

السلام عليكم ورحمة الله وبركاته

Ministère de l'enseignement supérieur et de la recherche scientifique
Université Dr."Yahia FARES" de Médéa.

Projet de fin d'étude

Pour l'obtention du diplôme de master en Génie électrique

OPTION : Système de Télécommunication

THEME

Génération des Clés Cryptographiques à Partir de la Parole Biométrique

Proposé et dirigé par :
Dr. SOLTANE

Réalisé par :
Mr : **SAHNINE Merzak**
Mr : AMER walid

PLAN DE TRAVAIL

Chapitre I: Introduction Et Motivation

Chapitre II: Les systèmes biométriques

Chapitre III: la biométrie basée sur le chiffrage

Chapitre IV : bases théoriques

Chapitre v: implémentations et évaluation

Conclusion générale



Chapitre I
Introduction Et Motivation

Motivation Pour La Biométrie Et La Sécurité

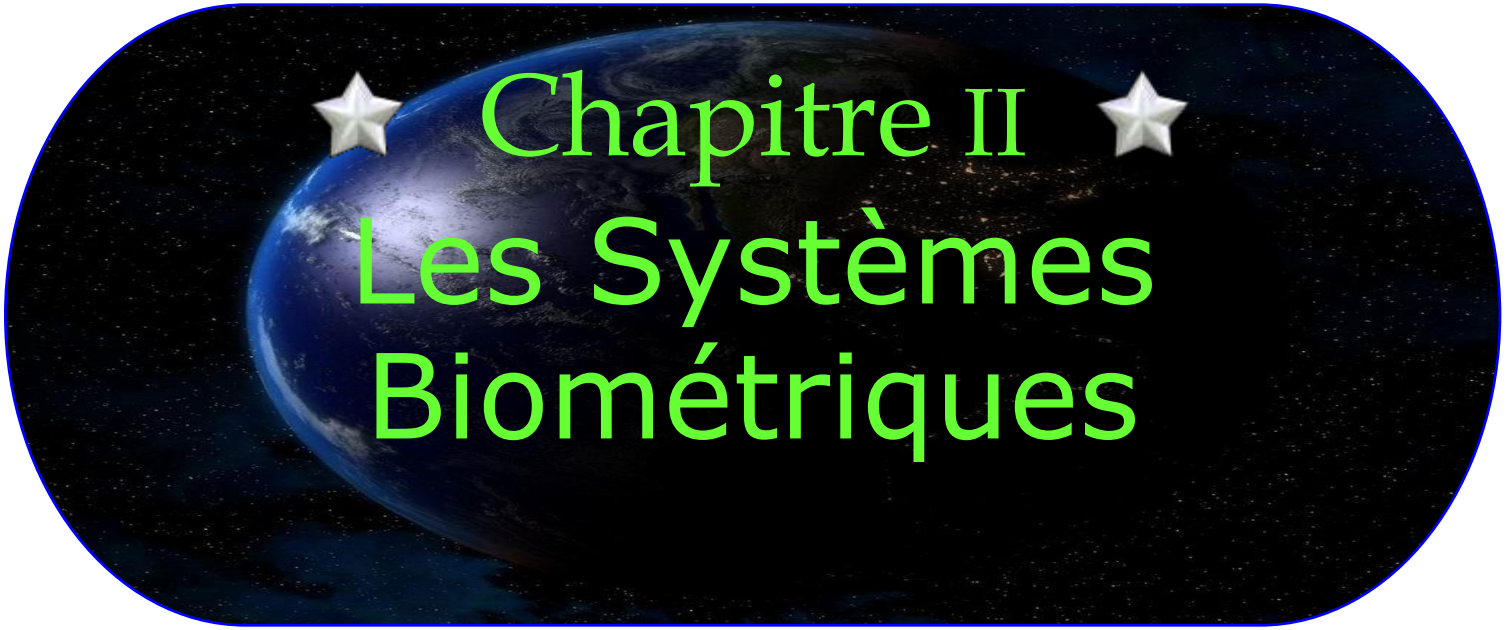
Un trait biométrique est défini comme un unique, mesurable, caractéristique biologique pour la reconnaissance automatique ou la vérification de l'identité d'un être humain.

Ces jours-ci, les technologies biométriques généralement utilisé pour analyser les caractéristiques de l'homme pour des raisons de sécurité sont les modèles biométriques analysées.

Le système Biométrique est vulnérable à une variété d'attaques visant l’atteinte à l'intégrité de l'authentification du processus.

Pour protéger le modèle d'informations biométriques à partir de non accès autorisée, des divers systèmes basés sur la cryptographie ont été développé.

Dans notre recherche, nous avons mis l'accent sur la recherche d'un moyen efficace et d'obtenir des informations biométriques, mettant l'accent sur le chiffrement et le déchiffrement.


Chapitre II
Les Systèmes
Biométriques

Introduction

Le terme « biométrie » vient du grec bio (vie) et metron (mesure).

La biométrie peut être définie comme étant ‘’la reconnaissance automatique d’une personne en utilisant des traits distinctifs ‘’.

➢Le système biométrique

Un système biométrie peut avoir trois modes opératoires :

1-L’enroulement :

-Capture de l'information.

- Traitement de l'information.

- la vérification.

2- L’identification :

le système biométrie pose et essaye de répondre à la question, ‘’ qui est la personne x ?

3-La vérification ou l'authentification :

Le système biométrique demande à l'utilisateur son identité et essaye de répondre à la question, '' est-ce la personne x'' ?

