UNIVERSITE KASDI MERBAH OUARGLA
Faculté des Nouvelles technologies de l'information et de la communication
Département D'informatique et de technologie de l'information

Mémoire
MASTER ACADEMIQUE

Domaine : Mathématique et Informatique
Filière : Informatique
Spécialité : Informatique Fondamentale

Présenté par:
BETTAHAR Abdessettar
SABER Fathi

Thème

Extraction des caractéristiques pour l'analyse biométrique d'un visage

Soutenu publiquement

le : 15 / 06 / 2014

Devant le jury :

M^{R}	MEFLAH Mohammed Salim	MA	Président	UKM Ouargla
M^{R}	BENKADDOUR Mohammed Kamel	MA	Encadreur	UKM Ouargla
M^{R}	KHERFI Mohammed Lamin	MA	Examinateur	UKM Ouargla

Année Universitaire : 2013 /2014

Dédicaces Abdessattar

Je dédie ce modeste travail:

*À mes très **chers parents** pour leur soutient durant toute ma vie d'études et sans Lesquels je n'aurais jamais devenu ce que je suis*

*A **Ma grand-mère et Mon grand père.***

*À mes amis : **Abdelghani, Sallaheddine, Laater, Said , Kamal, Mohamed, Hamoud, Nafaa, Zaki** .*

*À tous les citoyens de village **AinCheikh**.*

*À toutes les **professeurs** et **enseignants** que j'ai eu durant tout mon cursus scolaire et qui m'ont permis de réussir Dans mes études.*

*À mes amis d'étude **Khalifa ,Adel ,Fethi ,Salim.***

*À toute **personne** ayant contribué à ce travail de près ou de loin.*

Dédicaces Saber

Je dédie ce mémoire :

A mes très chers parents pour leur soutient et encouragement durant toutes mes années d'études et sans lesquels je n'aurais jamais réussi et a ma famille

A tous mes professeurs et enseignants que j'ai eu durant tout mon cursus scolaire et qui m'ont permis de réussir dans mes études.

A tous mes amis(es).

A toute personne ayant contribué à ce travail de près ou de loin.

Remerciements

Nos remerciements et nos profondes gratitudes vont à notre promoteur Monsieur BENKADDOUR Mohammed Kamel pour son encadrement, son suivi et ses conseils tout au long de cette période.

Nos remerciements et notre gratitude vont aux professeurs et enseignants de département d'informatique ainsi que ses étudiants et son personnel côtoyés tout au long de notre cursus universitaire.

Nous tenons aussi à remercier mesdames et messieurs les membres du jury pour leur précieux temps accordé à l'étude de notre mémoire.

Que toute personne ayant œuvré de près ou de loin à la réalisation de ce projet par une quelconque forme de contribution, trouve ici le témoignage de notre plus profonde reconnaissance.

Table des matières

Introduction générale	01
Chapitre I : *Biométrie & systèmes de reconnaissance de visage*	
I.1 Introduction	04
I.2 Modes de fonctionnement	04
I.3 Structure d'un Système Biométrique	05
I.4 La Biométrie	06
I.4.1 Les technologies biométriques	07
I.4.2 Evaluation des performances des Systèmes biométriques	10
I.4.3 Applications des systèmes biométriques	12
I.4.4 Mesure de la performance d'un système biométrique	12
I.5 La reconnaissance de visages	13
I.5.1 Motivation : (pourquoi la reconnaissance de visages ?)	14
I.6 Les classes des techniques de reconnaissance de visages	14
I.6.1 Méthodes globales	14
I.6.2 Méthodes locale	15
I.6.3 Méthodes hybrides	16
I.7 Systèmes de reconnaissance de visage	17
I.7.1 Le monde physique (L'extérieur)	18
I.7.2 L'Acquisition de l'image	18
I.7.3 Les prétraitements	18
I.7.4 L'extraction de paramètres	19
I.7.5 La classification (Modélisation)	19
I.7.6 L'apprentissage	19
I.7.7 La décision	19
I.8 Principales difficultés de la reconnaissance de visages	20
I.8.1 Changement d'illumination	20
I.8.2Variation de pose	20
I.8.3 Expressions faciales	21
I.8.4 Présence ou absence des composants structurels	21
I.8.5 Les vrais jumeaux	21
I.9 Conclusion	22
Chapitre II : Etat de l'art des techniques de reconnaissance de visages	
II.1 Introduction	23
II.2 Analyse en Composantes Principales	23
II.3 L'analyse Discriminante Linéaire (LDA)	24
II.4 Analyse en composantes indépendantes	25
II.5 Les réseaux de neurones (RNA)	27
II.6 Machine à Vecteurs de Support (SVM)	28
II.7 Modèle de Markov caché	28
II.8 Template matching	29
II.9 Les Modèles Actifs d'Apparence	31

II.10 Approches basées sur les graphes	31
II.10.1 Elastic Graph Matching	31
II.10 .2 Elastic Buch Graph Matching	32
II.11 Les systèmes biométriques existants pour la reconnaissance des visages	32
II.12 Conclusion	33
Chapitre III : Identification faciale par eigenface &LBP	
III.1 Introduction	34
III.2 Reconnaissance de visage Eigenface	34
III.2.1 Présentation de la méthode Eigenface	34
III.2.2 Utilisation des Eigenfaces pour la classification des images visage	38
III.2.3 Principales étapes de la techniques d'eigenfaces	39
III.2.4 Mesures de Distance	40
III.2.4.1 Distances Euclidiennes	40
III.2.4.2 Distances dans l'Espace de Mahalanobis	41
III.2.4.3 Cosinus de Mahalanobis (MahCosine)	42
III.2.4.4 Choix de la distance de similarité	43
III.2.5 Organigramme détaillé de l'approche Eigenface	43
III.2.5.1 Organigramme du prétraitement	44
III.2.5.2 Organigramme de la phase d'apprentissage	45
III.2.5.3 Organigramme de la phase d'identification	46
III.3 Reconnaissance de visage par Local Binary Pattern (**LBP**)	47
III.3.1 Présentation	47
III.3.2 LBP pour la reconnaissance de visages	48
III.3.3 Dernières avancées : Travail de Tan et Triggs	49
III.3.3.1 Les local ternary patterns	49
III.3.3.2 La méthode de préparation de l'image	50
III.3.3.3 La métrique utilisée pour comparer deux histogrammes	51
III.4 Conclusion	52
Chapitre IV : Expérimentation, résultats et discussions	
IV. Introduction	53
IV.2 Les bases de données de visage	53
IV.2.1 ORL	53
IV.2.2 FEI	54
IV.2.3 Séparation des bases de données	54
IV.3 Environnement du travail	55
IV.3.1 Environnement matériel	55
IV.3.2 Outils de développement	55
IV.3.2.1 Matlab 7.8.0 (R2009a)	55
IV.4 Système de reconnaissance faciale : principes et expérimentations	55
IV.4.1 Système de reconnaissance faciale basé sur ACP : Expérimentation et résultats	56
IV.4.2 Système de reconnaissance faciale basé sur LBP : Expérimentation et résultats	61
IV.4.3 Discussion	63

IV.5 Principe du système de reconnaissance 64
IV.5.1 Mode vérification 64
IV.5.2 Mode identification 64
IV.6 Présentation de l'application 64
IV.6.1 Interface de Présentation du projet 64
IV.6.2 L'interface PCA Algorithme de reconnaissance faciale 66
IV.6.3 Expérimentations 70
IV.6.4 L'interface de LBP Algorithme 71
IV.6.5 Résultats 73
IV.7 Tableau de comparaison entre les algorithmes 74
IV.8 Conclusions 74
Conclusion générale 75
Bibliographie

