République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Dr YAHIA FARES DE MEDEA

Faculté des sciences et de la technologie

Département du génie électrique et de l'informatique

Projet de fin d'études pour l'obtention du diplôme de Master en génie électrique

Option : Systèmes de Télécommunication

THEME

RECONNAISSANCE BIOMETRIQUE DU VISAGE PAR L'ANALYSE EN COMPOSANTES PRINCIPALES ET COMPOSANTES INDEPENDANTES

Proposé et dirigé par :
Dr. Mohamed SOLTANE

Présenté par:

MAHDID Samir

KHELFI Mohamed

Promotion : 2012/2013

Abréviations

TVA : taux de vrai acceptés

ROC: Receiver Operation Characteristic.

ICA: Analyse en Composantes Indépendantes.

PCA : Analyse en Composantes Principales

ORL: Olliviti Research Laboratory

EER: Equal Error Rate.

FAR: False Acceptance Rate

FRR: False Rejection Rate

MFCC Mel Frequency Cepstral Coefficients

MMC Modèles de Markov Cachés

DTW Dynamic Time Warping

WER Word Error Rate

WRR Word Recognition Rate

CUED Cambridge University Engineering Departement

HMM Hidden Markov Model

ADN Acide Désoxyribonucléique

Liste des Tableaux

Tableau .1.1 Les systèmes biométriques suppriment les risques.……..…….....…05

Tableau .1.2 : Etat de l'art des taux d'erreur:…….……12

Tableau .1.2 : Comparatif ……...……...……..…….…….20

Tableau.2.1 : Avantage et Inconvénient de la reconnaissance du visage……...…….33

Tableau.4.1 : Roc avec seuil =0.1….....……...……..…..…...…...66

Tableau.4.2 ROC avec seuil =0.29……..……...66

Tableau.4.3: Roc avec seuil=0.7…….….67

Tableau 4.4. Roc avec seuil=0.0013…….……...……68

Tableau 4.5. Roc avec seuil=0.0017….…….……69

Tableau 4.6. Roc avec seuil=60…….…70

Tableau 4.7. Roc avec seuil ==70……71

Figure 3.6 : Image moyenne…….……45
Figure 3.5 : Les 10 premiers vecteurs propres…….……44
Figure 3.6 : Image moyenne……45
Figure 3.7 : La représentation d' ACI = (hl, b2,…… bn) ……...……47
Figure 3.8 : Les deux architectures d' ACI ……..……...50
Figure 3.9 : Le modèle de synthèse d'image de l'architecture 1 d'ACI…….……..…….51
Figure 3.10 : Le modèle de système d'image de l'architecture 2 d'ACI…..…….……...52
Figure .3.11 : La représentation factorielle d'ACI = (u1,u2,….,un)……...….53
Figure.4.1 : Exemples d'images de deux personnes provenant de la base de données du laboratoire ORL de l'université de Cambridge……...……..55
Figure. 4.2- L 'ensemble des images d'apprentissage de la base ORL utilisées pour le calcul dutaux de la bonne identification…….……56
Figure. **4.3**- L 'ensemble des images de Test de la base OR_L utilisées pour le calcul du taux dela bonne identification…….56
Figure4.4 : La base de données…….……...……57
Figure .4.5 Normalisation de la base de données ORL……58
Figure .4.6. Affichage de la base de donnée ORL……..…….59
Figure 4.7 l'image moyenne et les images normalisées……...……...60
Figure 4.8 :l'image test et l'image construite par le système……...60
Figure 4.9 : Personne identifie……...……..61
Figure4.10 : Résultat d'identification de système……..……61
Figure 4.11 :l'image test et l'image construite par le système……61
Figure 4.12 : Personne non identifie……62
Figure4.13: Résultat d'identification rejetée FR avec un seul égal à 0.16……...…62
Figure 4.14 : Comparaison entre le visage d'entré et le visage de la base de donné……..….63
Figure4.15: Résultat authentique du système de vérification……..64
Figure 4.16 : Comparaison entre le visage d'entré et le visage de la base de donné……...64
Figure 4.17:Résultat du système de vérification…...……...65
Figure.4.18.ACI Arch I courbe ROC Avec seuil 0.0013……68
Figure.4.19.ACI Arch I courbe ROC Avec seuil 0.0017……69
Figure.4.20.ACI Arch II courbe ROC Avec seuil 60……..70
Figure.4.21.ACI Arch II courbe ROC Avec seuil 70……..71

Liste des figures

Figure. 1.1 : Différentes modalités biométriques…….04
Figure .1.2: Module d'apprentissage……...……06
Figure.1.3 : Illustration du FRR et du FAR.. ……..……08
Figure 1.4 Illustration des Authentique…….…...……...…09
Figure 1.5 Illustration des imposteur…….…...……...…10
Figure 1.6 Superposition des deux distributions ……...…….…...…….……10
Figure 1.7 Courbe Roc……..……...…….…….…. 12
Figure 1.8 : La Classification De La Biométrie……...13
Figure 1.9: Empreinte digitale acquise par un capteur optique ……..……..…..…….14
Figure 1.10: Reconnaissance de visage ……...……..….14
Figure 1.11: Image d'iris …….…….……...15
Figure 1.12: Spectre d'un signal voix……..……...……..……..... 15
Figure 1.13 : Signature ……..……..……....15
Figure 1.14 : Parts de marché des différentes méthodes biométriques ……...……. 16
Figure 1.15 : Schéma de fonctionnement d'un système biométrique ……..…..……...…….17
Figure. 2.1 . Scores de compatibilité pour différentes technologies biométriques dans un système MRTD……....23
Figure 2.1 : Détecter le visage……..……24
Figure 2.2 : Détecter points clés……..…..……...…….……24
Figure 2.2: Schéma d'Identification du visage…….…….……..……25
Figure 2.3: Schéma de vérification du visage…….……..……...……..26
Figure 2.5:Principe de fonctionnement de base d'un système de reconnaissance faciale…...27
Figure 2.6 : Schéma général d'un système de reconnaissance des visages……..……...29
Figure 2.7 : Principales techniques de reconnaissance…….…..……...…..31
Figure 2.8: Distances entre points caractéristiques…….……32
Figure 2.9 :L'utilisation de la région entière du visage connue entrée aux méthodes globales…….……32
Figure 2.10 : Méthodes hybrides …….……33
Figure 3.1 : Principe général d'un système de reconnaissance de visage……..……...……..35
Figure.3.2.Valeur propres en fonction de α……...…….…..……..40
Figure 3.3 : Base de données avec des images de références...…….……..42
Figure3.4 : Exemple de visage moyenne…….…43

IV.1. introduction.……..……..54
IV.2. Qu'est-ce que c'est Matlab.……..…….……..54
IV.3. Pourquoi utiliser Matlab ……...…….……54
IV.4. Base de données …….…….……55
IV.5.Algorithme ACP……..……..…….……..57
IV.5. 1.Phase d'enrôlement……...……57
IV.6. Test d'identification ……..……...……...60
IV.7. Test de vérification ..……...……62
IV.8.Performance du système ……...……...65
IV.8.1. Expérience1……..……66
IV.8.2.Expérience2…..……66
IV.8.3.Expérience 3……...……67
IV.9.L'algorithme ICA……..……...67
IV.9.1.ICA I…….…..……67
IV.9.2.ICA II……..……..67
IV.10.Performance du system…..……68
IV.10.1.Expérience 1 : pour L'ACI 1 avec une seuil = 0.0013…..……..68
IV.10.2.Expériences 2 : pour L'ACI 1 avec une seuil = 0.0017…..……69
IV.10.3.Expériences 1 : pour L'ACI 2 avec une seuil =60……..……70
IV.10.4Expériences 2 : pour L'ACI 2 avec une seuil =70……..……71
IV.11.Conclusion.……..72

CONCLUSION GENERALE

Conclusion …….……..73

Bibliographie

II.6.2 Changements d'éclairage……..……...28
II.6.3 Expressions faciales……..……...…28
II.6.4 Occultations partielles……...…….……29
II.7. Les classes des techniques de reconnaissance de visages ……..…..……29
II.8.Les méthodes de reconnaissance faciales ……..……30
II.8.1Méthodes locales…….…….30
II.8.2 Méthodes globales ……...…...31
II.8.3 Méthodes hybrides……...……31
II.9 Avantage et Inconvénient ……...……..…….……33
Conclusion :……...…….…….….34

CHAPITRE III

BASE THEORIQUE

III.1. Introduction……...…….…..….35
III.2.-Utilisation de l'ACP pour la reconnaissance des visages……...…….……36
III.3.Étapes de l'analyse en composantes principales……...……37
III.3.1.Matrice des corrélations……...……..…37
III.3.2.Composantes principales……...……..…38
III 3.3.Variance totale expliquée et communalité…….…….....……..…39
III 3.4.Nombre de composantes principales à retenir…….……..……40
III .4. Analyse par eigenfaces……...……...41
III .4 .1.Les différentes étapes……...……..….42
III.5.Conclusion……..…….……..…..….46
III.6 .Analyse en Composantes Indépendantes……...…….……47
III.6.1. Application de l'ACI : hypothèses et cohérence…….…….…….……49
III.7.Les architectures d'ACI……..…….……49
III.5.1.1 Architecture 1 ……...…….50
III.5.1.2 Architecture 2 ……...…….…...52
III.6.Conclusion……..……..53

CHAPITRE IV

IMPLEMENTATION ET RESULTAS

I.9. Caractérisation d'un système biométrique ……..…….17
I.9.1 Le module de capture……..…...…….……..…….…….17
I.9.2 Le module d'extraction.…….……..…..……..…….…...17
I.9.3.Le module de correspondance.……..…..…….……17
I.9.4. Le module de décision.…….……....……..…….……17

I.10. applications ……..……..…….…….……..……18
I.10.1. Contrôle d'accès..…..……..……..……...…….18
I.10.1.1 Contrôle d'accès physique….……...…….18
I.10.1.2. Contrôle d'accès virtuel.…..……...…..…….……18
I.10.2. Répression..…….……...……..…….……19
I.10.3. Personnalisation.…….…….……...……...…….……19
I.11 Comparatif.…….……20
I.12 Conclusion..…….....…….……..……21

CHAPITRE II

LA RECONNAISSANCE DU VISAGE

II.1. Introduction.…..…….……..……..……22
II.2. Historique…….……...…….……..……22
II.3 La place de la reconnaissance du visage parmi les autres techniques biométriques.…….22
II.4 La Reconnaissance de Visage……...……24
II.4.1 Prétraitements..……...……..…….……...…… 24
II.4.2 Identification..……..……...…..……..…….25
II.4.3 Vérification ……...…….……..……25
II.5 Biométrie du visage.…….……..……..……26
II.5.1.Capture du visage.……..…….……...…26
II.5.2.Détection.……...…….……26
II.5.3.Normalisation.…….……...…….……....27
II.5.4.Calcul de score……..……...…….……..…27
II.5.5.Décision ……..…….……..…….....27
II.6. Principales difficultés de la reconnaissance de visage.…….……..…..28
II.6.1 Variations de la pose…….…….……....28

Table des Matières

Remerciements**……..……..*i***
Dédicace**…….*ii***
Résumé **…….……..……..*iv***
Table des Matières**……...…….....*v***
Liste des Figures **……..…*ix***
Liste des Tableaux**……...…….……*xi***
Abréviations **…….……....…*xii***

I.INTRODUCTION ET MOTIVATION ……....……01

CHAPITRE I

LES SYSTEMES BIOMETRIQUE

I.1Introduction…….……..……...……..……..…..…..…….03

I.2. Différentes modalités biométriques…….…….……..…04

I.3.L'utilisation d'un system biométrique.....05

I.4. Les systèmes biométriques suppriment les risques……..…….……05

I.5. architecture…….…….....06

I.5.1. Module d'apprentissage ……..……..…….……...……..……06

I.5.2. Module de reconnaissance ……..…….07

I.5.3. Module d'adaptation ……...…….……..……07

I.6. Mesure de la performance d'un système biométrique **:** …..…….…… 08

I.6.1. Comptabilité des erreurs: FAR, FRR ……..……09

I.6.2. Les deux taux sont liés ……...…….09

I.7. Techniques biométriques …….…….13

I.7.1. Empreintes digitales …...…….14

I.7.2. Visage ……..……..…..……...14

I.7.3. Iris …..……...…..……....14

I.7.4. Voix …..……..…..……..14

I.7.5. Signature …….…….....……15

I.7.6 Les parts de marché par technologie…..……..……...……..15

I.8. Système biométrique ……...……..16

I.8.1.Enrôlement……..……16

I.8.2.Vérification ……..……...……16

I.8.3. Identification……....…….……16

ملخص:

هدا العمل ينطوي على تطبيق القياسات الحيوية للتعرف على وجوه الأشخاص باستخدام نهج شامل يسمى تحليل المكونات الرئيسية (PCA).يستخدم في البرمجة لغة MATLAB .

عملنا كان على قاعدة البيانات ORL التي تحتوي على 40 فرد، لكل فرد 10 وجوه مختلفة، يتم تطبيق التعلم على 6 وجوه لكل شخص 240 وجه والوجوه الأخرى 160 وجه للاختبار.

كلمات البحث:القياسات الحيوية،التعرف على الوجه ACI, ACP.

Résumé

Ce travail consiste à appliquer la biométrie de visage pour la reconnaissance des personnes, utilisent une méthode globale qui s'appelle l'analyse en composants principales (implémenté par le langage de programmation MATLAB.

On a travaillé sur la base de données ORL qui contient 40 personnes, chaque personne à 10 visages différents, l'apprentissage est appliqué sur 6 visages pour chaque personne (240visages) et les autres visages (160 visages) pour le test.

Mots clés : biométrie, reconnaissance de visages. ACP, ACI.

Abstract

This work is to apply biometrics for face recognition people use a holistic approach called principal components analysis (PCA) is used in our application programming language MATLAB.

We worked on the ORL database which contains 40 individuals, each at 10 different faces, learning is applied on 6 faces for each person (240 faces) and other faces (160 faces) for the test.

Key words:biometrics, recognition of faces.PCA, ICA.

Dédicaces

J'ai l'honneur de dédier ce mémoire

À mes très chers parents qui étaient présents pour moi

Durant toute ma vie.

A ma famille,

A mes amis,

A tous ceux qui me sont chers
A toute la promotion 2ème années Master L.M.D option

Télécommunication



KHELFI Mohamed

Dédicaces

A mon cher père,

Et ma chère mère,

Pour l'éducation et le grand amour dont ils m'ont entouré depuis ma naissance. Et pour leurs patiences et leurs sacrifices.

A mes chers frères et mes adorables sœurs,

A tous mes proches ;

A tous mes ami(e)s;

A tous ceux que j'aime.

A toute la promotion 2ème années Master

L.M.D option Télécommunication.

MAHDID Samir

Remerciements

Tout d'abord, louange à Allah qui m'a guidé sur le droit chemin tout au long du travail et m'a inspiré les bons pas et les justes reflexes. Sans sa miséricorde

Nous profitons de cette occasion pour remercier tous ceux qui nous ont aidés à réaliser ce projet dans les meilleures conditions.

Nous tenons à exprimer nos vifs remerciements en premier lieu à notre encadreur, ***DR.SOLTANE M*** *Pour l'aide déterminante qu'il nous a accordée et pour l'intérêt qu'il a porté à notre projet. Qu'il trouve ici l'expression de nos profonds respects.*

Je tiens par la même occasion à remercier mes enseignants qui ont pleinement contribué à ma formation.

Je remercie les membres du jury pour l'honneur qu'ils me font en acceptant de juger ce travail.

KHELFI Mohamed & MAHDID Samir.

paramètres maîtrisés par le système. Dans un environnement non contrôlé, une série de prétraitements sont souvent nécessaires avant de faire la reconnaissance à proprement parler. Il faut tout d'abord détecter la présence ou l'absence de visage dans l'image. Le visage doit ensuite être segmenté. [3].

Notre mémoire est organisée en cinq chapitres, de la manière suivant :

Dans le chapitre 1 nous présentons une description générale des déférents systèmes biométrique et comment mesuré les performances d'un système biométrique.

Dans le chapitre 2 nous détaillons la reconnaissance par visage, les étapes et les méthodes de reconnaissance.

Dans le chapitre 3 nous étudions l'approche globales de la reconnaissance de visage et en particularité l'algorithme de l'analyse de composants principales.

Dans le chapitre 4 nous présentons une application de reconnaissance de visage utilisons la méthode d'analyse des composants principales et l'analyse des composants indépendant, faire des tests de vérification et d'identification et voire des expériences montre l'influence du paramètre seuil sur le résultat de reconnaissance.

Introduction et Motivation

La sécurité des personnes, des biens ou des informations est l'une des préoccupations majeures de nos sociétés actuelles. L'authentification de l'identité des personnes permet de l'assurer. Ainsi, une personne désirant traverser une frontière sensible se verra systématiquement demander de décliner et prouver son identité à l'aide de son passeport par exemple; une autre voulant accéder à un service bancaire sur l'Internet devra la plupart du temps saisir un nom d'utilisateur et le mot de passe correspondant. La grande faiblesse des moyens actuels de vérification d'identité apparaît clairement ici: l'identité d'une personne est directement liée à ce qu'elle possède (un passeport, un badge magnétique, etc.) et/ou ce qu'elle sait (un code PIN de carte bancaire, un mot de passe, etc.). Or, un badge peut être volé, un mot de passe deviné ou cassé par force algorithmique brute: ceci menant à l'usurpation d'identité [1].

La biométrie trouve ses origines dans des procédés de reconnaissance anthropométrique, le plus ancien étant l'analyse des empreintes digitales. L'empreinte du pouce servait déjà de signature lors d'échanges commerciaux à Babylone dans l'Antiquité et en Chine au 7ème siècle. Dans une époque beaucoup plus proche, au 19ème siècle, Alphonse Bertillon, grand criminologiste français, invente une méthode scientifique appelée "anthropologie judiciaire" permettant l'identification de malfrats d'après leurs mesures physiologiques. De nos jours, la puissance de calcul grandissante des ordinateurs peut être mise à contribution pour reconnaître des individus, grâce à des appareils couplés à des programmes informatiques complexes [2].

La reconnaissance faciale fait partie des techniques biométriques. On remarque que dans la vie quotidienne chacun de nous identifie tout au long des journées différentes visages. Ainsi lorsque nous rencontrons une personne, notre cerveau va chercher dans notre mémoire et vérifier si cette personne est répertoriée ou non. La difficulté de la reconnaissance de visage par ordinateur varie énormément suivant que les conditions d'acquisition, dans un environnement contrôlé, des paramètres tels que l'arrière plan, la direction et l'intensité des sources lumineuses, l'angle de la prise de vue, la distance de la caméra au sujet sont des

I.1. Introduction:

Savoir déterminer de manière à la fois efficace et exacte l'identité d'un individu est devenu un problème critique dans notre société.

En effet, bien que nous ne nous en rendions pas toujours compte, notre identité est vérifiée quotidiennement par de multiples organisations : lorsque nous utilisons notre carte bancaire, lorsque nous accédons à notre lieu de travail, lorsque nous nous connectons à un réseau informatique, etc.

Il existe traditionnellement deux manières d'identifier un individu, la première méthode est basée sur une connaissance (knowledge-based), cette connaissance correspond par exemple au mot de passe utilisé au démarrage d'une session Unix ou au code qui permet d'activer un téléphone portable. La seconde méthode est basée sur une possession (token-based). Il peut s'agir d'une pièce d'identité, une clef, un badge, etc. Ces deux modes d'identification peuvent être utilisés de manière complémentaire afin d'obtenir une sécurité accrue comme pour la carte bleue. Cependant, elles ont leurs faiblesses respectives. Dans le premier cas, le mot de passe peut être oublié par son utilisateur ou bien deviné par une autre personne. On estime ainsi qu'une personne sur quatre écrit directement sur sa carte bleue son code secret afin de ne pas l'oublier, dans le second cas, le badge (ou la pièce d'identité ou la clef) peut être perdu ou volé [2].

Nous décrivons maintenant les propriétés souhaitables d'une caractéristique biométrique cette caractéristique doit être universelle, c'est-à-dire que toutes les personnes de la population à identifier doivent la posséder, elle doit être à la fois facilement et quantitativement mesurable, elle doit être unique, c'est-à-dire que deux personnes ne peuvent posséder exactement la même caractéristique, elle doit être permanente, ce qui signifie qu'elle ne doit pas varier au cours du temps, elle doit être performante, c'est-à-dire que l'identification doit être précise et rapide, elle doit être bien acceptée par les utilisateurs du système. Enfin elle doit être impossible à dupliquer par un imposteur.

I.2 Différentes modalités biométriques :

Le terme biométrie regroupe en fait ce que l'on appelle des modalités biométriques, contrairement à ce que l'on possède et que l'on peut donc perdre (une clé) ou ce que l'on sait et que l'on peut donc oublier (un mot de passe), les modalités biométriques représentent ce que l'on est et permettent de prouver notre identité.

Pour que des caractéristiques collectées puissent être qualifiées de modalités biométriques, elles doivent être :

– universelles (exister chez tous les individus),

– uniques (permettre de différencier un individu par rapport à un autre),

– permanentes (autoriser l'évolution dans le temps),

– enregistrables (collecter les caractéristiques d'un individu avec son accord),

– mesurables (autoriser une comparaison future).

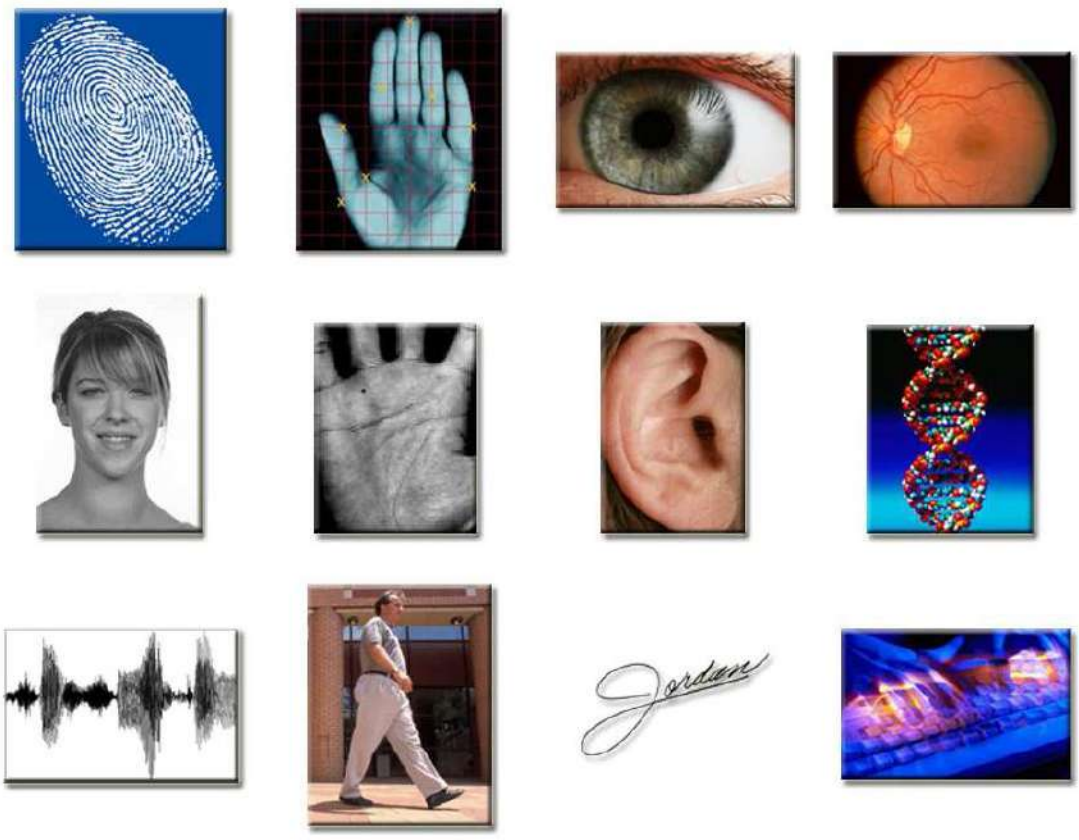


Figure. 1.1 : Différentes modalités biométriques.