- Les Techniques Biométriques

Il existe plusieurs techniques biométriques utilisées dans plusieurs applications et secteurs, on peut en distinguer trois catégories :

1-L’analyse morphologique (physiologique)

Elle est basée sur l’identification des traits physiques particuliers qui, pour toute personne, sont uniques et permanents. Cette catégorie regroupe :

-L’iris de l’œil, le réseau veineux de la rétine, La forme de la main, Les empreintes digitales, Les traits du visage,

2-L’analyse comportementale

Elle se base sur l’analyse de certains comportements d’une personne. Cette catégorie regroupe :

La reconnaissance vocale, La Dynamique des frappes au clavier , La dynamique de la signature.

3-L’analyse biologique

Il existe par ailleurs une autre catégorie qui est l’étude des traces biologiques telles que :

L’ADN, le sang, et l’odeur.

Chapitre III
la Biométrie Basée sur le Chiffrage

➢Introduction

Un système de gestion fiable d'identité est un besoin urgent afin de combattre les conditions peser de sécurité dans une variété d'applications s'étendre du passage des frontières international à fixer l'information dedans bases des données.

➢Attaque Contre Les Systèmes Biométriques

Les différentes causes de la vulnérabilité du système biométrique. Au niveau le plus élevé, les modes de défaillance d'un système biométrique peuvent être classés en deux catégories:

-L’insuffisance intrinsèque:

Les défaillances intrinsèques se produisent en raison à des limites inhérentes à la détection.

-L’échec en raison d'une attaque de l'adversaire

Dans les attaques de l'adversaire, un débrouillard pirate (ou éventuellement un groupe organisé) tente pour contourner le système biométrique pour des gains personnels.

1-L’échec intrinsèque

Les fausse d’acceptations des paiements (par exemple, la similitude dans les images de visage de jumeaux ou frères et sœurs).

2-Les attaque de l'adversaire

Nous classons les attaques de l'adversaire dans les critères principales suivante :

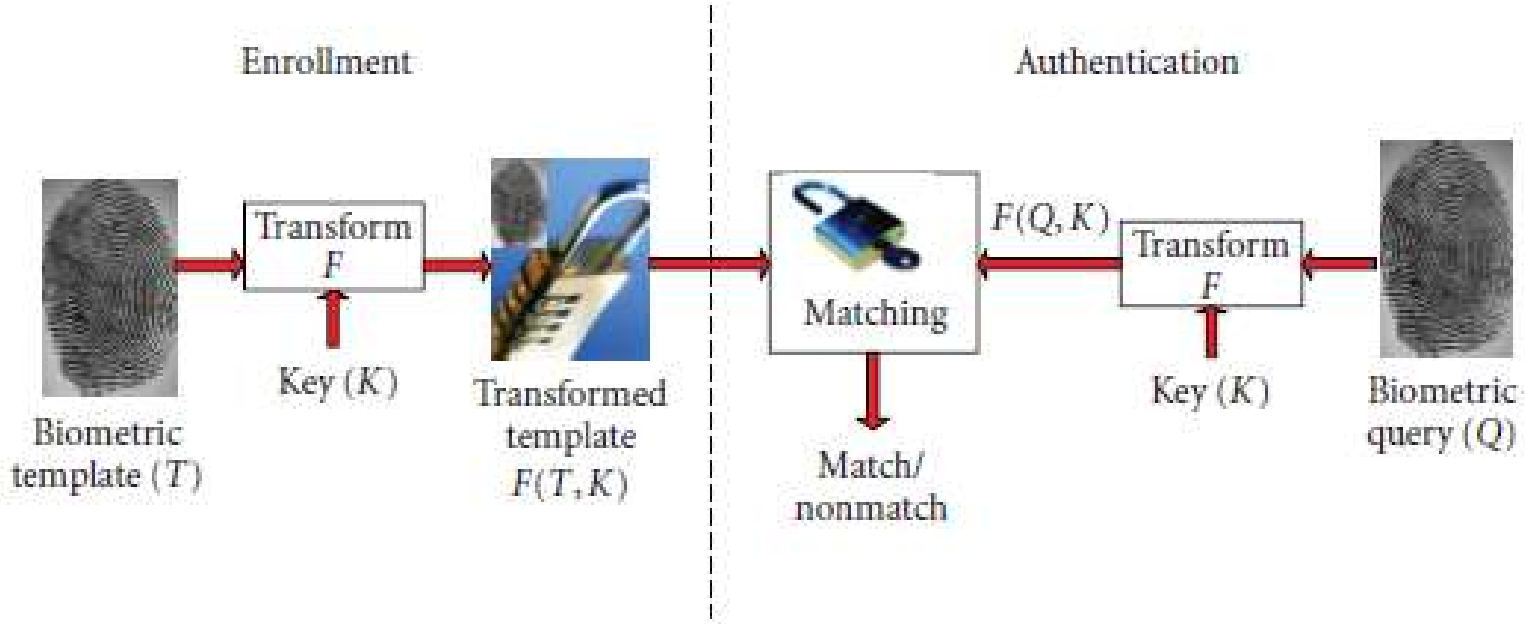
L’attaque d'administration, Infrastructure non sécurisée, Publiquement biométrique, Attaque à l'interface utilisateur, Attaques dans le domaine de l'interaction entre les unités, Les attaques sur des modules logiciels, Les attaques sur le modèle de base

➢ Les Systèmes Cryptographiques Biométriques:

