GMM super-vecteur[15]. 15

Figure II 1:*Vue d'ensemble du DES* 21
Figure II 2:*Le fonctionnement de DES. [17]* 22
Figure II 3:*Réseau de Feistel utilisant l'opérateur XOR* 23
Figure II 4:*Réseau de Feistel utilisant l'opérateur XOR* 24
Figure II 5:*Schéma de TDES.* 25
Figure II 6:*Algorithme AES.* 28
Figure II 7:*Mode ECB* 30
Figure II 8:*Mode CBC* 30
Figure II 9:*Mode CFB* 31
Figure II 10:*Mode OFB* 32
Figure II 11:*Mode CTR* 32
Figure II 12:*Deux exemples de courbes elliptiques.* 34
Figure II 13:*La loi d'addition sur les courbes elliptiques.* 35
Figure II 14:*La ligne L traversant P et P* 35

Figure III 1:*Schéma synoptique du système de vérification du locuteur en canal de transmission mobile (AWGN)* 41
Figure III 2:*Les performances du système de vérification en utilisant les paramètres cryptés MFCC-DESs par l'algorithme DES au canal AWGN.* 44

Figure III 3:*Les performances du système de vérification en utilisant les paramètres cryptés MFCC-AES par l'algorithme AES au canal AWGN*..... 45
Figure III 4:*Les performances du système de vérification en utilisant les paramètres cryptés MFCC-DES-ECC par l'algorithme DES-ECC au canal AWGN* 46
Figure III 5:*Les performances du système de vérification en utilisant les paramètres cryptés MFCC-AES-ECC par l'algorithme AES-ECC au canal AWGN* 47

Liste des tableaux

Tableau III 1:*Les performances du système de vérification en utilisant les paramètres cryptés MFCC-DES par l'algorithme DES au canal AWGN* 43
Tableau III 2:*Les performances du système de vérification en utilisant les paramètres cryptés MFCC-AES par l'algorithme AES au canal AWGN* 44
Tableau III 3:*Les performances du système de vérification en utilisant les paramètres cryptés MFCC-DES-ECC par l'algorithme DES-ECC au canal AWGN* 45
Tableau III 4:*Les performances du système de vérification en utilisant les paramètres cryptés MFCC-AES-ECC par l'algorithme AES-ECC au canal AWGN.* 46

Table des matières

Sommaire

Remerciements ii
Liste d'Abréviations iii
Liste des figures v
Liste des tableaux vii
Introduction générale 1
Chapitre I: Généralités sur de la reconnaissance du locuteur 4
I.1 Introduction 4
I.2 L'authentification biométrique 4
I.3 La reconnaissance du locuteur 5
I.3.1 Identification automatique du locuteur 6
I.3.2 Vérification automatique du locuteur 7
I.4 La variabilité du signal de parole 8
I.4.1 La variabilité intra-session 8
I.4.2 La variabilité inter-session 8
I.5 L'architecture d'un système RAL 8
I.5.1 La para-métrisation 9
I.5.1.1 Paramètres acoustique 9
I.5.1.2 Les paramètres prosodiques 12
I.5.2 Les Approches des modélisations du locuteur 12
I.5.2.1 Modèle de mélange de gaussiennes (GMM) 12
I.5.2.2 Modèle GMM-UBM 13
I.5.2.3 Machine à vecteur des supports SVM 14
I.5.2.4 GMM super-vecteur 14
I.5.2.5 Modèle d'analyse conjointe de facteurs (JFA) 15
I.5.2.6 Variabilité totale (i-vecteur) 16
I.5.2.7 Analyse discriminante linéaire probabiliste gaussienne (GPLDA) 16
I.6 Décision et mesure des performances du système RAL 17
I.6.1 Taux d'identification pour le système d l'IAL 17
I.6.2 Taux d'erreur (EER) pour le système VAL 18
I .7 Conclusion 18
II.1 Introduction 20
II.2 Le data encryptions standard (DES) 20
II.2.1 Le fonctionnement du DES 20
II.2.2 Le réseau de Feistel 22

II.2.3 Algorithme de DES[19] 24
II.2.4 Algorithme TDES (3 DES) 25
II.2.5 Le déchiffrement 26
II.2.6 Les avantages de DES 26
II.2.7 Les applications du DES 26
II.3 AES encryptions (Advanced Encryption Standard) 27
II.3.1 Les modes d'opération de l'AES 28
II. 3.1.1 Modes de chiffrement 29
II.3.1.2 Modes de chiffrement authentifié 29
II.4 La cryptographie sur les courbes elliptiques 33
II.4.1 Concepts de base sur les courbes elliptiques : 33
II.4.3 La cryptographie par les courbes elliptiques 36
II.5 Conclusion 37
Chapitre 3 : simulations et Résultats 39
III.1 Introduction 39
III.2 Logiciels et langages utilisés dans l'application 39
III.2.1 Logiciel Matlab 39
III.3 Description des bases de données utilisées 39
III.3.1 La base de données NIST-2008 39
III.4 Étapes de la réalisation des systèmes de vérification du locuteur: 40
III.5 La structure générale de Système de vérification du locuteur: 40
III.6 Extraction des paramètres 42
III.6.1 Para-métrisation des coefficients MFCC 42
III.6.2 Protocole d'évaluation des résultats 42
III.7 Simulations et résultats 42
III.7.1 Performance du système de vérification du locuteur en bruit AWGN pour les algorithmes de cryptage DES et AES 43
III.7.2 Performance du système de vérification du locuteur en bruit AWGN pour les algorithmes de cryptage DES-ECC et AES-ECC 45
III.8 Conclusion 47
Conclusion générale 49
Bibliographie 52

Introduction générale

Introduction générale

L'information est un élément constitutif et déterminant dans tous les domaines. Tout au long de l'histoire, l'humanité a essayé d'envoyer des informations d'une façon sécurisées et confidentielle. La dissimulation d'information a été utilisée comme instrument de sécurisation très important pour les stratégies militaires et échange de données secrètes entre les utilisateurs. La nécessité de transfert sécurisé d'information a traversé le temps et est encore énormément utilisée dans le monde numérique puisque la plupart de ces informations sont stockées sur des ordinateurs et envoyées à d'autres ordinateurs via internet.

Pour éviter que les données confidentielles ne tombent dans les mauvaises mains, les chercheurs ont étudié des différentes méthodes et techniques mathématiques reliées aux aspects de sécurité de l'information, parmi de ces méthodes, on a le chiffrement qui considère l'une des techniques utilisées pour protéger l'information importante. La cryptographie est devenue aujourd'hui une science à part entière car il joue un rôle essentiel dans la protection des informations contre les menaces. La cryptographie étant un sujet très vaste, ce document se focalisera essentiellement sur les méthodes de chiffrement, tels que DES, AES et ECC.

Le système de reconnaissance biométrique est l'authentification des individus sur la base de caractéristiques physiques ou comportementales propres. La vérification Automatique du Locuteur (VAL) est un processus d'authentification biométrique, elle consiste à reconnaître l'identité d'un individu à partir de sa voix. Les applications des systèmes de VAL se distinguent par leur contexte applicatif et leur niveau de sécurité. L'application téléphonique (téléphonie mobile), pour des services à distance, la validation des transactions bancaires (pour venir en complément d'un code d'accès confidentiel et améliorer ainsi le service bancaire). Ces systèmes impliquent une architecture client-serveur dans le réseau mobile, pour laquelle le serveur contient les informations, et le client sélectionne la parole qui est transmise au serveur sous une forme appropriée. La sécurité du système de vérification du locuteur dans un

environnement mobile fait objet de ce travail par l'utilisation de différents paramètres acoustiques codés par différentes méthodes de chiffrement, DES, AES et ECC.

Le présent mémoire est organisé en trois chapitres.

- Le premier chapitre fourniture présentation détaillée sur le principe de l reconnaissance automatique du locuteur et des approches de modélisations utilisés dans ce domaine ainsi que l'exploration des différentes tâches de la reconnaissance du locuteur.
- Le deuxième chapitre est consacré à quelques notions de base sur les algorithmes de cryptographie DES, AES et ECC.
- Le dernier chapitre est réservé pour la partie de simulation et résultats de performance du système de vérification du locuteur en sécurité de téléphonie mobile.

Chapitre I :

Généralités sur la reconnaissance du locuteur

Chapitre I: Généralités sur de la reconnaissance du locuteur

I.1 Introduction

Ce chapitre est consacré aux principes de la reconnaissance automatique du locuteur (RAL) et des approches de modélisations utilisés dans ce domaine. Nous présentons dans un premier temps quelques notions concernant l'authentification biométrique ainsi que les différentes tâches de la reconnaissance du locuteur qui peuvent être définies selon l'application visée. Nous décrivons aussi l'architecture générale d'un système RAL (para-métrisation et les approches de modélisation du locuteur). Enfin, nous donnons la mesure des performances de chaque tâche.

I.2 L'authentification biométrique

La biométrie est une nouvelle technique, qui consiste à vérifier ou déterminer l'identité d'une personne à partir des caractéristiques biologiques (comme l'ADN), comportementale (comme la voix) ou morphologiques (comme l'empreinte digitale) [1].

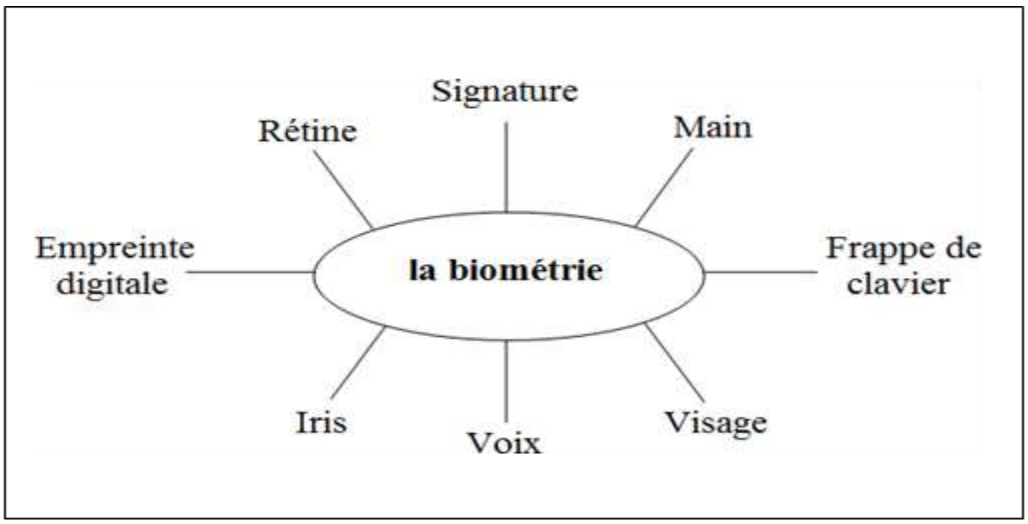


Figure I 1: *Les principales modalités biométriques.*

Les caractéristiques biométriques par les quelles il est possible de vérifier l'identité d'une personne sont appelées modalités biométriques. La Figure I.1 illustre un exemple de quelques modalités biométriques. Ces modalités sont basées sur l'analyse des données liées à l'individu et sont généralement classées en trois catégories : La biométrie biologique se base sur l'analyse des données biologiques liées à l'individu

(salive, ADN, etc.). La biométrie comportementale se base sur l'analyse de comportements d'un individu (manière de marcher, dynamique de frappe au clavier, la voix, etc.). La biométrie morphologique se base sur les traits physiques particuliers qui, pour toutes personnes, sont permanents et uniques (empreinte digitale, visage, etc.) [1].

I.3 La reconnaissance du locuteur

La reconnaissance du locuteur est la tâche d'authentification de l'identité d'une personne en analysant uniquement sa voix. La reconnaissance automatique du Locuteur –RAL- s'inscrit dans le domaine plus général du traitement de la parole, qui recouvre également un ensemble d'activités (voir Figure .I.2), telles que : le codage de la parole, l'analyse, la synthèse et la reconnaissance. Dans la reconnaissance, on peut trouver : la reconnaissance de la parole, la reconnaissance du locuteur et la reconnaissance de la langue.

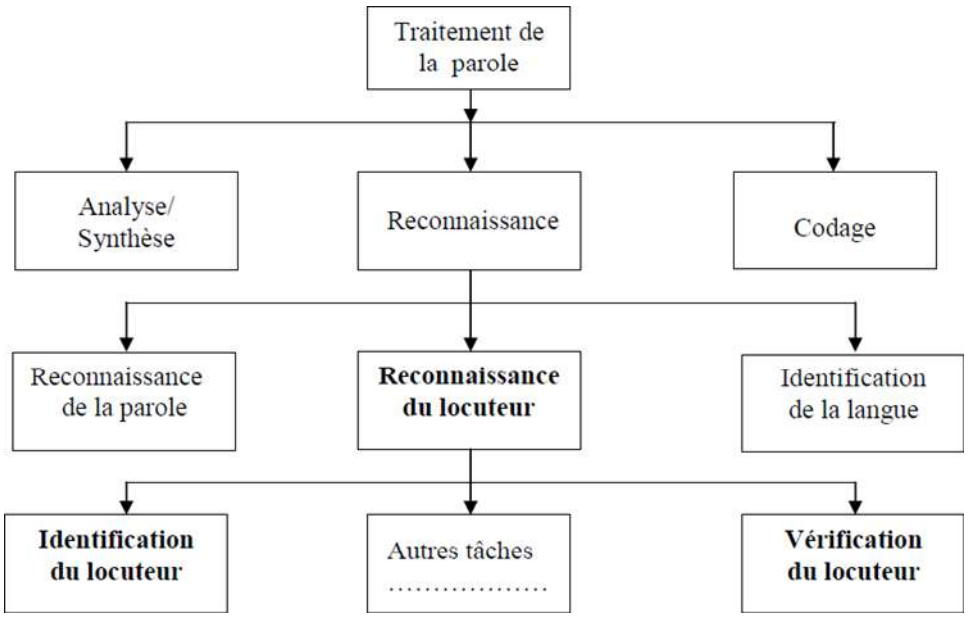


Figure I 2 : *Différentes tâches du traitement de la parole [2].*

La parole recouvre également une vaste panoplie d'activités tels que : le codage, la compression, la synthèse et la reconnaissance de la parole, la reconnaissance de locuteur. La reconnaissance du locuteur est un terme générique qui répond à plusieurs définitions selon le scénario applicatif envisagé .Les scénarios applicatifs sont regroupé sent deux catégories principales [2] :

a) L'identification de locuteurs.
b) La vérification du locuteur.

I.3.1 Identification automatique du locuteur

Le principe de l'identification automatique du locuteur l'IAL, consiste à retrouver l'identité du locuteur associé parmi un ensemble de locuteurs connus. D'un point de vue schématique, une séquence de parole est donnée en entrée du système d'IAL. Pour chaque locuteur connu du système, la séquence de parole est "comparée" à une référence caractéristique du locuteur. L'identité du locuteur dont la référence est la plus "proche" de la séquence de parole est donnée en sortie du système d'IAL [3].