L'empreinte digitale, la géométrie de la main, l'iris, la rétine, le visage, l'empreinte palmaire, la géométrie de l'oreille, l'ADN, la voix, la démarche, la signature ou encore la dynamique de frappe au clavier sont autant de modalités biométriques différentes.

I.3 L'utilisation d'un system biométrique :

La biométrique est un domaine émergeant où la technologie améliore notre capacité à identifier une personne. La protection des consommateurs contre la fraude ou le vol est un des buts de la biométrie. L'avantage de l'identification biométrique est que chaque individu a ses propres caractéristiques physiques qui ne peuvent être changées, perdues ou volées. La méthode d'identification biométrique peut aussi être utilisée en complément ou remplacement de mots de passe.

Plusieurs raisons peuvent motiver l'usage de la biométrie

- ***Une haute sécurité*** - En l'associant à d'autres technologies comme le cryptage, la carte à puce...
- ***Confort*** - En remplaçant juste le mot de passe, exemple pour l'ouverture d'un système d'exploitation, la biométrie permet de respecter les règles de base de la sécurité (ne pas inscrire son mot de passe à coté du PC, ne pas désactiver l'écran de veille pour éviter des saisies de mots de passe fréquentes), et quand ces règles sont respectées, la biométrie évite aux administrateurs de réseaux d'avoir à répondre aux nombreux appels pour perte de mot de passe (que l'on donne parfois au téléphone, donc sans sécurité).
- ***Sécurité / Psychologie*** - Dans certains cas, particulièrement pour le commerce électronique, l'usager n'a pas confiance. Il est important pour les acteurs de ce marché de convaincre le consommateur de faire des transactions. Un moyen d'authentification connu comme les empreintes digitales pourrait faire changer le comportement des consommateurs.

I.4. - Les systèmes biométriques suppriment les risques :

Ce tableau représente l'avantage de la biométrie par rapport d'autres systèmes sécuritaire.

	Copie	Vol	Oubli	Perte
Clé	X	X	X	X
Badge	-	X	X	X
Code	X	-	X	-
Biométrie	-	-	-	-

Tableau .1.1 Les systèmes biométriques suppriment les risques

I.5. Architecture :

Il existe toujours au moins deux modules dans un système biométrique : le module d'apprentissage et celui de reconnaissance [06], Le troisième module (facultatif) est le module d'adaptation. Pendant l'apprentissage, le système va acquérir une ou plusieurs mesures biométriques qui serviront à construire un modèle de l'individu, ce modèle de référence servira de point de comparaison lors de la reconnaissance, le modèle pourra être réévalué après chaque utilisation grâce au module d'adaptation.

I.5.1. Module d'apprentissage :

Au cours de l'apprentissage, la caractéristique biométrique est tout d'abord mesurée grâce à un capteur, on parle d'acquisition ou de capture, en général cette capture n'est pas directement stockée et des transformations lui sont appliquées. En effet, le signal contient de l'information inutile à la reconnaissance et seuls les paramètres pertinents sont extraits. Le modèle est une représentation compacte du signal qui permet de faciliter la phase de reconnaissance, mais aussi de diminuer la quantité de données à stocker. Il est à noter que la qualité du capteur peut grandement influencer les performances du système, meilleure est la qualité du système d'acquisition, moins il y aura de prétraitements à effectuer pour extraire les paramètres du signal.

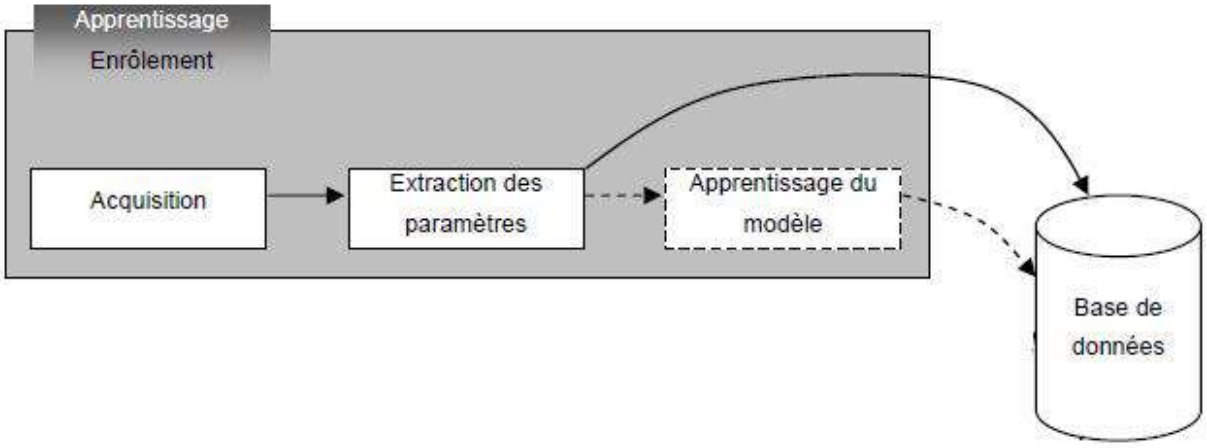


Figure 1.2: Module d'apprentissage

Cependant, les capteurs de qualité sont en général coûteux et leur utilisation est donc limitée à des applications de haute sécurité pour un public restreint.

Le modèle peut être stocké dans une base de données comme représenté sur la (**figure1.2**) ou sur une carte de type carte à puce.

I.5.2 Module de reconnaissance :

Au cours de la reconnaissance, la caractéristique biométrique est mesurée et un ensemble des paramètres est extrait comme lors de l'apprentissage, le capteur utilisé doit avoir des propriétés aussi proches que possibles du capteur utilisé durant la phase d'apprentissage.

Si les deux capteurs ont des propriétés trop différentes, il faudra en général appliquer une série de prétraitements supplémentaires pour limiter la dégradation des performances.

La suite de la reconnaissance sera différente suivant le mode opératoire du système : identification ou vérification, en mode identification, le système doit deviner l'identité de la personne, Il répond donc à une question de type : « Qui suis je ? ». Dans ce mode, le système compare le signal mesuré avec les différents modèles contenus dans la base de données (problème de type 1 : n), en général, lorsque l'on parle d'identification, on suppose que le problème est fermé, c'est-à-dire que toute personne qui utilise le système possède un modèle dans la base de données. En mode vérification, le système doit répondre à une question de type : « Suis-je bien la personne que je prétends être ? ».

L'utilisateur propose une identité au système et le système doit vérifier que l'identité de l'individu est bien celle proposée. Il suffit donc de comparer le signal avec un seul des modèles présents dans la base de données (problème de type 1 : 1). En mode vérification, on parle de problème ouvert puisque l'on suppose qu'un individu qui n'a pas de modèle dans la base de données (imposteur) peut chercher à être reconnu.

Identification et vérification sont donc deux problèmes différents.

L'identification peut-être une tâche redoutable lorsque la base de données contient des milliers, voire des millions d'identités, tout particulièrement lorsqu'il existe des contraintes de type « temps réel » sur le système. Ces difficultés sont analogues à celles que connaissent par exemple les systèmes d'indexation de documents multimédia.

I.5.3Module d'adaptation :

Pendant la phase d'apprentissage, le système biométrique ne capture souvent que quelques instances d'un même attribut afin de limiter la gêne pour l'utilisateur. Il est donc difficile de construire un modèle assez général capable de décrire toutes les variations possibles de cet attribut. De plus, les caractéristiques de cette biométrie ainsi que ses conditions d'acquiition peuvent varier. L'adaptation est donc nécessaire pour maintenir voire amélioré la performance d'un système après utilisation.

L'adaptation peut se faire en mode supervisé ou non-supervisé mais le second mode est de loin le plus utile en pratique. Si un utilisateur est identifié par le module de reconnaissance, les paramètres extraits du signal serviront alors à ré-estimer son modèle. En général, le taux d'adaptation dépend du degré de confiance du module de reconnaissance dans l'identité de l'utilisateur.

Bien entendu, l'adaptation non-supervisée peut poser problème en cas d'erreurs du module de reconnaissance, l'adaptation est quasi indispensable pour les caractéristiques non permanentes comme la voix [11] [09].

I.6. Mesure de la performance d'un système biométrique :

Le but fondamental de tout système biométrique opérant au niveau score, est de pouvoir séparer au maximum les distributions de score des imposteurs et des authentiques (Figure.2.3). En minimisant la zone de recouvrement entre ces deux distributions, on améliore la performance globale du système en augmentant le taux de reconnaissance.

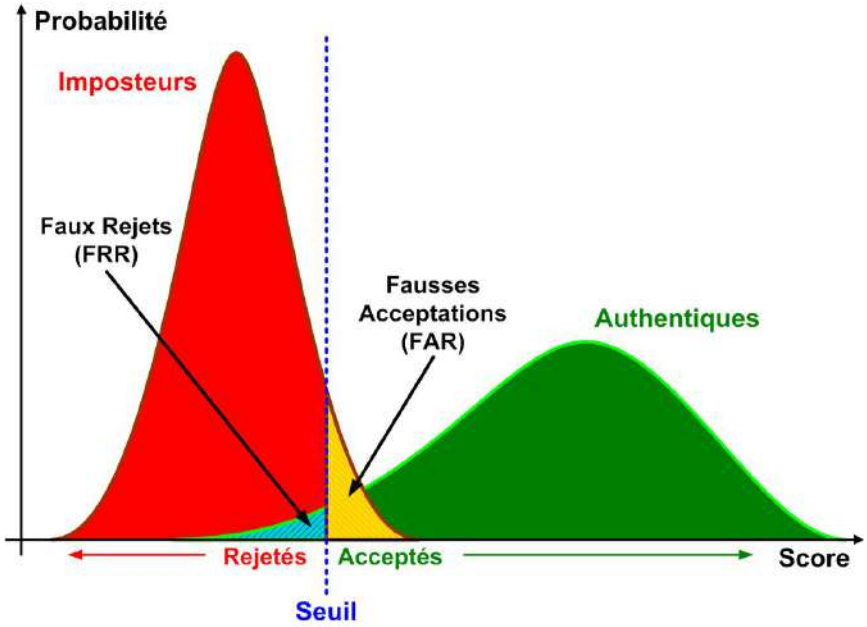


Figure 1.3 Illustration du FRR et du FAR.

I.6.1. Comptabilité des erreurs: FAR, FRR :

Il est donc désirable de connaitre les taux d'erreur:

- Quelle est la proportion de tentatives de gentils utilisateurs acceptées / rejetées?
- Quelle est la proportion de tentatives d'imposteurs rejetées / acceptées?

Il existe plusieurs manières d'annoncer ces taux:

- On peut indiquer la proportion des gentils utilisateurs acceptés et des imposteurs rejetés: ces taux doivent être aussi proches de 100% que possible. On les appelle taux de vrai acceptés TVA et taux de faux rejetés TFR.
- Inversement, on peut indiquer la proportion des gentils utilisateurs rejetés et d'imposteurs acceptés: ces taux doivent être aussi petit que possible, idéalement zéro, on les appelle taux de vrai rejetés TVR et taux de faux acceptés TFA, et évidemment, ils sont simplement liés aux précédents par les relations

$$\mathbf{TVA = 1 - TVR \quad et \quad TFR = 1 - TFA} \qquad \textbf{(II.1)}$$

I.6.2. Les deux taux sont liés :

Il ne faut jamais perdre de vue le fait que les deux taux sont toujours liés: un système réglé sur "dur" ou "haute sécurité" = avec un seuil élevé, laissera difficilement entrer un imposteur, donc aura un FAR très faible. Mais les gentils utilisateurs auront eux aussi du mal à entrer, et le FRR sera élevé. A l'inverse, un système permissif, réglé sur une sécurité faible, laissera facilement entrer les gentils utilisateurs (ils seront contents, le FRR sera faible), mais aussi les imposteurs, et le FAR sera relativement élevé.

Commençons par les gentils utilisateurs. Normalement, ils devraient toujours avoir des scores élevés, plutôt proche de 100 sur une échelle de 0 à 100. C'est évidemment le cas, mais on observe dans la réalité, que certains moins gentils utilisateurs obtiennent parfois des scores

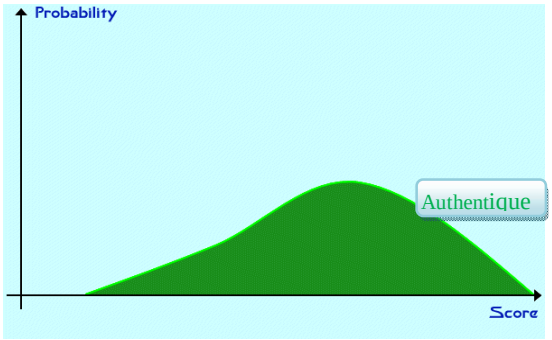


Figure 1.4 Illustration des Authentique

assez faibles. Pour l'instant, ce n'est pas très grave, et on obtient ce genre de distribution (le score en abscisse, le nombre d'utilisateurs ayant eu ce score (probabilité) en ordonnée:

Effectuons la même chose avec les imposteurs. Cette fois, les scores devraient être proche de zéro, mais il arrive parfois qu'un imposteur obtienne un score ma foi assez élevé, et on peut observer ce genre de distribution:

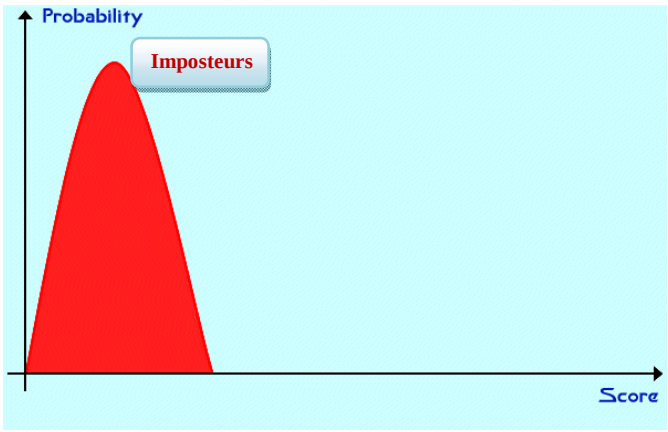


Figure 1.5 Illustration des imposteurs

La forme des distributions peut être très variable, peu importe, ce n'est pas les soucis ici. Par contre, lorsque l'on superpose les deux distributions, on a malheureusement toujours une zone de recouvrement. On aimerait évidemment avoir les deux distributions parfaitement disjointes, ce qui permettrait idéalement de séparer les gentils des méchants, mais ce n'est jamais le cas dans la dure réalité de la vie:

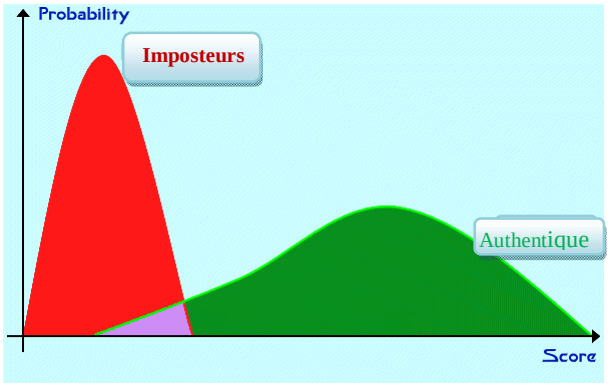


Figure 1.6 superposition des deux distributions

Le responsable du système biométrique devra choisir un seuil d'acceptation, mais où le placer ? Il a choix:

- soit il choisit un seuil faible, ce qui laissera passer tout les gentils utilisateurs (et il ne sera pas ennuyé par ses gentils utilisateurs, de loin les plus nombreux et à qui il a à faire tous les jours), mais alors un imposteur passera assez facilement
- soit il choisit un seuil fort, ce qui bloquera tous les imposteurs et protègera efficacement son système, mais alors il aura des ennuis avec les gentils utilisateurs qui viendront se plaindre que le système ne les laisse pas entrer.

Grâce aux courbes de distribution, on pourra calculer les taux de FAR et de FRR pour différentes valeurs de seuil **(**figure 2.3), et on se rend bien compte que ces deux nombres sont liés. On constate parfois des personnes peu scrupuleuses qui annoncent des FAR et FRR assez avantageux, parce qu'ils n'utilisent pas le même seuil pour les deux nombres. [23]

Pour mesuré la performance du système, on utilise ce que l'on appelle une courbe ROC (pour "Receiver Operating Characteristic" en anglais). La courbe ROC (Figure. 1.4) trace le taux de faux rejet en fonction du taux de fausse acceptation Plus cette courbe tend à épouser la forme du repère, plus le système est Performant, c'est-à-dire possédant un taux de reconnaissance global élevé , le taux d'erreur égal (Equal Error Rate ou EER) correspond au point FAR = FRR, c'est-à-dire graphiquement à l'intersection de la courbe ROC avec la première bissectrice.

Il est fréquemment utilisé pour donner un aperçu de la performance d'un système. Cependant, il est important de souligner que le EER ne résume en aucun cas toutes les caractéristiques d'un système biométrique. [8]

Le seuil doit donc être ajusté en fonction de l'application ciblée : haute sécurité, basse sécurité ou compromis entre les deux.

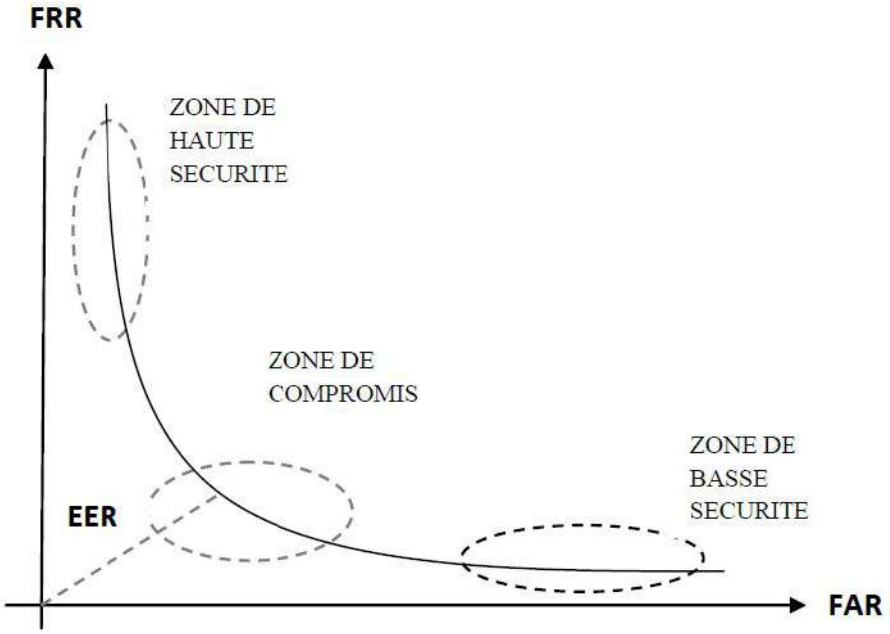


Figure 1.7 : Courbe Roc

Etat de l'art des taux d'erreur: Tableau (1.2)

Test	Conditions de tests	False Reject Rate	False Accept Rate
Empreinte digitale FVC [2006]	Population hétérogène, des ouvriers, vieux,…	2.2%	2.2%
Visage FRVT [2006]	Eclairage contrôlé, haute résolution	0.8%-1.6%	0.1%
Iris ICE [2006]	Eclairage contrôlé, bonne qualité d'images	1.1%-1.4%	0.1%
Voix NIST [2004]	Indépendant du texte, Multi-lagues	5-10%	2-5%

I.7.Techniques biométriques :

Il y a deux catégories de technique de biométrie:

· ***Les techniques d'analyse du comportement (Behavioral) :*** il s'agit d'un type de biométrie caractérisées par un trait d'attitude qui est appris et acquis au fil du temps, Par exemple la dynamique de la signature, La façon d'utiliser un clavier d'ordinateur, etc...).

· ***Les techniques d'analyse de la morphologie humaine:*** il s'agit d'un type de biométrie défini par les caractéristiques physiques (empreintes digitales, forme de la main, forme du visage, dessin du réseau veineux de l'oeil, la voix, etc...)

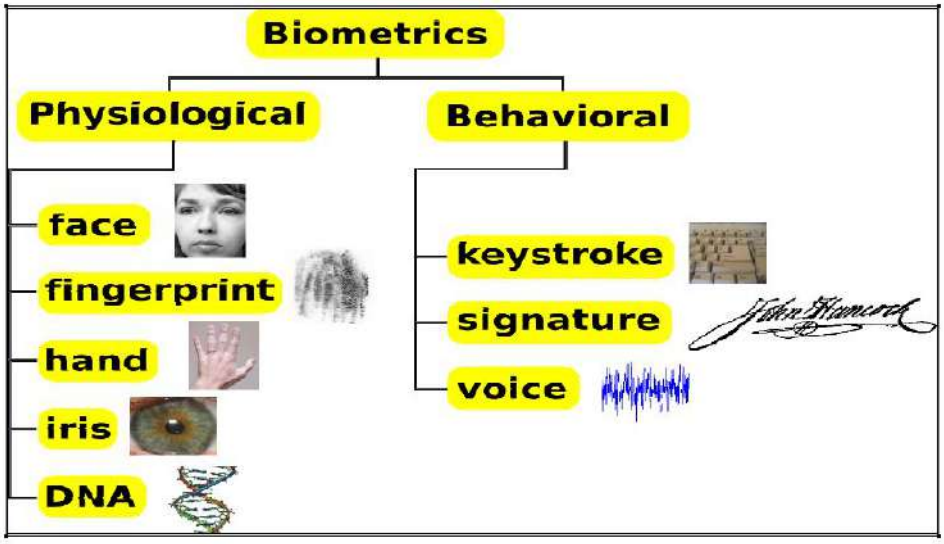


Figure 1.8 La Classification De La Biométrie.

I.7.1 Empreintes digitales

Empreinte digitale est la caractéristique d'un doigt. On le croit que chaque empreinte digitale est unique, chaque personne a ses propres empreintes digitales avec l'unicité permanente. Ainsi les empreintes digitales sont utilisées depuis longtemps pour 'identification et l'investigation juridique.



Figure 1.9: Empreinte digitale acquise par un capteur optique

I.7.2 Visage :

La reconnaissance de la forme du visage est la technique la plus commune et populaire. Elle est la plus acceptable parce que on peut l'utilise à distance sans la collaboration avec objet.