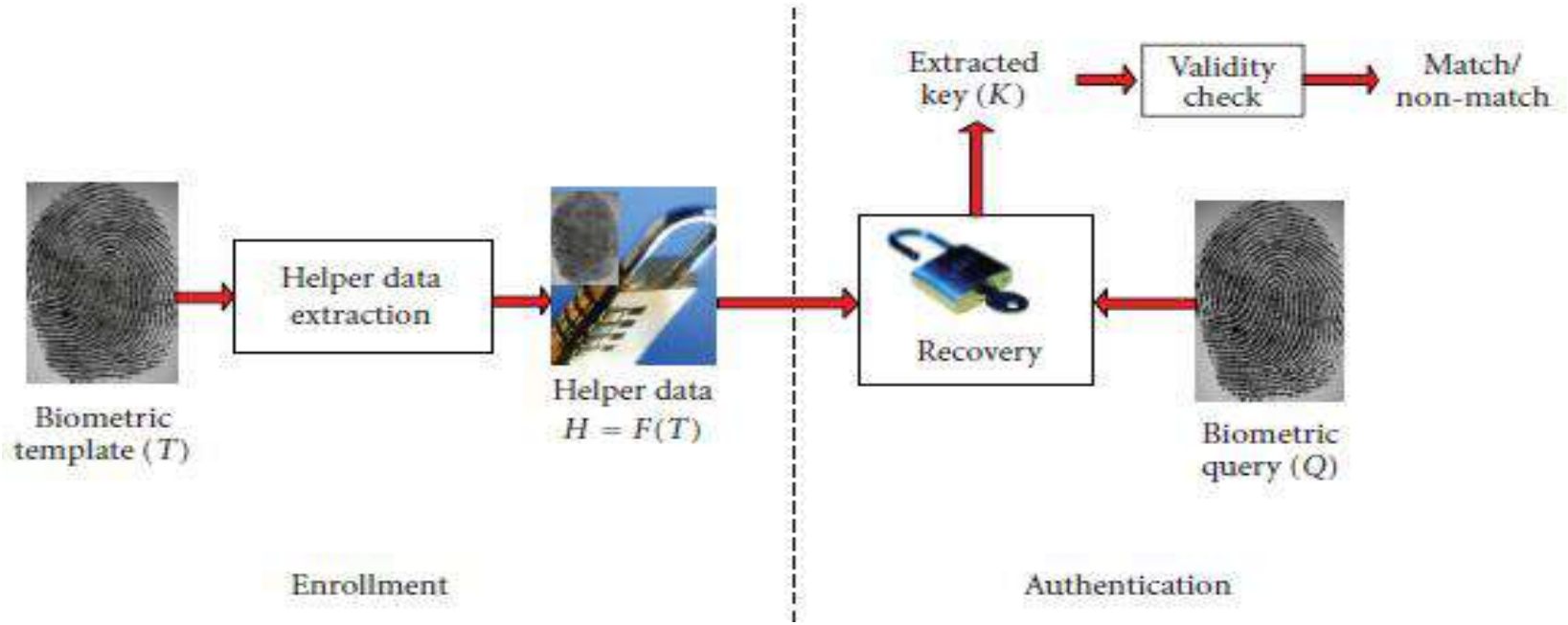
Pour les ordinateurs personnels utilisés, il est probable que les clés sont stockées en clair sur le disque dur de l'utilisateur, ce qui n'est pas sûr.

L’authentification biométrique peut remplacer l'utilisation de mots de passe pour sécuriser la clé.

Lors de l'inscription, un processus de chiffrement biométrique allie l’image biométrique avec une clé numérique pour créer un bloc sécurisé des données, connue sous le nom bioscrypt.



Mécanisme d'authentification lorsque le modèle biométrique est protégé en utilisant une approche de transformation de caractéristique



Mécanisme d'authentification lorsque le modèle biométrique est fixé à l'aide d'un système de chiffrement biométrique et génération de clé.



Chapitre IV
Bases Théoriques

1-Traitement Du Signal De La Parole

➢ Introduction:

Le signal de parole présente des variations entre les individus, ce qui permet de les différencier entre eux.

L'analyse acoustique du signal de parole consiste à extraire l'information pertinente et à réduire au maximum la redondance

➢Extraction des vecteurs acoustiques

Les étapes primordiales pour extraire les vecteurs acoustiques sont :

-Prétraitement

L'objectif du prétraitement est de modifier le signal de parole , pour qu'il soit plus adéquat à l'étape de l'extraction de paramètres.

Les opérations de prétraitement sont :

Préaccentuation, Elimination de silence

-Fenêtrage

Le but du fenêtrage est de découper le signal de parole en petites tranches (chacune de durée 10 à 30 ms).