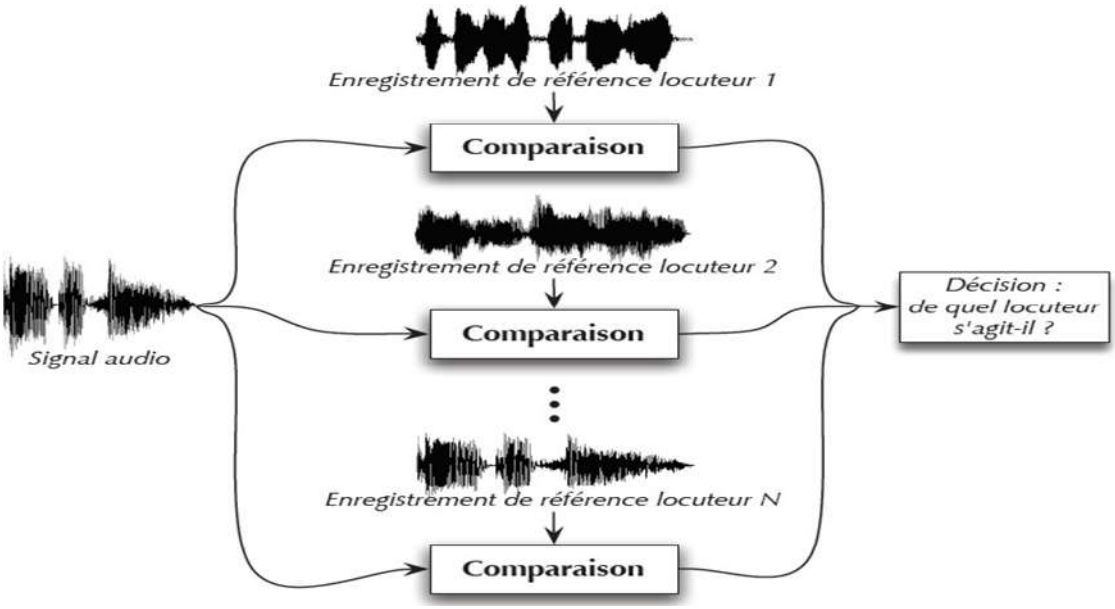


Figure I.3:*Principe de base de l'identification du locuteur [4].*

Applications

En IAL, les applications sont peu nombreuses. On peut retenir, par exemple, l'utilisation d'un système d'IAL en vue de faciliter l'adaptation au locuteur des

systèmes de reconnaissance automatique de la parole (RAP). Par ailleurs, il peut être intéressant pour des applications commercial les d'associer un même mot de passe pour une petite population de locuteurs (membres d'une famille, d'une société).Dans une telles situation, un système d'IAL en ensemble ouvert et dépendant du texte peut être utilisé pour contrôler l'accès à des données sensibles [3].

I.3.2 Vérification automatique du locuteur

La Vérification Automatique du Locuteur (VAL) (*Figure I 4)*est le processus décisionnel permettant de déterminer, au moyen d'un message vocal, la véracité de l'identité revendiquée par un individu dont représente le principe de VAL. L'identité ainsi que le message vocal constituent les deux entrées du système de VAL. L'identité, nécessairement connue du système, désigne automatique mental référence caractéristique d'un locuteur .Une mesure des similarités basées sur le rapport de vrai semblance est calculée entre cette référence et le message vocal puis comparée à un seuil de décision. Dans le cas où la mesure de similarité est supérieure au seuil l'individu est accepté. Dans le cas contraire, l'individu est considéré comme un imposteur et sera rejeté [5].

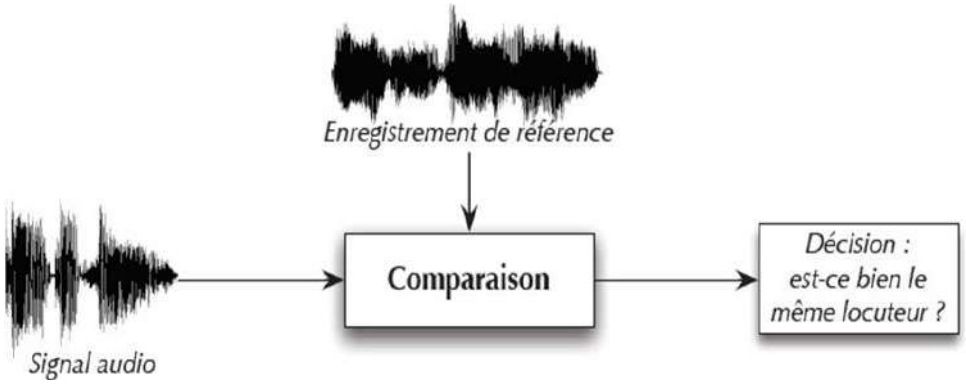


Figure I 5:*Vérification Automatique du locuteur [5].*

Applications

Les applications de VAL sont multiples et principalement commerciales [5]:

- Serrures vocales pour le contrôle d'accès à des locaux.
- Authentification pour l'accès à distance.
- Protection de matériel contre le vol (téléphones portables ,voitures, etc.)

I.4 La variabilité du signal de parole

Il est important d'introduire les types de variabilités de la parole. En plus du contenu linguistique, le signal vocal véhicule aussi des informations sur : l'identité du locuteur, son genre, son état émotionnel, son état de santé, sa tranche d'âge, etc. Dans une base de données de plusieurs locuteurs où chaque locuteur a au moins un enregistrement, les enregistrements d'un même locuteur peuvent être effectués dans différents lieux (par exemple : au bureau, à la maison, à l'extérieur, dans une chambre insonorisée, etc.) et en utilisant différents types de canaux (par exemple : téléphone fixe, téléphone portable, microphone, etc.). Usuellement, nous pouvons limiter toute cette gamme d'informations ou de variabilités dans ces trois catégories suivantes : [11] :

I.4.1 La variabilité intra-session : il s'agit de la variabilité perçue au cours d'un même enregistrement et qui peut être causée par un changement de l'état émotionnel, de lieu, d'emplacement par rapport au microphone ou bien du microphone lui-même, etc.

I.4.2 La variabilité inter-session:il s'agit de la variabilité perçue entre l'ensemble des enregistrements d'un même locuteur, elles ainsi des eaux mêmes causes quel 'intra-session, mais elle est susceptible d'être plus importante vu les différences possibles entre les dates et les circonstances d'enregistrement

I.4.3 La variabilité interlocuteurs: il s'agit de la variabilité perçue entre les distincts locuteurs et due principalement à la différence d'anatomie des cordes vocales, ça pourrait être aussi dû au genre, à l'âge, à la langue.

I.5 L'architecture d'un système RAL

Un système reconnaissance automatique du locuteur tel qu'il illustré par la Figure I.5, se compose de trois processus principaux, qui sont : la para-métrisation (analyse acoustique), la modélisation et la décision. En plus, un système de RAL possède deux phases [6]:

a) Phase d'apprentissage, où un modèle est estimé pour chaque locuteur « client » du système puis servira de référence pour les tâches de reconnaissance à venir.

b) P hase du test, où l'étape de reconnaissance (vérification, identification...) est effectuée. En sortie de cette phase, les sémèmes une réponse, une identité pour la tâche d'identification ou une décision accès/rejet pour la vérification.

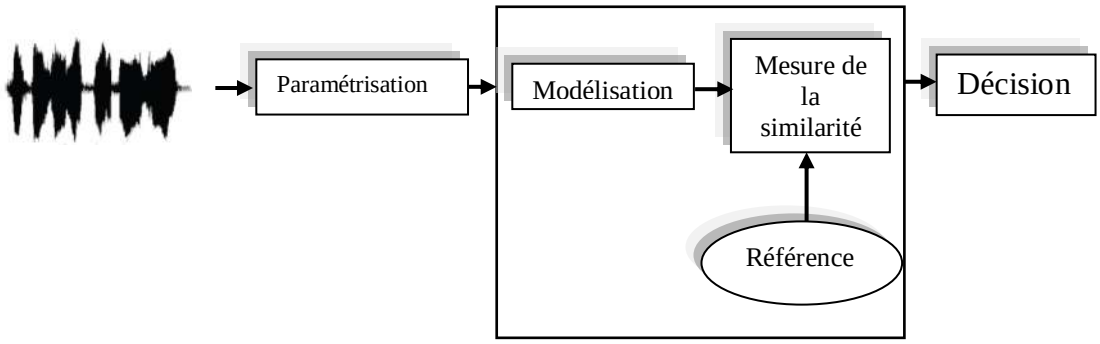


Figure I 6:*Structure générale d'un système RAL [6]*

I.5.1 La para-métrisation

Dans cette étape en décompose le signal parole en trames de longueur variantes de (10à30ms).car le signal vocal est supposé stationnaire dans cette durée (invariance par changement d'observation). Pour chaque fenêtre on fait L'extraction des paramètres acoustique qui peuvent fournir une représentation plus simple du signal parole. Il existe deux grandes catégories de paramètres [7]

I.5.1.1 Paramètres acoustique Ces paramètres sont utilisés en RAL .Ils se représentent l'influence des caractéristiques physiques de l'appareil phonatoire de chaque individu .Ces paramètres sont les LPCCs , et MFCCs [8].

a) Coefficients MFCCs:

Le coefficient MFCC (*Mel Frequency Cepstral Cofficients*) est une technique très utilisée entrainement de la parole. Il est basé sur la variation des bandes critiques de l'oreille humaine avec la fréquence, les filtres espacés linéairement aux basses fréquences et .Ces filtres sont modélisés par une échelle non-linéaire issue de connaissances sur la perception humaine : l'échelle Mel [10].Pour les MFCCs, on utilise la fenêtre de Hamming durant la transformation du domain et temporel au domaine fréquentiel. Cette transformation est faite en utilisant la transformée de Fourier. Un filtrage, est appliqué ensuite, par banc de filtres triangulaires qui vont chacun couvrir une fréquence, permettant de mieux simuler le fonctionnement de

l'oreille humaine.Par la suite les filtres sont espacés selon l'échelle de Mel. Cette échelle reproduit la sélectivité de l'oreille qui diminue avec l'accroissement de la fréquence. Après le calcul de log, une transformée en cosinus discrète est appliquée pour assurer un retour au domaine temporel [10].

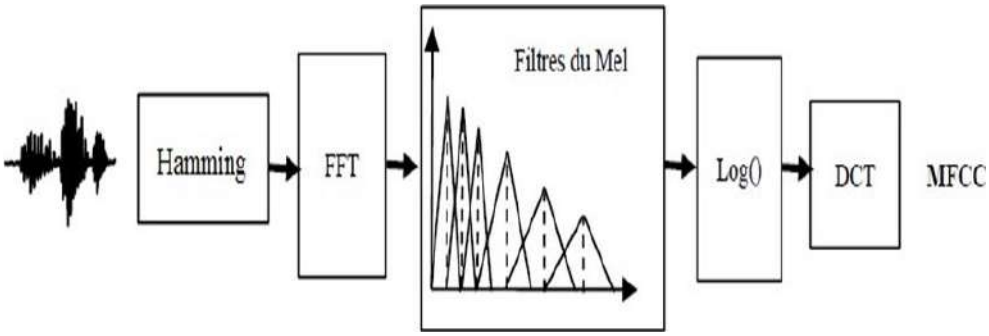


Figure I 7 : *Extraction des paramètres MFCCs [8].*

b) Les coefficients LPCCs

L'extraction des paramètres LPCC se base sur l'analyse LPC qui permet d'extraire les coefficients de prédiction. Les coefficients cestreaux peuvent être calculés à partir de la sortie d'un banc de filtres ou des coefficients de la prédiction linéaire. Ainsi les paramètres LPCC sont calculé sa partir d'une modélisation auto régressive du signal [16].Chaque trame est représentée par des coefficients statiques. Nous avons choisi d'utiliser 12 coefficients LPCC. Le principe de calcul de ces coefficients est présenté par la figure 1.6 [8].Après l'analyse du signal de parole, la procédure utilisée pour le para-métrisation par la technique LPCC est la suivante [8]:

a) Préaccentuation pour aplatir le spectre moyen du signal qui décroît de 6 dB par octave.
b) Fenêtrage : Chaque trame est multipliée par une fenêtre de Hamming.
c) Extraction descoefficients d'auto corrélation, on note que la fonction d'auto corrélation s'avère pour traîner M, où M est l'ordre de l'analyse désirée de LPC.

Les coefficients de prédiction linéaire calculés par l'algorithme de Le vinson-Durbin.

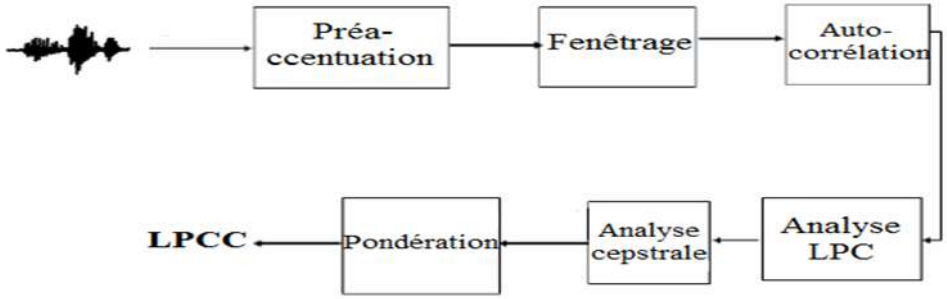


Figure I 8:*L'extraction des paramètres LPCCs [9]*

I.5.1.2 Les paramètres prosodiques

Ces paramètres illustrent le débit, la durée et les fréquences de pauses, pitch et l'énergie [7].

I.5.2 Les Approches des modélisations du locuteur

L'étape de modélisation exploite les données fournis dans l'étape de la paramétrisation afin de créer la représentation d'un individu qui servira, par la suite, à l'authentifier. Le modèle utilisé est généralement une représentation statistique des données acquises [6].Différentes approches ont été développées, néanmoins on peut les classer en quatre grande familles [6]:

a) **L'approche vectorielle :** le locuteur est représenté par un ensemble de vecteurs de paramètre dans l'espace acoustique .Ses principal es techniques sont la reconnaissance à base e DTW (dynamique time warning) et par quantification vectorielles [2].

b) **L'approche statistique :** consiste à représenter chaque locuteur par une densité de probabilité dans l'espace des paramètres acoustique. Elle couvre les techniques de modélisation par les modèles de Markov cachés, par les mélanges de gaussiennes et parades mesures statistiques du second ordre [2].

c) **L'approche connexionniste :** consiste principalement à modéliser les locuteurs parades réseaux de neurones [2].

d) **L'approche discriminante :** Les modèles des différentes classes sont appris simultanément et l'apprentissage vise à séparer le plus possible les classes entre elles (minimisation du taux d'erreur de classification) [12].

I.5.2.1 Modèle de mélange de gaussiennes (GMM)

Un modèle de mélange de gaussiennes (GMM, Gaussien Mixture Model) représente la distribution d'une variable aléatoire *X* par [13]:

$$p(x/\theta) = \sum_{i=1}^{M} w_i N(x\mu_i, \sum_i) \qquad (1.1)$$

ou wi le poids, *N* est probabilité de densité.

Les GMM sont utilisés d'une manière ou d'une autre dans la plupart des système de reconnaissance de parole et du locuteur .En augmentant le nombre de composants du mélange , il est théoriquement possible des approcher d'une densité de probabilité quelconque, mais en pratique le nombre de paramètres du modèle est limité par la quantité des données d'apprentissage disponible. On travaille le plus souvent avec des GMM à matrice de covariance diagonale .D'une part, les différentes dimensions des coefficients cestreaux habituellement utilisés sont faiblement corrélée sent réelles .D'autre part, à nombre de paramètres du modèle constant, l'estimation de GMM à matrices de covariance diagonales est plus robuste et les modèles obtenus sont plus performants que dans le cas de matrices de covariance pleines [13].

I.5.2.2 Modèle GMM-UBM

Un modèle GMM générique de référence, adopte l'architecture GMM-UBM présentéedanslafigure1.12.