Table des figures

Fig.I.1 : *Principaux modules d'un système biométrique ainsi que les différentes.*	05
Fig.I.2 : *La Classification De La Biométrie.*	07
Fig.I.3 : *Le processus de reconnaissance par empreinte digitale.*	07
Fig.I.4 : *Photo d'iris.*	08
Fig.I.5 : *Dispositif de reconnaissance par géométrie de la main.*	08
Fig.I.6 : *Photo de rétine.*	08
Fig.I.7 : *Capture de l'image d'un visage.*	09
Fig.I.8 : *Spectre d'un signal voix.*	09
Fig.I.9 : *Capture d'une signature.*	10
Fig.I.10 : *Comparaison entre les techniques biométriques*	11
Fig.I.11 : *Illustration du FRR et du FAR.*	13
Fig.I.12 : *le principe des méthodes globales.*	15
Fig.I.13 : *Une classification des algorithmes principaux utilisés en reconnaissance faciale.*	17
Fig.I.14 : *Système de reconnaissance.*	18
Fig.I.15 : *Exemple de variation d'éclairage.*	20
Fig.I.16 : *Exemples de variation de poses.*	20
Fig.I.17 : *Exemples de variation d'expressions.*	21
Fig.II.1 : *Les dix vues d'une personne dans la base de données ORL.*	24
Fig.II.2 : *les projections ACP et LDA d'un ensemble de données.*	25
Fig.II.3 : *Modèle général du mélange et de la séparation de sources.*	26
Fig.II.4 : *Le modèle de synthèse d'image de l'architecture d'ICA.*	26
Fig.II.5 : *Neurone formel.*	27
Fig.II.6 : *les 5 états du HMM (de haut en bas).*	29
Fig.II.7 : *Différentes régions utilisées pour la phase de template matching.*	30
Fig.II.8 : *La représentation des visages par graphe rectangulaire.*	31
Fig.III.1 : *Passage d'une image vers un vecteur colonnes.*	35
Fig.III.2 : *Image moyenne.*	35
Fig.III.3 : *Décroissance des valeurs propres de la base de données utilisée en fonction du nombre de vecteurs propres retenu.*	37
Fig.III.4 : *eigenfaces.*	38
Fig.III.5 : *Illustration des cas possibles de classification d'une image.*	39
Fig.III.6 : *Représentation d'une sphère avec la distance euclidienne (III.2.4.1.B) et la distance City-Block (III.2.4.1.A).*	41
Fig.III.7 : *Les deux vecteurs m et n dans l'espace de Mahalanobis.*	42
Fig.III.8 : *prétraitements.*	44
Fig.III.9 : *phase d'apprentissage.*	45
Fig.III.10 : *phase d'identification.*	46
Fig.III.11: *Opérateur LBP.*	47
Fig.III.12 : *(a): Trois voisinages pour des R et P différents, (b) :Textures particulières détectées par* LBP^{u2}	47

Fig.III.13: *Représentation d'un visage par les histogrammes du code LBP.*	49
Fig.III.14: *Opérateur LTP basique.*	50
Fig.III.15: *Illustration de l'application de la méthode de correction d'illumination proposée par Tan et Triggs.*	51
Fig.III.16 : *A gauche : Exemple de matrice binaire de distribution des patterns. A droite : Matrice de distances correspondante.*	52
Fig.IV.1 : *Exemples d'images de visages de la base ORL.*	53
Fig.IV.2 : *Exemples d'images de visages de la base FEI.*	54
Fig.IV.3 : *visages de la base ORL normaliser et leurs visage moyen.*	56
Fig.IV.4 : *Tracé des valeurs propres.*	57
Fig.IV.5 : *Eigen faces.*	57
Fig. IV.6 : *Exemple de changement d'illumination (galerie 1).*	58
Fig.IV.7 : *Exemple de changement d'expressions faciales (galerie 2).*	58
Fig.IV.8 : *Exemple de changement de pose (galerie 3).*	58
Fig.IV.9 : *Exemple d'individus neutre avec différent âges (galerie 4).*	59
Fig.IV.10 : *Taux de reconnaissance obtenus pour différentes galeries.*	59
Fig.IV.11 : *Taux d'identification en fonction du nombre d'exemples d'apprentissage par personne (ACP).*	60
Fig.IV.12 : *l'operateur LBP basique. Les entourages (8,1), (16,2), (8,2) sont Représentés.*	61
Fig.IV.13 : *Interface graphique de notre application.*	65
Fig.IV.14 : *L'interface graphique de reconnaissance faciale.*	65
Fig.IV.15 : *les visages normalisés.*	66
Fig.IV.16 : *Le visage moyen.*	67
Fig.IV.17 : *Eigenfaces.*	67
Fig.IV.18 : *Tracé du diagramme le des vecteurs propres.*	68
Fig.IV.19 : *interface ACP test.*	68
Fig.IV.20 : *message fin training.*	69
Fig.IV.21 : *chois de chemine d'image test.*	69
Fig.IV.22 : *l'affichage d'image de test.*	69
Fig.IV.23 : *fin étape de test.*	70
Fig.IV.24 : *l'interface test pour LBP de la base FEI.*	71
Fig.IV.25 : *Message de fin training.*	71
Fig.IV.26 : *le choix de l'image test pour la base FEI.*	72
Fig.IV.27 : *l'affichage de l'image test.*	72
Fig.IV.28 : *fin de l'étape test.*	73

Liste de tableaux

Tab.IV.1 : *T aux de reconnaissance (%) obtenus pour différentes galeries de la base ORL.*	59
Tab.IV.2 : *Taux de reconnaissance (%) obtenus en fonction de différents nombres de vecteurs propres.*	60
Tab.IV.3 : *Taux de reconnaissance (%) obtenus en utilisant LBP.*	62
Tab.IV.4 : *Tableau de comparaison entre les algorithmes.*	74

Introduction générale

La croissance internationale des communications, tant en volume qu'en diversité (déplacements physiques, transactions financières, accès aux services...), implique le besoin de s'assurer de l'identité des individus. En effet, l'importance des enjeux peut motiver les fraudeurs à mettre en échec les systèmes de sécurité existants. Il existe donc un intérêt grandissant pour les systèmes électroniques d'identification et de reconnaissance. Leur dénominateur commun est le besoin d'un moyen simple, pratique, fiable et peu onéreuse de vérifier l'identité d'une personne sans l'assistance d'un tiers. Le marché du contrôle d'accès s'est ouvert avec la prolifération de systèmes, mais aucun ne se révèle efficace contre la fraude, car tous utilisent un identifiant externe tel que : badge/carte, clé, code. Il est fréquent d'oublier un code d'accès. Il existe d'ailleurs de nombreux bureaux où les mots de passe sont notés dans des listes, ce qui représente une dangereuse faille dans la sécurité informatique de l'entreprise puisque toute confidentialité est alors perdue .de même, un badge ou une clé peuvent être, volés ou copiés par des personnes mal intentionnées. Le défaut commun à tous les systèmes d'authentification est que l'on identifie un objet (code, carte...) et non la personne elle-même. Face à la contrainte de l'authentification par « objets », la biométrie apporte une simplicité et un confort aux utilisateurs.