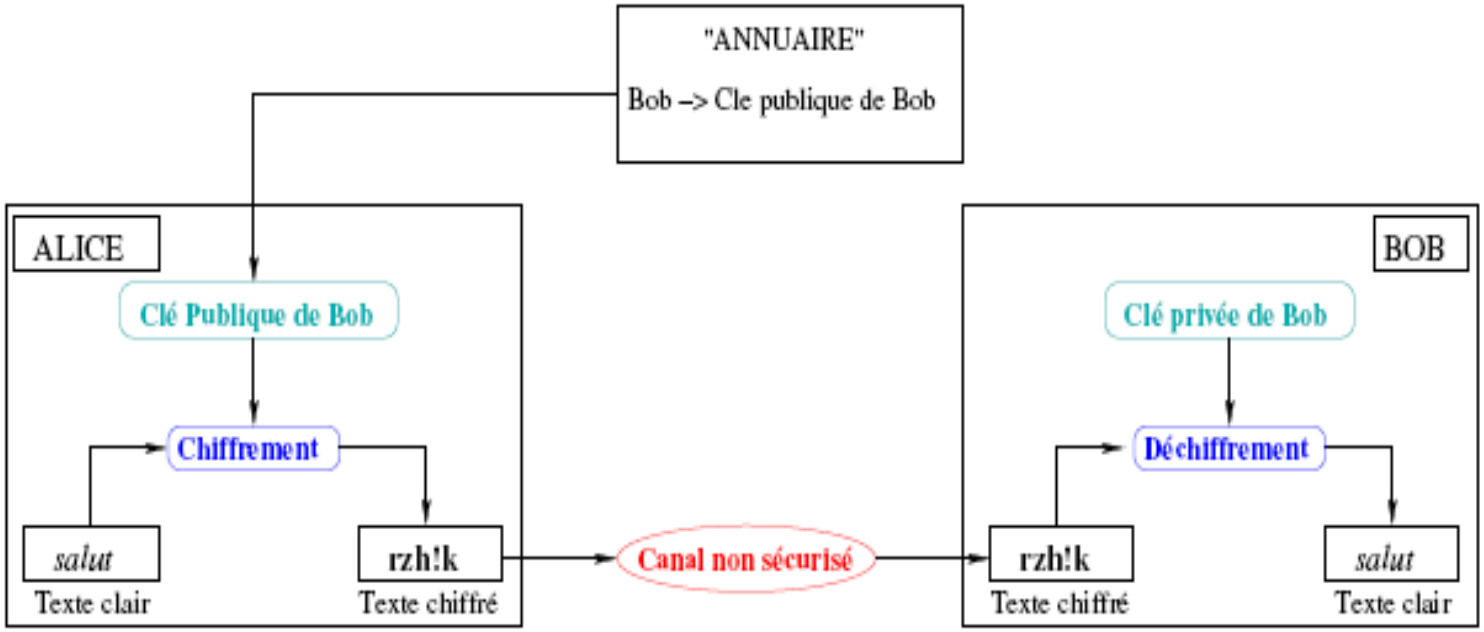
-Extraction des paramètres

- Mel Frequency Cepstral Coefficients (MFCC)
- Linear Prediction Cepstrum Coefficients (LPCC)

2-Génération Des Clés Cryptographique A Partir De La Parole

La cryptographie est la science qui utilise les mathématiques pour le cryptage et le décryptage.On ‘a deux types de la cryptographie

- ✓ Cryptographie a clé privé (symétrique) : deux utilisateurs utilisent même clé.
- ✓ Cryptographie a clé publique (asymétrique) : deux utilisateurs utilisent une clé différente.



Principe du chiffrement à clé publique

Crypto-system de RSA

L'algorithme le plus célèbre d'algorithme à clef publique a été inventé en 1977 par Ron Rivest, Adi Shamir et Len Adleman.

RSA est basé sur la difficulté de factoriser un grand nombre en produit de deux grands facteurs premiers.

❖Génération des clefs

a- p et q, deux grands nombres premiers sont générés au hasard grâce à un algorithme de test de primalité probabiliste, avec n = p x q.

b- Un nombre entier e premier avec [(p-1) x (q-1)] est choisi. Deux nombres sont premiers entre eux s'ils n'ont pas d'autre facteur commun que 1.

c-L'entier d est l'entier de l'intervalle [2, (p-1) x (q-1)] tel que (e x d) soit congrue à 1modulo (p-1) (q-1), c'est-à-dire tel que (e x d)-1 soit un multiple de (p-1) (q-1).

❖Distribution des clefs

Le couple (n, e) constitue la clef publique de Bob.

Le couple (n, d) constitue quant à lui sa clef privée.

❖Chiffrement du message

Pour crypter le message Alice représente le message sous la forme d'un ou plusieurs entiers M compris entre 0 et n-1. Elle calcule : $C = M^e \bmod n$

Grâce à la clef publique (n, e) de Bob et envoie C à Alice.

❖Déchiffrement du message

Bob reçoit C et calcule grâce à sa clef privée :

$$M = C^d mod\, n.$$

.

Il obtient ainsi le message initial M.

Algorithmes de Diffie-Helman (DH)

LES CRIATURES : Whitfield Diffie et Martin Hellman

Procédure

Nous allons vous présenter la procédure étape par étape. Elle permet d'échanger des clés de manière sécurisée. Considérons deux individus, A et B, qui souhaitent s'envoyer un message crypté. Les données et les échanges sont les suivants :

- Tout d'abord A et B se mettent d'accord sur un nombre premier p. Puis ils conviennent d'une racine primitive g.

- A choisi un nombre secret $0 \leq a \leq p-1$
- A envoie la valeur $g^a \bmod p$ à B.
- B choisi un nombre secret $0 \leq b \leq p-1.$
- B envoie la valeur $g^b \bmod p$ à A.
- B procède de manière analogue et obtient la même clé que A :

$$key = (g^a \bmod p)^b \bmod p$$

A et B sont alors en possession chacun de la même clé secrète (key) et peuvent ainsi utiliser un simple algorithme de clé privée.

Algorithmes de chiffre du jet RC4 (Stream cipher algorithmes)

C'est un chiffre principal variable de jet de taille avec des opérations niveau octet. L'algorithme est basé sur l'utilisation des permutations aléatoires.