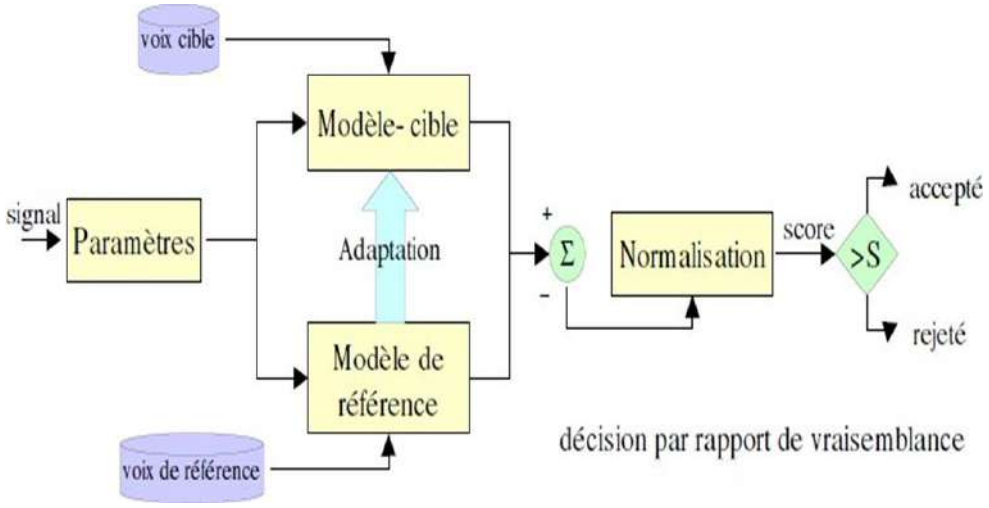


Figure I 9:*Architecture GMM-UBM d'un système de vérification du locuteur [13].*

Un modèle GMM générique de référence, encore appelé UBM (*Universal Back ground Model*) ou modèle du monde, est préalablement appris sur une ensemble données d'échantillons de voix le plus représentatif possible. Lors de la phase d'enrôlement, ce modèle UBM est adapté par MAP à la voix du locuteur cible en utilisant les données d'enrôlement.Lors de la phase d'exploitation, les deux

hypothèses que l'échantillon *X* ait été généré par lemodèle cible *M* ou par le modèle de référence B sont comparées au moyen du logarithme du rapport de vrai semblance.

I.5.2.3 Machine à vecteur des supports SVM

Les machines a support de vecteurs est une nouvelle technique discriminante dans la théorie de l'apprentissage statistique. Elle permet d'aborder des problèmes très divers comme la classification, la régression, la fusion, etc.[14].Le principe de cette technique est de projeter les données de l'espace d'entrée (appartenant à deux classes différent est non-linéairement séparables)dans une espace de plus grande dimension appelé espace de caractéristiques. Dans cet espace, on construit un hyper plan optimal séparant les deux classes tel que [14]:

a) Les vecteurs appartenant aux différentes classes se trouvent de différentes cotes de l'hyperplan.
b) La plus petite distance entre les points et l'hyperplan (la marge) est maximale.

I.5.2.4 GMM super-vecteur

Le super-vecteur GMM est défini comme la concaténation des composantes des moyennes des gaussiennes du GMM. Si D est la dimension de l'espace du paramètre, la dimension du super vecteur est M*D où M est le nombre de gaussienne dans le GMM [15]. La notion de super-vecteur implique une transformation d'un signal de parole vers un vecteur de plus grande dimension [15].

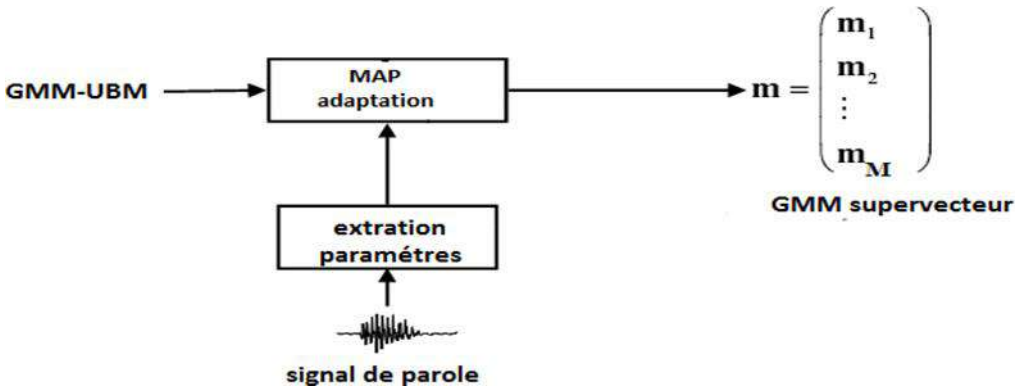


Figure I 10:*concept du GMM super-vecteur[15].*

I.5.2.5 Modèle d'analyse conjointe de facteurs (JFA)

Le modèle d'analyse conjointe de facteurs est un modèle génératif des variables cachées quinte principalement des attaquer au problème de la disparité entre les données d'enrôlement et celles de test dans l'espace des super-vecteurs des GMM. L'hypothèse de base de ce modèle stipule qu'un super-vecteur S de dimension CF dépendant du locuteur et du canal (c.-à-d. un super-vecteur estimé d'un segment donné d'un locuteur donné) peut se diviser en deux super-vecteurs statistiquement indépendants comme suit [11]:

$$M_{s,r} = s + c \qquad (1.2)$$

Où *s* est représenté la voix propres et *c*est les canaux propres. Les deux sous-espaces sont recouverts par les matrices *V* et *U*, comme nous l'avons décrit précédemment dans les parties de voix propre et canaux propres.

La formule de voix propre et canaux propres, on obtient une nouvelle formule de la méthode JFA comme suite

$$M_{s,r} = m + Vy_s + Dz + Ux_h \qquad (1.3)$$

C'est donc la méthode de JFA est seul modèle, qui prend en compte les quatre composantes du GMM super-vecteur,

I.5.2.6 Variabilité totale (i-vecteur)

Les extracteurs d'i-vecteurs sont devenus la technique la plus avancée dans le domaine de la reconnaissance du locuteur. Un espace des i-vecteurs représente des segments de parole sous forme de vecteurs de caractéristiques de petite dimension appelés i vecteurs. La technique par i-vecteur est inspirée par la méthode de modélisation JFA, qui est définie par deux espaces séparés, à savoir l'espace du locuteur et l'espace du canal. Dehak et al, ont observé que les facteurs du canal dans JFA contiennent également des informations dépendantes du locuteur. Cet espace, à l'inverse des deux sous-espaces de JFA, ne fait aucune distinction entre les différents types de variabilité (c.-à-d. la variabilité interlocuteur et celle due au canal). La définition la plus élémentaire d'un i-vecteur est de le considérer comme étant la projection d'un super-vecteur dans un espace de dimension réduite. Mathématiquement, un super-vecteur M d'un segment audio dépendant du locuteur et du canal peut se réécrire sous la forme suivante [11]:

$$M_{s,r} = m + Tw \qquad (1.4)$$

Où *m* est le super-vecteur moyen de dimension *CF* dépendant de modèle du monde UBM, la matrice rectangulaire *T* est un vecteur de faible dimension appelé l'i-vecteur de dimension, est un vecteur caché de dimension *D* qui suit une distribution normale standard

I.5.2.7 Analyse discriminante linéaire probabiliste gaussienne (GPLDA)

L'approche PLDA est considère comme un modèle discriminatif à caractère probabiliste visant à minimiser la variabilité intra-individu et maximiser la variabilité inter-individus. Dans le domaine de la reconnaissance du locuteur, la PLDA décompose chaque i-vecteur w en une composante dépendante du locuteur, une composante dépendante de la session et une composante résiduelle à savoir:

$$w_{s,r} = \eta + Hz_k + H_1 y_{s,r} + \varepsilon_{s,r} \qquad (1.5)$$

Où η est un vecteur de dimension N qui correspond à une moyenne globale sur l'espace des i-vecteurs, il représente la composante indépendante du locuteur et du canal.

C'est une matrice désignant les sous-espaces de voix propres (eigen-voices) et est une matrice de rang faible représentant une base sur le sous-espace canal (eigen-channel), z et y sont les facteurs latents dépendants du locuteur et du canal, respectivement. $\varepsilon_{s,r}$ est une variable aléatoire représentant le bruit résiduel.

I.6 Décision et mesure des performances du système RAL

Un module de reconnaissance fournit en sortie un score. La nature de ce score varie selon les modules de reconnaissance utilisés. Il s'agit dans la plupart du temps d'une distance, d'une probabilité ou d'une vraisemblance. Un module de décision doit, à partir de ce score, fournir une décision qui constituera la réponse finale du système de reconnaissance. Le module de décision décrit dans le paragraphe précédent reçoit, en entrée et pour chaque test, un score. Celui-ci résulte de la comparaison entre les caractéristiques biométriques de l'utilisateur testé et la référence apprise lors de la phase d'enrôlement. Un score élevé signifiera que la probabilité pour que l'utilisateur testé corresponde à l'identité qu'il annonce est élevée et un score faible signifiera que cette probabilité est faible. La décision binaire qui constitue la sortie du module résulte de la comparaison de ce score avec un seuil défini à l'avance. Si le score est supérieur au seuil, l'utilisateur est accepté et s'il est inférieur au seuil, l'utilisateur est rejeté.

I.6.1 Taux d'identification pour le système d l'IAL

L'identification du locuteur consiste à reconnaître un locuteur parmi un ensemble de locuteurs en comparant son identité vocale à des références connues**.** Les performances du système d'identification sont données en termes de taux d'identification correcte Ic ou incorrecte I_i, soit :

$$Ic = \frac{\text{Nombre de tests correctement identifiés}}{\text{Nombre total de tentatives}} \qquad (1.6)$$

$$I_i = \frac{\text{Nombre de tests mal identifiés}}{\text{Nombre total de tentatives}} \qquad (1.7)$$

Avec $I_C + I_i = 100\%$

I.6.2 Taux d'erreur (EER) pour le système VAL

La vérification du locuteur est une décision en tout ou rien. Les performances de vérification de locuteur sont données en termes des faux rejets FRR et de fausses acceptations FAR, elles sont définies comme suit:

$$FRR = \frac{\text{Nombre de tentative s d'abonnés rejetées}}{\text{Nombre total de tentative s d'abonnés}} \quad (1.8)$$

$$FAR = \frac{\text{Nombre de tentative s d'imposteurs acceptées}}{\text{Nombre total de tentative s d'imposteurs}} \quad (1.9)$$

Le taux d'erreur égal (EER: *EqualError Rate*) est défini comme si les valeurs FAR et FRR devenaient égales. C'est-à-dire, en changeant le seuil, nous trouvons un point où le FAR et le FRR deviennent presque égaux.

$$FRR = FAR$$

I .7 Conclusion

Dans ce chapitre, nous avons introduit le principe de la reconnaissance automatique du locuteur ainsi que les différentes étapes du système. Le système de reconnaissance automatique du locuteur est probablement la méthode la plus ergonomique pour résoudre les problèmes d'accès. Cependant, la voix ne peut être considérer comme une caractéristique biométrique d'une personne compte tenu de la variabilité intra et inter -locuteur. Ce système se résume en trois étapes principales : l'analyse acoustique du signal de parole, la modélisation du locuteur et une dernière étape de décision qui se base sur les deux processus d'identification et / ou de vérification de locuteur, et cela quelle que soit l'application ou la tâche visée.

Chapitre 2 :

Sécurité du système VAL par des algorithmes de cryptographie DES, AES et ECC

II.1 Introduction

Le développement remarquable des réseaux de communication a favorisé l'essor des nouveaux moyens de paiement à distance, notamment les cartes à puce et le commerce. Ces nouveaux types de communications nécessitent de plus en plus des méthodes de transaction dites sécurisées pouvant résister à diverses attaques de cryptanalyse. Dans ce chapitre nous allons décrire le principe de fonctionnement de *(DES : Data Encryption Standard)* tout en définissant les étapes et son algorithme et nous présentons aussile standard de chiffrement avancé appelé (*AES : Advanced Encryption Standard)* avec les différents modes d'opération .Nous traiterons enfinla cryptographie sur les courbes elliptiques *(ECC : Ellipticcurvecryptography*)qui est largement utilisé dans divers algorithmes cryptographiques à clé publique, en particulier logarithme discret impliqué.

II.2 Le data encryptions standard (DES)

Le data encryptions standard (*Data Encryption Standard* : DES) est un algorithme de cryptographie qui a été sélectionné comme un standard pour (*Federal Information Processing Standard* : FIPS). L'algorithme DES opère un chiffrement par bloc a clé symétrique, il prend une chaîne de caractères ou nombres d'une taille fixée à 64 –bits du texte en clair et le transforme à l'aide d'opérations compliquées vers un texte crypté de la même taille .En apparence la clé est constituée de 64-bits en fait seulement 56 de ces 64-bits sont vraiment utilisés dans l'algorithme. Huit bits sont employés pour faire la vérification de parité. Il existe 16 étapes de calcul identiques, dites rondes*(rounds).* Il y a aussi des permutations, l'une initiale(PI)et l'autre finale (PF). Il semblerait que PI et PF ne sont pas de signification cryptographique mais qui ont été inclus dans l'algorithme pour faciliter le chargement de données, Le bloc est divisé en deux moitiés de 32-bits chacune, qui sont calculées de façon alternée. Ce croisement est connu comme le schéma de Feistel

II.2.1 Le fonctionnement du DES

Il s'agit d'un système de chiffrement symétrique par blocs de 64 bits, dont 8 bits (un octet) servent de test de parité (pour vérifier l'intégrité de la clé). Chaque bit de parité de la clé (1 tous les 8 bits) sert à tester un des octets de la clé par parité impaire, c'est-à-dire que chacun des bits de parité est ajusté de façon à avoir un nombre impair de '1' dans l'octet à qui il appartient. La clé possède donc une longueur « utile » de 56 bits, ce qui signifie que seuls

56 bits servent réellement dans l'algorithme. L'algorithme consiste à effectuer des combinaisons, des substitutions et des permutations entre le texte à chiffrer et la clé, en faisant en sorte que les opérations puissent se faire dans les deux sens(pour le déchiffrement). La combinaison entre substitutions et permutations est appelée code produit. La clé est codée sur 64 bits et formée de 16 blocs de 4 bits, généralement notés k1 à k16. Etant donné que « seuls » 56 bits servent effectivement à chiffrer, il peut exister 256 clés différentes

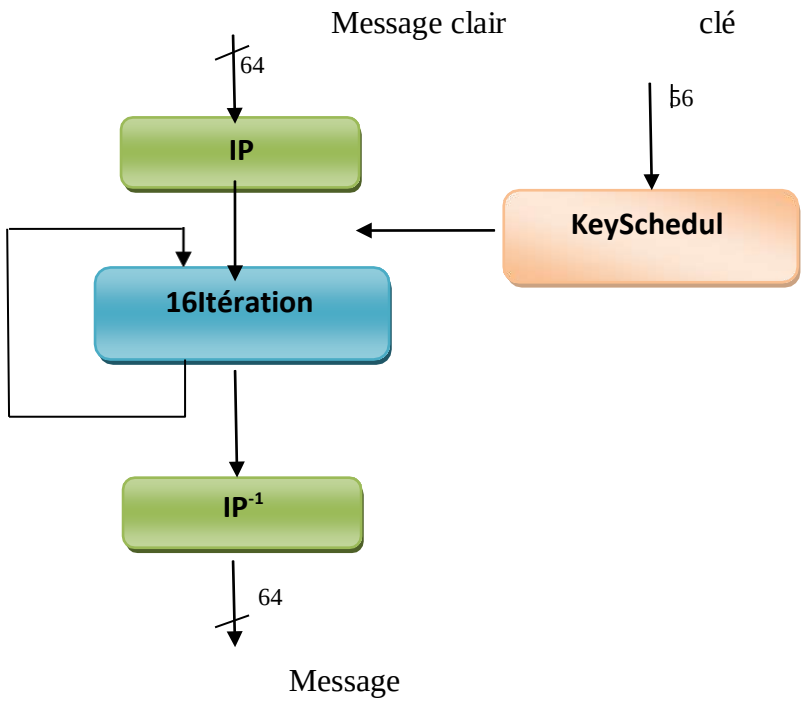


Figure II 1:*Vue d'ensemble du DES*

L'algorithme DES utilise seulement 3 types d'opérations différentes : des permutations, des rotations et des substitutions. Ceci est un point fort du DES, il n'utilise pas de lourdes opérations comme des additions ou des multiplications qui demanderaient beaucoup de ressources de calcul. Comme la montre Fig.2.1 et Fig. 2.2, les blocs à chiffrer sont d'abord sujets à une permutation initiale IP, puis on leur applique 16 itérations de chiffrement avant de les faire passer finalement dans une permutation initiale inverse IP-1. Le Key Schedule transforme la clé de 56 bits en 16 clés partielles ou 'sous-clés' de 48 bits chacune.