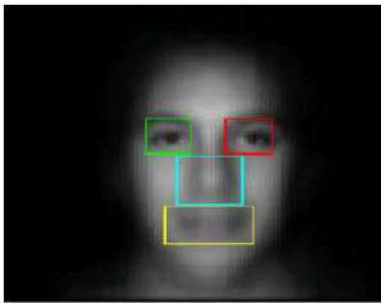


Figure 1.10: Reconnaissance de visage

I.7.3 Iris :

La reconnaissance de l'iris est considérée comme la technique biométrique la plus exacte. L'iris est la partie colorée de l'oeil qui entoure la pupille noire. Son inspection attentive révèle de nombreuses structures détaillées. Ces structures se développent dès le plus jeune âge et sont considérées comme uniques, même chez les vrais jumeaux.

Les structures de l'iris restera constantes jusqu'à la mort.

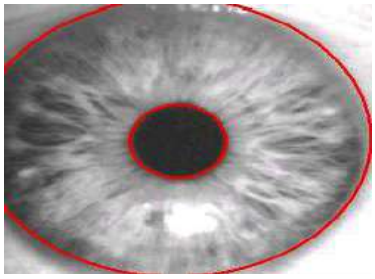


Figure 1.11: Image d'iris

I.7.4 Voix :

L'identification de la voix est considérée par les utilisateurs comme une des formes les plus normales de la technologie biométrique, car elle n'exige aucun contact physique avec le lecteur du système.

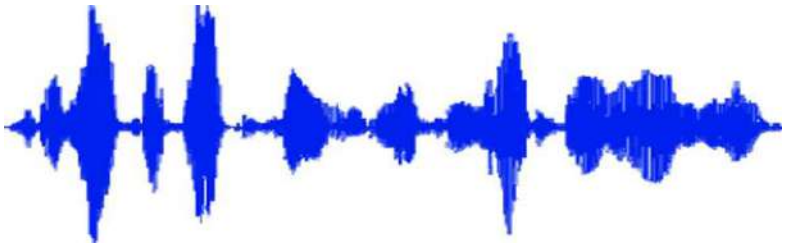


Figure 1.12: Spectre d'un signal voix

I.7. 5 Signature :

Signer un document pour s'identifier est un geste naturel pour tout le monde. Dans la vie de tous les jours, nous signons régulièrement des documents. La reconnaissance de la signature est une des techniques biométriques comportementales.

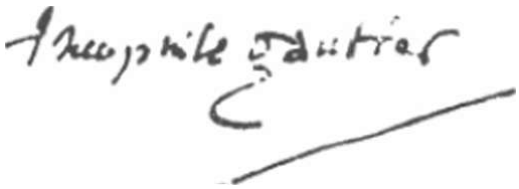


Figure 1.13 : Signature

I.7.6 Les parts de marché par technologie :

Les empreintes digitales continuent à être la principale technologie biométrique en termes de part de marché, près de 44% du chiffre d'affaires total (hors applications judiciaires). La reconnaissance du visage, avec 19% du marché (hors applications judiciaires), dépasse la reconnaissance de la main, qui avait avant la deuxième place en termes de source de revenus après les empreintes digitales.

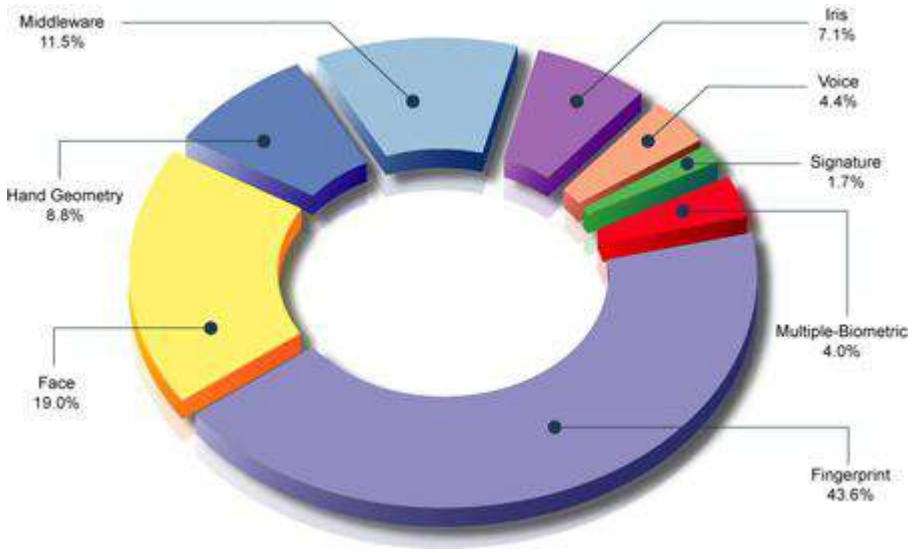


Figure 1.14 : Parts de marché des différentes méthodes biométriques [4]

I.8.Système biométrique :

Un système biométrique est essentiellement un système de reconnaissance de formes qui fonctionne en acquérant des données biométriques à partir d'un individuel, extrayant un ensemble de caractéristiques à partir des données acquises, et comparant ces caractéristiques contre le signature dans la base de données. Selon le contexte d'application, un système biométrique peut fonctionner en mode d'enrôlement ou en mode de vérification ou mode d'identification:

I.8.1.*Enrôlement :* est une phase d'apprentissage qui a pour but de recueillir des informations biométriques sur les personnes à identifier. Plusieurs campagnes d'acquisitions de données peuvent être réalisées afin d'assurer une certaine robustesse au système de reconnaissance aux variations temporelles des données.

Pendant cette phase, les caractéristiques biométriques des individus sont saisies par un capteur biométrique, puis représentées sous forme numérique (signatures), et enfin stockées dans la base de données. Le traitement lié à l'enrôlement n'a pas de contrainte de temps, puisqu'il s'effectue « hors-ligne ».

I.8.2.*Vérification* *:* le système valide l'identité d'une personne en comparant les données biométriques capturées à sa propre base de données. Dans un tel système, un individu qui désire être identifié réclame une identité, habituellement par l'intermédiaire d'un PIN (numéro d'identification Personnelle), d'un nom d'utilisateur, d'une carte futée, etc., et le système conduit une comparaison d'un-à-un pour déterminer si la réclamation est vraie ou faux (Est-ce que ces données biométriques appartiennent à Bob?).

I.8.3.*Identification:* le système identifie un individu en recherchant les signatures(templates) de tous les utilisateurs dans la base de données. Par conséquent, le système conduit plusieurs des comparaisons pour établir l'identité d'un individu (ou échoue si le sujet n'est pas inscrit dans la base de données de système) sans devoir soumis réclamer une identité.

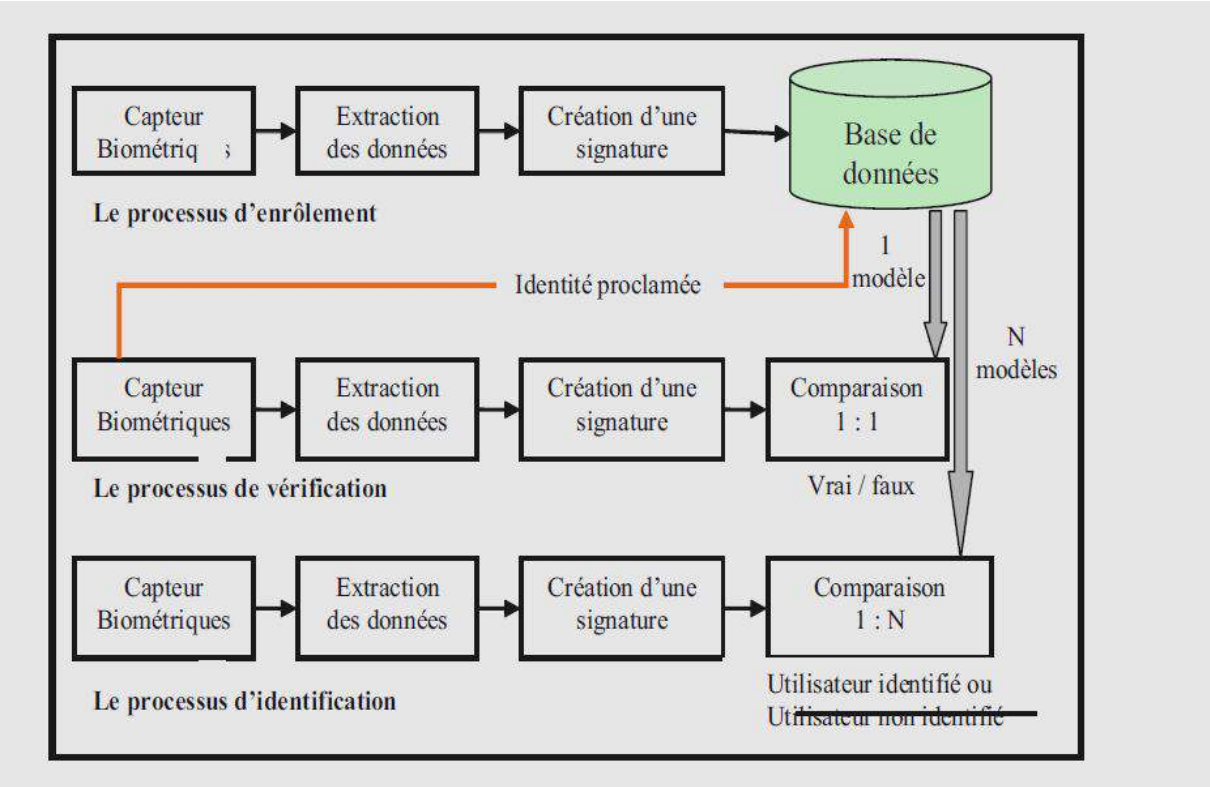


Figure 2.15 : Schéma de fonctionnement d'un système biométrique

I.9 Caractérisation d'un système biométrique :

Un système biométrique typique peut être représenté par quatre modules principaux:

I.9.1 Le module de capture est responsable de l'acquisition des données biométriques d'un individu (cela peut être un appareil photo, un lecteur d'empreintes digitales, une caméra de sécurité, etc.,

I.9.2 Le module d'extraction de caractéristiques prend en entrée les données biométriques acquises par le module de capture et extrait seulement l'information pertinente afin de former une nouvelle représentation des données. Idéalement, cette nouvelle représentation est censée être unique pour chaque personne et relativement invariante aux variations intra-classe,

I.9.3 Le module de correspondance compare l'ensemble des caractéristiques extraites avec le modèle enregistré dans la base de données du système et détermine le degré de similitude (ou de divergence) entre les deux,

I.9.4 Le module de décision vérifie l'identité affirmée par un utilisateur ou détermine l'identité d'une personne basée sur le degré de similitude entre les caractéristiques extraites et le(s) modèle(s) stocké(s).

I.10 applications :

On peut distinguer quatre grands types d'applications de la biométrie : le contrôle d'accès (access control), l'authentification des transactions (transaction authentication), la répression (law enforcement) et la personnalisation (personalization).

I.10.1. contrôle d'accès

Le contrôle d'accès peut être lui même subdivisé en deux sous catégories : le contrôle d'accès physique et le contrôle d'accès virtuel. On parle de contrôle d'accès physique lorsqu'un utilisateur cherche à accéder à un lieu sécurisé. On parle de contrôle d'accès virtuel dans le cas où un utilisateur cherche a accéder à une ressource ou un service.

I.10.1.1 contrôle d'accès physique :

Longtemps, l'accès à des lieux sécurisés (bâtiments ou salles par exemple) s'est fait à l'aide de clefs ou badges. Les badges étaient munis d'une photo et un garde était chargé de la vérification. Grâce à la biométrie, la même opération peut être effectuée automatiquement de nos jours.

L'une des utilisations les plus célèbres de la géométrie de la main pour le contrôle d'accès est le système INSPASS [09] (Immigration and Naturalization Service Passenger Accelerated Service System) déployé dans plusieurs grands aéroports américains (New-York, Washington, Los Angeles, San Francisco, etc.). Cette application permet aux passagers répertoriés dans le système d'éviter les files d'attente pour le contrôle des passeports.

Ceux-ci possèdent une carte magnétique qui contient l'information sur la géométrie de leur main. Lorsqu'ils présentent leur main au système, celle-ci est comparée à l'information contenue dans la carte.

I.10.1.2. contrôle d'accès virtuel :

Le contrôle d'accès virtuel permet par exemple l'accès aux réseaux d'ordinateurs ou l'accès sécurisé aux sites webs. Le marché du contrôle d'accès virtuel est dominé par les systèmes basés sur une connaissance, typiquement un mot de passe. Avec la chute des prix des systèmes d'acquisition, les applications biométriques devraient connaître une popularité croissante, un exemple d'application est l'intégration par Apple dans son système d'exploitation MAC OS 9 d'un module de reconnaissance du locuteur [1] de manière à protéger les fichiers d'un utilisateur, tout particulièrement lorsque l'ordinateur est utilisé par plusieurs indi vidus ce qui est de plus en plus souvent le cas.

I.10.2 Répression :

Une des applications les plus immédiates de la biométrie à la répression est la criminologie. La reconnaissance d'empreintes digitales en est l'exemple le plus connu. Elle fut acceptée dès le début du XXe siècle comme moyen d'identifier formellement un individu et son utilisation s'est rapidement répandue. Il existe aussi des applications dans le domaine judiciaire. T-Netix [10] propose ainsi des solutions pour le suivi des individus en liberté surveillée en combinant technologies de l'internet et de reconnaissance du locuteur.

I.10.3 Personnalisation :

Les technologies biométriques peuvent être aussi utilisées afin de personnaliser les appareils que nous utilisons tous les jours. Cette application de la biométrie apporte un plus grand confort d'utilisation.

Afin de personnaliser les réglages de sa voiture, Siemens propose par exemple d'utiliser la reconnaissance des empreintes digitales [10]. Une fois l'utilisateur identifié, la voiture ajuste automatiquement les sièges, les rétroviseurs, la climatisation, etc.

I.11 Comparatif

La colonne "Physique Logique" précise l'usage le plus courant de chaque technique.

Techniques	Avantages	Inconvénients	Physique/ Logique
Empreintes digitales	Coût. Ergonomie moyenne. Facilité de mise en place. Taille du capteur.	Qualité optimale des appareils de mesure (fiabilité). Acceptabilité moyenne. Possibilité d'attaque, (rémanence de l'empreinte...)	PL
Forme de la main	Très ergonomique. Bonne acceptabilité.	Système encombrant. Coût. Perturbation possible par des blessures et l'authentifie a tion des membres d'une même famille.	P
Visage	Coût. Peu encombrant. Bonne acceptabilité.	Jumeaux. Psychologie, religion. Déguisement... Vulnérable aux attaques.	P
Rétine	Fiabilité. Pérennité.	Coût. Acceptabilité faible. Installation difficile.	P
Iris	Fiabilité.	Acceptabilité très faible. Contrainte d'éclairage.	P
Voix	Facile.	Vulnérable aux attaques.	PL
Signature	Ergonomie.	Dépendance de l'état émotionnel de la personne. Fiabilité.	L
Frappe au clavier	Ergonomie.	Dépendant de l'état physique de la personne	L

Tableau 1.3 : comparaison entre les déférentes techniques biométries.

Conclusion :

Ce chapitre a présenté un aperçu général, d'une part, quelques notions et définitions de base liées à la biométrie et d'autre part le principe de fonctionnement des systèmes biométriques ainsi que les outils utilisés pour mesurer leurs performances.

L'objectif du chapitre suivant est de présenter en détails le technique de la reconnaissance de visage parmi les autres techniques biométriques, car elle constitue l'objectif de ce travaille.

Conclusion :

La reconnaissance de visages est une technologie biométrique qui est trop utilisée dans les applications de contrôle de frontières, dans la sécurité des établissements et des zones urbaines et dans l'identification des conducteurs, c'est une technique commune, populaire, simple et qui offre beaucoup d'avantages.

II.9 Avantage et Inconvénient

On trouve quelque avantage et inconvénient dans la reconnaissance de visage

Avantages	Inconvénients
• Technique peu coûteuse. peu encombrante • Absence de contact avec le capteur, méthode non intrusive pour la personne ; pas de risques pour la santé.	• Les vrais jumeaux ne sont pas différenciés. • Psychologiquement, certaines personne: rejettent leur image photographique (refus de son image, ajout d'accessoires, rôle, religion, critique de la qualité de la caméra, etc.). L'image est considérée comme trop personnelle pour être utilisée. • En tant que contrôle d'accès, le visage n'est pas. traditionnellement. reconnu comme un mécanisme fiable d'authentification (Peut être dupe par l'utilisation de maquillage ou d'un masque en silicone) • Dans l'état des systèmes actuels, technique trop sensible au changement d'éclairage, changement d'échelle (taille du visage ou distance de la caméra), présence d'arrière plan non stationnée, changement de position lors de l'acquisition de l'image (inclinaison de la tête ou expression). • Tout élément tel que lunettes de soleil chapeau, moustache, barbe, percing, blessure peut causer des anomalies avec des systèmes d'identification du visage.

Tableau 2.1 : Avantage et Inconvénient de la reconnaissance du visage

afin de réduire la dimension des données. La figure 3.10 fournit une classification des algorithmes principaux de méthodes hybrides.

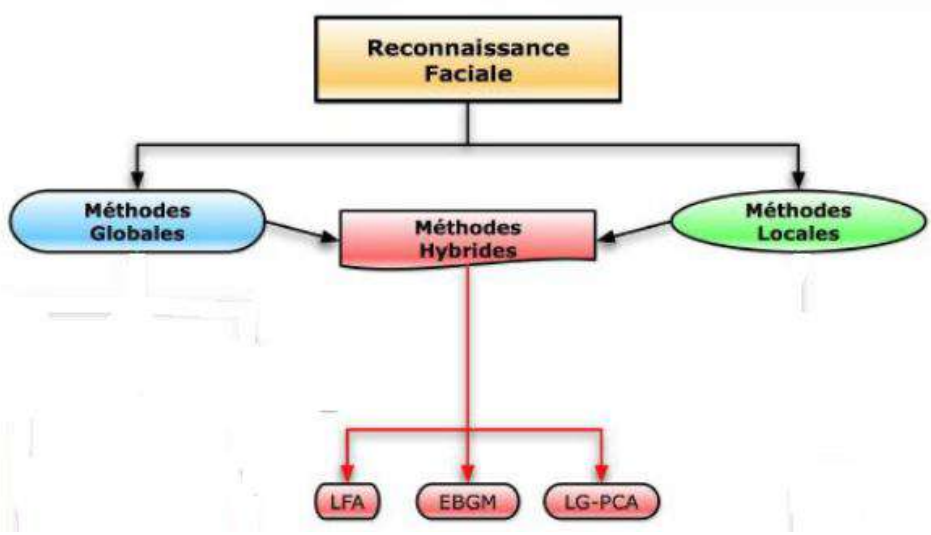


Figure 2.10 : Méthodes hybrides

II.8.2 Méthodes globales :

Les méthodes holistiques appelées aussi méthodes globales, sont des méthodes qui sont normalement utilisées dans la reconnaissance de visage, ces méthodes utilisent la région entière du visage connue entrée à l'algorithme de reconnaissance. Ce sont des techniques très réussies et bien étudiées. Ces méthodes offrent les meilleures performances, mais le problème de stockage des informations extraites lors de la phase "apprentissage" reste l'inconvénient majeur [7]. Parmi les méthodes les plus connues il y'a: PCA. LDA/FLD. PDBNN...

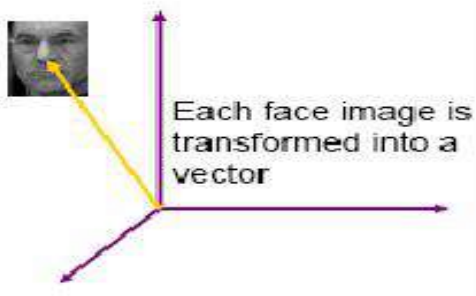


Figure 2.9 : L'utilisation de la région entière du visage connue

entrée aux méthodes globales

II.8.3 Méthodes hybrides

Les méthodes hybrides permettent d'associer les avantages des méthodes globales et locales en combinant la détection de caractéristiques géométriques (ou structurales) avec l'extraction de caractéristiques d'apparence locales, elles permettent d'augmentera stabilité de la performance de reconnaissance lors de changements de pose, d'éclairement et d'expressions faciales, l'analyse de caractéristiques locales (LFA) et les caractéristiques extraites par ondelettes de Gabor (comme l'Elastic Bunch Graph Matching, EBGM), sont des algorithmes hybrides typiques. Plus récemment, l'algorithme Log Gabor PCA (LG-PCA) effectue une convolution avec des ondelettes de Gabor orientées autour de certains points caractéristiques du visage afin de créer des vecteurs contenant la localisation et la valeur d'amplitudes énergétiques locales ces vecteurs sont ensuite envoyés dans un algorithme PCA

II.8Les méthodes de reconnaissance faciales :

II.8.1 Méthodes locales :

Ce sont des méthodes Géométriques, on les appelle aussi les méthodes à traits, à caractéristiques locales, ou analytiques, l'analyse du visage humain est donnée par la description individuelle de ses parties et de leurs relations. Ce modèle correspond à la manière avec laquelle l'être humain perçoit le visage, c'est à dire, à nos notions de traits de visage et de parties comme les yeux, le nez. la bouche, etc. La plus paît des travaux réalisés se sont concentrés sur l'extraction des traits à partir d'une image du visage et sur la définition d'un modèle adéquat pour représenter ce visage, un certain nombre de stratégies automatiques et semi-automatiques ont modélisé et classé les visages sur la base de distances normalisées et angles entres points caractéristiques, la stratégie est qualifiée d'automatique ou non selon que la phase d'extraction des points est faite par l'ordinateur ou qu'elle est assistée par un péraàteur. Cette phase constitue l'étape clé du processus, car la performance du système entier dépend de la précision avec laquelle les informations utiles sont extraites [3] [6] [7].

L'avantage de ces méthodes réside dans la prise en compte de la particularité du visage en temps que forme naturelle à reconnaître, en exploitant les résultats de la recherche en neuropsychologie et psychologie cognitive sur le système visuel humain. La difficulté éprouvée lors de la considération de plusieurs vues du visage, ainsi que le manque de précision dans la phase "extraction" des points, constituent leur inconvénient majeur. En plus ces techniques sont facilement affectées par l'information non pertinente.

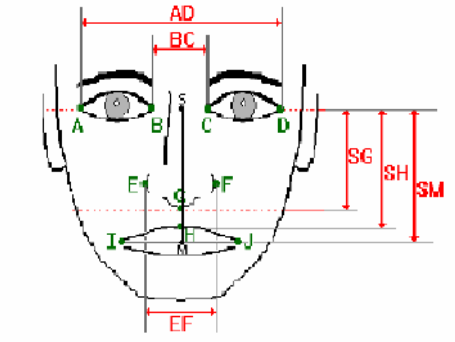


Figure 2.8: Distances entre points caractéristiques

Dans cette catégorie, on trouve plusieurs méthodes connue: Pure méthodes géométrique. Dynamique et l'architecture. HMM...

l'expression faciale sur la reconnaissance est donc difficile à évaluer avec précision. Cependant, du fait que ce facteur affecte la forme géométrique et les positions des caractéristiques faciales, les techniques globales ou hybrides y sont généralement plus robustes que la plupart des techniques géométriques.