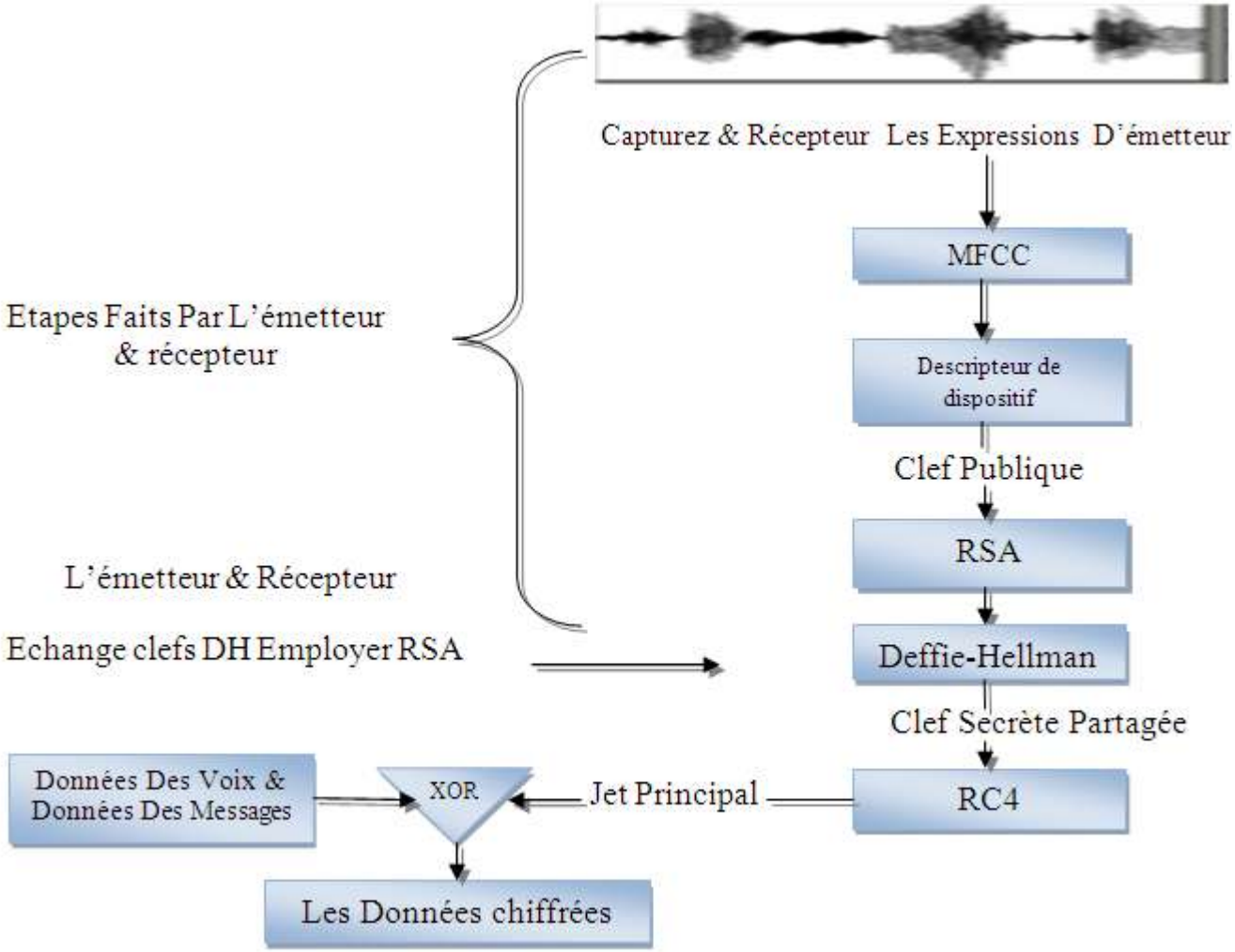
Chapitre V
Implémentation et Evaluation

➢Introduction

Cette section donne une vue sur l’ensemble méthodologie dérivait une clef cryptographique de la parole d'utilisateur.