Cette discipline s'intéresse en effet, à l'analyse du comportement ainsi qu'à l'analyse de la morphologie humaine et étudie, par des méthodes mathématiques (statistiques, probabilités,…), les variations biologiques des personnes. Ce thème se situe dans la problématique générale de la biométrie qui est une science qui propose d'identifier les personnes à partir de la mesure de leurs indices biologiques. La biométrie recouvre deux approches principales : analyse comportementale (vitesse de signature, marche,…) ou analyse de la morphologie humaine (empreintes digitales, iris, rétine, voix, main, visage, …). Un des objectifs de la biométrie est de sécuriser des accès à des locaux ou à des matériels. Ceci peut se faire aujourd'hui par un contrôle de pièce d'identité ou par la saisie d'un mot de passe, mais les deux modes de contrôle sont contraignants et peuvent donner lieu à des falsifications. L'utilisation de techniques biométriques doit permettre d'identifier une personne à travers la consultation d'une base de données, ou de vérifier l'identité affirmée d'un individu. Nous avons retenu la modalité « visage » car c'est un indice biologique très fort contenant de nombreuses indications sur l'identité de la personne et dont l'image peut être acquise de manière non invasive. La reconnaissance de la forme du visage est la technique la plus commune et populaire. Elle est la plus acceptable parce qu'on peut l'utiliser à distance sans contact avec

l'objet. Utiliser une caméra permet d'acquérir la forme du visage d'un individu et puis retirer certaines caractéristiques. Les caractéristiques essentielles pour la reconnaissance du visage sont: les yeux, la bouche, le tour du visage, le bout du nez,… etc. Selon le système utilisé, l'individu doit être positionné devant la caméra où peut être en mouvement à une certaine distance. Les données biométriques qui sont obtenues sont comparées au fichier référence. Le logiciel doit être capable d'identifier un individu malgré différents artifices physiques (moustache, barbe, lunettes, etc..).

Le visage est une biométrie relativement peu sûre. En effet, le signal acquis est un sujet à des variations beaucoup plus élevées que d'autres caractéristiques. Celles-ci peuvent être causées, entre autres, par le maquillage, la présence ou l'absence de lunettes, le vieillissement et l'expression d'une émotion. La méthode de la reconnaissance du visage est sensible à la variation de l'éclairage et le changement de la position du visage lors de l'acquisition de l'image.

Ce mémoire traite un sujet portant sur l'authentification du visage. Un système d'authentification a pour but de vérifier l'identité d'un individu après que celui-ci se soit identifié. Il ne s'agit donc pas d'un système d'identification qui lui se charge de découvrir l'identité a priori inconnue d'un individu.

Plusieurs méthodes ont été développées dans la littérature pour la reconnaissance de visage. Dans notre travail nous avons opté pour deux techniques d'extraction des caractéristiques de l'image de visage :

- ✓ La première méthode est Eigenface qui se base sur une analyse en composante principale. L'ACP est une méthode mathématique qui peut être utilisée pour simplifier un ensemble de données, en réduisant sa dimension.
- ✓ La second méthode est la technique LBP (local Binary Pattern),c'est une méthode mathématique dont son principe consiste à caractériser la texture d'une image par calcule du code LBP pour tous les pixels d'image ensuite calcule l'histogramme de cette image LBP pour former un vecteur de caractéristiques représentant l'image faciale.

Nous avons choisi d'articuler notre étude autour de quatre chapitres principaux.

Le premier chapitre est consacré à la présentation générale de la biométrie. Il décrit le principe de fonctionnement des systèmes biométriques puis définit les outils utilisés pour évaluer leurs performances. Ensuite, la place de la reconnaissance faciale parmi les autres techniques biométriques est analysée. A travers ce chapitre, nous voulons positionner le problème de la reconnaissance faciale et présenter ses enjeux et intérêts par rapport aux autres techniques. Enfin, nous mettons en lumière les difficultés rencontrées par les systèmes de reconnaissance de visage.

Dans le deuxième chapitre, nous évoquerons l'état de l‘art des techniques de reconnaissance de visages. Nous n'allons pas décrire tous les algorithmes de reconnaissance de visages mais nous nous focaliserons sur les algorithmes les plus populaires et sur ceux les plus adaptés à notre contexte d'étude.

Le troisième chapitre est partagé en deux parties. Dans la première partie nous présenterons l’algorithme eigenface basé sur une analyse en composante principale, qui est une méthode mathématique qui peut être utilisée pour simplifier un ensemble de données, en réduisant sa dimension, elle est utilisée pour représenter efficacement les images de visages, qui peuvent être approximativement reconstruites à partir d’un petit ensemble de poids et d’une image de visage standard. Nous verrons plusieurs approches pour améliorer les performances de PCA. Dans la deuxième partie nous présenterons l’approche LBP (Local Binary Pattern). C’est une méthode mathématique qui basé sur caractérisation de la texture d’image par le calcul des valeurs LBP pour chaque pixel d’image,

Dans le quatrième chapitre, Nous présentons les résultats expérimentaux obtenus par chaque méthode en analysons leurs performances, suivi d'une discussion avec interprétation des résultats.

Enfin, la conclusion générale résumera les résultats obtenus par les différentes approches et donnera quelques perspectives sur les travaux futurs.

I.1 Introduction

Un système biométrique est essentiellement un système de reconnaissance de formes qui utilise les données biométriques d'un individu. Les systèmes biométriques sont de plus en plus utilisés depuis quelques années. L'apparition de l'ordinateur et sa capacité à traiter et à stocker les données ont permis la création des systèmes biométriques informatisés.

Nous introduirons dans ce chapitre quelques notions et définitions de base liées à la biométrie. Nous donnerons le principe de fonctionnement des systèmes biométriques ainsi que les outils utilisés pour mesurer leurs performances. Nous insisterons surtout sur la place de la reconnaissance faciale parmi les autres techniques biométriques, car elle constitue l'objectif de ce thème.

I.2 Modes de fonctionnement

Tout système biométrique peut fonctionner en mode d'enrôlement ou en mode de vérification ou bien en mode d'identification :

- ✓ Le mode d'**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 ».
- ✓ Le mode de ***vérification ou authentification*** est une comparaison "1 à 1", dans lequel le système valide l'identité d'une personne en comparant les données biométriques saisie avec le modèle biométrique de cette personne stockée dans la base de données du système. Dans un tel mode, le système doit alors répondre à la question suivante: *«Suis-je réellement la personne que je suis en train de proclamer?»*. Actuellement la vérification est réalisée via un numéro d'identification personnel, un nom d'utilisateur, ou bien une carte à puce.
- ✓ Le mode **d'*identification*** est une comparaison "1 à N", dans lequel le système reconnaît un individu en l'appariant avec un des modèles de la base de données. La personne peut ne pas être dans la base de données. Ce mode consiste à associer une identité à une personne. En d'autres termes, il répond à des questions du type: *« Qui suis-je ? »*.

I.3 Structure d'un Système Biométrique

Un système biométrique est conçu à l'aide des quatre modules principaux suivants [19], (voir Fig. I.1) :