II.6.4 Occultations partielles :

Le visage peut être partiellement masqué par des objets ou par le port d'accessoires tels que des lunettes, un chapeau, une écharpe, etc. Les occultations peuvent être intentionnelles ou non, dans le contexte de la vidéosurveillance, il peut s'agir d'une volonté délibérée d'empêcher la reconnaissance. Il est clair que la reconnaissance sera d'autant plus difficile que peu d'éléments discriminants seront simultanément visibles.

II.7. Les classes des techniques de reconnaissance de visages :

Une fois la détection de la personne et de son visage complété, l'image résultante ainsi que les informations pertinentes sont fournies au moteur de reconnaissance, celui-ci, composé de plusieurs sous modules, est basé sur une architecture orientée objets facilitant la gestion et l'ajout de techniques supplémentaires, utilisant une banque d'informations centralisée, le moteur de reconnaissance doit tout d'abord effectuer l'apprentissage des sous modules pour les différentes personnes à reconnaître.

Plusieurs techniques de reconnaissance d'individus ont été développées au cours des dernières années, la plupart d'entre elles ont le visage comme zone d'intérêt.

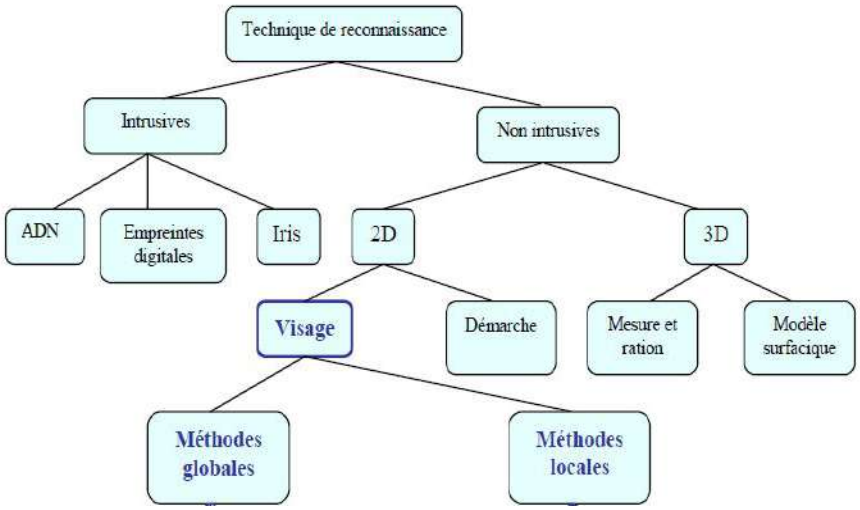


Figure 2.6 : Principales techniques de reconnaissance

II.6. Principales difficultés de la reconnaissance de visage :

Pour le cerveau humain, le processus de la reconnaissance de visages est une tâche visuelle de haut niveau. Bien que les êtres humains puissent détecter et identifier des visages dans une scène sans beaucoup de peine, construire un système automatique qui accomplit de telles tâches représente un sérieux défi. Ce défi est d'autant plus grand lorsque les conditions d'acquisition des images sont très variables, il existe deux types de variations associées aux images de visages : inter et intra sujet. La variation inter-sujet est limitée à cause de la ressemblance physique entre les individus. Par contre la variation intra-sujet est plus vaste, elle peut être attribuée à plusieurs facteurs que nous analysons ci-dessous.

II.6.1 Variations de la pose :

Les changements d'orientation et les changements de l'angle d'inclinaison du visage engendrent de nombreuses modifications d'apparence dans les images collectées, une phase préliminaire de normalisation de l'image du visage permet de corriger d'éventuelles rotations dans le plan de celle-ci. Les rotations en profondeur engendrent l'occultation de certaines parties du visage comme pour les vues de trois-quarts. D'autre part, elles amènent des différences de profondeur qui, projetées sur le plan 2D de l'image, provoquent des déformations qui font varier la forme globale du visage, ces déformations qui correspondent à l'étirement de certaines parties du visage et la compression d'autres régions font varier aussi les distances entre les caractéristiques faciales.

II.6.2 Changements d'éclairage :

L'intensité et la direction d'éclairage lors de la prise de vue influent énormément sur l'apparence du visage dans l'image. En effet, dans la plupart des applications courantes, des changements dans les conditions d'éclairage sont inévitables, notamment lorsque les vues sont collectées à des heures différentes, en intérieur ou en extérieur. Etant donnée la forme spécifique d'un visage humain, ces variations d'éclairage peuvent y faire apparaître des ombres accentuant ou masquant certaines caractéristiques faciales.

II.6.3 Expressions faciales :

Les visages sont des éléments non rigides. Les expressions faciales véhiculant des émotions, combinées avec les déformations induites par la parole, peuvent produire des changements d'apparence importants, et le nombre de configurations possibles est trop important pour que celles-ci soient décrites in extenso de façon réaliste. L'influence de

_ ***Normalisation*** : La normalisation est constituée de deux processus : géométrique et photométrique. La normalisation géométrique est nécessaire parce que la taille du visage à l'intérieur de l'image acquise peut varier en fonction de la distance entre le module d'acquisition et la personne. Le visage doit donc être extrait à partir de l'image et une transformation géométrique, pour obtenir une taille fixe, est appliquée. L'approche standard consiste à définir l'emplacement des centres des yeux dans une position constante au sein de l'image de sortie.

L'étape de normalisation photométrique tente d'éliminer ou de réduire les effets de l'illumination de l'image. Dans certains cas, l'étape de normalisation photométrique peut être appliquée avant, ou avant et après l'étape de normalisation géométrique. Elle peut aussi être appliquée pendant la phase de détection.

_ ***Calcul de score*** : L'image normalisée est ensuite comparée à une ou plusieurs images stockées (si un modèle utilisant une galerie d'images est utilisé).

Cette comparaison produit un score, représentant la similarité ou la distance de l'image test par rapport à l'image ou au modèle référence.

_ ***Décision*** : Le score est comparé à un seuil qui détermine si l'image est acceptée ou rejetée en tant que représentant de l'identité proclamée.

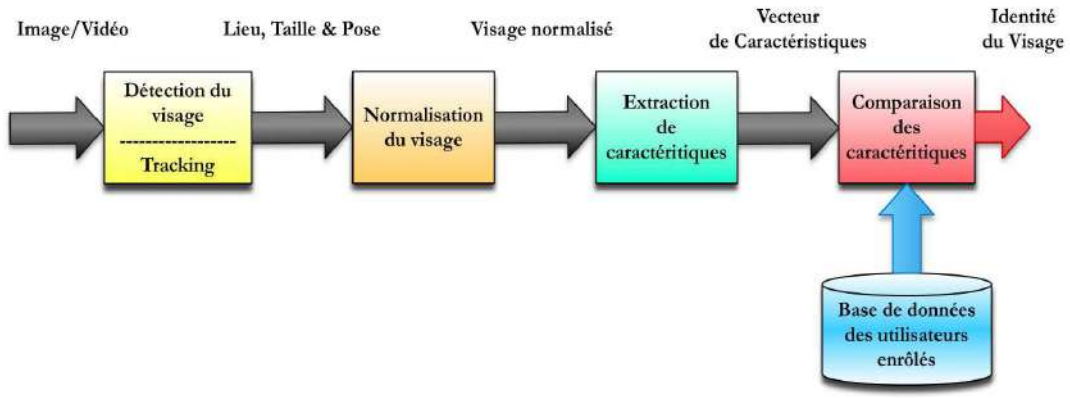


Figure. 2.5 : Principe de fonctionnement de base d'un système de reconnaissance faciale.

l'utilisation de la biométrie, ainsi on peut trouver des appareils électroniques personnels utilisant la biométrie tels que les ordinateurs portables, les coffres forts, les téléphones etc.

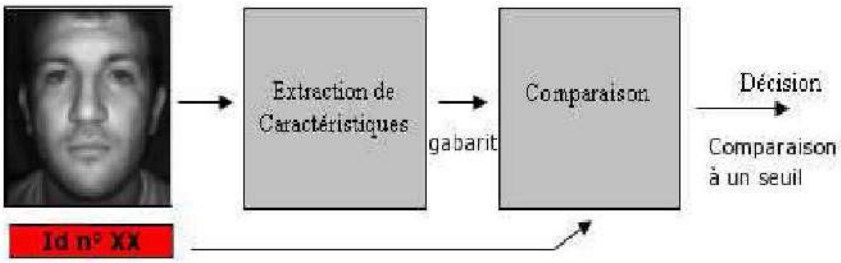


Figure 2.3: schéma de vérification du visage

II.5 Biométrie du visage :

De nos jours, le visage peut être utilisé pour identifier une personne dans une base mais il est plus communément utilisé pour vérifier l'identité. Il s'agit alors de déterminer si une identité réclamée est correcte ou fausse. Pour la vérification des visages, ce processus est effectué en comparant un modèle du demandeur (une ou plusieurs images de test), avec un modèle stocké (une ou plusieurs images de référence), le processus complet de vérification des visages est décrit ci-dessous :

- ***Capture du visage*** : le visage d'une personne est numérisé par des capteurs comme des appareils photo numériques pour la représentation 2D du visage, des scanners 3D pour avoir l'information de profondeur de l'image combinée avec l'image de la texture ou aussi des capteurs infrarouges ou proche infrarouge. Des informations spécifiques à la capture peuvent être déterminées aussi lors de l'acquisition de l'image, comme la pose de la personne par rapport à la caméra, l'expression ou aussi les conditions d'illumination de la capture de l'image. Dans cette thèse nous nous consacrons à l'étude exclusive du problème de la reconnaissance des visages 2D.

_ ***Détection*** **:** les méthodes de détection de visages peuvent être classées en « approche globale » dans laquelle on analyse le visage dans son entier, ou en« approche locale », dans laquelle on va essayer de détecter, localiser et regrouper les différents éléments constitutifs du visage : nez, yeux, bouche,… Des informations complémentaires peuvent aussi être utilisées pour détecter les différents composants du visage, telles que la couleur, le mouvement ou encore la forme.

II.4.2 Identification :

Ayant un flux d'image, ou une image qui contient un visage, l'identification est la reconnaissance à partir d'une base de données sans autre connaissance a priori de l'identité de la personne. Cette tâche donne lieu à une comparaison de type 1- to-N : on compare une image du flux avec les images enregistrées dans la base de donnée (figure 2.2). Une application est la reconnaissance de personnes "dangereuses" enregistrées dans une (watch list). Cette application est sujette à des contraintes de temps de calcul d'où l'enregistrement de caractéristiques du visage au lieu de l'image entière. Aussi l'enregistrement d'une base de donnée de visage est conditionné, en France par l autorisation de la CNIL (Commission Nationale Informatique et Liberté) qui cautionne la protection des données personnelles. Cette autorisation n'est donnée qu'en fonction du fort besoin de sécurité nécessité par l'application.

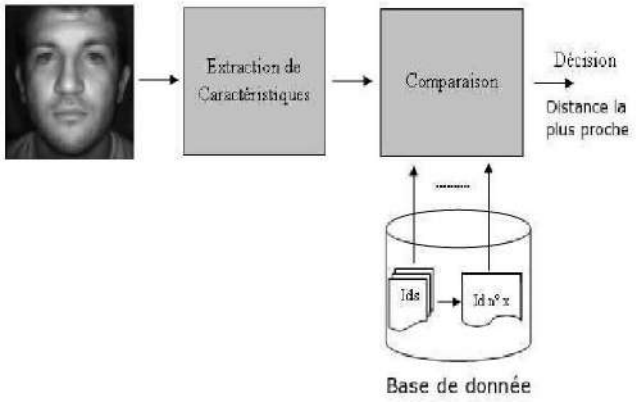


Figure 2.2: schéma d'Identification du visage

II.4.3 Vérification :

Ayant un flux d'image, ou une image qui contient un visage, la vérification est la reconnaissance de visage à partir d'une image de référence enregistrée au préalable dans une puce ou un fichier, c'est une vérification de l'identité revendiquée c'est à dire que la personne décline au préalable son identité (figure 2.3). Cette tâche donne lieu à une comparaison 1-to-l. Une des applications est le contrôle ou vérification d'identité à l'entrée des Etats-Unis par exemple(le nouveau passeport biométrique).

La référence biométrique peut alors être enregistrée dans une base de données mais aussi sur une carte à puce détenue par la personne, dans ce cas émet un avis moins restrictif à

II.4 La Reconnaissance de Visage :

La reconnaissance de visage est un problème difficile en vision par ordinateur nous allons utiliser ce problème pour illustrer quelques techniques en reconnaissance de forme.

Dans ces exemples nous allons exploiter quelque "prétraitements" issue du domaine de la vision par ordinateur, Conditions d'acquisition d'images:

Nous allons supposer que les images étaient prises dans les conditions favorables :

1) Les images seront prises du vue frontal avec un sujet coopérative.

2) Le visage est bien éclairé et l'éclairage ne change pas.

3) La distance entre le visage et la caméra et fixe (plus/mois quelque cm).

Pour simplifier la reconnaissance nous allons normaliser l'image par quelque "Prétraitements".

II.4.1 Prétraitements :

1) Détecter le visage et éliminer le fond de l'image.

(exemple par détection de couleur, ou par différence avec un fond adaptatif).

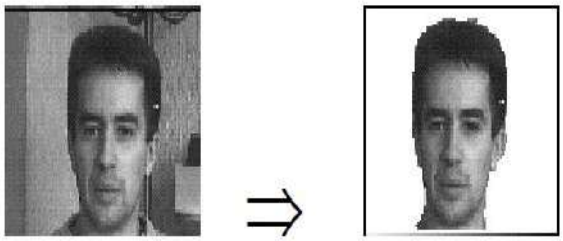


Figure 2.1 : détecter le visage

2) Détecter points clés. (Keypoints). Par exemple les yeux et bouche.

Ceci est faire par "inter corrélation" avec des motifs à chaque pixel

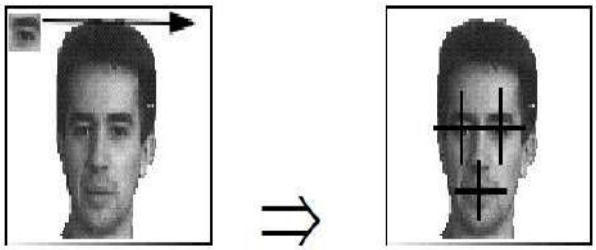


Figure 2.2 : détecter points clés

d'applications. De plus, une méthode comme l'identification de l'iris reste contraignante pour les utilisateurs qui n'apprécient pas de placer leur œil devant un appareil. A l'inverse, des systèmes d'identification basés sur l'analyse des images de visage ne présentent aucune contrainte pour les utilisateurs. La reconnaissance faciale est une modalité qui peut être implémentée de manière indépendante des autres modalités biométriques, elle est souvent utilisée dans des applications de surveillance. La reconnaissance faciale offre plusieurs avantages : le système de capture (c.à.d. les caméras) est facile à installer, il est accepté dans les lieux publics ce qui permet d'avoir des bases de données de plus en plus grandes et ainsi d'améliorer les performances de la reconnaissance [16], le visage occupe la seconde place en biométrie [10].

La reconnaissance faciale possède plusieurs avantages sur les autres technologies biométriques : elle est naturelle, non intrusive et facile à utiliser. Parmi les six attributs biométriques considérés par Hietmeyer [24], les caractéristiques faciales marquent un score de compatibilité le plus élevé dans un système MRTD (Machine Readable Travel Documents) [25], ce score étant basé sur plusieurs facteurs d'évaluation tels que l'enrôlement, le renouvellement des données, les requismatériels et la perception des utilisateurs (Figure. 3.1).

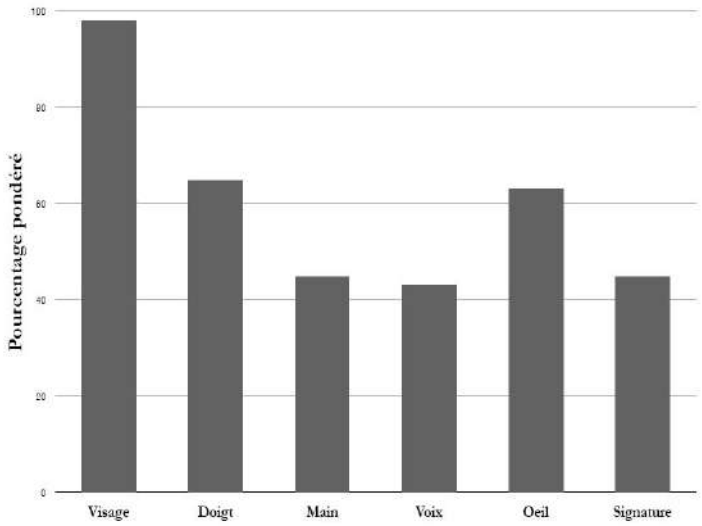


Figure. 2.1 .Scores de compatibilité pour différentes technologies biométriques dans un Système MRTD.

II.1 Introduction :

L'analyse de visages par traitement d'images est encore aujourd'hui un sujet de recherche très actif puisqu'il concerne de nombreux domaines d'application tels que par exemple la sécurité (biométrie, surveillance), la robotique (interaction homme machine, affective computing), le handicap (communication par le visage), les jeux vidéo ou les télécommunications à très bas débits (clones synthétiques).

Les recherches englobent la détection, le suivi, le codage, la reconnaissance et la synthèse de visages en tenant compte des variations possibles de leur apparence (pose tridimensionnelle, regard, lèvres, expressions, âge, genre, mouvements faciaux et comportement facial, occultations, etc.).

La reconnaissance faciale possède plusieurs avantages sur les autres technologies biométriques : elle est naturelle, non intrusive et facile à utiliser.

II.2 Historique :

La reconnaissance faciale est une technique biométrique qui a une longue histoire ,si l'empreinte digitale est la technique biométrique la plus ancienne et la plus répandue et qui a été adoptée par Scotland Yard dès 1901 et par la préfecture de Police de Paris, dès 1903 pour rechercher les criminels, la reconnaissance des visages a été développé par Benton et Van Allen en 1968 pour évaluer la capacité d'identification des visages non familiers. Il ne s'agit pas d'un test de reconnaissance mnésique de visages familiers ou non familiers, mais d'une épreuve consistant à apparier des photographies de visages non familiers présentés sous différents éclairages et selon des angles différents et nécessitant une bonne capacité d'intégration Visio-spatiale.

II.3. La place de la reconnaissance du visage parmi les autres techniques biométriques :

Les empreintes digitales sont les caractéristiques biométriques les plus communément Utilisées pour la reconnaissance de criminels. Le premier système automatique d'authentification utilisant les empreintes digitales a été commercialisé au début des années soixante. D'autres parts, plusieurs études ont démontré que l'iris est la caractéristique la plus fiable car la texture de l'iris reste stable au cours de la vie. Toute fois, ces méthodes présentent l'inconvénient majeur d'être intrusives, ce qui limite énormément leurs domaines

d'images "image causes" fondamentales statistiquement indépendantes en **S**. L'algorithme d' ACI essaye d'inverser les images de base en trouvant un ensemble de filtres W_i qui produisent des sorties statistiquement indépendantes.

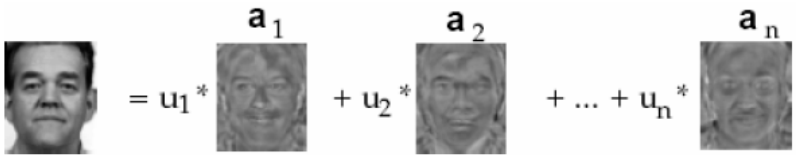


Figure .3.11 : La représentation factorielle d'ACI = (u1,u2,….,un)

La représentation factorielle du code est constituée des coefficients indépendants u, de la combinaison linéaire des images de bases en A qui forment chaque image de visage **X** [20].

III.8.Conclusion :

L'analyse des composantes indépendantes (ACI) offre la possibilité de contourner une autre des limitations théoriques de l'ACP, c'est-à-dire, l'obligation de produire un sous-espace dont chacun des axes est perpendiculaire aux autres. En maximisant l'indépendance des composantes, l'ACI permet d'exploiter des relations inter pixels à un plus haut niveau que l'ACP [19]. Par contre, il reste toujours un doute sur la performance réelle sur des problèmes de reconnaissance de visages d'ACI relativement à celle de l'ACP dû à des résultats conflictuels [15].

Alors que les images de base obtenue en architecture I sont statistiquement indépendantes, les coefficients qui représentent les images d'entrée dans le sous-espace défini par les images de base ne sont pas. L'objectif de l' ACI en architecture II est de trouver des coefficients statistiquement indépendants pour les données d'entrée. Dans cette architecture, l'entrée est transposée de l'architecture I, qui est, les pixels sont des variables et les images sont l'observation, la séparation de sources est effectuée sur les pixels, et chaque rangée de la matrice de poids **W** est apprise une image **A,** la matrice inverse de **W** contient les images de base dans ses colonnes**,** les coefficients de sources statistiquement indépendantes en S qui composent les images d'entrée sont récupérées dans les colonnes de **U** (Figure 3.9). Cette architecture a été utilisée pour trouver des filtres d'image qui produit des résultats statistiquement indépendants de scènes naturelles[19].

Dans ce travail, l' ACI est effectuée sur les coefficients ACP plutôt que directement sur les images d'entrée pour réduire la dimensionnalité . En suivant la même notation décrit ci-dessus, les coefficients statistiquement indépendants sont calculés comme

$$\mathbf{U = W * C}^{\mathbf{T}} \qquad \textbf{(III.27)}$$

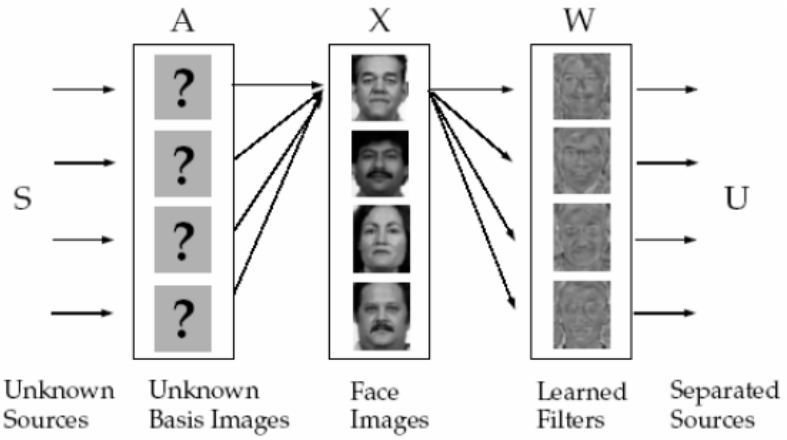


Figure 3.10 : Le modèle de système d'image de l'architecture 2 d' ACI

Dans l'architecture 2 d' ACI, chaque image de l'ensemble de données est considérée comme étant créée à partir d'un ensemble d'images de base en **A**, et d'un vecteur de causes

$$C = X * R \quad \textbf{(IV.23)}$$

et $$X = C * R^{T} \quad \textbf{(IV.24)}$$

De $U = W * R^{T}$ et l'hypothèse que W est inversible, nous obtenons

$$R^{T} = W^{-1} * U \quad \textbf{(IV.25)}$$

Par conséquent,

$$X = (C * W^{-1)} * U = B * U \quad \textbf{(IV.26)}$$

Chaque ligne de **B** contient les coefficients pour combiner linéairement les images de base pour constituer l'image de visage dans la rangée correspondante de **X.** De plus, **X** est la reconstruction des données d'origine avec une erreur quadratique minimale selon la ACP.