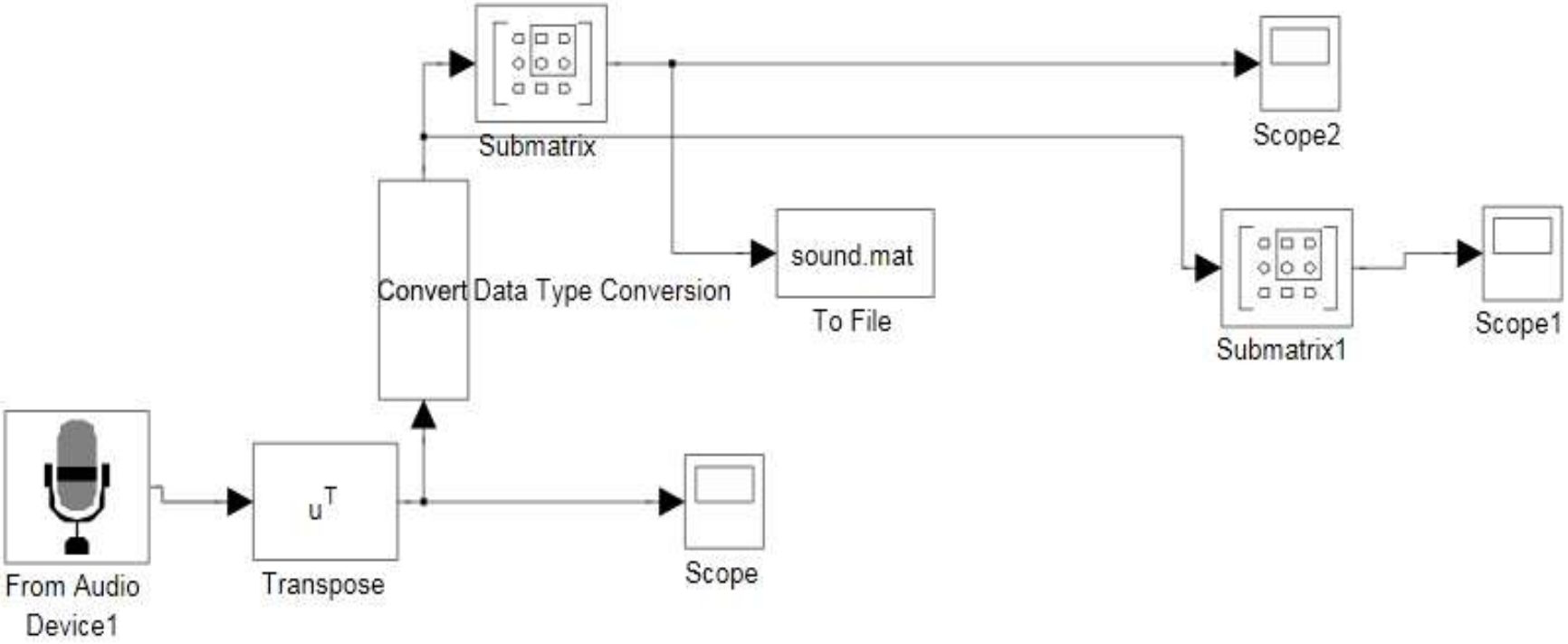
➢Organigramme

L’organigramme dans le schéma suivant détailler les différentes étapes nécessaires a l’écoulement de chiffrage.



L'écoulement de chiffrage.

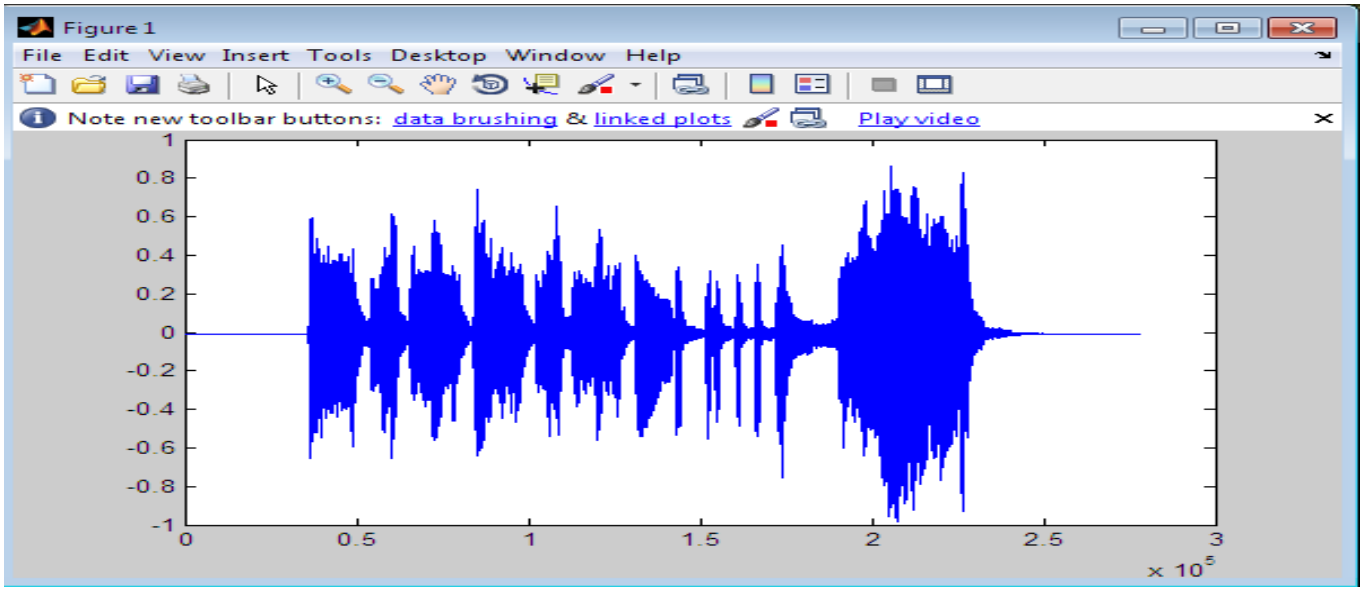
➢Capturez Et Réception Les Expressions D'émetteur



Erenregistrement et affichage du signal de la parole en temps réel

➢MFCC: Mel Frequency Cepstral Coefficients

Les étapes principales pour obtenir MFCC sont: Nous avons utilisez la commende wavread pour analysé l'échantillon ‘’signal \s1.wav’’ On obtient



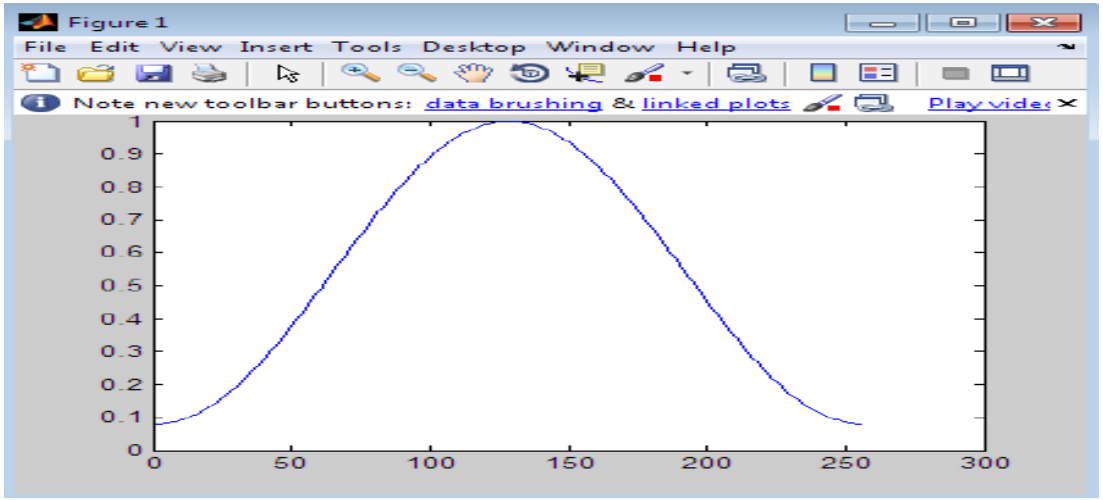
Le signale de la parole.