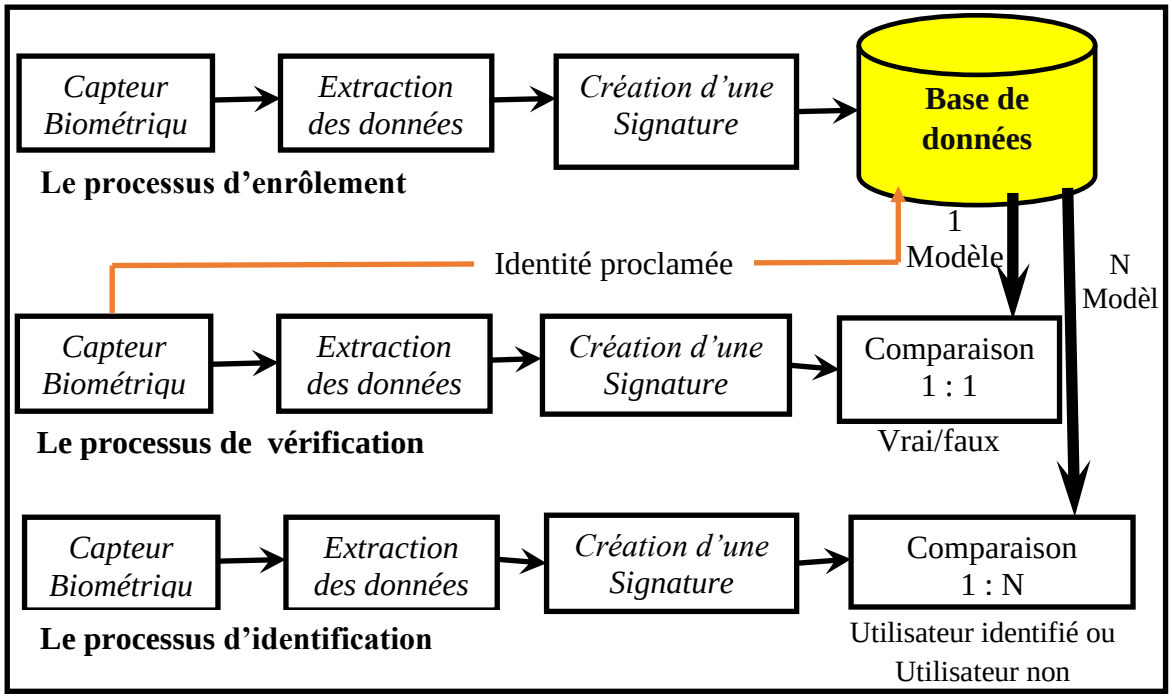

Fig.I.1 : *Principaux modules d'un système biométrique ainsi que les différentes.*

Les différents modules qui composent un système biométrique sont représentés sur la Fig. I.1. Leur fonctionnement peut être résumé comme suit :

- *Module capteur biométrique* : correspond à la lecture de certaines caractéristiques physiologiques, comportementales ou biologiques d'une personne, au moyen d'un terminal de capture biométrique (ou capteur biométrique).
- *Module extraction des données* : extrait les informations pertinentes à partir des données biométriques brutes, par exemple des images de visage ou des régions caractéristiques de visage.
- *Module création d'une signature* : crée un modèle numérique afin de représenter la donnée biométrique acquise. Ce modèle, appelé aussi signature, sera conservé sur un support portable (puce ou autre) ou dans une base de données.
- *Module comparaison :* compare les caractéristiques biométriques d'une personne soumise à contrôle (volontairement ou à son insu) avec les « signatures »mémorisées. Ce module fonctionne soit en mode vérification (pour une identité proclamée) ou bien en mode identification (pour une identité recherchée).

- *Module base de données :* stocke les modèles biométriques des utilisateurs enrôlés.
- *Le module d'inscription ou d'enregistrement* : est responsable de l'inscription des individus dans la base de données du système biométrique. Pendant la phase d'inscription, la caractéristique biométrique d'un individu est d'abord scannée par un lecteur biométrique pour produire une représentation numérique de la caractéristique. La capture de données pendant le processus d'inscription peut être ou non pas être dirigée par un humain selon l'application. Un contrôle de qualité est généralement exécuté pour garantir que l'échantillon acquis peut être sûrement traité par les étapes successives.

Afin de faciliter la comparaison, la représentation numérique d'entrée est de plus traitée par un extracteur de caractéristique pour produire une représentation compacte mais expressive, appelée un *modèle* ou *pattern*. Selon l'application, le modèle peut être stocké dans la base de données centrale du système biométrique ou enregistré sur une *carte à puce* livrée à l'utilisateur. Généralement, les modèles dans la base de données peuvent être mis à jour dans le temps.

I.4 La Biométrie

Une des définitions de la biométrie est donnée par Roethenbaugh [1] : « La biométrie s'applique à des particularités ou des caractères humains uniques en leur genre et mesurables, permettant de reconnaître ou de vérifier automatiquement l'identité ». Mais Aucune modalité biométrique n'est en elle-même fiable à 100 %. Il existe des problèmes, liées aux dispositifs de capture des données, à l'utilisateur lui-même ou au condition lors de la capture, dans lesquelles une modalité quelconque peut s'avérer défaillante. Parmi les principales modalités biométriques physiologiques et comportementales.

-Biométriques physiologiques

Ce type est basé sur l'identification de traits physiques particuliers qui, pour toute personne, sont uniques et permanents. Cette catégorie regroupe la reconnaissance des empreintes digitales, de la forme de la main, de la forme du visage, de la rétine, de l'ADN et de l'iris de l'œil.

-Biométriques comportementales

Ce type se base sur l'analyse de certains comportements d'une personne comme le tracé de sa signature, sa démarche et sa façon de taper sur un clavier.

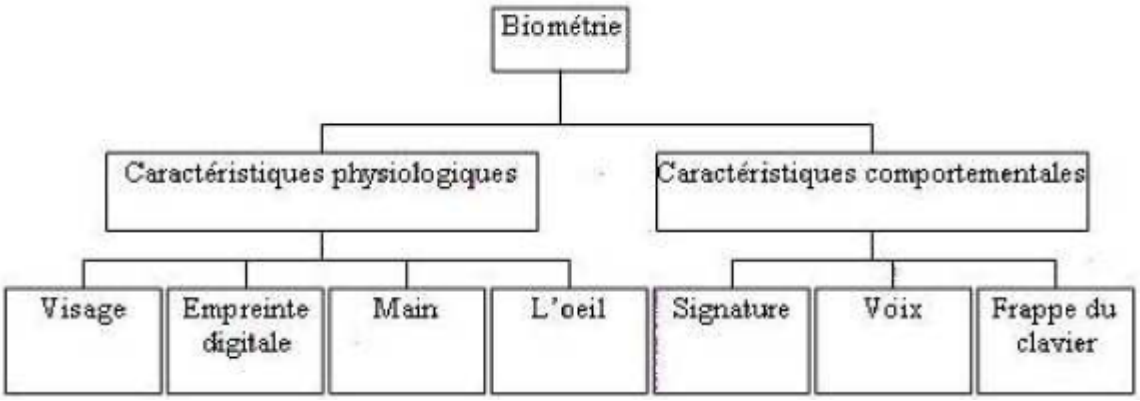

Fig.I.2 : *La Classification De La Biométrie.*

I.4.1 Les technologies biométriques

Les empreintes digitales : Une empreinte digitale est constituée d'un ensemble de lignes localement parallèles formant un motif unique pour chaque individu. On distingue les stries (ou crêtes, ce sont les lignes en contact avec une surface au toucher) et les sillons (ce sont les creux entre deux stries). Les stries contiennent en leur centre un ensemble de pores régulièrement espacés. Chaque empreinte possède un ensemble de points singuliers globaux (les centres et les deltas) et locaux (les minuties). Les centres correspondent à des lieux de convergence des stries tandis que les deltas correspondent à des lieux de divergence. L'acquisition des données est faite par un capteur électronique de type optique, thermique, capacitif ou à ultrasons [2].

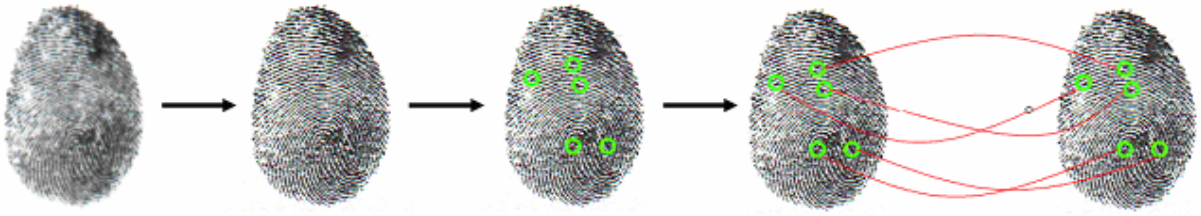

Fig.I.3 : *Le processus de reconnaissance par empreinte digitale.*

L'iris : L'iris est une technique extrêmement fiable car il contient une infinité de points caractéristiques (ensemble fractal), la fraude étant néanmoins possible en utilisant des lentilles. L'acquisition de l'iris est effectuée au moyen d'une caméra pour pallier aux mouvements inévitables de la pupille. Elle est très sensible (précision, reflet…) et relativement désagréable pour l'utilisateur car l'œil doit rester grand ouvert et il est éclairé par une source lumineuse pour assurer un contraste correct [3][19].