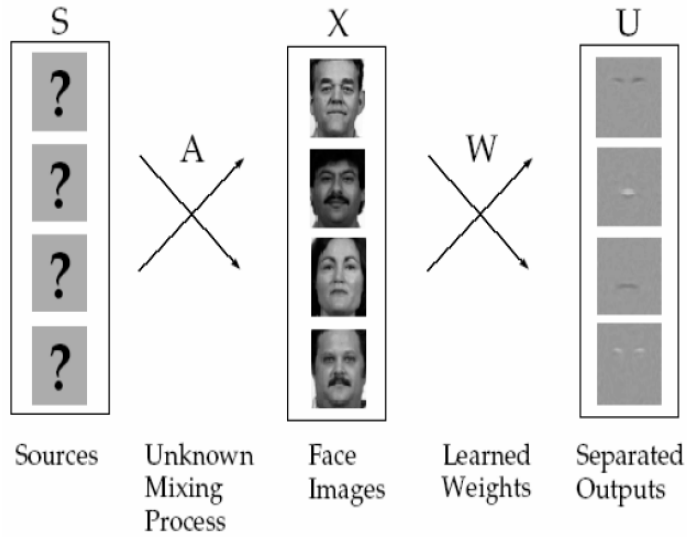


Figure 3.9 : Le modèle de synthèse d'image de l'architecture 1 d' ACI

III.7.2 Architecture 2 :

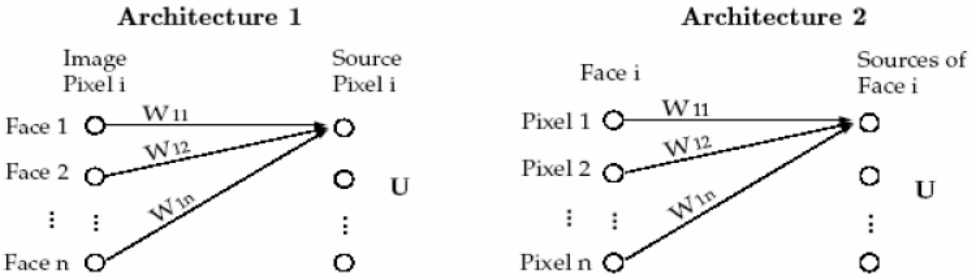


Figure 3.8 : Les deux architectures d' ACI

III.7.1 Architecture 1 :

Peu importe quel algorithme est utilisé pour calculer l' ACI, il ya deux façons fondamentalement différentes à appliquer ICA à la reconnaissance faciale Dans l'architecture I, les images de visages d'entrée dans **X** sont considérés comme un mélange linéaire des images de base statistiquement indépendantes **S** combiné par une matrice de mélange inconnu **A** L'algorithme ACI apprend la matrice de poids **W**, qui est utilisé pour récupérer un ensemble d'images de manière indépendante dans les rangs de **U** (Figure 4.9). Dans cette architecture, les images de visage sont des variables et des valeurs de pixel fournissent des observations pour les variables, le tri à la source, par conséquent, est effectuée dans l'espace du visage projeter des images d'entrée sur les vecteurs de poids tirés produit les images de manière indépendante. La représentation compressée d'une image de visage est un vecteur de coefficients utilisés pour combiner linéairement les images de base indépendants pour générer l'image [18].

Pour décrire les bases mathématiques de l'architecture I, soit **R** a **p** par **m** matrices contenant les **m** premiers vecteurs propres d'un ensemble de **n** images de visages, soit **p** le nombre de pixels dans une image de la formation Les lignes de la matrice d'entrée à l' ACI sont les variables et les colonnes sont des observations, par conséquent, l' ACI est effectuée sur R^T. Les **m** images de façon indépendante dans les rangs de U sont calculés comme $U = W * R^T$. Ensuite, le **n** par m ACI coefficients matrice **B** pour la combinaison linéaire des images de manière indépendante en U est calculé comme suit:

Soit **C** le **n** par **m** matrice de ACP coefficients. Ensuite,

III.6.1. Application de l'ACI : hypothèses et cohérence

Les premiers travaux sur l'application de l' ACI en télédétection optique ont été orientés vers la recherche d'une solution au problème des pixels mixtes [26].

Ces travaux ont proposé d'extraire les membres extrêmes et d'estimer leurs signatures spectrales ainsi que leurs fractions (appelé fractions d'abondance), en utilisant seulement les données observées (pixels mixtes), d'où l'intérêt d'utiliser l' ACI. Les deux hypothèses de départ dans l'application de l' ACI dans ces travaux sont : 1) le contenu de chaque pixel mixte est considéré comme étant un mélange linéaire des réponses spectrales (sources) des membres extrêmes, dont les coefficients sont les fractions d'abondance correspondantes ; 2) les sources sont supposées être statistiquement indépendantes.

La première hypothèse est vérifiée puisque la dispersion multiple entre les membres extrêmes distincts est négligeable et la surface du pixel est partagée entre les abondances partielles propres aux membres extrêmes.

Cependant, la deuxième hypothèse est inadmissible due aux contraintes physiques du procédé d'acquisition. En fait, la somme des fractions d'abondance associées à chaque pixel mixte est

constante et, par conséquent, les réponses spectrales (sources) des membres extrêmes, qui constituent le mélange linéaire, ne peuvent pas être statistiquement indépendantes [27] En d'autres termes, ces travaux sont principalement concentrés sur la séparation de sources (réponses spectrales des membres extrêmes).

La quantification d'abondance des sources est timidement abordée et exige plus de développement. Le problème important de la détermination du nombre de sources à séparer était aussi absent dans ces travaux. Ce problème demeure non résolu et il est d'intérêt dans la communauté de traitement du signal.

III.7.Les architectures d'ACI

L'architecture 1 pour trouver des images de base statistiquement indépendantes (la séparation des images de visages produit des images composantes indépendantes), et l'architecture 2 pour trouver un code factoriel (la séparation des pixels produit un code factoriel)

La représentation d' ACI est constituée des coefficients **b** de la combinaison linéaire des images de base **U** qui forment chaque image de visage.

Le n Il est supposé que les signaux sources sont indépendants les uns des autres et le mélange Une matrice est inversible. Sur la base de ces hypothèses et les mélanges observés, l'ACI algorithmes essaient de trouver la matrice de mélange **A** ou les séparant **W** de la matrice telle que :

$$\boldsymbol{U = W.X = W.A.S} \qquad \textbf{(IV.24)}$$

ombre de composantes indépendantes extraites par l'algorithme d' ACI est égal à la dimension de l'entrée (le nombre d'images d'apprentissage), et si on veut contrôler ce nombre, au lieu d'exécuter ACI sur les n images originales, on l'exécute sur un ensemble de **m** combinaisons linéaires de ces images, où **m** < **n**. Communément, on choisi pour ces combinaisons linéaires un sous ensemble formé des premières composantes principales de la matrice de donnée, ainsi l' exécution d' ACI sur l'ensemble de ces **m** composantes principales produit **m** images sources $\mathbf{U_i}$ statistiquement indépendantes.

Dans cette première architecture d' ACI, les images de base $\mathbf{U_i}$ sont statistiquement indépendantes, mais les coefficients $\mathbf{b_i}$ ne le sont pas. Au lieu de séparer les images de visages en ensembles d'images indépendantes, il existe une deuxième architecture d' ACI, dans laquelle les coefficients sont statistiquement indépendants, en séparant les pixels en un ensemble de variables indépendantes codant les images.

III.6. Analyse en Composantes Indépendantes :

ACP est une technique optimale de recherche de représentation réduite qui minimise l'erreur de reconstruction, cependant les vecteurs de base tenant compte de l'erreur de reconstruction peuvent ne pas être optimaux pour coder l'information appropriée de l'image à la classification. L'analyse en composantes indépendantes (ACI) est une généralisation de ACP qui utilise en plus des statistiques d'ordre 2, les statistiques d'ordre plus supérieur, ce qui paît produire une représentation de données plus puissante [16].

Le but d' ACI est de trouver des vecteurs de base (images de base) localisés dans l'espace et qui sont statistiquement indépendants, en réduisant au minimum la dépendance statistique.

Avant l'apprentissage, on soustrait l'image moyenne des images d'apprentissage X et on les filtre par un filtre de blanchiment pour supprimer les statistiques d'ordre 1 et 2 (la moyenne et les covariances sont mises à zéro et les variances sont égalisées),pour trouver un ensemble d'images composantes indépendantes, les images d'apprentissage X sont considérées comme étant une combinaison linéaire d'images de base statistiquement indépendantes S, où A est une matrice de mixage inconnue. Les images de base sont retrouvées par une matrice de filtre d'apprentissage Wi = W * Wz. qui produit des sorties U statistiquement indépendantes. Ces images de base sont considérées comme un ensemble de caractéristiques faciales statistiquement indépendantes, où les valeurs des pixels de chaque image caractéristique sont statistiquement indépendantes des valeurs des pixels des autres images caractéristiques [17].

$$\boldsymbol{X = A.S} \qquad \textbf{(IV.23)}$$

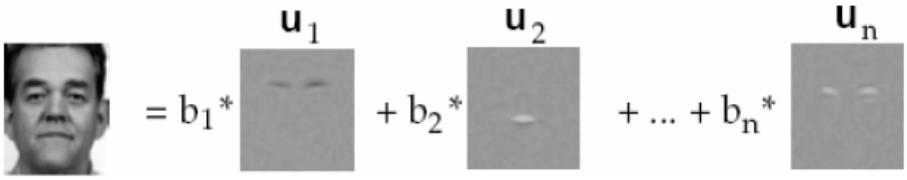


Figure 3. 7: La représentation d' ACI = (hl, b2,…… bn)

III.5.Conclusion :

L’analyse en composantes principales est une excellente approche pour explorer la structure des données en tenant compte de leur caractère multidimensionnel. Cette méthode est l’origine de la plupart des méthodes descriptives multidimensionnelles. Elle sert à mieux connaitre les données sur lesquelles on travaille en construisant de nouvelles variables artificielles et fournit des représentations graphiques qui permettent de visualiser des liaisons entre les variables.

La reconnaissance des visages par l’approche Eigenfaces, est très utilisée pour des raisons de sécurité, utilisée par la institutions policière, agents d’immigration, dans les prisons et pour permettre à une personne l'accès à une zone sécurisée.

Chaque visage (moins la moyenne) sera représenté comme étant une combinaison linéaire des K vecteurs propres choisis.

$$\hat{\phi}_i - \psi \text{ (moyenne)} = \sum_{j=1}^{k} w_j u_j \qquad \text{où} \qquad w_j = u_j^T \phi_i \qquad \textbf{(III.20)}$$

Donc chaque visage d'apprentissage ϕ_i sera représenté dans l'espace comme suit :

$$\Omega_i = \left[w_1^i, w_1^i, \dots, w_k^i\right]^T \quad i = 1,2, \dots, M \qquad \textbf{(III.21)}$$

Ayant une image Γ à tester en main, on suit les étapes suivantes :

- On détermine $\Gamma - \psi$ (moyenne)
- On projette notre image dans le nouvel espace

$$\hat{\phi} = \sum_{j=1}^{k} w_j u_j \qquad \text{où} \qquad w_j = u_j^T \phi_i \qquad \textbf{(III.22)}$$

- On représente ϕ comme $\Omega = (w_1, w_2, \dots, w_k)$
- On cherche la distance entre le visage à reconnaitre et les visages de la base de données et on prend la plus petite.

Si je prend la première image parmi les 10 suivantes :



On trouve avec MATLAB

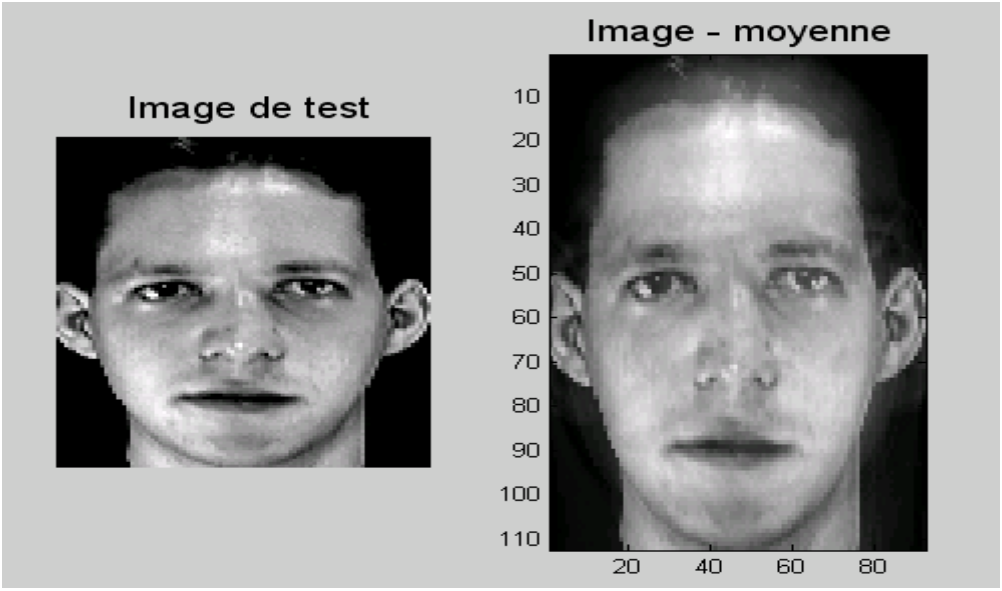


Figure 3.6 : image moyenne

g) On détermine les vecteurs propres u_i de la matrice C.

Cette matrice est très grande donc non praticable, à ce niveau, nous allons procéder à une déviation qui nous permettra de détourner le problème.

Considérons la matrice $A^T A$ ($M \times M$), si on essaye de calculer les valeurs propres de cette dernière, on remarquera que ce sont les mêmes que celles de la matrice C. De plus il existe un lien entre les vecteurs propres de chacune des deux matrices qui est le suivant: $u_i = Av_i$.

On notera que pour la matrice AA^T on aura N^2 valeurs et vecteurs propres. Et pour la matrice $A^T A$ on aura M valeurs et vecteurs propres.

Ainsi, les M valeurs propres de $A^T A$ correspondent aux M plus grandes valeurs de la matrice AA^T (en correspondance avec leurs vecteurs propres).

Notons que les vecteurs u_i doivent être normalisés ($\|u_i\| = 1$).

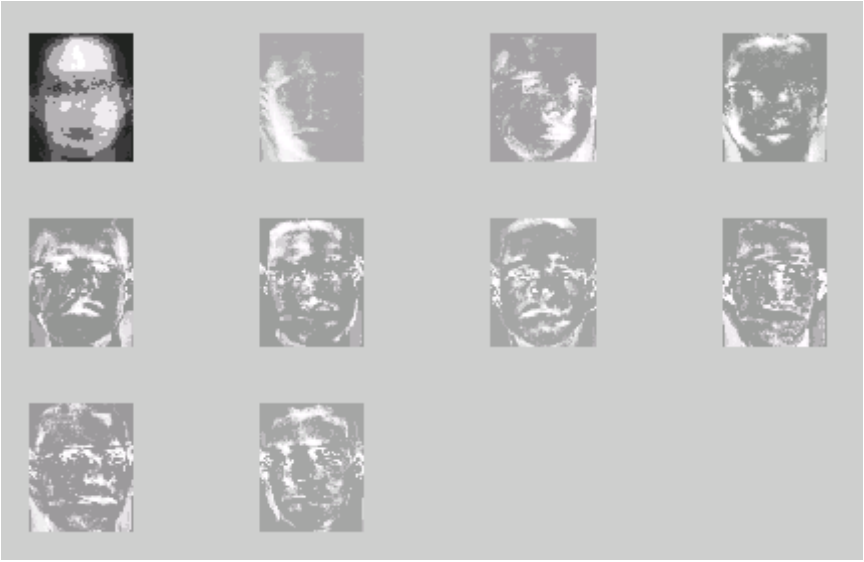


Figure 3.5 : Les 10 premiers vecteus propres

h) Cette étape est assez simple à réaliser, elle consiste à prendre K vecteurs propres correspondant aux K plus grandes valeurs propres.

Une fois les vecteurs bases trouvés, il ne reste plus qu'à déterminer la représentation des visages dans notre nouvel espace, pour cela on procède comme suit :

par exemple si $I_1 = \begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix}$ on aura $\Gamma_i = \begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \end{pmatrix}$

d) On cherche la moyenne de toutes les images, en d'autres termes on enlève tous ce qui est commun aux individus.

$$\psi_{moy} = \frac{1}{N}\sum_{i=1}^{N} I_i \quad \textbf{(III.17)}$$

Par exemple la moyenne de l'image présentée plus haut est :



La moyenne des 10 premières images



est :



Figure 3.4 : Exemple de visage moyenne

e) On construit la matrice $\phi_i = \Gamma_i - \psi_{moy}$ **(III.18)**

f) On construit la matrice covariance C, c'est tout simplement une matrice d'image modifiées. Elle représente l'interaction entre les individus.

$$C = \frac{1}{M}\sum_{n=1}^{M} \phi_n \phi_n^T = AA^T \quad \text{où} \quad A = (\phi_1, \phi_2, \dots, \phi_M)\ (N^2 \text{x} M) \quad \textbf{(III.19)}$$

III.4.1.Les différentes étapes :

a) on construit une base de données avec des images de références, ces images doivent être centrées et de même taille.



Figure 3.3 : base de données avec des images de références

b) Chaque image est représenté par un vecteur I_i contenant des pixels.

$$I_i = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \quad \text{ou} \quad 1 \leq a_{ij} \leq 255 \qquad \textbf{(III.15)}$$

c) Chaque image sera traité comme un tableau à une dimension pour Matlab.

$$\Gamma_i = \begin{pmatrix} a_{11} \\ \vdots \\ a_{m1} \\ \vdots \\ a_{1n} \\ \vdots \\ a_{mn} \end{pmatrix} \qquad \textbf{(III.16)}$$

- ***Test de sphéricité (de Bartlett) :*** tester l'hypothèse que les $(p-k)$ dernières valeurs propres sont identiques. H_0^k: $\lambda_{k+1} = \lambda_{k+2} = \cdots = \lambda_p$. introduire toutes les autres valeurs propres. En pratique, on teste successivement H_0^k à partir de $k = 0$ et on s'arrête à la valeur propre λ_k. dès que n'est pas H_0^k rejetée. La variable de décision pour ce test est :

$$d^k = \left(n - \frac{2p+11}{6}\right)(p-k)ln\left(\frac{a_k}{g_k}\right) \quad \textbf{(IV.12)}$$

Où:

- a_k est la moyenne arithmétique des dernières valeurs propres

$$a_k = \frac{\lambda_{k+1}+\lambda_{k+2}+\cdots+\lambda_p}{p-k} \quad \textbf{(IV.13)}$$

- g_k est la moyenne géométrique des dernières valeurs propres

$$g_k = \sqrt[p-k]{\lambda_{k+1}\lambda_{k+2}\ldots\lambda_p} \quad \textbf{(IV.14)}$$

Sous H_0^k la variable de décision $d^k \sim \chi^2\left[\frac{(p-k+2)(p-k-1)}{2}\right]$ pour un échantillon suffisamment grand.

III.4.Analyse par eigenfaces

La reconnaissance de visages par Eigenfaces est une approche de type « image ». Chaque image de visage est considérée comme un vecteur dans un espace ayant autant de dimensions que de pixels dans l'image.

Le concept d'Eigenface a été introduit par TURK et PENTLAND en 1991 à des fins de reconnaissances de visages, basé sur l'analyse en composante principale, il utilise une représentation des éléments caractéristiques d'une image de visage à partir d'images modèles au niveau de gris. Autrement dit, chaque partie du visage correspond à une nuance de gris.

On prend un grand ensemble des images digitalisées des visages humains, prises dans les mêmes conditions d'éclairage, pour bâtir une base de données.

III.3.4.Nombre de composantes principales à retenir :

Combien de facteurs doit-on alors retenir? Le choix de facteurs constitue une décision souveraine de la part du chercheur. Voici quatre critères permettant de faire apparaître cette décision comme plus objective et moins arbitraire.

- ***Critère de Joliffe :*** s'arrêter dès que la proportion expliquée de la variance globale atteint une proportion fixée, par exemple 80%.

- ***Critère de Kaiser :*** ne garder que les valeurs propres $\lambda_1, \lambda_2, \dots, \lambda_k$ supérieures à la moyenne $\frac{\lambda_1+\lambda_2+\cdots+\lambda_p}{p}$. Si l'on travaille avec la matrice des corrélations, cela revient à exclure les valeurs propres inférieures à 1.

- ***Critère de Cattell :*** Faire le diagramme des valeurs propres consistant à représenter les λ_α en fonction de α. Souvent, un « coude » apparaît, marquant un changement de régime dans la décroissance des valeurs propres. Il faut alors garder que les valeurs propres avant l'apparition du coude. Par exemple, le diagramme des valeurs propres suivant, nous conduit à conserver que les deux premières valeurs propres.

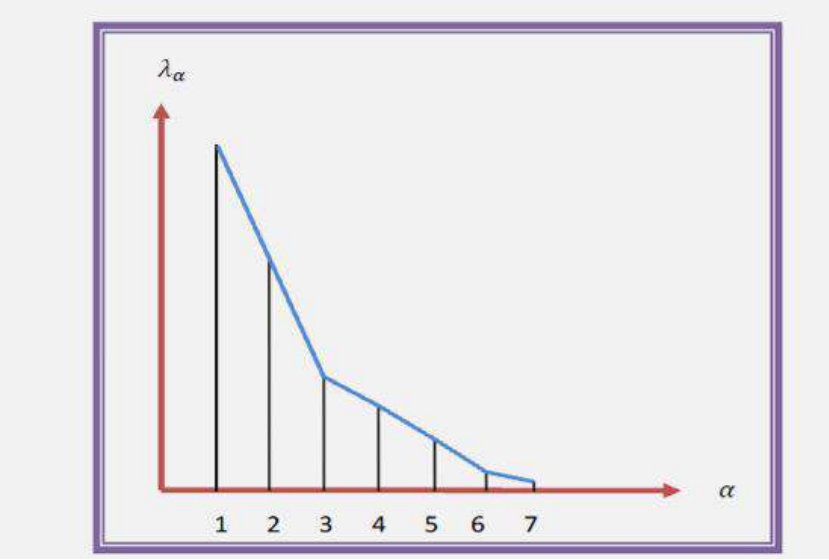


Figure.3.2.Valeur propres en fonction de α

En d'autres mots, il faut rejeter les valeurs propres formant la base de la falaise formée par la pente abrupte (formée par les valeurs propres 1 et 2).

La matrice des saturations de dimension est la matrice composée des saturations telle que

$$S = \begin{pmatrix} S_{11} & \cdots & \cdots & S_{1p} \\ S_{21} & \cdots & \cdots & S_{2p} \\ \cdots & \cdots & \cdots & \cdots \\ S_{p1} & \cdots & \cdots & S_{pp} \end{pmatrix} \quad \textbf{(IV.8)}$$

III.3.3.Variance totale expliquée et communalité :

La matrice possède les propriétés suivantes :

$$\sum_{\alpha=1}^{p} S_{j\alpha}^2 = 1 \qquad \text{et} \qquad \sum_{j=1}^{p} S_{j\alpha}^2 = \lambda_\alpha \quad \textbf{(IV.9)}$$

Donc

$$\sum_{\alpha=1}^{p} \sum_{j=1}^{p} S_{j\alpha}^2 = \sum_{\alpha=1}^{p} \lambda_\alpha = p \quad \textbf{(IV.10)}$$

Puisque $var\left(X_j^2\right) = 1$pour$j = 1,2, \dots, p$. D'autre part, la variance totale contenue dans les p facteurs vaut également p .