Structures bloqué

De cette façon nous obtenons 256 * 129 la matrice M.

Fenêtrage

Nous créons la matrice de Hamming et transformons la matrice M dans la nouvelle matrice m2.



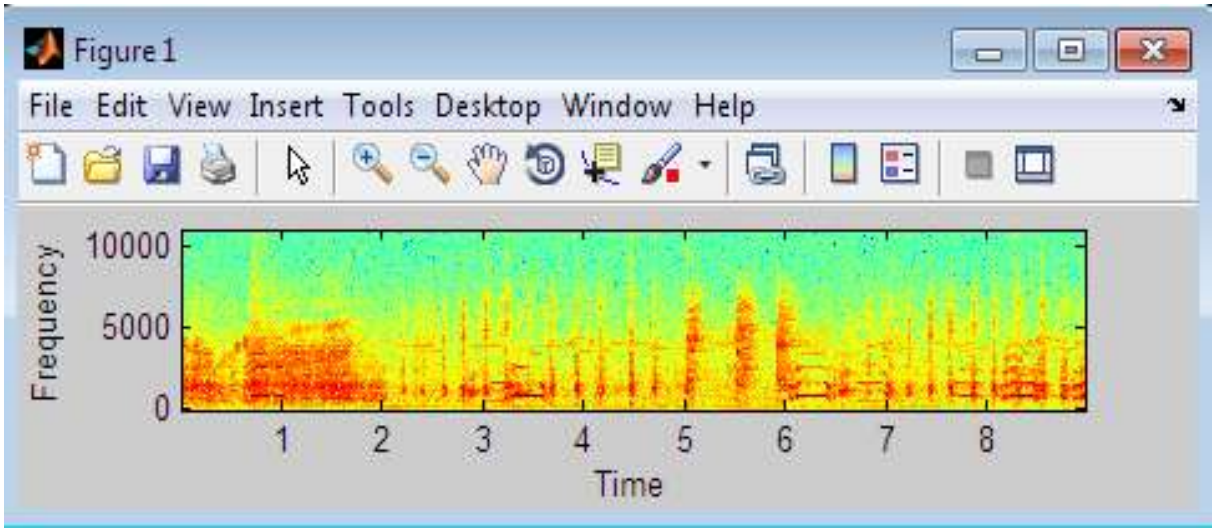
Fenêtre de Hamming.

FFT (Transformer de Fourier Rapide)

Nous créons une nouvelle matrice M3 où les vecteurs de colonne sont les FFTs des vecteurs de colonne du M2.

Spectre de puissance

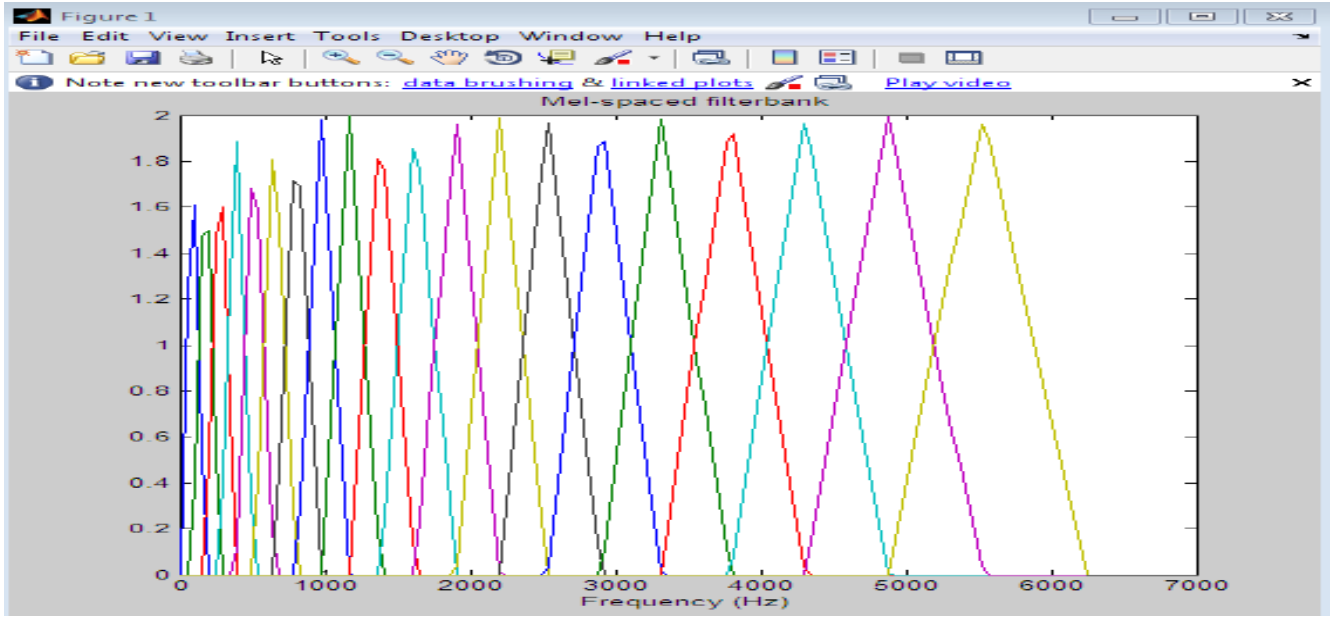
La matrice M3 des colonnes contiennent les structures du signal original, filtrées par le filtre de Hamming et transformé avec le FFT.