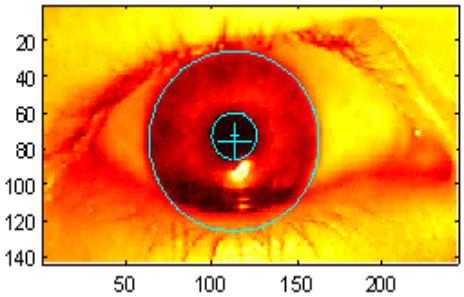

Fig.I.4 : *Photo d'iris.*

La géométrie de la main : jusqu'à 90 caractéristiques de la main sont mesurées (forme de la main et des articulations, longueur et largeur des doits, longueur inter articulations…). Le taux d'erreurs dans la reconnaissance est assez élevé, en particulier pour des personnes appartenant à une même famille en raison d'une forte ressemblance. De plus, la forme de la main évolue beaucoup avec l'âge [5].

Fig.I.5 : *Dispositif de reconnaissance par géométrie de la main.*

La rétine : Cette technique se base sur le fait que les vaisseaux sanguins d'une rétine sont uniques pour chaque personne. L'utilisateur doit placer son œil face à un orifice de capture situé sur le dispositif d'acquisition. Un faisceau lumineux traverse l'œil jusqu'aux vaisseaux sanguins capillaires de la rétine. Le système localise et capture ainsi environ 400 points de référence. Cette technique requiert une collaboration étroite de la part de l'utilisateur, car il doit placer son œil extrêmement près de la caméra [8].

Fig.I.6 : *Photo de rétine.*

Le visage : Plusieurs parties du visage (joues, yeux, nez, bouche…) sont extraites d'une photo ou d'une vidéo et analysées géométriquement (distance entre différents points, positions, formes…). Le problème de cette méthode vient des possibles perturbations pouvant transformer le visage (maquillage, faible luminosité, présence d'une barbe ou d'une lunette, expression faciale inhabituelle, changement avec l'âge, etc.) [6][7].

Fig.I.7 : *Capture de l'image d'un visage.*

La voix : La voix humaine est une caractéristique biométrique intéressante, puisqu'elle dépend de la structure anatomique de l'individu ainsi que de l'apprentissage du langage fait lors de l'enfance. La capture de la voix est relativement facile à effectuer, à l'aide d'un microphone, mais elle est susceptible à être corrompue par les bruits ambiants.

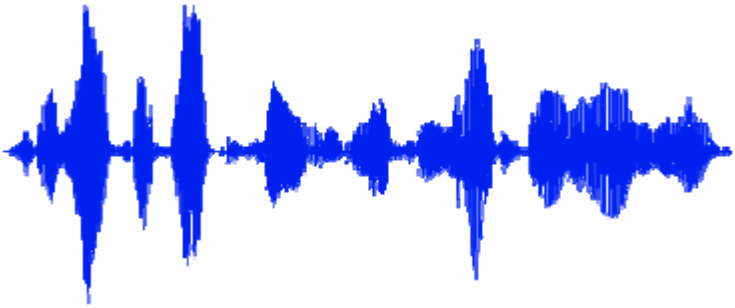

Fig.I.8 : *Spectre d'un signal voix.*

La dynamique du tracé de la signature : Il s'agit d'une analyse comportementale où différents éléments (mesure da la vitesse, ordre d'écriture, pression exercée, accélération…) sont mesurés lors de la signature. La falsification est possible en passant par une phase d'apprentissage, la signature peut carier selon le stress de l'utilisateur [9].

Fig.I.9 : *Capture d'une signature.*

La dynamique de frappe au clavier : Un système basé sur la dynamique de frappe au clavier ne nécessite aucun équipement particulier, chaque ordinateur disposant d'un clavier. Il s'agit d'un dispositif logiciel qui calcule le temps où un doigt effectue une pression sur une touche et le temps où un doigt est dans les airs (entre les frappes). Cette mesure est capturée environ mille fois par seconde. La séquence de frappe est prédéterminée sous la forme d'un mot de passe. Initialement l'utilisateur doit composer son mot de passe à quelques reprises afin que soit constitué un gabarit de référence.

Ce dispositif biométrique est utilisé comme méthode de vérification pour le commerce électronique et comme mécanisme de contrôle d'accès à des bases de données [10].

I.4.2 Evaluation des performances des Systèmes biométriques

Bien que n'importe quelle mesure physiologique ou comportementale puisse être utilisée dans un système de reconnaissance biométrique, elles ne sont pas toutes aussi performantes les unes que les autres. Ainsi, toute bonne mesure biométrique doit satisfaire les critères suivants (Jain, Ross et Prabhakar, 2004) :

- Universelle : Par ceci, nous voulons dire que la caractéristique biométrique doit être présente pour tous les individus. Par exemple, il est impossible de recueillir l'empreinte digitale d'un individu qui a été amputé de la main ou bien de mesurer la démarche d'une personne quadriplégique.
- Distinctive : La mesure effectuée sur un individu doit être suffisamment différente de celles effectuées sur les autres individus pour permettre de discriminer entre eux. Ici, on peut penser au code génétique qui varie significativement d'une personne à l'autre tandis que la taille est une mesure que plusieurs individus partagent.
- Permanente : Le fait que le corps humain vieillit implique qu'après un certain laps de temps, une mesure biométrique faite sur un individu peut être très différente de la

mesure initiale utilisée pour l'inscription dans le système. Par conséquent, il est important de choisir une caractéristique biométrique qui reste stable durant la vie de l'individu. Un bon exemple de ceci est le motif présent dans l'iris ou même le code génétique de l'individu.

- Facile à mesurer : Ceci représente à quel point il est facile de recueillir et de quantifier la mesure biométrique. Il est facile d'enregistrer le son de la voix d'un individu à l'aide d'un microphone, mais il est beaucoup moins facile d'obtenir une image de bonne qualité de la rétine des individus.
- Efficace : L'efficacité fait référence à la quantité de ressources nécessaires afin d'obtenir le niveau de qualité désiré dans le temps requis. Un test sanguin chimique requiert du matériel sophistiqué et une longue période de temps avant d'obtenir un résultat comparativement à recueillir l'image du visage d'un individu à l'aide d'une caméra numérique.
- Acceptable : Ceci correspond aux aspects socioculturels de la reconnaissance biométrique. Même si avec la surabondance de caméras de sécurité, la population normale ne se soucie plus d'avoir son image recueillie par de multiples systèmes.
- Robuste : Par ceci, nous faisons référence à la difficulté de forcer le système à produire une prédiction erronée par l'utilisation d'une technique frauduleuse. L'utilisation de technique de maquillage pour effets spéciaux a déjà permis de tromper autant les humains que les machines lors de reconnaissance faciale.