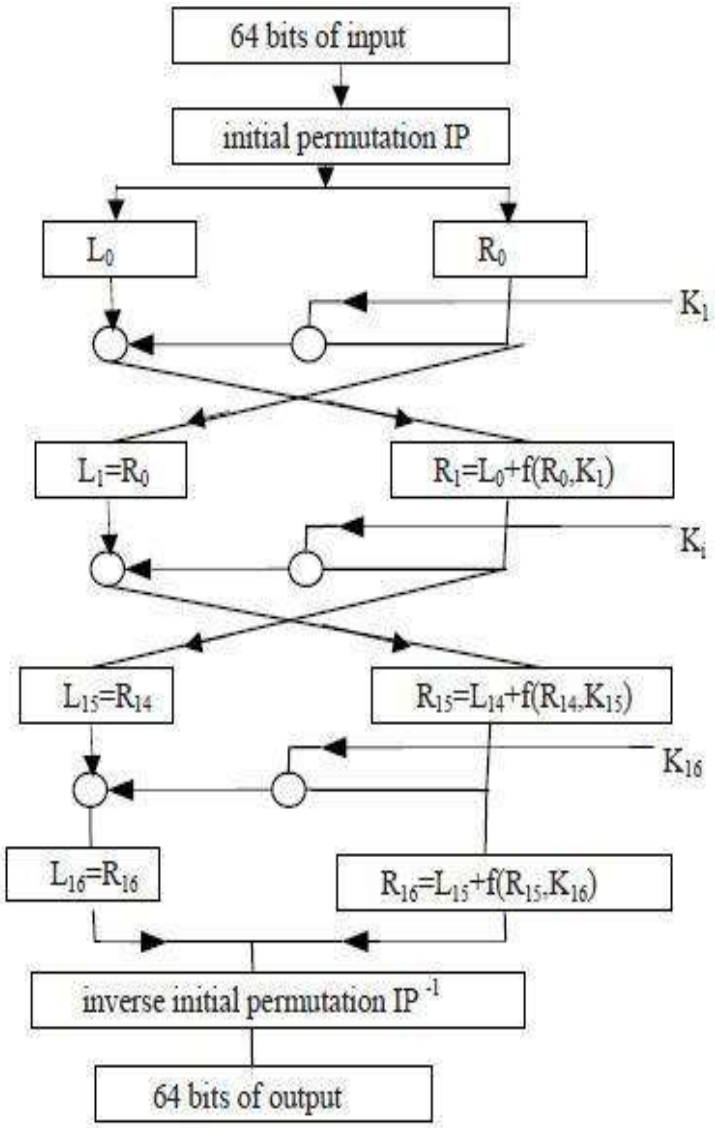


Figure II 2:*Le fonctionnement de DES. [17]*

II.2.2 Le réseau de Feistel

Un réseau de Feistel est une construction utilisée dans les algorithmes de chiffrement par bloc, nommée d'après la cryptologie d'IBM, Horst Feistel. Elle a été utilisée pour la première fois dans Lucifer et DES. Cette structure offre plusieurs avantages, le chiffrement et le déchiffrement ont une architecture similaire voire identique dans certains cas .L'implémentation matérielle est aussi plus facile avec un tel système même si les choses ont passablement changé depuis la fin des années 70. Un réseau de Feistel repose sur des principes simples dont des permutations, des substitutions ,des échanges de blocs de données et une fonction prenant en entrée une clé intermédiaire à chaque étage L'algorithme de chiffrement va procéder en chiffrant des blocs de 2n bits, qu'onpartageen2parties de n

bits chacune , comme la montre la Figure.**2.3.**Les parties gauche(G) et droite(D).L'image du bloc (G_i, D_i) est le bloc (G_{i+1}, D_{i+1}) ,avec $G_{i+1} = D_i$ et $D_{i+1} = G_i \; D_{i+1} = G_i \otimes f(D_i)$.

La partie droit en' a pas été transformée (juste en volée à gauche).Il faut donc répéter le schéma de Feistel un certain nombre de fois (on parle de tours).

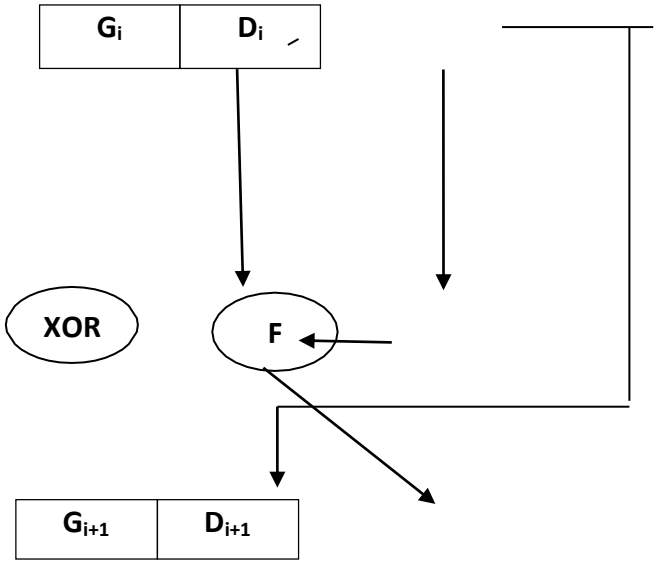


Figure II 3:*Réseau de Feistel utilisant l'opérateur XOR*

Dans le cas de DES, le réseau de Feistel possède 16 tours, chacun avec une sous-clé. Ces différentes clés permettent d'améliorer la robustesse d'un algorithme face à la crypta analyse .L'avantage de ce type d'algorithmes est que chiffrement et déchiffrement sont structurellement identiques.

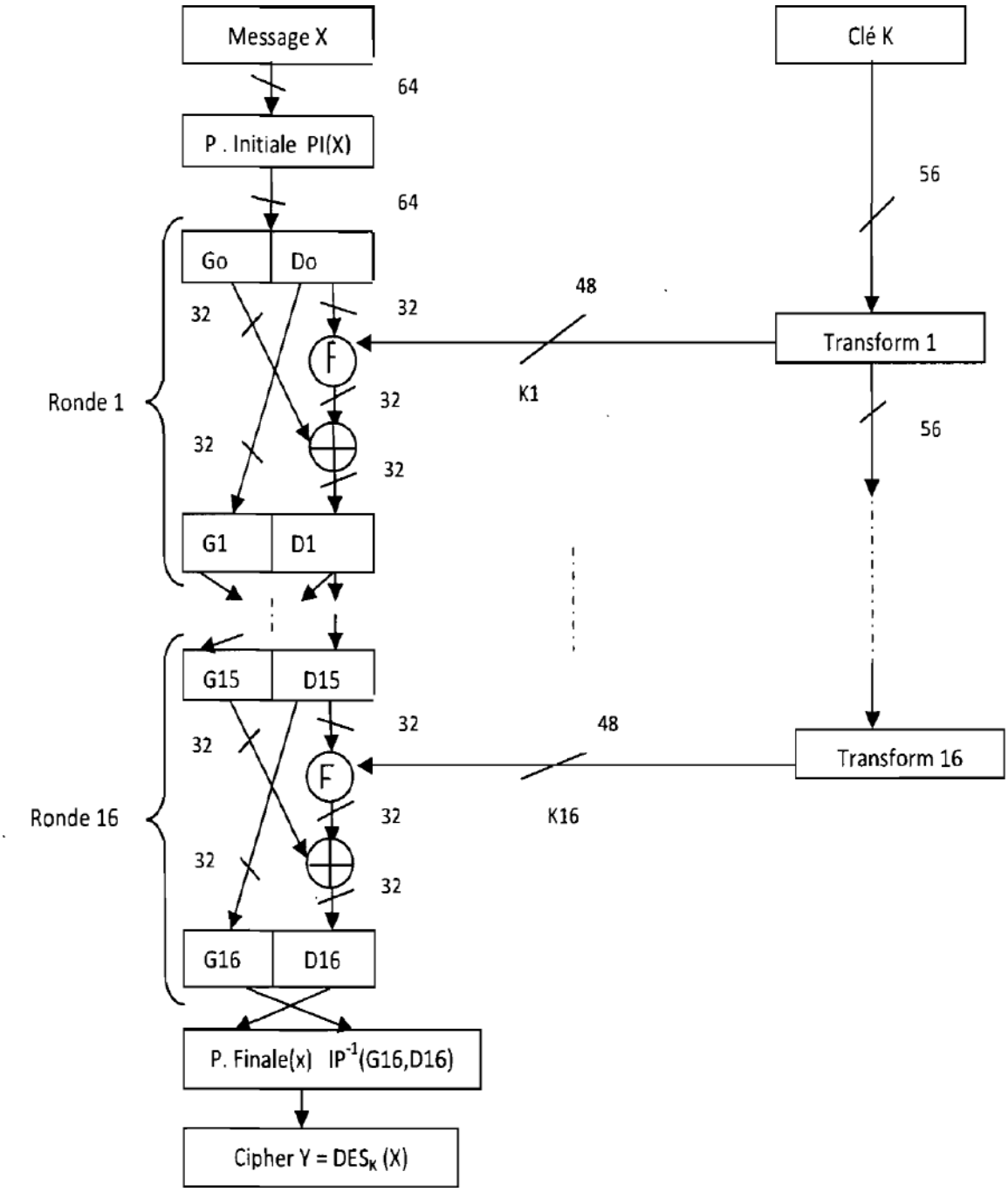


Figure II 4:*Réseau de Feistel utilisant l'opérateur XOR*

II.2.3 Algorithme de DES[19]

Les grandes lignes de l'algorithme LES sont décrites comme suit :

II Fractionnement du texte en blocsde64bits (8octets). Permutation initiale des blocs.

III Découpage des blocs en deux parties : gauche et droite , nommées GetDou(LetR).

IV Etapesdepermutationet desubstitutionrépétées16 fois(appeléesrondes).

V Recollement des parties gauche et droite puis permutation initiale inverse,Ou bien (permutation fin

II.2.4 Algorithme TDES (3 DES)

En 1990 Eli Biham et Adi Shamir ont mis au point la cryptanalyse différentielle qui recherche des paires de texte en clair et des paires de texte chiffrées. Cette méthode marche jusqu'à un nombre de rondes inférieur à 15, or un nombre de 16 rondes sont présentes dans l'algorithme présenté ci-dessus.D'autre part, même si une clé de 56 bits donne un nombre énorme de possibilités, de nombreux processeurs permettent de calculer plus de 10 clés par seconde, voir la **Figure II.5)** ainsi, utilisés parallèlement sur un très grand nombre de machines, il devient possible pour un grand organisme (un Etat par exemple) de trouver la bonne clé...Une solution à court terme consiste à chaîner trois chiffrement DES à l'aide de deux clés de 56 bits (ce qui esquivait à une clé de 112 bits). Ce procédé est appelé **Triple DES**, noté TDES (parfois3DES ou 3-DES). [20]

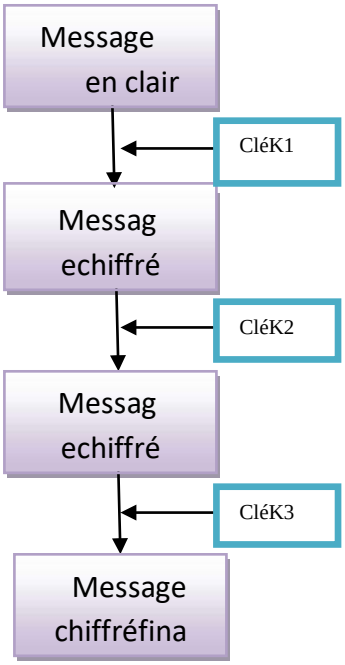


Figure II 5:*Schéma de TDES.*

TDES permet d'augmenter significativement la sécurité du DES, toutefois il a l'inconvénient majeur de demander également plus de ressources pour le chiffrement et le déchiffrement. On distingue habituellement plusieurs types déchiffrement triple DES:

- DES-EEE3: 3chiffrements DESavec3clés différentes.

- DES-EDE3 : une clé différente pour chacune des 3 opérations DES (chiffrement, déchiffrement, chiffrement)
- DES-EEE2etDES-EDE2 :une clé différente pour la seconde opération (déchiffrement).

II.2.5 Le déchiffrement

Le DES étant un algorithme symétrique, c'est la même clé qui sera utilisée pour déchiffrer des données .La structure déchiffrement étudiée ci-dessus sera celle utilisée pour le déchiffrement. La configuration et l'ordonnancement des encrypte rounds ne seront pas modifiées. Par contre, les Key rounds changeront légèrement. Les rotations de bits vers la gauche seront simplement remplacées par des rotations vers la droite, le reste demeurant inchangé. La structure de déchiffrement du DES est une opération basée sur la condition de remplacer les rotations vers la gauche des Key rounds en rotations vers la droite. Le texte chiffré sera introduit dans la boîte de permutation IP et le texte en clair sera produit en sortie de la permutation IP^{-1}.Cette propriété du DES lui accorde encore un nouvel avantage : la facilité avec laquelle on peut passer d'une unité de chiffrement à une unité de déchiffrement. Il n'y adonc pas besoin de construire deux outils différents pour le chiffrement et le déchiffrement .En général, la même unité pourra opérer dans les deux sens, et elle sera conçue sans nécessiter l'ajout substantiel de ressources. [20].

II.2.6 Les avantages de DES

L'algorithme DES contient les S-Boxes qui utilisent des ressources logiques, sur lesquelles repose la grande sécurité, étant non linéaires très efficaces pour diluer les informations. Par conséquent, nous pourrons appliquer la même approche sur les algorithmes successeurs de DES tels que:, 3DES, tant qu'ils contiennent les S-Boxes. Quant à la performance, les algorithmes symétriques, en général, nécessitent une capacité de calcul moins intensive que les algorithmes asymétriques [21]. Cela occasionne une rapidité de cryptage et décryptage atteignant des centaines ou des milliers de fois supérieure à celle des algorithmes à clé publique.

II.2.7 Les applications du DES

Le DES est présenté dans bien des applications associées à des opérations électroniques, comme par exemple la sécurité du courrier électronique, le transfert sécurisé de fichiers (notamment entre banques), ainsi que le paiement électronique.