L'application de l'ACP mène à une condensation de l'information, on ne conservera alors, que les k premiers facteurs$(k < p)$, tels que $var(f_\alpha) = \lambda_\alpha$ est plus grande. La proportion de la variance totale expliquée par les k premiers facteurs est :

$$\frac{\lambda_1+\lambda_2+\cdots+\lambda_k}{\lambda_1+\lambda_2+\cdots+\lambda_p} = \text{(un pourcentage)}$$

Cette quantité représente la mesure globale de la qualité de l'ACP. Ainsi, en ne conservant que les premiers facteurs, la quantité

$$h_j^2 = \sum_{\alpha=1}^{k} S_{j\alpha}^2 \qquad j = 1,2, \dots, p \quad \textbf{(IV.11)}$$

Nommée communalité (ou communauté) est inférieure à 1 $\left(h_j^2 = 1 \; si \; k = p\right)$.

La communalité est la proportion de variance d'une variable expliquée par les k premiers facteurs. La communalité est donc une mesure de la qualité d'une ACP spécifique pour chacune des p variables.

sphéricité de Bartlett nous confirme que les variables sont suffisamment corrélées, nous procédons à appliquer l'ACP.

La matrice R des corrélations est une matrice symétrique et semi-définie positive. Ainsi par la décomposition spectrale, elle peut être écrite comme suit :

$$R = U\Lambda U' \quad \textbf{(IV.3)}$$

où Λ est la matrice des valeurs propres ordonnées telles que $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_p \geq 0$ avec

$$\Lambda = \begin{pmatrix} \lambda & 0 & \dots & 0 \\ 0 & \lambda & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \lambda \end{pmatrix} \quad \textbf{(IV.4)}$$

Et $U(pxp) = (u_1|u_2|\dots|u_p)$, est la matrice des vecteurs propres associés aux valeurs propres. Les p vecteurs propres de R chacun de norme unité et tous orthogonaux entre eux.

III.3.2.Composantes principales

L'ACP consiste à trouver *p* facteurs au départ et de n'en garder que *k (k ≤ p).* L'utilisation du théorème de décomposition spectrale appliqué à la matrice des corrélations permet de trouver ces *p* facteurs qui sont de la forme suivante :

$$f_\alpha = u_{1\alpha}X_1^s + u_{2\alpha}X_2^s + \cdots + u_{p\alpha}X_p^s = \sum_{j=1}^{p} u_{j\alpha}X_j^s \qquad \alpha = 1,2,\dots,p \quad \textbf{(IV.5)}$$

où $X_1^s, X_2^s, \dots, X_p^s$ sont les *p* variables standardisés.

La matrice $F(n,p) = X^s U$ est la matrice des scores factoriels, formée des n composantes de chaque facteur $f_\alpha \quad \alpha = 1,2,\dots,p$ et peut être écrite comme suit :

$$F = (f_1|f_2|\dots|f_p) \quad \textbf{(IV.6)}$$

la matrice X_s des scores standardisés s'obtient en soustrayant à chaque observation le score moyen et en divisant par l'écart-type de chaque variable (en colonne). Pour pouvoir interpréter les facteurs et les nommer, il faut déterminer les corrélations entre les variables et les facteurs appelées également saturations notées par :

$$S_{j\alpha} = corr(X_j, f_\alpha) = corr(X_{j\alpha}^s, f_\alpha) \qquad j,\alpha = 1,2,\dots,p \quad \textbf{(IV.7)}$$

III.3. Étapes de l'analyse en composantes principales :

Avant de procéder à une ACP, une petite inspection des corrélations entre les variables est conseillée :

Si, au départ, les corrélations entre les variables sont trop faibles, il est inutile de procéder à une ACP, car les facteurs obtenus seraient alors très proches des variables originales.

Si, au contraire, deux variables sont très corrélées, il vaut peut-être mieux en éliminer une des deux avant de procéder à l'ACP.

De plus, il faut vérifier que les liaisons entre les variables soient à-peu-près linéaires, ce dont on peut s'assurer en produisant les diagrammes de dispersion pour tous les couples de variables. Il ne doit pas avoir de courbure marquée, sinon il serait judicieux de tenter d'avoir des relations linéaires (au moyen de transformations de variables adéquates) et ce, avant de procéder à une ACP.

III.3.1. Matrice des corrélations :

Soit X_{nxp} une matrice contenant les observations suivantes :

$$X = \begin{pmatrix} x_{11} & \cdots & \cdots & x_{1p} \\ x_{21} & \cdots & \cdots & x_{2p} \\ \cdots & \cdots & \cdots & \cdots \\ x_{n1} & \cdots & \cdots & x_{np} \end{pmatrix} \quad \textbf{(IV.1)}$$

Où x_{ij} est la valeur de l'individu i pour la variable j.

La première étape consiste à trouver la matrice R des corrélations définies ainsi :

$$R = \begin{pmatrix} 1 & r_{21} & \cdots & r_{1p} \\ r_{21} & 1 & \cdots & r_{2p} \\ \cdots & \cdots & \cdots & \cdots \\ r_{p1} & r_{p2} & \cdots & 1 \end{pmatrix} \quad \textbf{(IV.2)}$$

où $r_{ij} = \mathrm{corr}(X_i, X_j)$ est le coefficient de corrélation entre les variables X_i et X_j.

Pour juger de l'existence de corrélations suffisantes entre les variables, nous utiliserons le test de sphéricité de Bartlett lequel consiste à comparer la matrice des corrélations avec l'identité en utilisant un test de Khi-deux. Une valeur élevée avec une signification proche de nulle, permet de rejeter la non-corrélation globale des variables. De ce fait, on s'assure alors, que les variables sont suffisamment corrélées entre-elles pour permettre une réduction significative de la dimension qui est une condition indispensable pour faire une ACP. Une fois, le test de

III.2. Utilisation de l'ACP pour la reconnaissance des visages :

L'analyse en composantes principales est un ensemble de méthodes qui permettant de procéder à des transformations linéaires d'un grand nombre de variables intercorrélées de manière à obtenir un nombre relativement limité de composantes non corrélées. Cette approche facilite l'analyse en regroupant les données en des ensembles plus petits et en permettant d'éliminer les problèmes de multi colinéarité entre les variables.

Etant donné un ensemble d'observations décrites par des variables exclusivement numériques

$$\{X_1, X_2, \ldots, X_p\},$$

l'ACP a pour objectif de décrire ce même ensemble de données par de nouvelles variables en nombre réduit. Ces nouvelles variables seront des combinaisons linéaires des variables originales, et porteront le nom de Composantes Principales (CP).

En général, la réduction du nombre de variables utilisées pour décrire un ensemble de données provoque une perte d'information. L'ACP procède de façon à ce que cette perte d'information soit la plus faible possible, selon un sens précis et naturel que l'on donnera au mot "information".

L'Analyse en Composantes principales peut donc être vue comme une technique de réduction de dimensionnalité.

Bien que l'objectif soit en général de n'utiliser qu'un petit nombre de Composantes Principales, l'ACP en construit initialement$p$, autant que de variables originales. Ce n'est que par la suite que l'analyste décidera du nombre de Composantes à retenir. "Retenir k Composantes Principales" veut dire "Remplacer les observations originales par leur projections orthogonales dans le sous-espace à k dimensions défini par les k premières Composantes Principales.".

III.1.Introduction :

Étant donnée une image de visage, on souhaite déterminer l'identité de la personne correspondante. Pour ce faire, il est nécessaire d'avoir des images de référence, sous la forme d'une base de données de visages de toutes les personnes connues par le système a chaque visage est associé un vecteur de caractéristiques, ces caractéristiques sont supposées être invariantes pour une même personne, et différentes d'une personne à l'autre, la reconnaissance consiste alors à comparer le vecteur de caractéristiques du visage à reconnaître avec celui de chacun des visages de la base. Ceci permet de retrouver la personne ayant le visage le plus ressemblant, qui est celui dont le vecteur est le plus similaire.

Il existe plusieurs types de méthodes, qui se distinguent par le type de caractéristiques utilisées

- Les approches par modèles de visage procèdent à une analyse biométrique des visages pour déterminer des mesures telles que la distance entre les yeux, la longueur du nez, la forme du menton…
- Les approches « image » comparent au contraire directement les visages, en les considérant comme des images, pour lesquelles des mesures de similarité pré-attentives (sans modèle a priori) sont définies.
- Des approches hybrides utilisent les notions de similarité entre images, mais en rajoutant des connaissances a priori sur la structure d'un visage.

La méthode qu'on va traiter ici est la méthode eigenfaces qui est une approche « image ». Les caractéristiques de l'image sont extraites par une méthode mathématique de réduction de dimensionnalité basée sur l'analyse en composante principales (ACP).

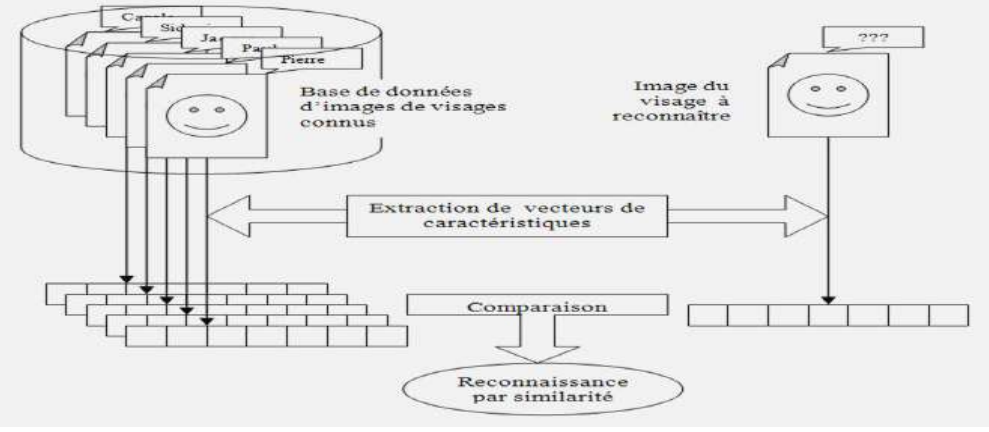


Figure 3.1 : principe général d'un système de reconnaissance de visage

IV.11.)Conclusion

Dans ce chapitre on a trouvé que l'algorithme étudiée (ACI) est une amélioration de (ACP). Et d'après les différents résultats obtenus, comme conséquence, l'architecture II (ACI II) est plus précisé que l'architecture I (ACI II).

IV.10.4Expériences 2 : pour L'ACI 2 avec une seuil =70

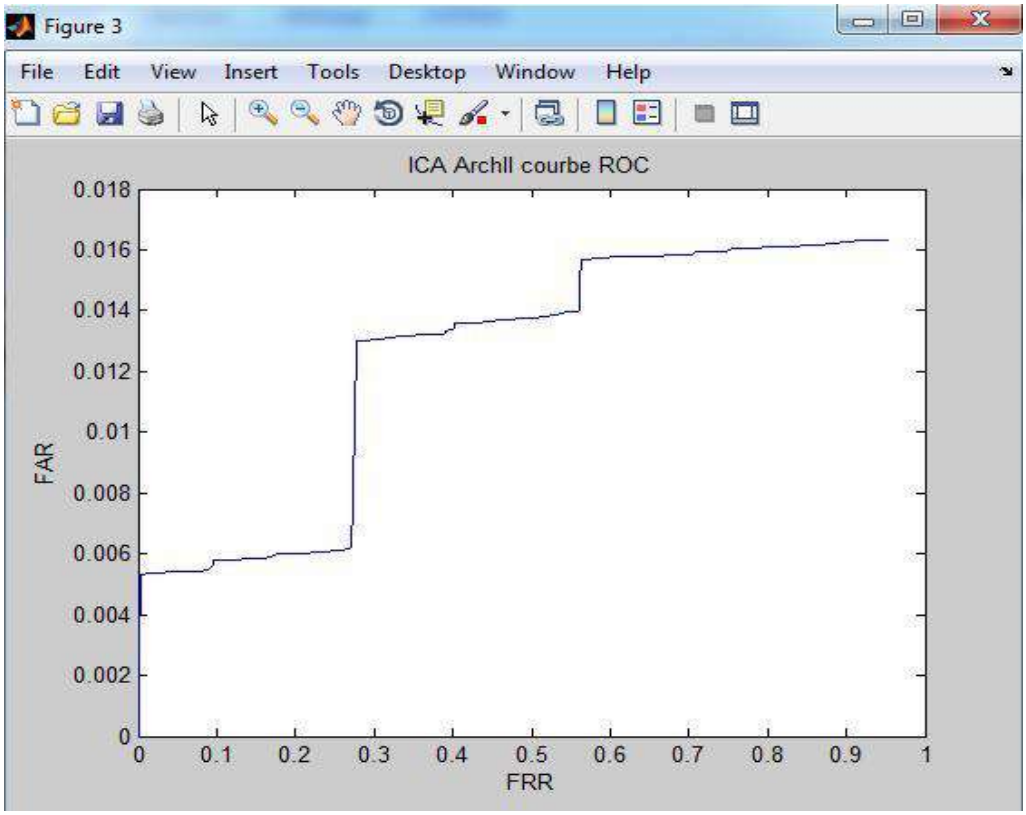


Figure.4.21.ACI Arch II courbe ROC Avec seuil 70

FRR%	**10**	**20**	**30**	**40**	**50**	**60**	**70**	**80**	**90**
FAR%	**0.41**	**0.6**	**0.61**	**1.3**	**1.34**	**1.4**	**1.52**	**1.6**	**1.62**

Tableau 4.7. Roc avec seuil =70

Le tableau 4.7. Définie ROC avec un seuil égale à 70, on remarque que si FAR=40% FRR=1.3% donc FAR<FRR donc le nombre des personnes acceptés plus grand ou nombre des personnes rejeté donc avec le seuil 70 on a un système de très grand sécurité.

IV.10.3.Expériences 1 : pour L'ACI 2 avec une seuil =60

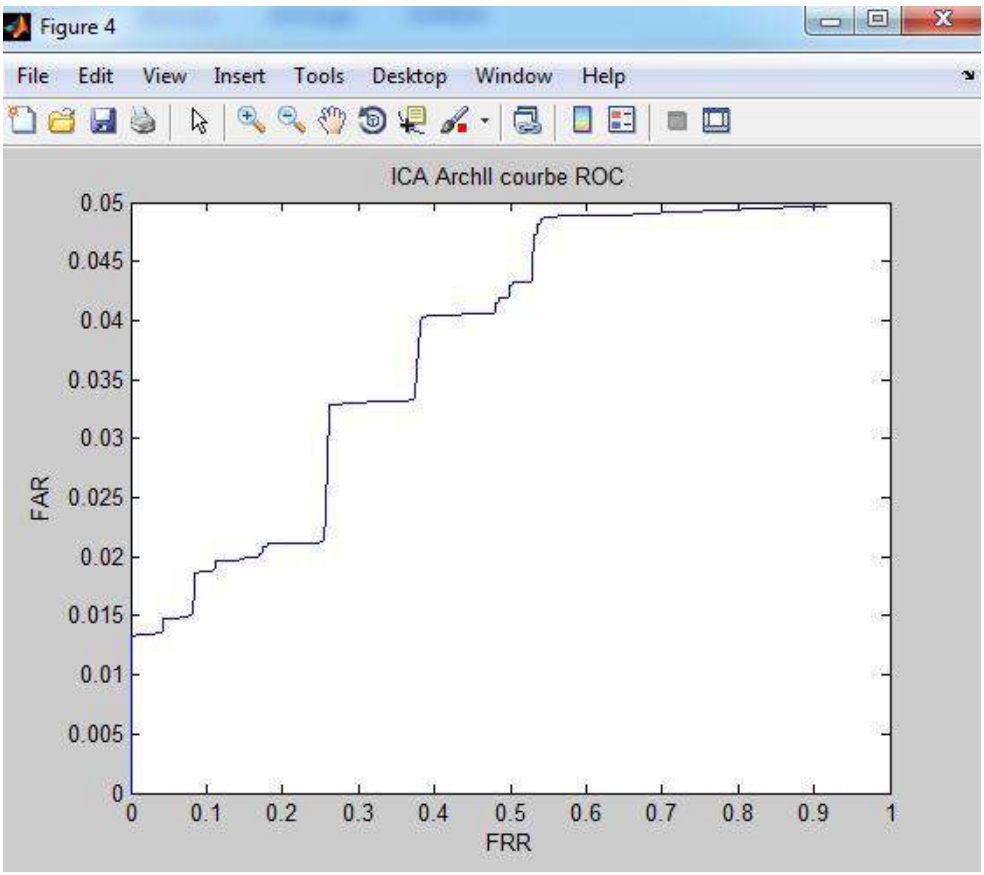


Figure.4.20.ACI Arch II courbe ROC Avec seuil 60

FRR%	**10**	**20**	**30**	**40**	**50**	**60**	**70**	**80**	**90**
FAR%	**1.5**	**2.2**	**2.3**	**3.4**	**4.1**	**4.5**	**4.55**	**0.57**	**0.59**

Tableau 4.6. Roc avec seuil =60

Le tableau 4.6. Définie ROC avec un seuil égale à 60, on remarque que si FRR=40% FAR=3.4% donc FAR<FRR donc le nombre des personnes acceptés plus grand ou nombre des personnes rejetés donc avec le seuil 60 on a un système de grand sécurité.

IV.10.2.Expériences 2 : pour L'ACI 1 avec une seuil = 0.0017

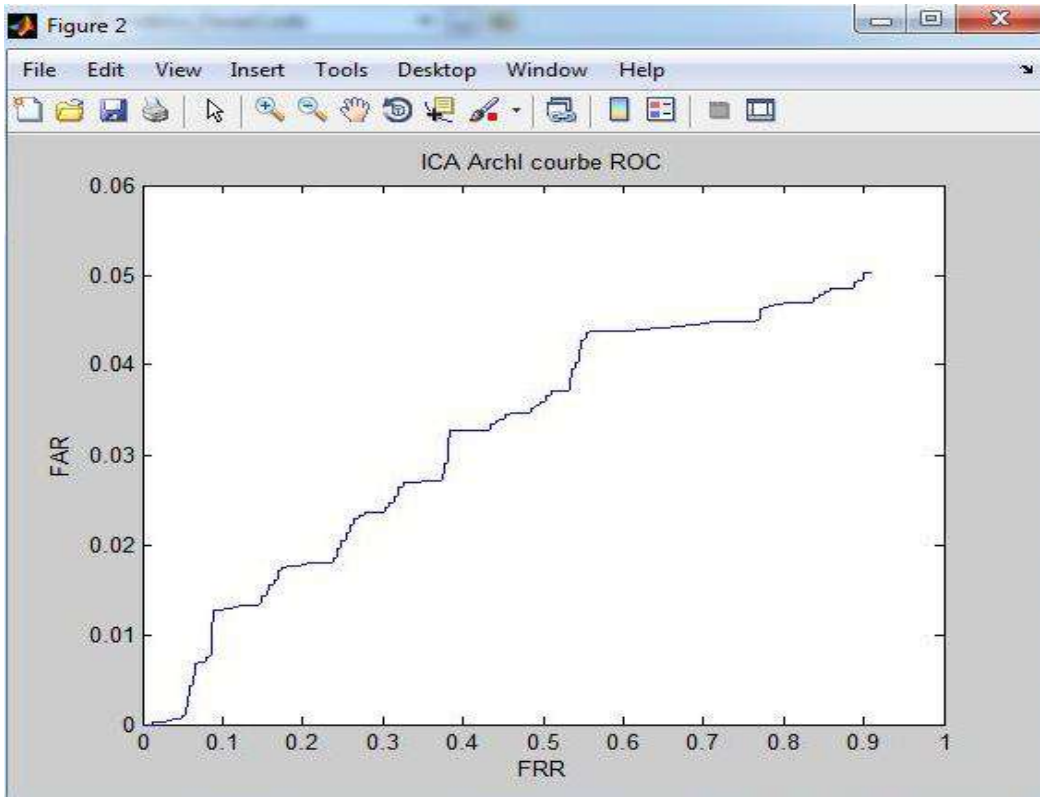


Figure.4.19.ACI Arch I courbe ROC Avec seuil 0.0017

FRR%	**10**	**20**	**30**	**40**	**50**	**60**	**70**	**80**	**90**
FAR%	**0.5**	**1.5**	**1.9**	**2.8**	**3.5**	**4.5**	**4.6**	**4.7**	**4.8**

Tableau 4.5. Roc avec seuil=0.0017

Le tableau 4.5. Définie ROC avec un seuil égale à 0.0017, on remarque que si FRR=40% FAR=2.8 %donc FAR<<FRR donc le nombre des personnes acceptés plus grand ou nombre des personnes rejeté donc avec le seuil 0.0017 on a un système de grand sécurité.

IV.10.Performance du system:

IV.10.1.Expérience 1 : pour L'ACI 1avec une seuil = 0.0013

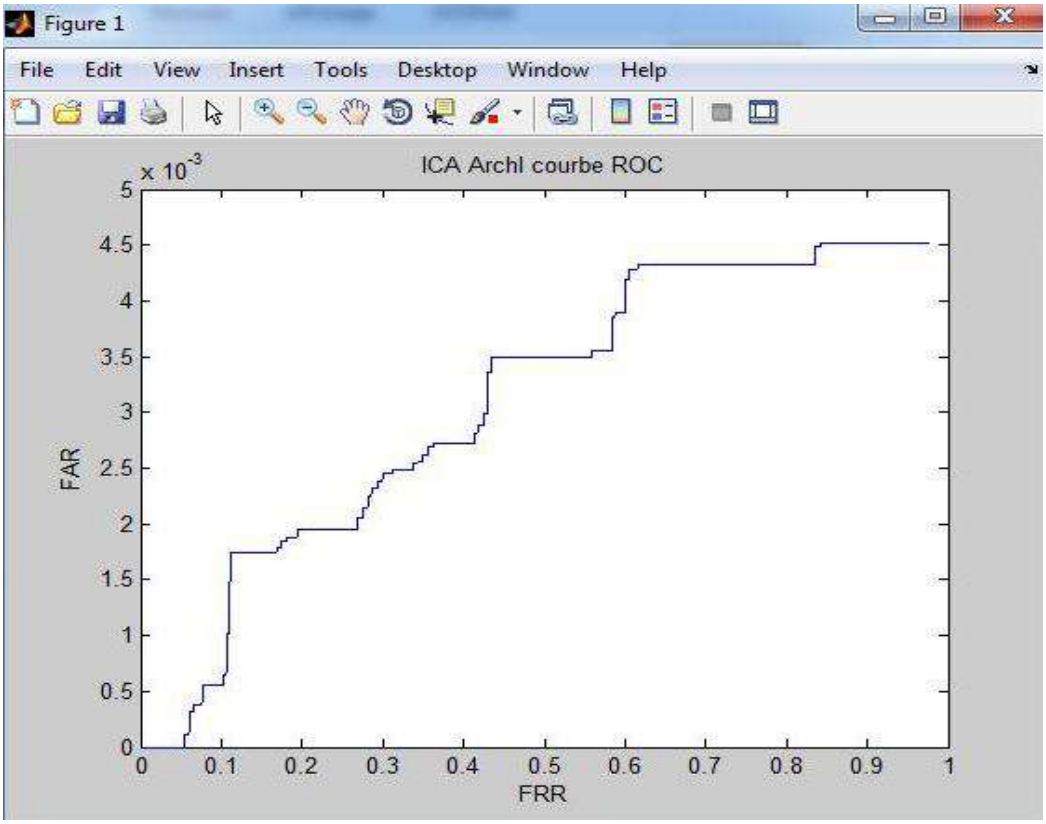


Figure.4.18.ACI Arch I courbe ROC Avec seuil 0.0013

FRR%	**10**	**20**	**30**	**40**	**50**	**60**	**70**	**80**	**90**
FAR%	**0.052**	**0.158**	**0.200**	**0.255**	**0.350**	**0.356**	**0.430**	**0.430**	**0.450**

Tableau 4.4. Roc avec seuil=0.0013

Le tableau 4.4. Définie ROC avec un seuil égale à 0.0013, on remarque que si FRR=40% FAR=0.255% donc FAR<<FRR donc le nombre des personnes acceptés plus grand ou nombre des personnes rejeté donc avec le seuil 0.0013 on a un système de très grand sécurité.