Biométrie	Universalité	Unicité	Permanence	Mesurabilité	Performance	Acceptabilité	Circonvention
DNA	Haute	Haute	Haute	Faible	Haute	Faible	Faible
Oreille	Moyenne	Moyenne	Haute	Moyenne	Moyenne	Haute	Moyenne
Visage	Haute	Faible	Moyenne	Haute	Faible	Haute	Haute
Thermo Visage	Haute	Haute	Faible	Haute	Moyenne	Haute	Haute
Empreinte	Moyenne	Haute	Haute	Moyenne	Haute	Moyenne	Moyenne
Démarche	Moyenne	Faible	Faible	Haute	Faible	Haute	Moyenne
Géométrie Main	Moyenne	Moyenne	Moyenne	Haute	Moyenne	Moyenne	Moyenne
Veines Main	Moyenne	Moyenne	Moyenne	Moyenne	Moyenne	Moyenne	Faible
Iris	Haute	Haute	Haute	Moyenne	Haute	Faible	Faible
Frappe Clavier	Faible	Faible	Faible	Moyenne	Faible	Moyenne	Moyenne
Odeur	Haute	Haute	Haute	Faible	Faible	Moyenne	Faible
Rétine	Haute	Haute	Moyenne	Faible	Haute	Faible	Faible
Signature	Faible	Faible	Faible	Haute	Faible	Haute	Haute
Voix	Moyenne	Faible	Faible	Moyenne	Faible	Haute	Haute

Fig.I.10 : *Comparaison entre les techniques biométriques [11].*

I.4.3 Applications des systèmes biométriques

Les applications de la biométrie peuvent être divisées en trois groupes principaux:

-Applications commerciales: telles que l'ouverture de réseau informatique, la sécurité de données électroniques, l'e-commerce, l'accès Internet, la carte de crédit, le contrôle d'accès physique, le téléphone cellulaire, la gestion des registres médicaux, l'étude à distance, etc.

-Applications gouvernementales: telles que la carte d'identité nationale, le permis de conduire, la sécurité sociale, le contrôle des frontières, le contrôle des passeports, etc.

-Applications légales : telles que l'identification de corps, la recherche criminelle, l'identification de terroriste, etc.

De nos jours les systèmes biométriques sont de plus en plus utilisés dans des applications civiles. Par exemple, le dispositif de Schiphol Privium à l'aéroport d'Amsterdam, utilise un capteur de l'iris pour accélérer la procédure de contrôle des passeports et des visas [12]. Les passagers insèrent leur carte dans un lecteur et se mettent en face d'un appareil-photo, ce dernier acquiert l'image de l'œil. Des processus de traitement d'images sont alors lancés afin de localiser l'iris et de calculer une signature appelée « Iris code »[13]. Une fois l'Iris code calculé, il est comparé aux données stockées dans la carte pour identifier le passager. Un dispositif semblable est également employé pour vérifier l'identité des employés de l'aéroport qui travaillent dans des secteurs de haute sécurité.

I.4.4 Mesure de la performance d'un système biométrique

Tout d'abord, afin de comprendre comment déterminer la performance d'un système biométrique, il nous faut définir clairement trois critères principaux.

1. Le premier critère s'appelle le **taux de faux rejet** ("**F**alse **R**eject **R**ate" ou **FRR**). Ce taux représente le pourcentage de personnes censées être reconnues mais qui sont rejetées par le système.

$$\boldsymbol{TFR = \frac{nombre\ des\ clients\ rejetés(FR)}{nombre\ total\ d'accés\ de\ clients}}$$

Telle que *FR* Le faux rejet correspond au cas où le système rejette un client légitime.

2. Le deuxième critère est le **taux de fausse acceptation** ("**F**alse **A**ccept **R**ate" ou **FAR**).Ce taux représente le pourcentage de personnes censées ne pas être reconnues mais qui sont tout de même acceptées par le système.

$$\boldsymbol{TFA = \frac{nombre\ des\ imposteurs\ acceptés(FA)}{nombre\ total\ d'accésimposteurs}}$$

Telle que *FA* correspond au cas où le système accepte un individu qui a proclamé une identité qui n'est pas la sienne.

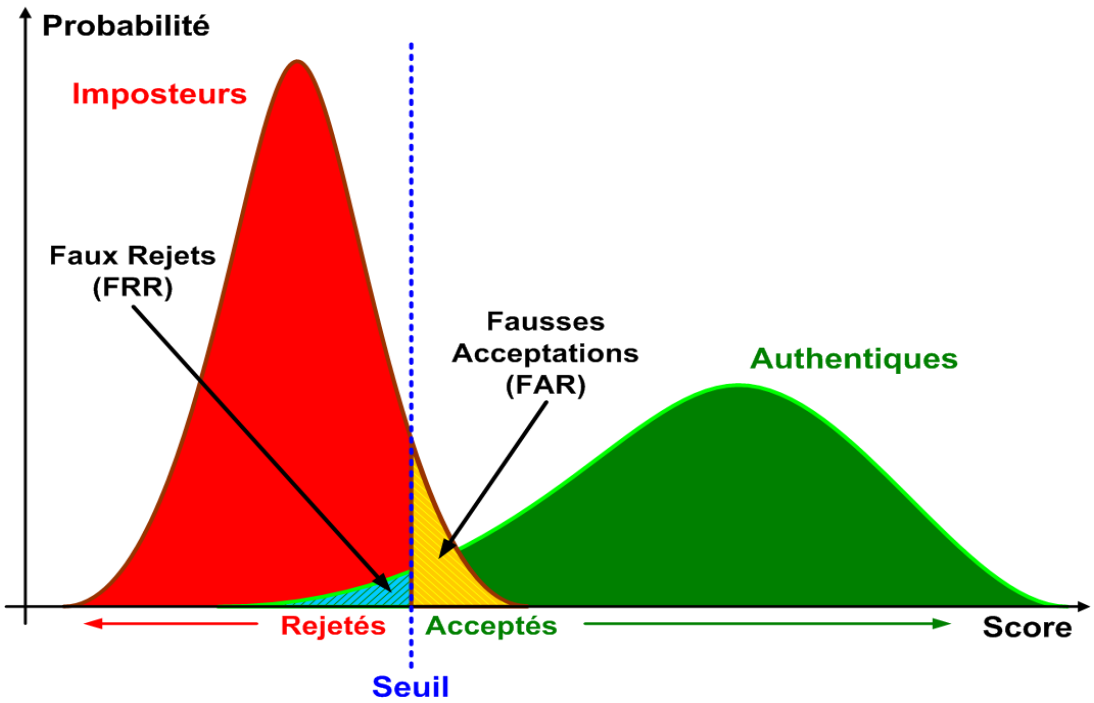

Fig.I.11 : *Illustration du FRR et du FAR.*

3. Le troisième critère est connu sous le nom de **taux d'égale erreur** ("**E**qual **E**rror **R**ate" ou **EER**). Ce taux est calculé à partir des deux premiers critères et constitue un point de mesure de performance courant. Ce point correspond à l'endroit où FRR = FAR, c'est-à-dire le meilleur compromis entre les faux rejets et les fausses acceptations.

I.5 La reconnaissance de visages

Vu la demande grandissante pour la surveillance et le contrôle d'accès des lieux publics tels que les aéroports, banques et administrations, la reconnaissance du visage a connu un grand intérêt parmi la communauté scientifique.

Si pour un être humain, reconnaître un visage relève d'une action naturelle et facile, il en va tout autrement pour un système biométrique autonome. Pour un ordinateur, une telle opération se base au contraire sur une chaîne de traitements complexes, reposant sur des algorithmes complexes.

Les systèmes de reconnaissance du visage reposent sur des algorithmes d'analyse de l'image, pouvant identifier les personnes qui y sont associées. Ces programmes créent une image du visage, en mesurant ses caractéristiques. Ils en produisent ensuite un fichier individuel, dénommé "Template ou signature". Les Template sont alors comparées avec toutes les images existantes au niveau de la base de données, en ressortant un score de similitude.

Les sources typiques des images valorisées dans le cadre de la reconnaissance du visage incluent les caméras vidéo et les appareils photo numériques. Il s'agit ensuite de détecter la présence d'un visage sur l'image en faisant appel à des techniques d'intelligence artificielle. La détection du visage est un domaine très vaste et ne fera pas l'objet de notre étude.

Par ailleurs, on peut classifier les systèmes de reconnaissance du visage en deux grandes catégories selon la source de capture de l'image : reconnaissance du visage dans une séquence vidéo ou bien à partir d'images fixes. Dans ce dernier cas, on peut aussi différencier les systèmes basés sur des images 3D [16] de ceux utilisant des images 2D.