II.3 AES encryptions (Advanced Encryption Standard)

L'AES est un algorithme de chiffrement symétrique par blocs, dans lequel l'émetteur et le récepteur utilisent la même clé pour le chiffrement et le déchiffrement .L'algorithme AES a une structure itérative qui traite des blocs de données de 128bits en utilisant des clés cryptographiques de 128, 192 ou 256 bits[22]. Le nombre des itérations est déterminé par la taille de la clé utilisée. Pour les trois tailles de clé de 128, 196 et 256 bits, un nombre de 10, 12 et 14 tours est requis, respectivement. La conception de l'algorithme AES est basée sur le concept de réseau de substitution-permutation dans lequel les octets du message en clair sont substitués et permutés à chaque tour à travers quatre opérations (transformations) appelées (SubBytes ,ShiftRows ,Mix Columns et Add Round Key[23]. La transformation *Add Round Key* est le point où la clé secrète entre dans le processus de chiffrement et contribue au résultat final. Ces quatre opérations sont répétées à chaque tours au fau dernier tour qui n'utilise pas la transformation Mix Columns. Le déchiffrement est simplement l'inverse du chiffrement car les quatre transformations sont réversibles .La Figure. 2.6 montre la structure générale de l'algorithme. AES..[24]

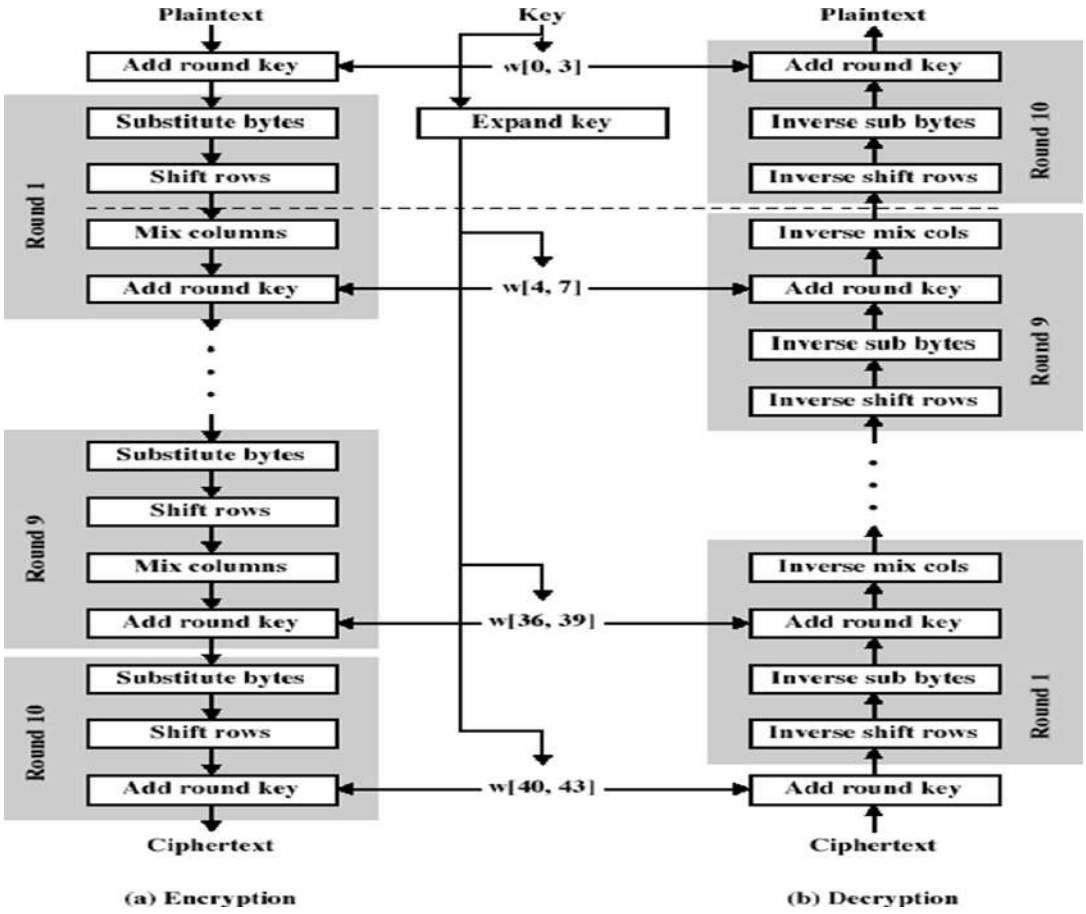


Figure II 6:*Algorithme AES.*

II.3.1 Les modes d'opération de l'AES

L'AES admet un bloc de données (128 bits) et un bloc de clé pour produire le bloc chiffré. Les blocs de données d'entrée et de sorties ont de taille identique. Par conséquent , et comme tous les algorithmes déchiffrement par blocs ,l'AES est combiné avec une série d'opérations simples pour pouvoir chiffrer plus que 128 bits de données et améliorer la sécurité sans pénaliser l'efficacité de l'algorithme, cette combinaison est appelée un mode de chiffrement [25][26]. On peut classer les modes d'opération de l'AES en deux catégories:

II. 3.1.1 Modes de chiffrement:

Dans cette catégorie, on a cinq modes de chiffrement sont principalement utilisés pour assurer la confidentialité (mode ECB, CBC, CFB, OFB et le mode CTR) [27].Les trois derniers modes (CFB, OFB et CTR) sont similaires au chiffrement par flots . Ils génèrent un flux de nombres pseudo-aléatoires qui dépend ou non du message en clair [28].

II.3.1.2 Modes de chiffrement authentifié :

Ces modes sont utilisés dans les applications où la confidentialité et l'intégrité de données sont traitées conjointement .Dans cette catégorie, trois modes sont généralement utilisés [29]

1. CounterwithCBC-MAC(CCM)
2. OffsetCodebookMode(OCB)
3. Galois/CounterMode(GCM)

Dans notre travail, on s'intéresse uniquement à la confidentialité et aux modes déchiffrement.

a) Mode ECB

En mode ECB (**Figure. 2.7**),le chiffrement est appliqué directement et indépendamment à chaque bloc du message en clair. La séquence résultante des blocs de sortie est le message chiffré [22]

b) Mode CBC

Le mode CBC, illustré dans la **Figure . 2.8** est le mode dans lequel le bloc en clair, avant d'être chiffré ,est XOR avec le bloc précédemment chiffré. Un vecteur initial doit être utilisé pour initialiser le processus. Ce vecteur remplace le premier bloc qui n'est pas encore défini. [26]

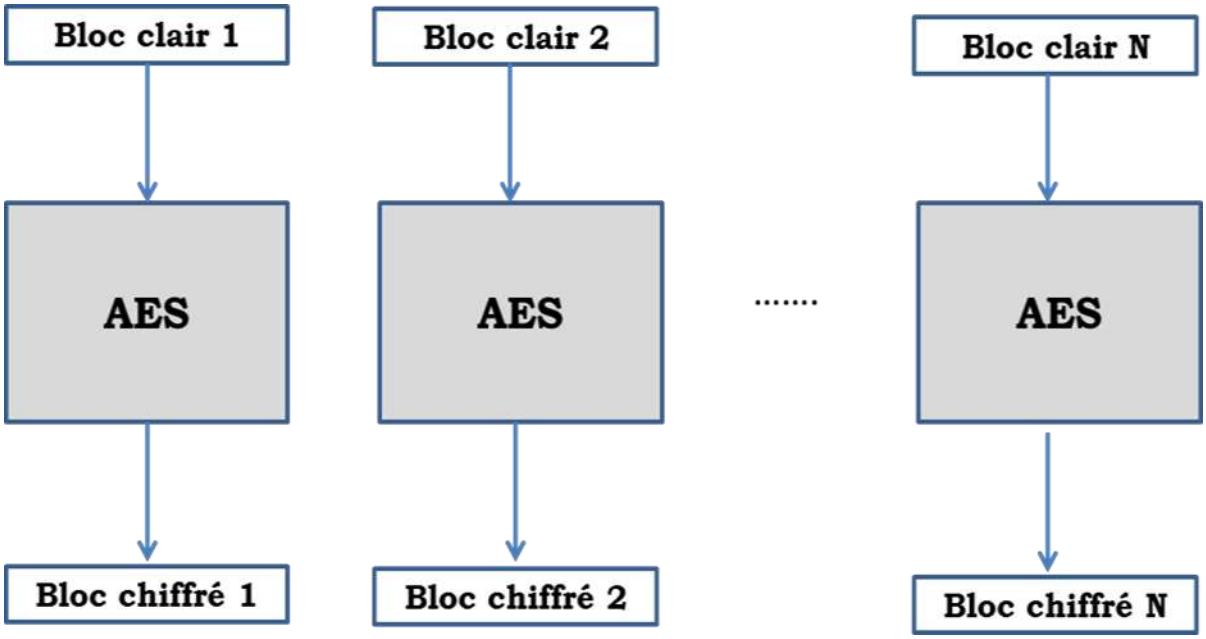


Figure II 7:*Mode ECB*

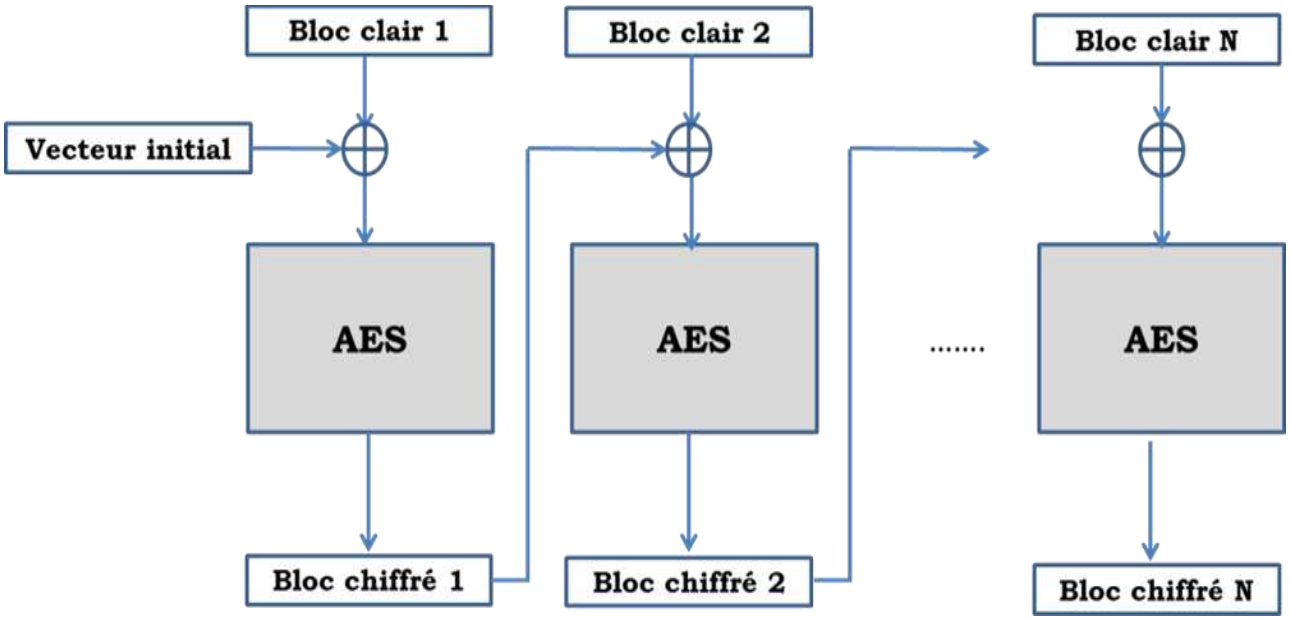


Figure II 8:*Mode CBC*

c) Mode CFB

Dans ce mode Fig. 2.9, un vecteur initial est utilisé pour démarrer le processus de chiffrement et générer le premier bloc chiffré, ce dernier est utilisé comme une entrée pour chiffrer le deuxième bloc . Le processus se répète séquentiellement jusqu'au dernier bloc[22][30]

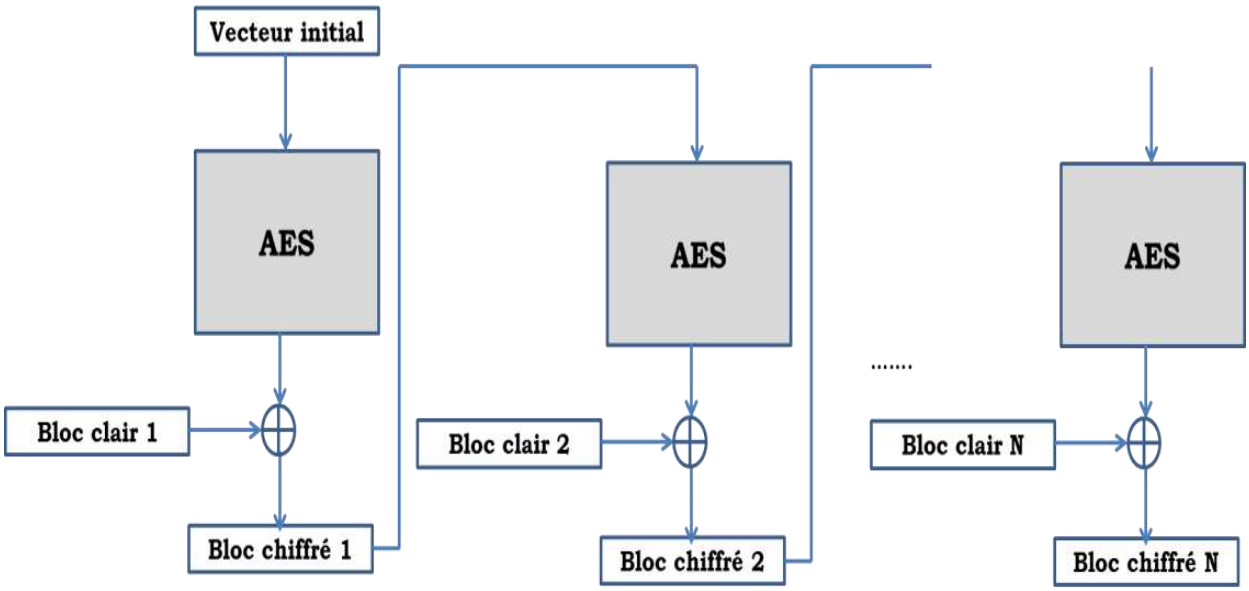


Figure II 9:*Mode CFB*

d) Mode OFB

Dans ce mode (**Figure 2.10**), un vecteur initial est initialement chiffré pour démarrer le processus, le flux de clé en sortie de ce bloc sera réinjecté en entrée pour calculer le prochain flux de clé.