IV.8.3.Expérience 3 :

FAR	**10%**	**20%**	**30%**	**40%**	**50%**	**60%**	**70%**	**80%**
FRR	**0.1%**	**0.2%**	**0.3%**	**0.4%**	**0.6%**	**1.2%**	**1.4%**	**2.5%**

Tableau.4.3 Roc avec seuil=0.7

Le tableau 4.3 définie ROC avec un seuil égale à 0.7, on remarque que si FAR=40% FRR=0.4% donc FAR>>FRR donc le nombre des personnes acceptés plus grand ou nombres des personnes rejeté donc avec le seuil 0.7 on a un système de très grand sécurité.

IV.9.L'algorithme ICA :

En calcul la matrice de covariance pour l'apprentissage et pour le test :

C = matrice covariance pour l'apprentissage $C_{training}$ = <240x10304 double>

C=la matrice de covariance pour le test $C_{testing}$ = <160x10304 double>

IV.9.1.ICA I :

La représentation des images horizontalement pour l'apprentissage et le test dans une matrice F.

$Arch1_{Training}$ = <240x150 double>

Arch 1 $_{testing}$ = <160x150 double>

IV.9.2.ICA II:

La représentation des images verticalement pour l'apprentissage et le test dans une matrice F

$Arch2_{Training}$ = <240x150 double>

Arch 2 $_{testing}$ = <160x150 double>

On fait la comparaison entre les deux architectures (ICA I et ICA II) et utilise Performance du système.

IV.8.1. Expérience1;

FAR %	10 %	20 %	30 %	40%	50%	60%	70%	80%
FRR %	1 %	2 %	3 %	6 %	8 %	10 %	12 %	16 %

Tableau.4.1. ROC avec seuil =0.1

Le tableau 4.1 définie ROC avec un seuil égal à 0.1, on remarque que si FAR=0.5 FRR=0.08 donc FRR<FAR donc le nombre des personnes acceptés supérieur ou nombre des personnes rejeté donc avec le seuil 0.1 on a un système de faible sécurité.

IV.8.2.Expérience2 :

FAR	**5 %**	**10%**	**15%**	**20%**	**25%**	**30%**	**35%**	**40%**
FRR	**6%**	**12%**	**16%**	**25%**	**35%**	**40%**	**60%**	**70%**

Tableau.4.2. ROC avec seuil =0.29

Le tableau 4.2 définie ROC avec un seuil égale à 0.29 on remarque que si FAR=35% FRR=60% donc FAR>FRR donc le nombre des personnes rejetés supérieur ou nombre des personnes accepté donc avec le seuil 0.29 on a un système de faible sécurité.



Figure4.17:Résultat du système de vérification.

IV.8.Performance du système:

Pour notre application on utilise 40 personnes nommé s1…s40 et 10 visages nommé y1…y10 pour chaque personne. 240 visages pour l'apprentissage et 160 visages pour le test .pour reconnaitre les performances de ce système de reconnaissance (trace le courbe ROC) on va faire 38400 test de vérification.

Par exemple l'image X doit être testé avec tous les 80 images de la base de données, si le test avec l'image de la même colonne d'image X donc personne accepté(FA=FA+1) sinon le personne rejeté(FR=FR+1),dans le cas idéal on a le nombre des personnes accepté authentiques FA= [(10-6)*6*40]=960et le nombre des personnes rejeté imposteurs FR= [(240-6)*(10-6)*40]=37440,le taux de fausse acceptation FAR et le taux de false rejet FRR sont calculé par les formules suivantes.

$$FAR = \frac{\text{nb de FA}}{\text{nb des imposteur}} \qquad \textbf{(IV.3)}$$

$$FRR = \frac{\text{nb de FR}}{\text{nb des geniune}} \qquad \textbf{(IV.4)}$$



Figure4.15: Résultat authentique du système de vérification.



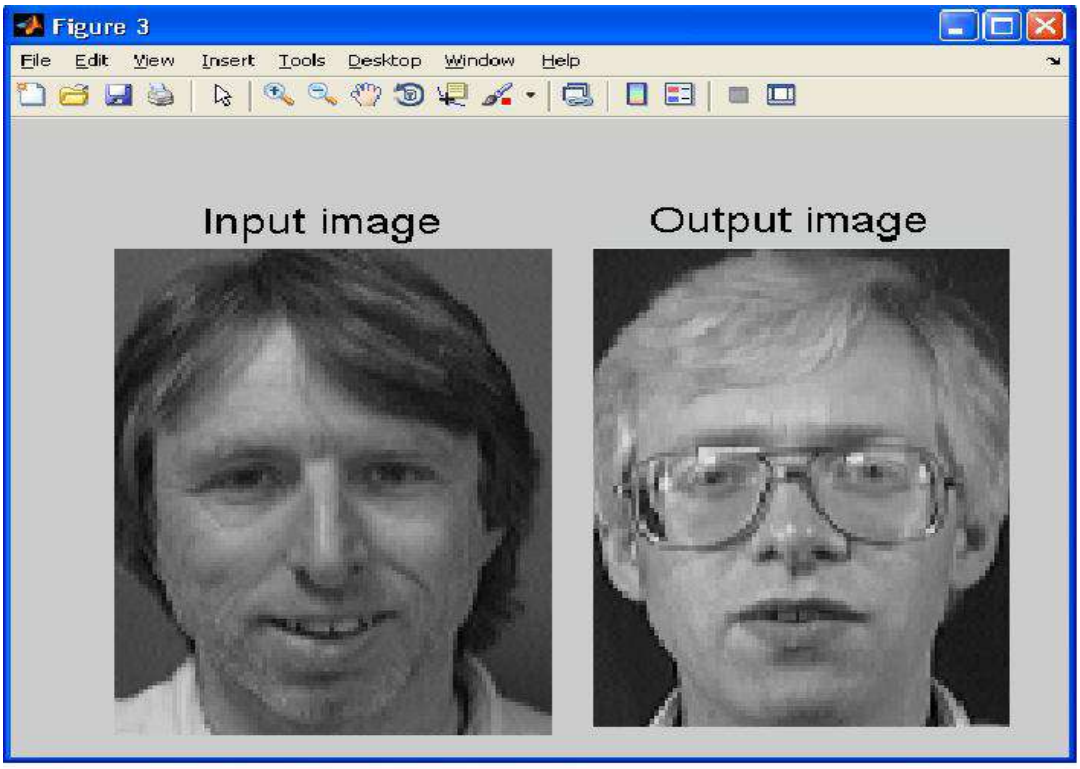


Figure 4.16 : Comparaison entre le visage d'entré et le visage de la base de donné.



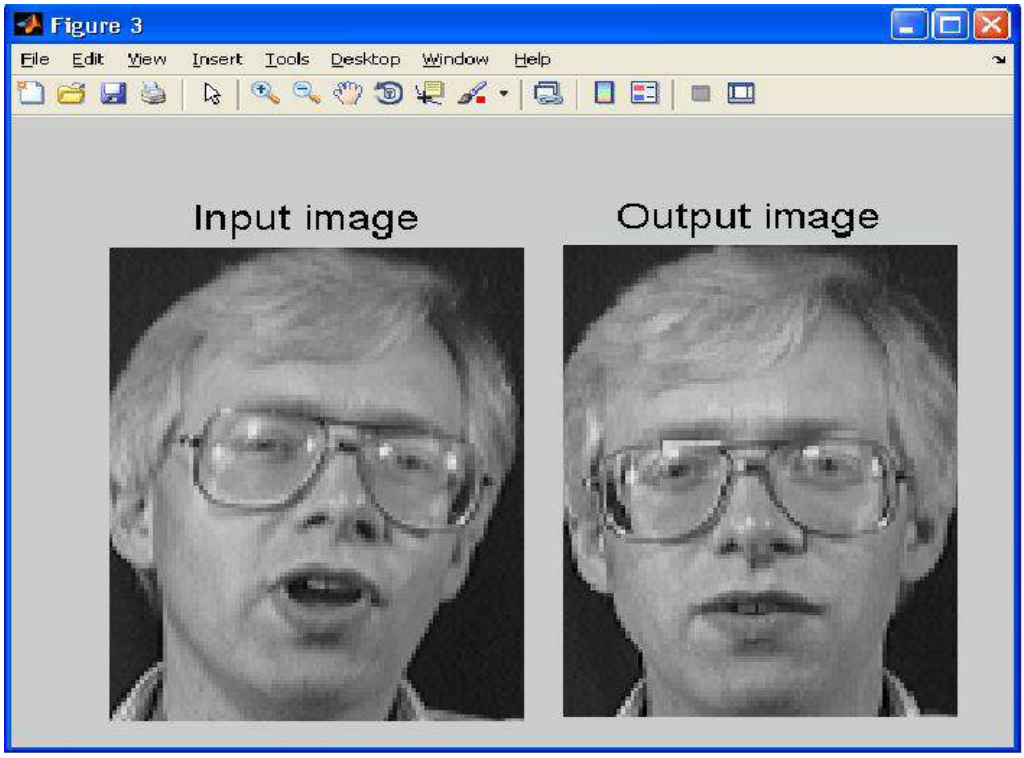


Figure 4.14 : Comparaison entre le visage d'entré et le visage de la base de donné.

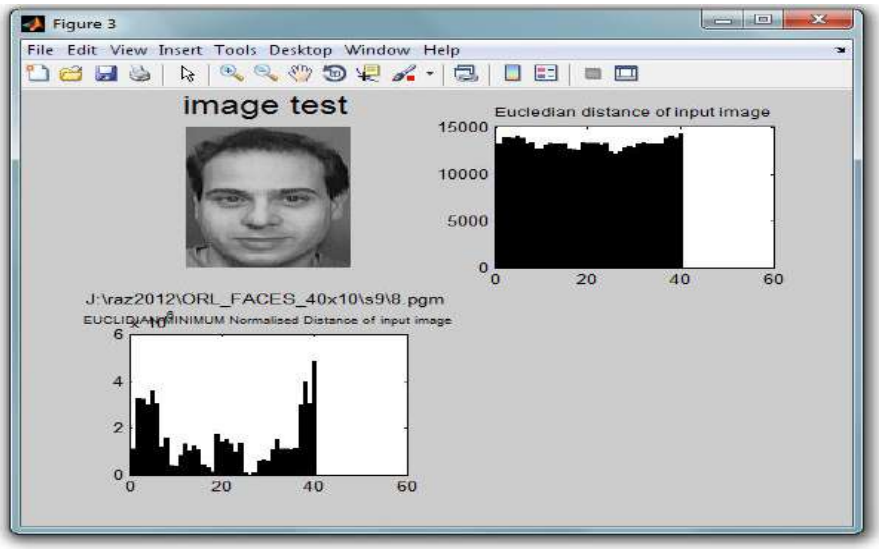


Figure 4.12 : personne non identifié.



Figure4.13: Résultat d'identification rejetée FR avec un seul égal à 0.6.

IV.7. Test de vérification :

Un système de vérification vérifie l'identité d'une personne en comparant la signature biométrique extraite avec son propre modèle biométrique préenregistré dans le système. Il effectue une comparaison un à un (on note généralement 1:1) pour déterminer si l'identité revendiquée par l'individu est vraie. Un système d'authentification accepte ou rejette la demande d'un utilisateur

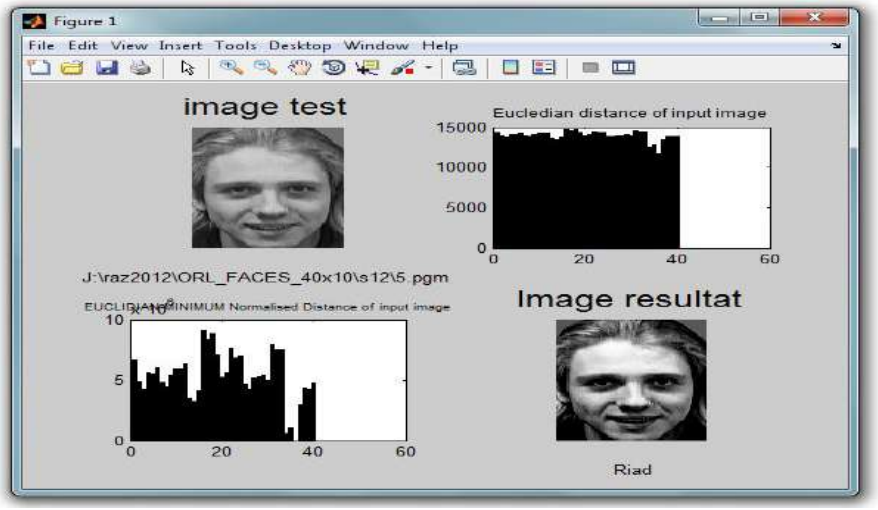


Figure 4.9: personne identifie.



Figure4.10 : Résultat d'identification de système.

Test 2

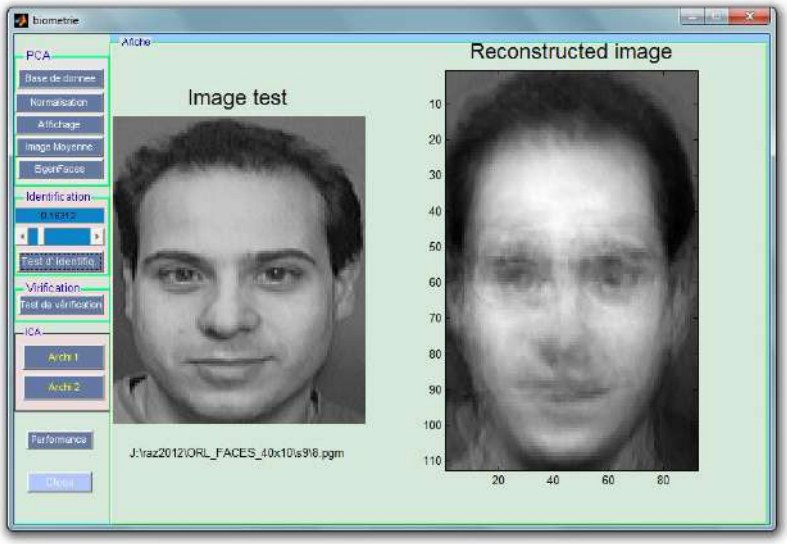


Figure 4.11 :l'image test et l'image construite par le système

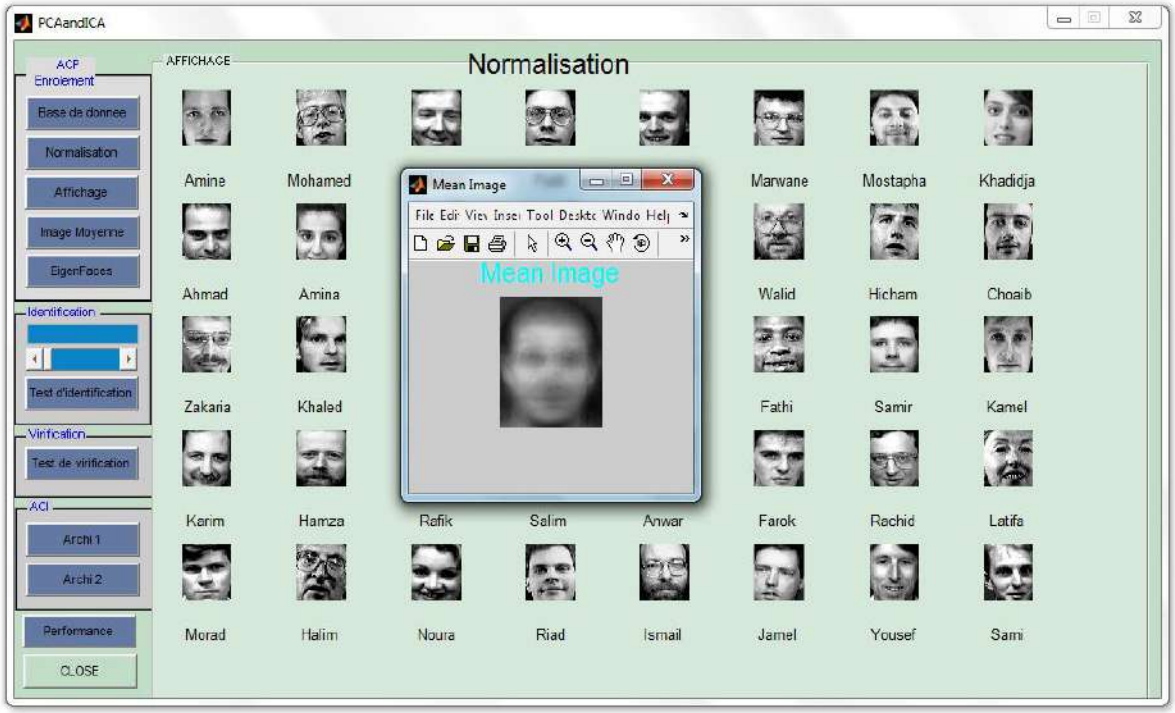


Figure4.7 l'image moyenne et les images normalisées.

IV.6. Test d'identification :

Avant de faire un test d'identification on choisir un seuil égal à 0.174, et ouvrir un fichier de visage à reconnaitre, et les figure suivant montre la procédure d'identification

Test 1 :

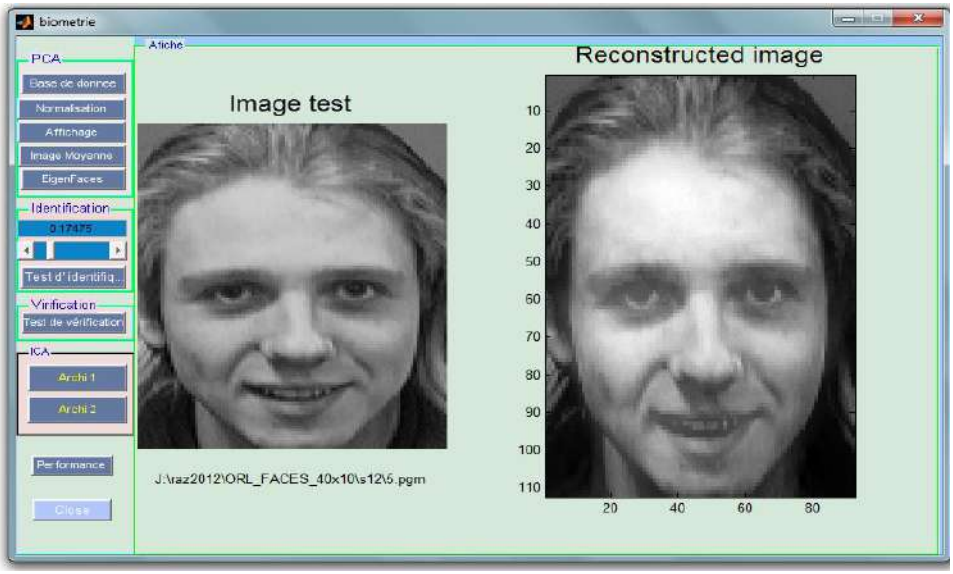


Figure 4.8 :l'image test et l'image construite par le système.

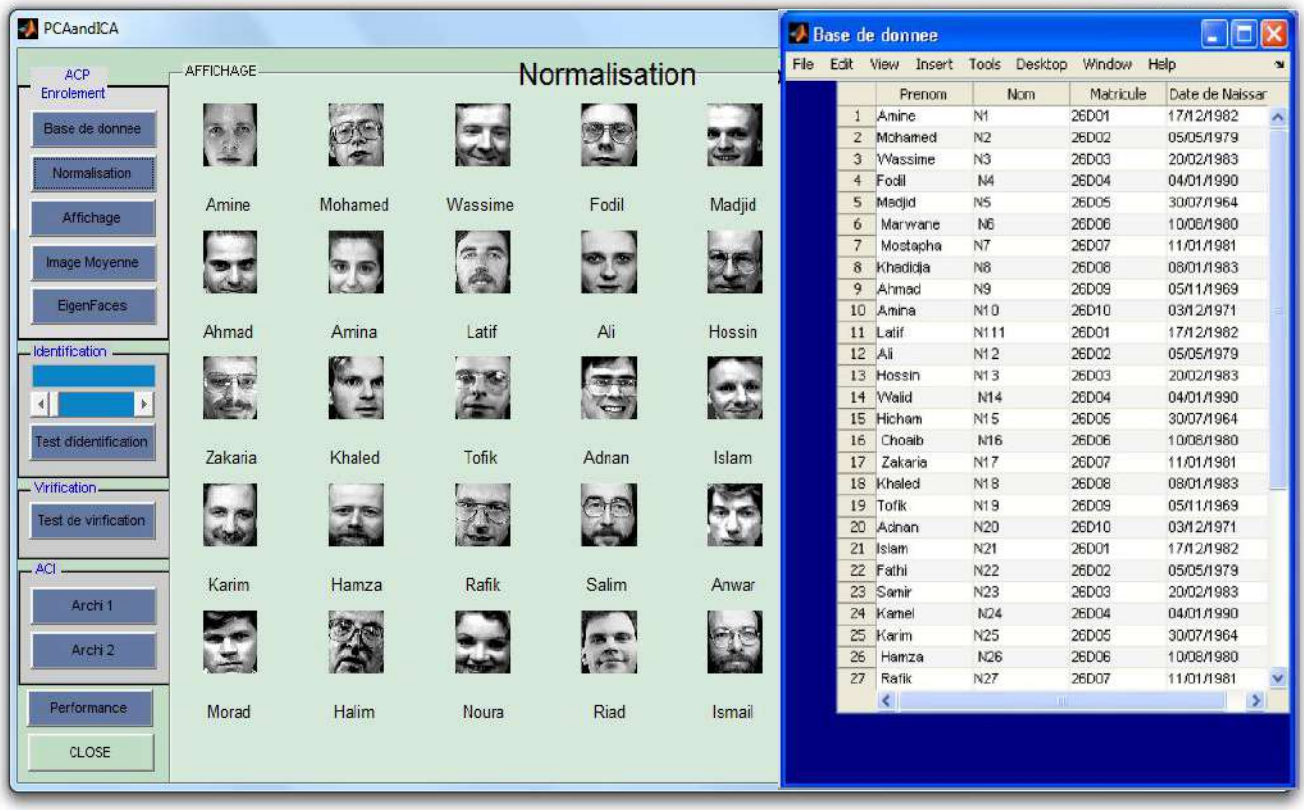


Figure .4.6. Affichage de la base des données ORL.