Spectre de puissance.

Le niveau le plus élevé de l'énergie est montrés dans le rouge.

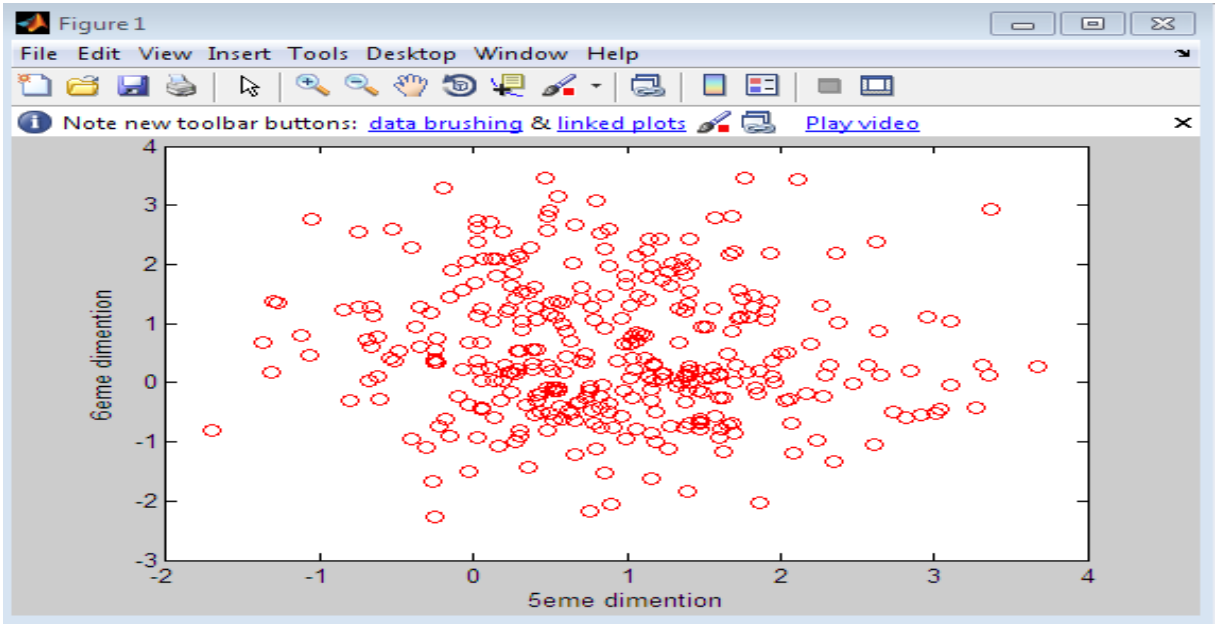
Banc de filtre Mel-Space



Banc de filtre Mel.

Il mesure la zone du spectre de fréquence.

Les vecteurs acoustiques



L'espace acoustique (vecteurs de MFCC).

C’est seulement une partie de terrain bidimensionnelle. Le vecteur réel contient 20 dimensions.

L’algorithme RSA

Cette clef publique est encore employée pour produire de la clef privée correspondante de RSA. Après celle, la clef privée de RSA sera employée comme clef privée de DH.

Dans cette étape nous avons appliqué l’algorithme RSA sur le résultat obtenu à partir le programme de (MFCC).

>>

ans =

1283027416455272001930979395772965892901225571903717178495923861553346710278872893273101335921198086374058663294864532573116367753075397425087827484019585038098869657383301275957739684601817776519870068183140511287927032644714492892516653246518238493136246207822389003038673027766029740180748355020452432950 3

L’algorithme de Diffie-Hellman

préciser un nombre premier = 23

Entrer la base = 5

Choisir un nombre secret d A = 6

Choisir un nombre secret de B = 15

Voila la clef secrète est le : 2

La clef publique correspondante de DH sera calculée et échangée d'une façon bloquée. La clef publique de DH sera chiffrée en utilisant l'algorithme de RSA et transférée à l'autre côté.


Conclusion Générale

Conclusion Générale:

Ce travaille discuté un domaine très avancé dans la sécurisation des données biométrique a partir des clés cryptographiques, et étudie le développement d'un système combinant l'extraction de dispositif audio et la cryptographie principal de public, la qualité des résultats et d'elle est applicable à n'importe quel mot parlé.

dans ce travaille, afin d'effectuer l'authentification, MFCC a été mis en application pour authentifier d'autres en produisant d'une clef de la voix de l'utilisateur.

RSA et DH sont employés pour produire de la clef partagée secrète, cette clef est encore utilisée comme une clef RC4.

De façon générale, les résultats pour ce projet sont comme suit:

(i) L'authentification principale est faite implicitement et employer automatiquement l'extraction de dispositif de MFCC.

(ii) La clef produite est bloquée contre l'homme -dedans - attaque moyenne.

(iii) le protocole est base sur RSA, DH et le crypto-système RC4.

(iv) L’utilisation de pseudo-nombres aléatoires pour les clefs privées et les clefs de session. À l'aide également du générateur de nombre pseudo-aléatoire pour les jets principaux, ces clefs sont non déterministes.

وما توفيقي إلا بالله