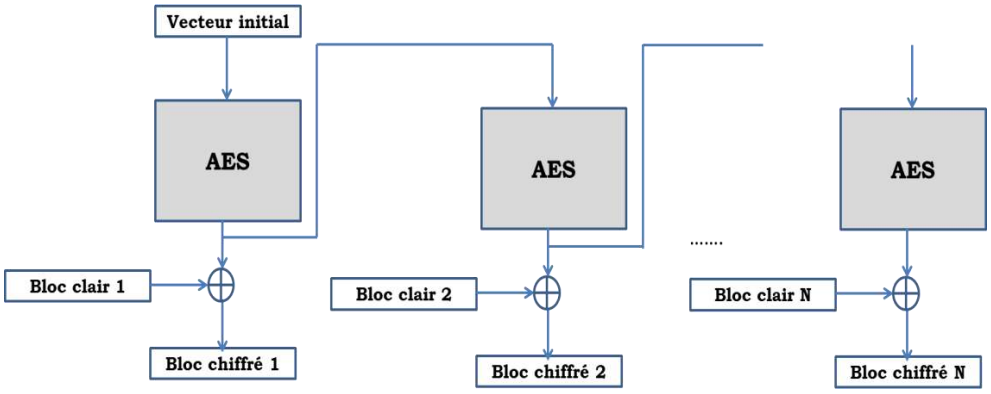


Figure II 10:*Mode OFB*

En utilisant ce mode, le prétraitement du flux de clé est possible car il ne dépend pas de message en clair.

e) Mode CTR

Ce mode est simple, il crée un flux des nombres pseudo-aléatoires indépendant du texte en clair. La Figure. 2.11 montre le mode compteur (CTR). Dans ce mode, le flux de clé (keystream) est obtenue n chiffrant des valeurs successives d'un compteur qui est ensuite XOR avec le message en clair pour générer le message chiffré[30].

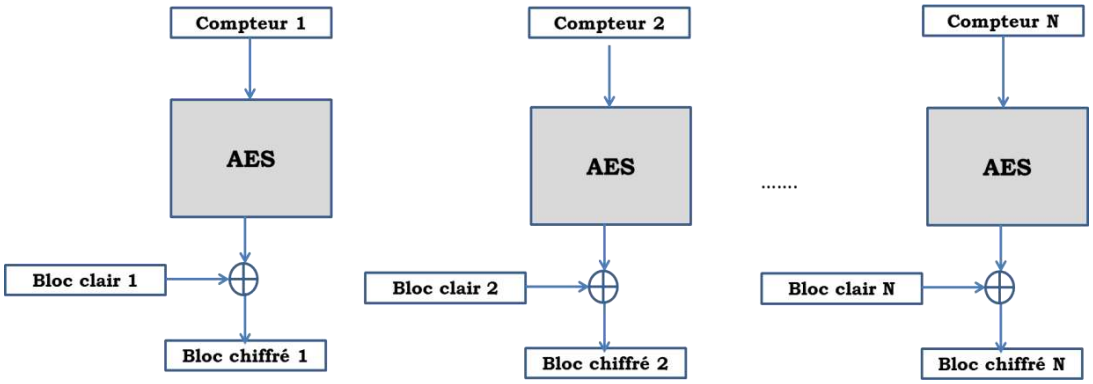


Figure II 11:*Mode CTR*

Les valeurs du compteur utilisées avec une clé déchiffrement doivent être des nonces, car le flux de clé ne doit jamais être répété. Dans ce mode, contrairement aux autres, il n'y a pas des feedback ou un traitement séquentiel des blocs. Par conséquent, il est possible d'effectuer plusieurs chiffrements en parallèle un avantage

significatif dans les applications à haute performance [26][31]. Ce mode est recommandé par le CCSDS pour le chiffrement des télémesures(TM)et les télécommandes (TC) [32]

II.4 La cryptographie sur les courbes elliptiques

La cryptographie sur les courbes elliptiques *(ECC : Ellipticcurvecryptography)*une cryptographie à clé publique basée sur la génération de courbes elliptiques sur un corps fini. Le calcul du processus de cryptage et de décryptage ne nécessite qu'une petite taille de clé. De plus, la technologie assure l'authentification et la confidentialité. Mais le principal inconvénient de cette méthode est le problème du logarithme discret à courbe elliptique (PLDCE) [33]. En prenant un nombre premier (p) plus grand, on peut éviter cet PLDCE. Dans le cryptage de texte, le texte est mappé à sa valeur ASCII. Les valeurs décimales correspondantes sont mappées aux points de génération [34-35], qui sont générés à l'aide d'équations.

$$y^2 = (x^3 + ax + b) \bmod P, (4a^3 + 27b^2) \bmod P \neq 0 \qquad (2.1)$$

Où a et b sont les coordonnées de l'équation ci-dessus, et P est un nombre premier. La cryptographie à courbe elliptique [36] implique de multiples opérations.

II.4.1 Concepts de base sur les courbes elliptiques :

Une courbe elliptique est l'ensemble des solutions satisfaisant l'équation

$$Y^2 = X^3 + AX + B \qquad (2.2)$$

Les équations de ce type s'appellent les équations de Weierstrass [37] d'après le mathématicien qui les a étudiés au cours du 19ème siècle, les courbes elliptiques illustrées dans la Figure.2.12.Soient deux exemples de courbes elliptiques,

$E_1 : \quad Y^2 = X^3 - 3X + 3 \quad$ et $\quad E_2 : \quad Y^2 = X^3 - 6X + 5$

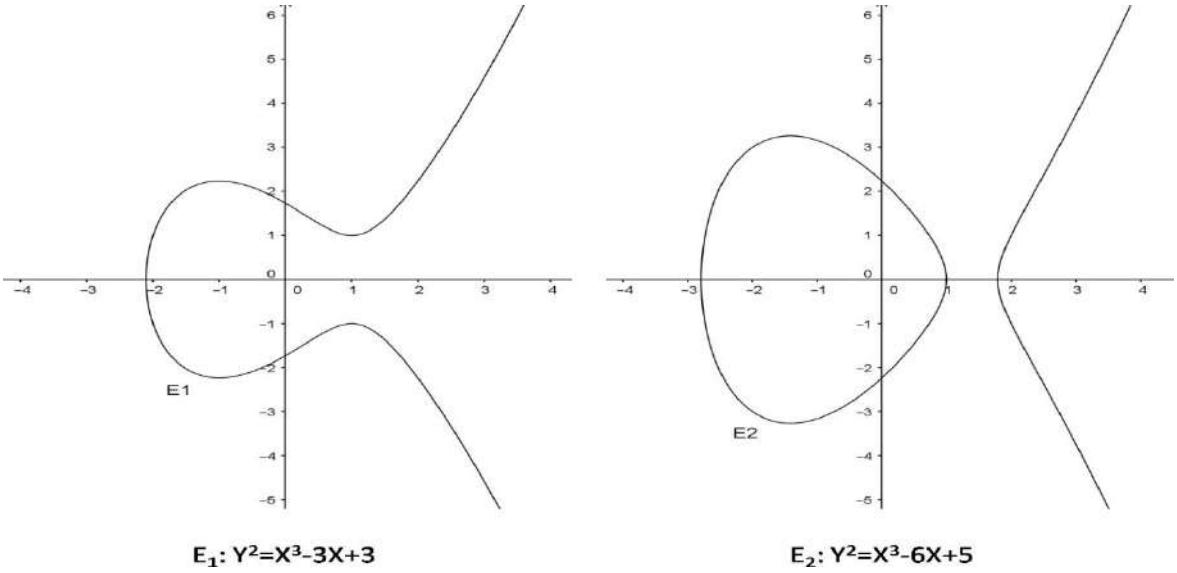


Figure II 12: *Deux exemples de courbes elliptiques.*

Une caractéristique étonnante des courbes elliptiques est qu'il existe un moyen naturel de prendre deux points sur une courbe elliptique et de les "additionner" pour donner un troisième point [38] . Mettons des guillemets au tour du mot, «additionner» parce que nous parlons d'une opération qui combine deux points,d'une manière analogue à l'addition (elle est commutatif, associatif, et il y a un élément neutre), mais très différente de l'addition traditionnelle. La manière la plus normale de décrire la «loi additionnelle » sur les courbes elliptiques consiste à utiliser la géométrie .Soit P et Q deux points sur une courbe elliptique E ,comme l'illustre la Figure.2.12, la ligne L qui traverse P et Q. Cette ligne L coupe E en trois points, P ,Q et R. Prenons ce point R et projetons le sur l'axe des X (c-à-d., multiplions sa coordonnée Y par-1) pour obtenir un nouveau point R_i .Le point R_i s'appelle la "somme de P et Q" .Pour l'instant, désignons cette étrange loi d'addition par le symbole $\oplus$. Ainsi, nous écrivons :

$$P \otimes Q = R_i$$

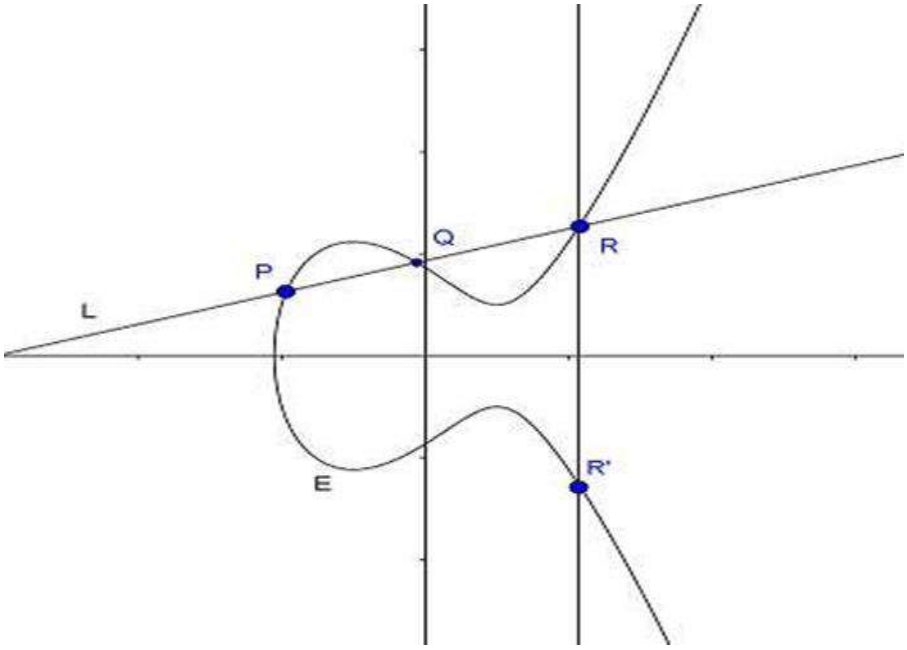


Figure II 13:*La loi d'addition sur les courbes elliptiques.*

La ligne L qui traverse P et P est la ligne verticale x = a, e cette ligne coupe E en deux points seulement P et P .

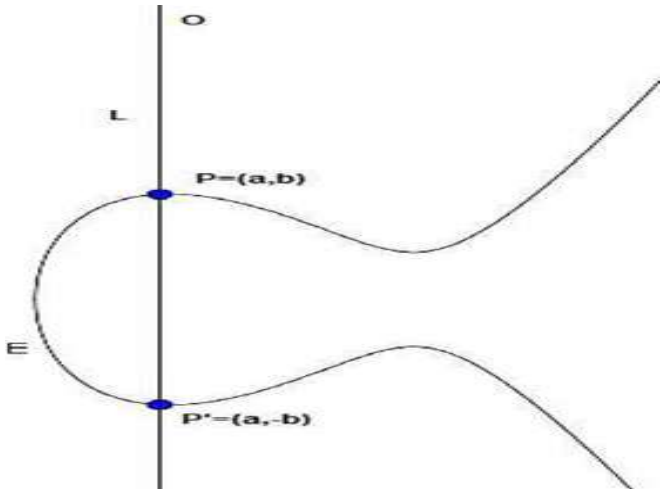


Figure II 14:*La ligne L traversant P et P*

(Voir la Figure 2.13) Il n'y a pas de troisième point d'intersection, il semble donc que nous soyons bloqués mais il y a une sortie. La solution est de créer un extra-point O qui se situe «à l'infini». Plus précisément, le point O n'existe pas dans le plan XY , mais nous prétendons qu'il se trouve sur chaque ligne verticale.

Nous posons ainsi:

$$P \otimes P_i = O$$

Nous devons également trouver comment additionner O avec un point ordinaire P = (a, b) sur E. La ligne L reliant P à O est la ligne verticale par P , puisque O se trouve sur les lignes verticales, et cette ligne verticale coupe E aux points P , O et P *j* = (a, −b). Pour additionner P et O, nous allons faire la projection du point P *j* sur l'axe X, ce qui nous ramène à P. En d'autres termes, P $\oplus$ O = P , donc O agit comme le zéro de l'addition pour les courbes elliptiques.

II.4.2 Courbes elliptiques sur les corps finis

Dans la section précédente, nous avons développé la théorie des courbes elliptiques géométriquement. Par exemple, la somme de deux points distincts P et Q sur une courbe elliptique E est définie en dessinant la ligne L reliant P à Q, puis nous trouvons le troisième point où L et E se croisent, comme illustré à la Figure 2.13. Cependant, pour appliquer la théorie des courbes elliptiques à la cryptographie, il faut considérer des courbes elliptiques dont les points ont des coordonnées dans un corps fini Fp. Cela est facile à faire. Nous définissons simplement une courbe elliptique sur Fp par une équation de la forme [39].

$$E : Y\,2 = X3 + AX + B$$

avec A, B $\in$Fp satisfaisant 4A3 + 27B2 /= 0

Aussi, nous considérons les points sur E avec des coordonnées en Fp, que nous désignons par :

$$E(Fp) = \{(X, Y) : X, Y \in Fp \text{ tel que : } \quad Y\,2 = X3 + AX + B\} \cup$$

II.4.3 La cryptographie par les courbes elliptiques

Les applications des courbes elliptiques à la cryptographie donne par une simple application, qui définit par l'échange de clés Diffie-Hellman [37], [40],[39], qui implique un peu plus le remplacement du problème de logarithme discret dans le corps fini F_p avec le problème du logarithme discret dans une courbe elliptique $E(F_p)$.

II.5 Conclusion

Dans ce chapitre, nous avons présenté les différents types des algorithmes cryptographiques tels que DES, AES et ECC avec une explication détaillée sur son principe de fonctionnement et quelques concepts mathématiques utilisés dans la cryptographie. Nous allons entamer dans le chapitre suivant, l'implémentation des trois versions des algorithmes cryptographiques pour crypter des paramètres acoustiques MFCC et améliorer la sécurité du système de vérification du locuteur.

Chapitre 3 :

Simulations et Résultats

Chapitre 3 : simulations et Résultats

III.1 Introduction

Dans ce chapitre, nous allons présenter la simulation et les résultats obtenus après l'évaluation de notre système de vérification du locuteur. Notre objectif étant de développer un système de reconnaissance sécurisé basé sur des paramètres acoustiques MFCC cryptés par des algorithmes DES, AES, DES-ECC et AES-ECC dans un canal de transmission mobile.

Les protocoles de développement et d'évaluation de cette technique de paramétrisation sont décrits dans cette section. Ils mettent en jeu des modules d'extraction des paramètres acoustiques à savoir MFCC-DES,MFCC-AES,MFCC-DES-ECC,MFCC-AES-ECC.

III.2 Logiciels et langages utilisés dans l'application

III.2.1 Logiciel Matlab

Nous avons utilisé un logiciel MATLAB (matrix laboratory) version 18.02 sous Windows 10, Matlab est un langage de programmation émulé par un environnement de développement, il est utilisé à des fins de calcul numérique et commercialisé par la société américaine the Math Works. Ce langage est basé essentiellement sur le calcul matriciel à syntaxe simple, avec des fonctionnalités mathématiques spécialisées et graphiques étendues.

III.3 Description des bases de données utilisées

Les simulations ont été effectuées en utilisant les bases de données NIST-2008.