Nous allons nous intéresser essentiellement aux systèmes de reconnaissance du visage basés sur des images 2D fixes à travers des bases de données d'images construites et partagées par les laboratoires de recherche spécialisés dans ce domaine.

I.5.1 Motivation : (pourquoi la reconnaissance de visages ?)

Durant les vingt dernières années, la reconnaissance automatique des visages est devenue un enjeu primordial, notamment dans les domaines de l'indexation de documents multimédias et surtout dans la sécurité, ceci est dû aux besoins du monde actuel mais aussi à ses caractéristiques avantageuses dont on peut citer :

- La disponibilité des équipements d'acquisition, leur simplicité et leurs coûts faibles.
- Passivité du système : un système de reconnaissance de visages ne nécessite aucune coopération de l'individu, du genre : mettre le doigt ou la main sur un dispositif spécifique ou parler dans un microphone. En effet, la personne n'a qu'à rester ou marcher devant une caméra pour qu'elle puisse être identifiée par le système.

En plus, cette technique est très efficace pour les situations non standards, c'est les cas où on ne peut avoir la coopération de l'individu à identifier, par exemple lors d'une arrestation des criminels. Certes que la reconnaissance des visages n'est pas la plus fiable comparée aux autres techniques de biométrie, mais elle peut être ainsi si on utilise des approches plus efficaces en plus du bon choix des caractéristiques d'identification représentant le visage en question.

I.6 Les classes des techniques de reconnaissance de visages

I.6.1 Méthodes globales

Les méthodes globales sont basées sur des techniques d'analyse statistique bien connues. Il n'est pas nécessaire de repérer certains points caractéristiques du visage (comme

les centres des yeux, le centre de la bouche, etc.) à part pour normaliser les images. Dans ces méthodes, les images de visage (qui peuvent être vues comme des matrices de valeurs de pixels) sont traitées de manière globale et sont généralement transformées en vecteurs, plus faciles à manipuler.

L'avantage principal des méthodes globales est qu'elles sont relativement rapides à mettre en œuvre et que les calculs de base sont d'une complexité moyenne. En revanche, elles sont très sensibles aux variations d'éclairement, de pose et d'expression faciale. Ceci se comprend aisément puisque la moindre variation des conditions de l'environnement entraîne des changements inéluctables dans les valeurs des pixels qui sont traités directement.

Ces méthodes utilisent principalement une analyse de sous-espaces de visages. Cette expression repose sur un fait relativement simple : une classe de "*formes*" qui nous intéresse (dans notre cas, *les visages*) réside dans un sous-espace de l'espace de l'image d'entrée. Ainsi, la représentation de l'image originale est très redondante et la dimensionnalité de cette représentation pourrait être grandement réduite si l'on se concentre uniquement sur les formes qui nous intéressent. L'utilisation de techniques de modélisation de sous-espace a fait avancer la technologie de reconnaissance faciale de manière significative.

Nous pouvons distinguer deux types de techniques parmi les méthodes globales, les techniques linéaires et les techniques non linéaires.

Parmi les méthodes globale les plus connues il y'a: PCA, LDA/FLD, …

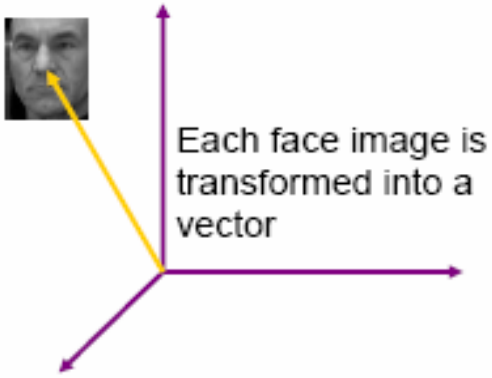

Fig.I.12 : *le principe des méthodes globales.*

I.6.2 Méthodes locale

Les méthodes locales, basées sur des modèles, utilisent des connaissances a priori que l'on possède sur la morphologie du visage et s'appuient en général sur des points caractéristiques de celui-ci. Kanade présenta un des premiers algorithmes de ce type [17] en détectant certains points ou traits caractéristiques d'un visage puis en les comparants avec des

paramètres extraits d'autres visages. Ces méthodes constituent une autre approche pour prendre en compte la non-linéarité en construisant un espace de caractéristiques local et en utilisant des filtres d'images appropriés, de manière à ce que les distributions des visages soient moins affectées par divers changements.

Toutes ces méthodes ont l'avantage de pouvoir modéliser plus facilement les variations de pose, d'éclairage et d'expression par rapport aux méthodes globales. Toutefois, elles sont plus lourdes à utiliser puisqu'il faut souvent placer manuellement un assez grand nombre de points sur le visage alors que les méthodes globales ne nécessitent de connaître que la position des yeux afin de normaliser les images, ce qui peut être fait automatiquement et de manière assez fiable par un algorithme de détection [18].

Dans cette catégorie, on trouve plusieurs méthodes comme: filtres de gabor, Dynamic link architecture, HMM…

I.6.3 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'augmenter la stabilité de la performance de reconnaissance lors de changements de pose, d'éclairement et d'expressions faciales.

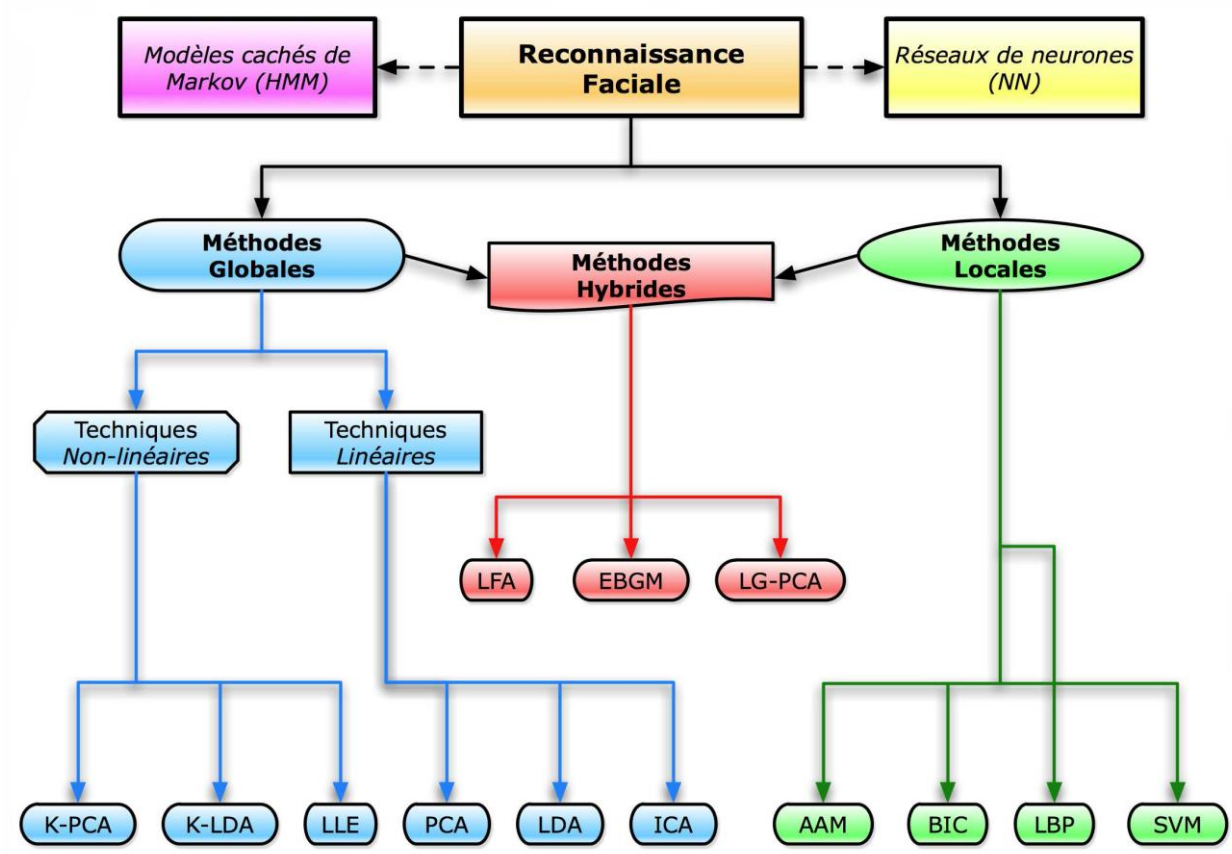

Fig.I.13 : *Une classification des algorithmes principaux utilisés en reconnaissance faciale.*