La prochaine étape consiste à calculer les vecteurs propres et les valeurs propres et affiche l'image moyenne et les 80eigenface.

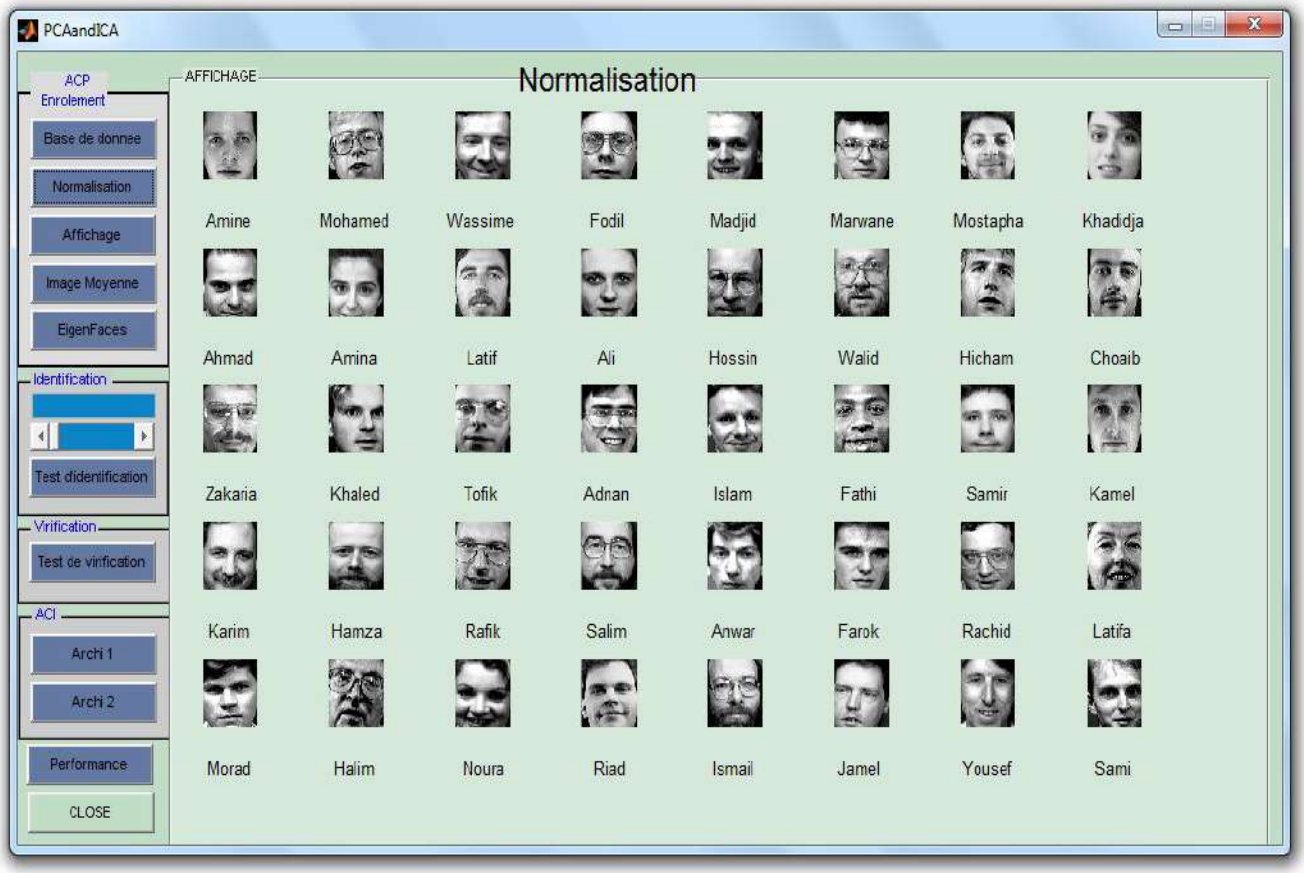


Figure .4.5 Normalisation de la base de données ORL.

On réduit la taille des images pour centré l'extraction d'information (figure5.3) et Pour la simplification on donne un nom, prénom, matricule et date de naissance à chaque personne (figure4.4).

IV.5.Algorithme ACP

IV.5. 1.Phase d'enrôlement

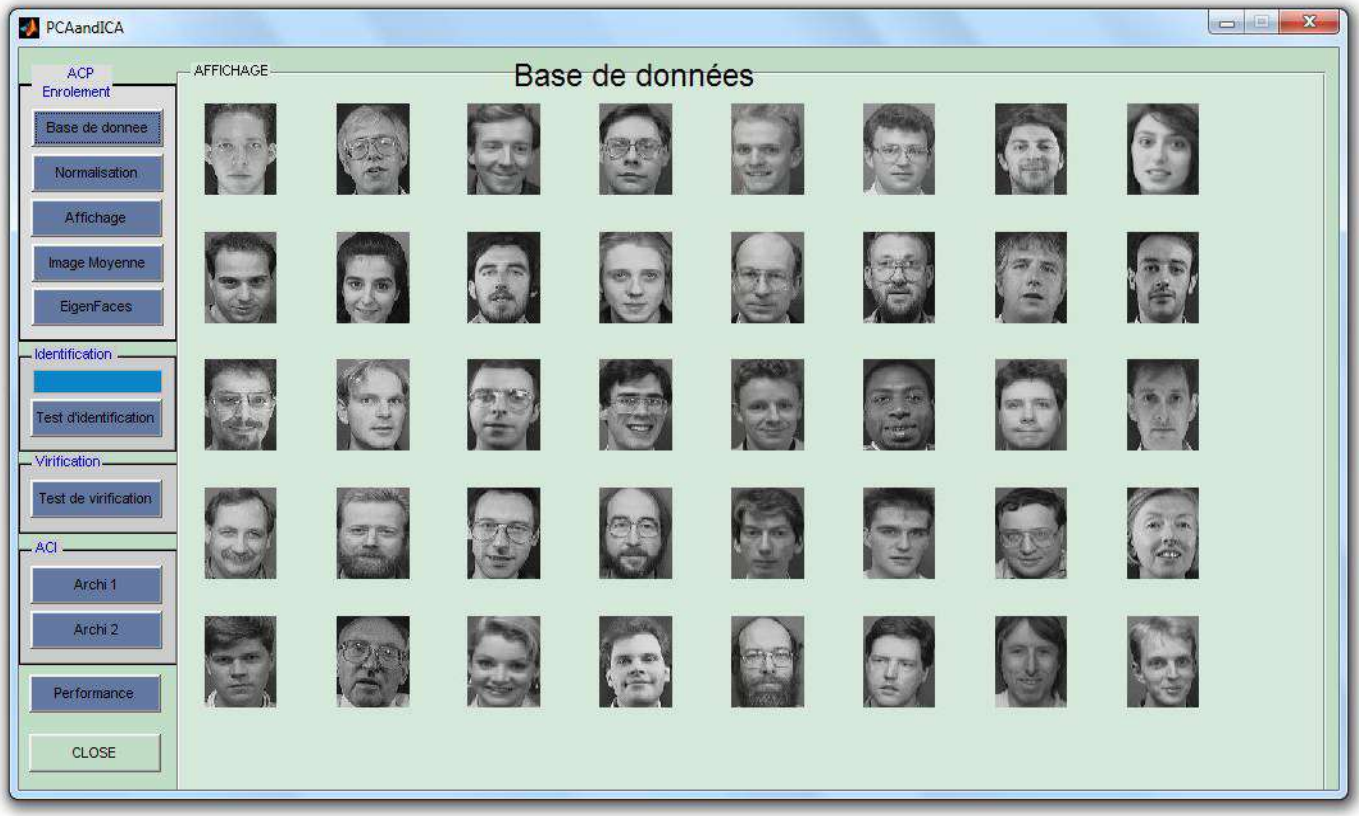


Figure4.4 : la base de données.

Pour l'apprentissage on utilise 6 images pour chaque personnes de la base, chaque image traitée comme un vecteur de 10304 (M=112*92) valeurs, puis rassemblé les 240images dans une unique matrice, nous obtenons une matrice d'images V (240*10304), où chaque colonne représente une image.

On calcule ensuite l'image moyenne Moy de toutes les images collectées, cette image peut être vu comme le centre de gravité du jeu d'images :

$$Moy = \frac{1}{M}\sum_{i=1}^{M} V_i \qquad \textbf{(IV.1)}$$

On ajuste ensuite les données par rapport à la moyenne. L'image moyenne est alors soustraite de chaque image avec la formule suivante

$$I\ moy_{i=}v_i - Moy \ \ ,i=1\ldots M \qquad \textbf{(IV.2)}$$

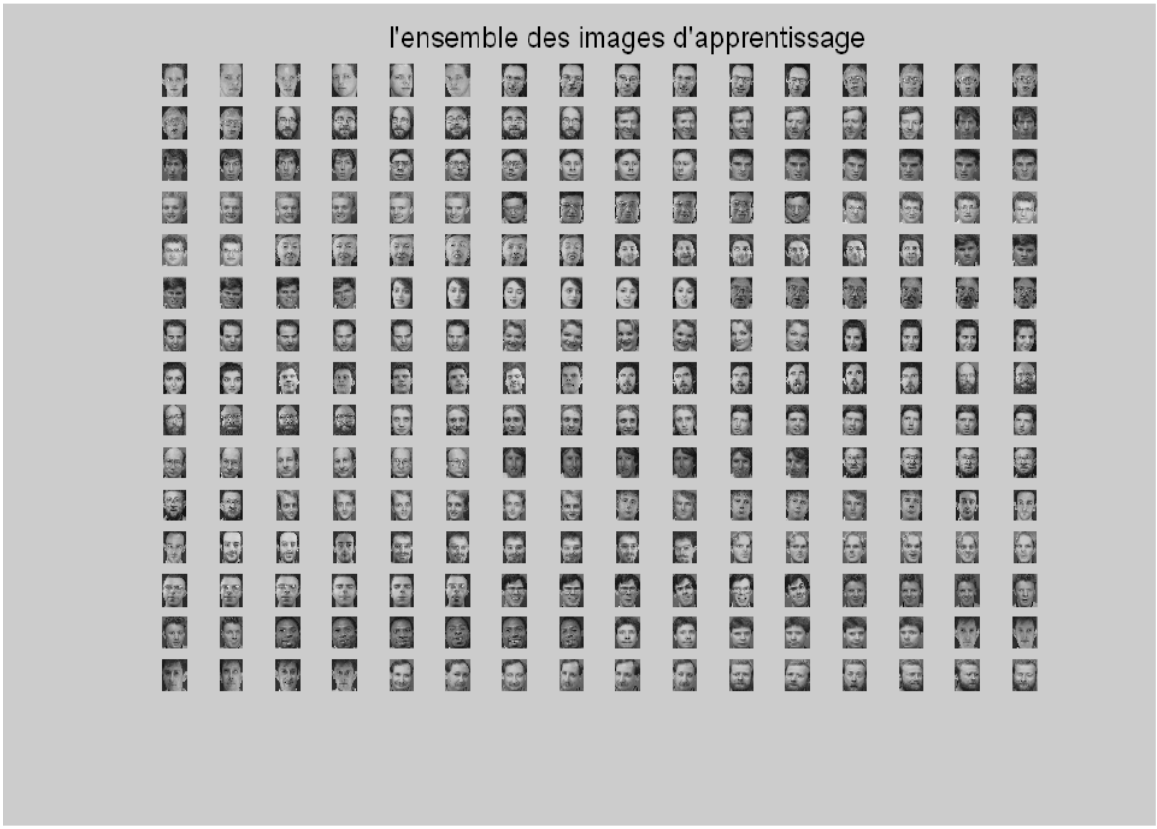


Figure. 4.2- L 'ensemble des images d'apprentissage de la base ORL utilisées pour le calcul dutaux de la bonne identification

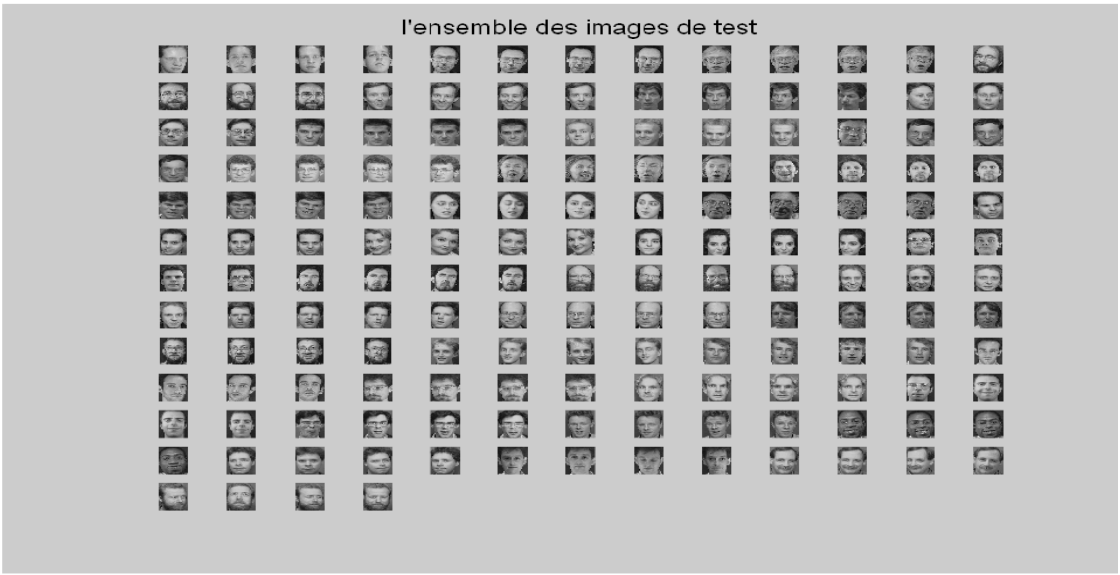


Figure. 4.3- L 'ensemble des images de Test de la base OR_L utilisées pour le calcul du taux dela bonne identification

IV.4. Base de données :

Nos expériences ont été exécutées sur des images frontales de visage de la base de données ORL [21]. ORL94 « ormerly 'The ORL Database of Faces' » est une base de données enregistrée spécifiquement pour évaluer les exécutions des approches biométriques à la vérification d'identité. Elle contient 10 images par visage de 40 personnes. Les images de format pgm 112x92 pixels organisé dans 40 dossiers nommés $\boldsymbol{S_X}$, chaque un à10visage nommé y.pgm ou y indique le numéro d'image.

Il n'est pas suffisant d'utiliser la même base de données pour pouvoir honnêtement comparer des résultats. Il est nécessaire également de définir un protocole de test. Dans notre travail la base de données est scindée en deux ensembles : ensemble d'apprentissage et l'ensemble de test. L'ensemble d'apprentissage contient 6 images de chaque personne (240 images), utilisé comme ensemble de référence. Il sert d'ensemble de base, maintenant ainsi l'information concernant les personnes connues du système et permet de fixer les paramètres du système de reconnaissance de visages, l'ensemble de test contient les autres images des personnes (160 images), permet de tester le système en lui présentant des images de personnes lui étant inconnues.

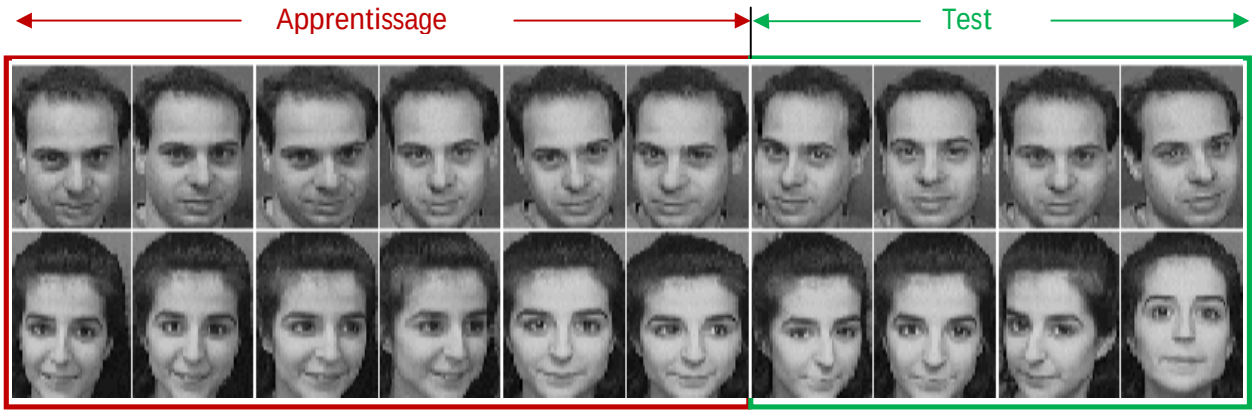


Figure.4.1 : Exemples d'images de deux personnes provenant de la base de données du laboratoire ORL de l'université de Cambridge.

Implémentation et Résultat

IV.1. Introduction

Dans cette partie on propose une application pour la reconnaissance de visage, utilisant l'algorithme de l'analyse des composantes principale et l'analyse des composantes indépendant qui a été bien détaillé dans le chapitre précédant. Dans notre application on utilise le langage Matlab.

IV.2.Qu'est-ce que c'est Matlab

Matlab est un logiciel commercial développé par Math worksInc ,est un outil très efficace qui est largement utilisé pour le calcul numérique et la visualisation graphique[17],développé à l'origine pour le calcul matriciel (le nom Matlab est dérivée de cette représentation «matrix laboratory».il contient des bibliothèques(toolbox) qui répondent à des besoins spécifiques :analyse numérique, traitement du signal, traitement d'image, etc.

IV.3. Pourquoi utiliser Matlab :

Matlab est déjà en usage dans de nombreux établissements.il est utilisé dans la recherche scientifique dans le milieu universitaire et industriel.les solutions prototype sont généralement obtenues plus rapidement dans Matlab que dans d'autre langages de programmation.Matlab est rapide, car les routines de base dans Matlab sont affinées pour les différentes architectures informatiques.

Conclusion

De nos jour la biométrie est considérée comme moyen le plus sûr pour la sécurité, elle est de plus en plus appliqué dans la réalité grâce à ses avantages. Ses applications sont diverses: applications de contrôle d'accès, applications dans les téléphone portables, application dans l'e-commerce etc... Cependant la biométrie elle a aussi des limitations comme la précision des techniques biométriques est faible, on n'a pas encore d'habitude d'utiliser le système biométriques.

Dans cet étude nous avons déjà présenté une vue générale de la biométrie, un survol sur quelques techniques biométriques basé sur la reconnaissance biométrique du visage une étude de cas a été donnés pour montrer la fonctionnement des algorithmes présentées.

Actuellement, il y a une nouvelle tendance qui arrive et qui commence à susciter les efforts, c'est le multimodale, dans lequel on combine plusieurs technologies biométriques ou plusieurs algorithmes de reconnaissance pour essayer d'améliorer les performances.

[22] ROSS A, NANDAKUMARK, JAIN.A. "*Handbook of Multibiometrics. Springer-Verlag*" New York, Inc., 2006.

[23] http://fingerchip.pagesperso-orange.fr/biometrics/accuracy.htm

[24] HIETMEYER. R"*Biometric identification promises fast and secure processing Of airline passengers*". The International Civil Aviation Organization Journal, Vol. 17, No. 9, pp. 10–11, 2000

[25] http://www2.icao.int/en/mrtd/Pages/default.aspx."*Machine ReadableTravel Documents (MRTD)*". 2008

[26] BAYLISS J, GUALTIERIA,CROMP R"*Analysinghyperspectral*" data with independent component analysis(1998).

[27] SETTLE J.J,DRAKE N.A. "*Linear mixing and the estimation of ground cover proportion*". International Journal of RemoteSensing, vol. 14, n° 6, p. 1159-1177(1993).

[12] BAEK, K., DRAPERB,BEVERIDGER , K. SHE K,"*PCA vs. ICA: A Comparison on theFERET Data Set* ". In 4th International Conference on Computer Vision, Pattern Recognition and Image Processing in conjunction with the 6th JCIS. (Durham, NC, 8-14 March, 2002), p. 824–827.2002

[13] LIU.S, SILVERMAN .M,"*A Practical Guide to Biometric Security Technology*", IEEE Computer Society, IT Pro-Security, Janvier-Février 2001.

[14] PRABHAKAR .S, JAIN. A,"*Decision-Level Fusion in Biometric Verification*", Pattern Recognition, Vol. 35, n°4, p. 861-874, 2002.

[15] PHILLIPS.P, HYEONJOON.H, RIZVI.S, RAUSS.P, "*The FERET EvaluationMethodology for Face-Recognition Algorithms*", IEEE Transactions onPattern Analysis and Machine Intelligence, Vol. 22, n°10, Octobre2000.

[16] CARDOSOJ.F "*Infomax and maximum likelihood for source separation*", IEEE Letters on SignalProcessing 4 (1997) 112–114.

[17] HYARINEN .A,KARHUNEN.J,OJA.E, "*Independent Component Analysis*" Wiley, New York, 2001.

[18] LIU.C,WECHSLER .H,"*Comparative Assessment of Independent Component Analysis (ICA) for Face Recognition, presented at International Conference on Audio and Video Based Biometric Person Authentication*"Washington, DC, 1999.

[19] Bell. J.A, T.J. SEJNOWSKI. T.J, "*The _Independent Components_ of natural scenes are edge filters*" VisionResearch 37 (1997) 3327–3338.

[20] CHEN.X, GU L, LI S.Z,ZHANG .H.J,"*Learning Representative Local Features for Face Detection*"presented at IEEE Conference on Computer Vision and Pattern Recognition, Kauai, HI, 2001.

[21] http://www.cl.cam.ac.uk/research/dtg/attarchive/facedatabase.html.

[01] ANDRZEJ D,*"Biometrics"*. http://scgwww.epfl.ch/coursesn

[02] GENDARMERIE ROYALE DU CANADA"*Les technologies biométriques : une Evaluation d'applications pratiques.*juin 2002".

[03] DANGHOANG V"*Biométrie pour l'Identification*" Institut de la Francophonie pour l'Informatique Hanoï Vietnam 2003.

[04] MORIZETN "*Reconnaissance Biométrique par Fusion Multimodale du Visage et de l'Iris*" d'Ecole Nationale Supérieure des Télécommunications Spécialité Signal et Images.18 Mars 2009.

[05] http://www.biometricgroup.com

[06] DAVIDE M, DARIO M,ANIL K "*Fingerprint Handbook*"2003

[07] http//biometrie_online.Net

[08] http://fr.wikipedia.org/w/index.php?title=D%C3%A9tection_de_visage&oldid69908711.

[09] BARTLETT M.LADESH. SEJNOWSKIT., "*Independent component representations for face recognition*", Proceedings of the SPIE Symposium on Electronic Imaging: Science and Technology "*Human Vision and Electronic Imaging III*, volume 3299, San José", January 1998.

[10] BARTLETT M, MOVELLAN J.Ret SEJNOWSKI T.J" *Face recognition by independentcomponent analysis* ". Neural Networks, IEEE Transactions on, vol. 13, 2002.

[11] JAIN.A, BOLLE R,PANKANTI S, "*Biometrics: Personal Identification inNetworked Society*", Kluwer, New York, 1998.