III.3.1 La base de données NIST-2008

L'évaluation de système de reconnaissance du locuteur fait une partie des séries continued'évaluations annuelles menées par le NIST (National Institute of Standards and Technology).En effet, depuis 1996 une série d'évaluations SRE (Speaker Recognition Evaluation), dans le but de promouvoir la recherche en reconnaissance automatique du locuteur. NIST-SRE 2000, qui était d´éditée à la vérification du locuteur. La base de données contient des fichiers audio (hommes et femmes) sous format (WAV.file), avec une fréquence d'échantillonnage égale à 8 KHz. La durée des fichiers varie de 10 s À trois minutes. Le répertoire « WAV » est divisé en 2 sous

répertoire « Apprentissage » pour créer un modèle du locuteur et le (test) pour la reconnaissance. Nous avons pris 50 locuteurs à partir de cette base. La base de données est passée ensuite à travers le codec standard AMRWB pour aboutir à la base de données transcodée mobile et le canal de transmission est simulé par un bruit additif AWGN avec différent niveau RSB (-5dB,0dB,5dB,10dB) .

III.4 Étapes de la réalisation des systèmes de vérification du locuteur:

Différentes étapes sont nécessaires à la construction et à la validation de notre système:

- Créer l'ensemble d'apprentissage: la base de données que nous avons utilisée est constituée de 300 fichiers, prononcés par 50 locuteurs de différents sexes qui répètent la même phrase 6 fois.
- Faire des opérations de cryptage de données par l'algorithme tel que : DES,AES et ECC.
- Effectuer l'analyse acoustique: l'ensemble des fichiers de la base de données ont été convertis en une série de vecteurs (MFCC) d'apprentissage et le test.
- Faire l'apprentissage des modèles du locuteur cible.
- L'apprentissage d'un sous-espace de variabilité totale à partir des statistiques.
- Créer un modèle GPLDA Gaussian avec des i-vecteurs de développement.
- Calcule le score entre les modèles d'i-vecteurs de développements et le test.
- Faire la reconnaissance et évaluer la performance des systèmes.

III.5 La structure générale de Système de vérification du locuteur:

La Figure 3.1 représente le synoptique du système de vérification du locuteur basé sur les différentes techniques de para-métrisation mises en œuvre (MFCC-DES , MFCC-AES,MFCC-DES-ECC,MFCC-AES-ECC). Dans cette structure, on distingue deux phases : la phase d'apprentissage et la phase de vérification (test).

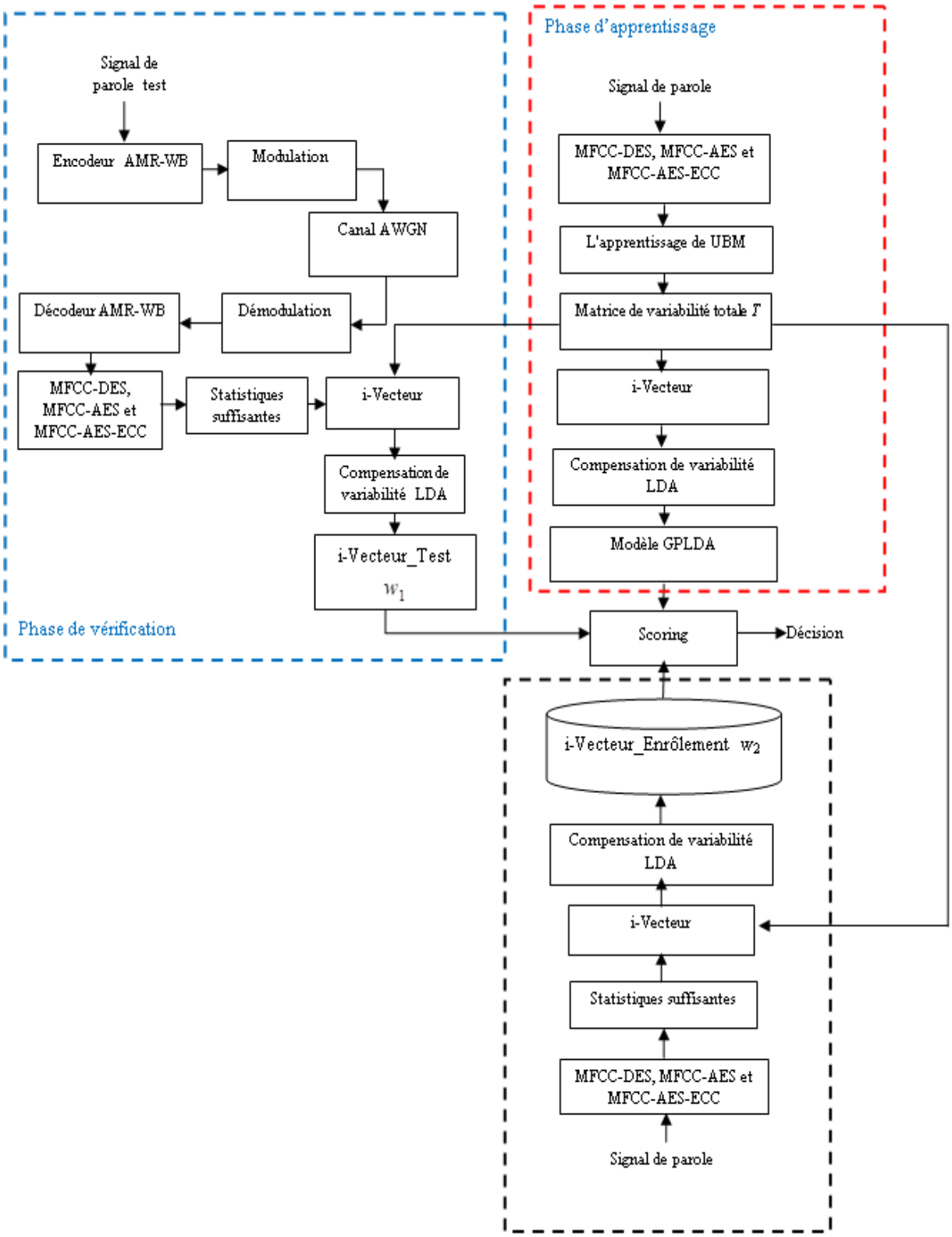


Figure III 1:*Schéma synoptique du système de vérification du locuteur en canal de transmission mobile (AWGN)*

III.6 Extraction des paramètres

III.6.1 Para-métrisation des coefficients MFCC

Le signal de parole est paramétré en utilisant les coefficients MFCC. Ces paramètres sont extraits toutes les 10ms, sur des fenêtres de 25 ms. La fenêtre de pondération utilisée est la fenêtre de Hamming et puis appliquer Douze (20) coefficients MFCC, ils sont calculés pour chaque trame dans l'échelle fréquentielle Mel. Les coefficients différentiels du premier et du second ordre (ΔΔ).

III.6.2 Protocole d'évaluation des résultats

Pour évaluer notre système, nous avons structuré les bases de données comme suivant:

- **La base d'apprentissage:**elle est composée de 300 fichiers vocaux prononcés par 50 locuteurs comprenant les deux sexes. Chaquelocuteurrépétela phrase 6 fois.
- **La base de test:**elle est composée de 300 fichiers vocaux prononcés par 50 locuteurs, comprenant les deux sexes Chaque locuteur répète la phrase 6 fois.

III.7 Simulations et résultats

Pour évaluer la robustesse des systèmes de vérification du locuteur à base de coefficients tels que : MFCC-DES, MFCC-AES, MFCC-DES-ECC et MFCC-AES-ECC.Nous avons réalisé des expériences devérificationdu locuteur par un type du bruit (Canal de transmission AWGN)Pour l'entrainement des modèles acoustiques a été réalisé avec la base de données NIST-2008 non bruitée, le bruit AWGN a été seulement ajouté pour la base de test, en utilisant les niveaux RSBsuivants : -5dB, 0dB, 5dB, 10dB.

Nous avons validé notre système de vérification du locuteur en utilisant comme entrée les coefficients « MFCC-DES, MFCC-AES, MFCC-DES-ECC et MFCC-AES-ECC vecteurs »cette étude est faite en fonction de bruit du canal de transmission mobile. Dans la phase de vérification (test), les données de test sont codées par un codeur de la parole AMR-WB.

Les effets de bruit sont modélisés par un bruit gaussien blanc additif (AWGN) avec une densité spectrale de puissance et canal d'évanouissement qui dépend du rapport

signal sur bruit (SNR : -5dB, 0dB, 5dB, 10dB, 15 dB).Le rapport de l'énergie du signal divisé par l'énergie du bruit, appelée "Rapport signal/bruit" (SNR en anglais).

Pour : $$s(t) = x(t) + n(t)$$

Le rapport signal sur bruit est défini par :

$$RSB(dB) = \frac{E_S}{E_n}$$

Es :représente l'énergie moyenne du signal x(t).

E_n *:* représente l'énergie moyenne du bruit *n(t)*.

III.7.1 Performance du système de vérification du locuteur en bruit AWGN pour les algorithmes de cryptage DES et AES

Dans cette partie, nous étudions l'effet du canal AWGN avec différents paramètres (MFCC-DES et MFCC-AES) sur les performances globales du système. Nous évaluons et comparons les performances des différents paramètres en utilisant différents niveaux de RSB (-5, 0, 5, 10dB). Le Tableau.3.1 et la Figure .3.2 présentent les résultats obtenus avec les cryptés par l'algorithme DES pour MFCC-DESs au canal AWGN

EER(%)				
RSB AWGN	-5	0	5	10
MFCC-DES	25.8	20.62	18.10	11.08

Tableau III 1:*Les performances du système de vérification en utilisant les paramètres cryptés MFCC-DES par l'algorithme DES au canal AWGN*

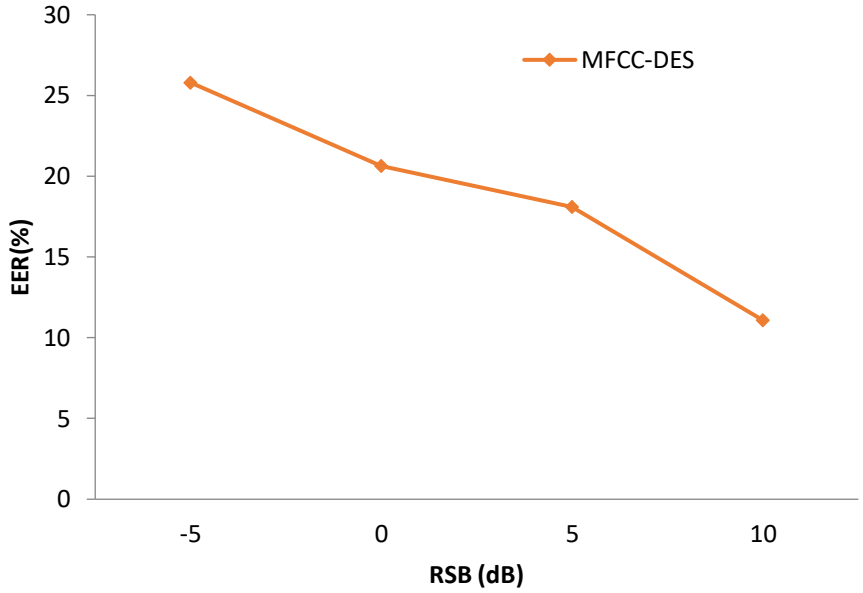


Figure III 2:*Les performances du système de vérification en utilisant les paramètres cryptés MFCC-DESs par l'algorithme DES au canal AWGN.*

Le Tableau 3.2 et la Figure. 3.3 illustrent les résultats obtenus avec les paramètres avec les cryptés par l'algorithme AES pour MFCC-AESs au canal AWGN

EER(%)				
RSB AWGN	-5	0	5	10
MFCC-AES	23.50	22.34	19.49	10.98

Tableau III 2:*Les performances du système de vérification en utilisant les paramètres cryptés MFCC-AES par l'algorithme AES au canal AWGN*

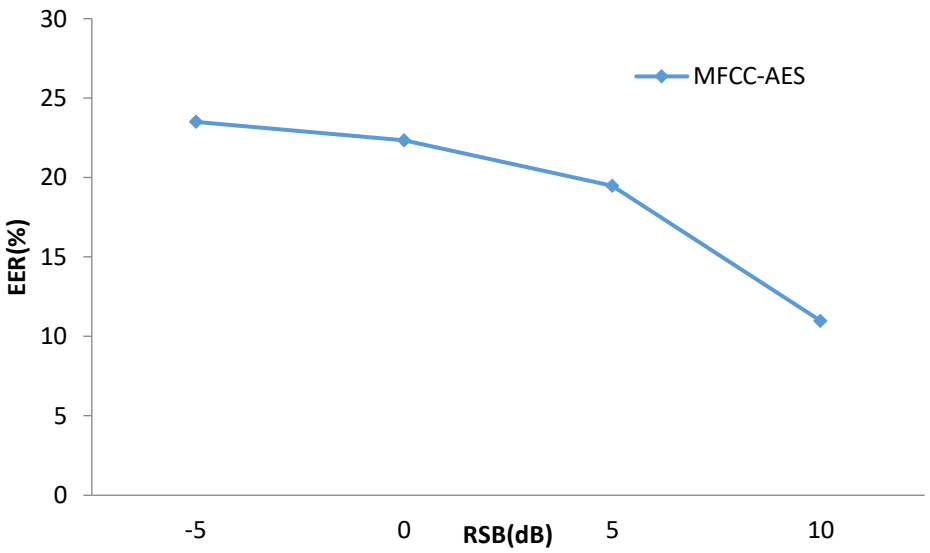


Figure III 3:*Les performances du système de vérification en utilisant les paramètres cryptés MFCC-AES par l'algorithme AES au canal AWGN*

Les résultats des Tableau.3.1, Tableau.3.2 et les Figure3.2, Figure3.3 montrent que les paramètres MFCC-AES donnent de meilleurs résultats de reconnaissance en terme de taux EER (%) par rapport au paramètres MFCC-DES.

III.7.2 Performance du système de vérification du locuteur en bruit AWGN pour les algorithmes de cryptage DES-ECC et AES-ECC

L'objectif de la prochaine simulation est d'évaluer les performances du système de vérification du locuteur à l'aide des paramètres MFCC-DES-ECC et MFCC-AES-ECC et de la combinaison des algorithmes de cryptages DES et AES par ECC. Les résultats des performances des systèmes vérification du locuteur en utilisant différents paramètres sont présentés dans le Tableau 3.3, Tableau 3.4 et les Figure.3.4 et Figure.3.5

EER(%)				
RSB AWGN	-5	0	5	10
MFCC-DES-ECC	23.12	19.47	18.24	11.00

Tableau III 3:*Les performances du système de vérification en utilisant les paramètres cryptés MFCC-DES-ECC par l'algorithme DES-ECC au canal AWGN*

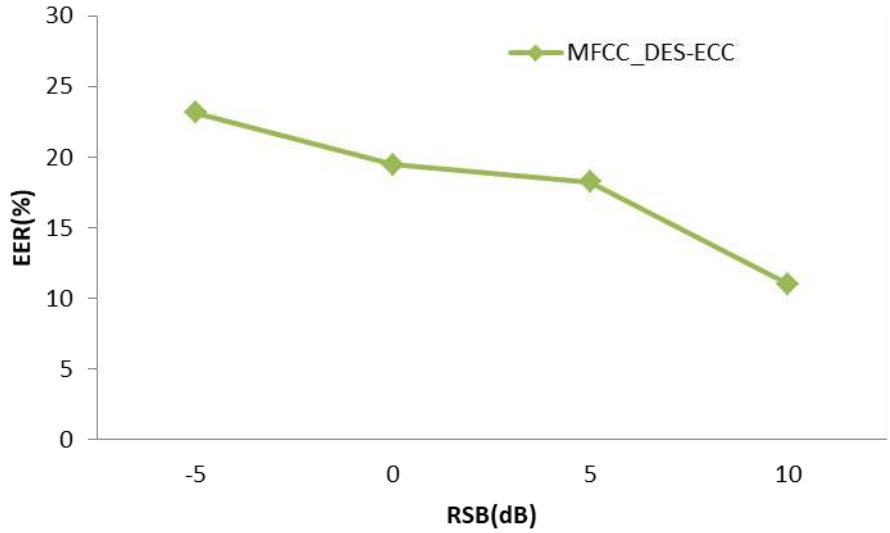


Figure III 4:*Les performances du système de vérification en utilisant les paramètres cryptés MFCC-DES-ECC par l'algorithme DES-ECC au canal AWGN*

EER(%)				
RSB AWGN	-5	0	5	10
MFCC-AES-ECC	21.12	20.30	17.80	10.55

Tableau III 4:*Les performances du système de vérification en utilisant les paramètres cryptés MFCC-AES-ECC par l'algorithme AES-ECC au canal AWGN.*

.

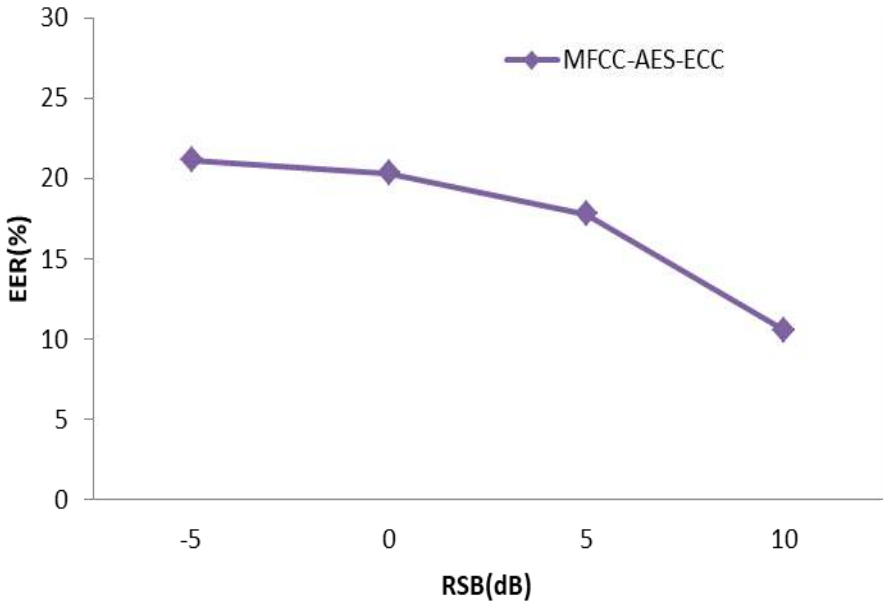


Figure III 5:*Les performances du système de vérification en utilisant les paramètres cryptés MFCC-AES-ECC par l'algorithme AES-ECC au canal AWGN*

Les résultats des Tableau.3.3, Tableau.3.4 et les Figure.3.4, Figure.3.5 montrent que les paramètres MFCC-AES-ECC donnent de meilleurs résultats de reconnaissance en terme de taux EER (%) par rapport au paramètres de base MFCC-DES-ECC, plus particulièrement à faible niveau de SNR (-5dB et 0 dB). Les résultats obtenus via les paramètres MFCC-AES-ECC sont meilleurs que ceux de les MFCC-AES, MFCC-DES.

III.8 Conclusion

Dans ce chapitre, on a proposé une technique de paramétrisation basée sur les différents algorithmes de cryptages de sécurité du canal de transmission DES, AES, DES-ECC et AES-ECC. La technique proposée améliore les performances du système de vérification du locuteur en utilisant la modélisation i-vecteur-GPLDA. Les performances du système ont été évaluées à l'aide de la base de données NIST 2008. Le système est analysé en présence dubruit de transmission du canal: le bruit gaussien blanc (AWGN) à divers niveaux du rapport signal-bruit (SNR : -5dB à 10dB). L'analyse des résultats obtenus montre que l'utilisation des paramètres proposés pour les bruits des canaux mobiles permet d'améliorer la performance du système de vérification du locuteur par rapport aux coefficients conventionnels MFCC

Conclusion générale

Conclusion générale

Ce projet de fin d'étude traite la performance et la sécurité du système de vérification du locuteur dans un environnement mobile à base des paramètres acoustiques cryptés par de différents algorithmes de cryptages. La performance du système de vérification du locuteur est étroitement liée à la qualité du signal parole, les signaux transmis par le réseau mobile montrent une dégradation plus importante à cause de l'effet du canal de transmission.

Pour réaliser le travail dans un environnement mobile, nous avons utilisé une base de données NIST 2008. Cette base de donnéesest codée par un codeur AMRWB (Adaptive Multi Rate-Wide Band) pour obtenir une base de données des signaux mobile.Le bruit du canal de transmission a été lui simulé par un bruit blanc additif AWGN (*Additive White Gaussian Noise*) à différents niveaux SNR *(Signal to Noise Ratio*), -5dB, 0dB, 5dB, 10dB. Nous avons utilisé comme un vecteur d'entré pour le système de reconnaissance les paramètres : MFCCs avec différents algorithmes de cryptages DES, AES, DES-ECC et AES-ECC.

Les résultats obtenus en utilisant les paramètres acoustiques cryptés MFCC-DES-ECC et MFCC-AES-ECC montrent que le système de reconnaissance du locuteur est plus performant et plus sécuriseque le système de reconnaissance avec le paramètre MFCC, MFCC-DES et MFCC-AES.

Références bibliographiques

Bibliographie

[1] M. Mohamad El Abed, « **Evaluation de systèmes biométriques** ». Thèse de doctorat, Spécialité Informatique et applications, Université de Caen/Basse-Normandie.

[2] Yassine Mami, « **Reconnaissance de locuteurs par localisation dans un espace de locuteurs de référence** ».Thèse de doctorat, spécialité d'images et de signal, École nationale supérieure des Télécommunications Paris Tech, 2003.

[3] Sayoud Halim, « **Reconnaissance Automatique du Locuteur-Approche connexionniste** »,Thèse de Doctorat spécialité d'électronique et Electrotechnique, Faculté d'Electronique et d'Informatique USTHB, 2003.

[4] Vincent Jousse, « **Identification nommée du locuteur: exploitation conjointe du signal Sonore et de sa transcription**». Thèse de doctorat, spécialité d'informatique, Université du Maine, 2011. Français.

[5] Teva Merlin. «**Amiral, une plateforme générique pour la reconnaissance automatique du locuteur de l'authentification à l'indexation**". Thèse académie d'Aix-Marseille, spécialité d'informatique, université d'Avignon et des Pays de Vaucluse, 2004.

[6] Ben Mahria Bilal, «**L'approche hybride GMM-SVM pour l'identification des locuteurs en mode indépendant du texte en milieu fermé**», thèse de master, spécialité de système intelligent et réseau, Université Sidi Mohamed Ben Abdallah, 2014-2015.

[7] Fredouille, Corinne, « **Approche statistique pour la reconnaissance automatique du locuteur : informations dynamiques et normalisation bayésienne des vrais emblances** ». Thèse de doctorat**,** spécialité d'informatique**,** Université d'Avignon et des Pays de Vaucluse Donneur de grade 2000.

[8] Antonio M. Peinado, José C. Segura, «**Reconnaissance de la parole sur les canaux numériques: Robustesse et normes »,** 2006. www.onlinelibrary.wiley.com/book/10.1002/0470024720

[9] Ajgou Riadh, « **Reconnaissance Automatique du Locuteur à Travers les Canaux Digitaux** », Thèse de Doctorat, spécialité d'électronique, Université Mohamed Khider Biskra, 2016.

[10] Houda Kadi. « **La reconnaissance automatique du locuteur par la voix IP** » Thèse de master, spécialité de système intelligent et réseau Université sidi Mohamed ben abdallâh, 2014.

[11] Mohammed Senoussaoui, « **Amélioration de la robustesse des systèmes de reconnaissance automatique du locuteur dans l'espace des i-vecteurs** ». Thèse de doctorat, spécialité génie électrique, École de technologie supérieure université du Québec 2014

.

[12] Laurent Besacier, «**Un modèle parallèle pour la reconnaissance automatique du locuteur** » thèse de doctorat, Spécialité mathématique et Informatique l'Université d'Avignonet des Pays de Vaucluse, 1998

[13] Claude Barras, « **Reconnaissance automatique des locuteurs pour la structuration en tours de parole** ». Thèse de master, spécialité d'Informatique pour la Mécanique et les Sciences de l'Ingénieur, Université Paris-Sud11, 2011.

[14] Mr.Ramou Naim, «**Amélioration des performances de la reconnaissance automatique locuteur par des méthodes de fusion de données »,** thèse de master, spécialité électronique ,thèse de master, spécialité électronique, Université des sciences et de la technologie Houari Boumediène (USTHB), 2010.

[15] Imen Trabelsi, Dorra Ben Ayed, « **Evaluation d'une Approche Hybride GMM-SVM pour l'Identification de Locuteurs »,** article volume 8, N°1, pp 61-65, 2011.

[16] Nassim Elabed, Zied Sakka, Mounir SAMET et Abdennaceur Kachouri, « **Approche Multi-Bandes pour la Reconnaissance Automatique des Mots Isolés et Phonèmes Arabes ».** Conférence international de Sfax, Tunisie, 2009.

[17] C. Liua et Jin-shui Ji et Zi-long Liu, « Implementation of DES Encryption Arithmetic based on FPGA », 2013 AASRI Conference on Parallel and Distributed Computing Systems, Northwest University for nationalities Lanzhou, Gansu, China.

[18] F. Germain, « Sécurité cryptographique par la conception spécifique de circuits intégrés », Thèse Ph. D, Ecole Polytechnique, Paris VI, Juin 2006.

[19] https://fr.wikipedia.org/wiki/Constantes_du_DES.

[20] M. Sébastien, « Implémentation du DES et cryptanalyse sur FPGA », mémoire d'ingénieur civil électricien, Université Catholique de Louvain, Septembre 1999.

[21] O. Mencer, M. MORF ET MJ Flynn, « Hardware Software tri-design of Encryption for mobile Communication Units », In Proceeding, volume 5, 1998.

[22] Katz, J., & Lindell, Y. (2014). *Introduction to modern cryptography*: CRC press

[23] Stallings, W. (2006). *Cryptography and network security: principles and practices*: Pearson Education India.

[24] FIPS, P. (2009). 197, Advanced Encryption Standard (AES), National Institute of Standards and Technology, US Department of Commerce, November 2001.

[25] Banu, P. S. R. (2007). *Satellite on-board encryption.* University of Surrey (United Kingdom

[26] Burr, W. E. (2003). Selecting the advanced encryption standard. *IEEE Security & Privacy*, *99*(2), 43-52.

[27] Dworkin, M. (2001). Special Publication 800-38A: Recommendation for block cipher modes of operation.

[28] Hudde, H. (2009). Building stream ciphers from block ciphers and their security. *Seminararbeit Ruhr-Universität Bochum, February*.

[29] Chen, H., & Paar, I. C. (2009). Authenticated Encryption Modes of Block Ciphers, Their Security and Implementation Properties.

[30] Stavroulakis, P., & Stamp, M. (2010). *Handbook of information and communication security*: Springer Science & Business Media

[31] McGrew, D. (2002). Counter mode security: Analysis and recommendations. *Cisco Systems, November, 2*, 4.

[32] CCSDS. (350.9-G-1, 2012). CCSDS cryptographic algorithms

[33] Moumita Roy, Nabamita Deb, Amar Jyoti Kumar, "Point Generation And Base Point Selection In ECC An Overview", International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 5, May 2014.

[34] Neal Koblitz, "Elliptic Curve Cryptosystems", Mathematics of Computation, Volume 4. Number 177. Pages 201-209.

[35] Geetha G, Padmaja Jain, "Implementation of Matrix based Mapping Method Using Elliptic Curve Cryptography", International Journal of Computer Applications Technology and Research, Volume 3– Issue 5, 312 - 317, 2014, ISSN: 2319–8656.

[36] KefaRabah, "Elliptic curve ElGamal Encryption and Signature Schemes", Information technology Journal 4(3): 299-306,2005, ISSN1812-5638.

[37] Ian Blake, Gerald Seroussi, Gadiel Seroussi, and N Smart. *Elliptic curves*

in cryptography, volume 265. Cambridge university press, 1999.

[38] Jeffrey Hoffstein, Jill Catherine Pipher, Joseph H Silverman, and Joseph H Silverman. *An introduction to mathematical cryptography*, volume 1. Springer, 2008.

[39] Andreas Enge. *Elliptic curves and their applications to cryptography : an introduction*. Springer Science & Business Media, 2012.

[40] Neal Koblitz. *Algebraic aspects of cryptography*, volume 3. Springer Science & Business Media, 2012.

ملخص

ينتمي هذا العمل إلى مجال التعرف على المتحدث ، والهدف من ذلك هو التعرف على الشخص من خلال تحليل صوته. عادةً ما يتم استخدام إعدادات أمان التحقق من نظام مكبرات الصوت MFCC كتمثيل صوتي للإشارة الصوتية. لا تزال إعدادات MFCC حساسة للغاية لإشارة التغييرات في بيئة الهاتف المحمول. لجعل هذه الإعدادات أكثر قوة ضد الضوضاء والهجمات في قناة الإرسال. في هذا السياق ، اقترحنا معلمات صوتية مختلفة مشفرة MFCC. لقد أجرينا دراسة مقارنة حول أداء نظام التحقق من السماعات في قناة الإرسال ، توضح أن استخدام المعلمات المشفرة -MFCC- MFCC-DES-ECC AES-ECC يحسن أداء النظام إلى أداء المعلمات MFCC و MFCC - DES و MFCC-AES.

كلمات مفتاحية :

نظام التحقق من السماعات ، MFCCs، DES، AES، ECC ، بيئة الهاتف المحمول.

Résumé

Ce travail appartient au domaine de la reconnaissance du locuteur, dans lequel L'objectif est d'identifier une personne en analysant sa voix. La sécurité de vérification du système des locuteurs sont généralement utilisés Les paramètres MFCC comme représentation acoustique du signal vocal. Les paramètres MFCCsont encore très sensibles aux changements de signal dans l'environnement mobile. Pour rendre ces paramètres plus robustes contre le bruit et les attaques dans un canal de transmission. Dans ce contexte, nous avons proposé des différents paramètres acoustiques MFCC cryptés. Nous avons fait une étude comparative portant sur la performance du système de vérification du locuteur en canal de transmission, montre que l'utilisation des paramètrescryptés MFCC-DES-ECC et MFCC-AES-ECCaméliore la performance du système à celle de paramètres MFCC, MFCC-DES et MFCC-AES.

Mots clés : Système de vérification du locuteur,MFCCs, DES, AES, ECC, environnement mobile.

.

Abstract :

This work be longs to the field of speaker recognition, in which the objective is to identif ya person by analyzinghis voice. The speaker verification systemis generally used MFCC, featureas an acousticre presentation of the voice signal. MFCC settings are still very sensitive to signal changes in the mobile environment. To make these settings more robust against noise and attacks in a transmission channel. In this context, we have proposed different feature extraction techniques encrypted. We made a comparative study on the performance of the speaker verification system in transmission channel, shows that use the feature extraction techniques encryptedsuch as MFCC-DES-ECC and MFCC-AES-ECC improves the performance of system that the MFCC and MFCC-DES and MFCC-AES.

Keywords :

Speaker verification system, MFCC-DES,AES and ECC , Mobile environment