I.7 Systèmes de reconnaissance de visage

Le système de reconnaissance exploite les caractéristiques du visage ainsi extraites pour créer une signature numérique qu'il stocke dans une base de données. Ainsi, à chaque visage de la base est associée une signature unique qui caractérise la personne correspondante. La reconnaissance d'un visage requête est obtenue par l'extraction de la signature requête correspondante et sa mise en correspondance avec la signature la plus proche dans la base de données. La reconnaissance dépend du mode de comparaison utilisé : vérification ou identification. On peut représenter les systèmes de reconnaissance par la figure suivant :

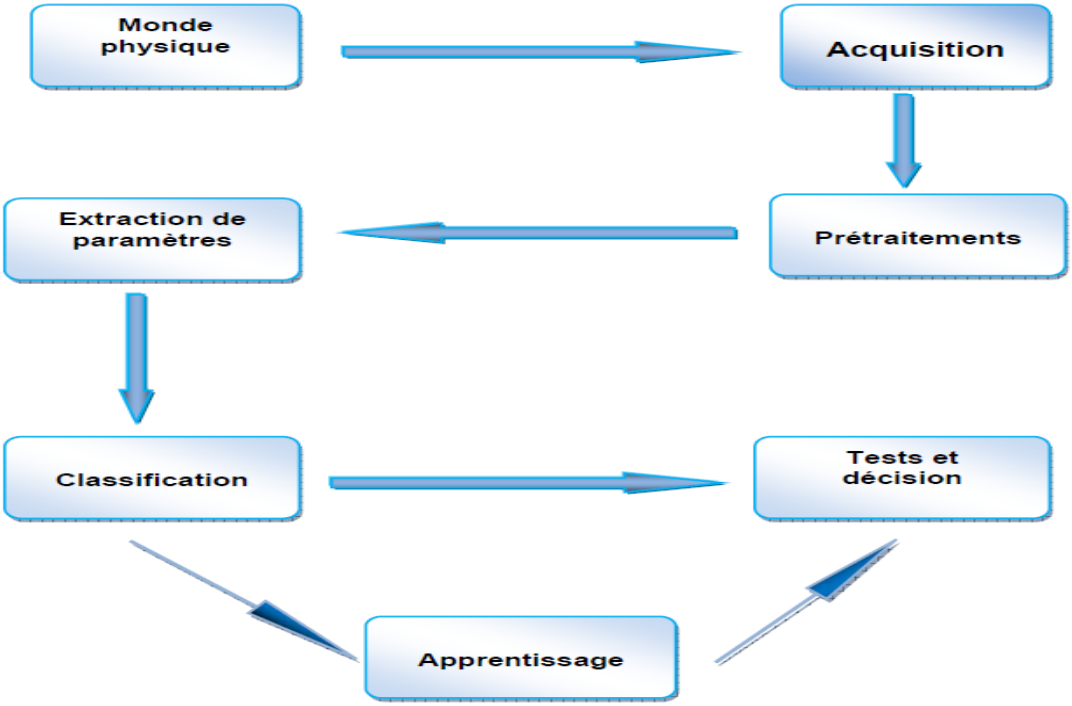

Fig.I.14 : *Système de reconnaissance.*

Donc pour être identifié, l'image d'une personne dans un système de reconnaissance de visages suit les étapes suivantes :

I.7.1 Le monde physique (L'extérieur)

C'est le monde réel en dehors du système avant l'acquisition de l'image. Dans cette étape, on tient compte généralement de trois paramètres essentiels : L'éclairage, la variation de posture et l'échelle. La variation de l'un de ces trois paramètres peut conduire à une distance entre deux images du même individu, supérieure à celle séparant deux images de deux individus différents, et par conséquence une fausse identification.

I.7.2 L'Acquisition de l'image

Cette étape consiste à extraire l'image de l'utilisateur du monde extérieur dans un état statique à l'aide d'un appareil photo ou dynamique à l'aide d'une caméra. Après, l'image extraite sera digitalisée ce qui donne lieu à une représentation bidimensionnelle au visage, caractérisée par une matrice de niveaux de gris. L'image dans cette étape est dans un état brut ce qui engendre un risque de bruit qui peut dégrader les performances du système.

I.7.3 Les prétraitements

Le rôle de cette étape est d'éliminer les parasites causés par la qualité des dispositifs optiques ou électroniques lors de l'acquisition de l'image en entrée, dans le but de ne

conserver que les informations essentielles et donc préparer l'image à l'étape suivante. Elle est indispensable car on ne peut jamais avoir une image sans bruit à cause du background et de la lumière qui est généralement inconnue. Il existe plusieurs types de traitement et d'amélioration de la qualité de l'image, telle que : la normalisation, l'égalisation et le filtre médian. Cette étape peut également contenir la détection et la localisation du visage dans une image, surtout là ou le décor est très complexe.

I.7.4 L'extraction de paramètres

En plus de la classification, l'étape de l'extraction des paramètres représente le cœur du système de reconnaissance, elle consiste à effectuer le traitement de l'image dans un autre espace de travail plus simple et qui assure une meilleure exploitation de données, et donc permettre l'utilisation, seulement, des informations utiles, discriminantes et non redondantes.

I.7.5 La classification (Modélisation)

Cette étape consiste à modéliser les paramètres extraits d'un visage ou d'un ensemble de visages d'un individu en se basant sur leurs caractéristiques communes. Un modèle est un ensemble d'informations utiles, discriminantes et non redondantes qui caractérise un ou plusieurs individus ayant des similarités.

I.7.6 L'apprentissage

C'est l'étape où on fait apprendre les individus au système, elle consiste à mémoriser les paramètres, après extraction et classification, dans une base de données bien ordonnées pour faciliter la phase de reconnaissance et la prise d'une décision, elle est en quelque sorte la mémoire du système.

I.7.7 La décision

C'est l'étape qui fait la différence entre un système d'identification d'individus et un autre de vérification. Dans cette étape, un système d'identification consiste à trouver le modèle qui correspond le mieux au visage pris en entrée à partir de ceux stockés dans la base de données, il est caractérisé par son taux de reconnaissance. Par contre, dans un système de vérification il s'agit de décider si le visage en entrée est bien celui de l'individu (modèle) proclamé ou il s'agit d'un imposteur, il est caractérisé par son EER (equal error rate).

I.8 Principales difficultés de la reconnaissance de visages

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.

I.8.1 Changement d'illumination

Les variations d'éclairage rendent la tache de reconnaissance de visage très difficile. En effet, le changement d'apparence d'un visage du a l'illumination, se révèle parfois plus critique que la différence physique entre les individus, et peut entrainer une mauvaise classification des images d'entrée.

Fig.I.15 : *Exemple de variation d'éclairage.*

I.8.2Variation de pose

Le taux de reconnaissance de visage baisse considérablement quand des variations de pose sont présentes dans les images. La variation de pose est considérée comme un problème majeur pour les systèmes de reconnaissance faciale. Quand le visage est de profil dans le plan image (orientation < 30°), il peut être normalisé en détectant au moins deux traits faciaux (passant par les yeux). Cependant, lorsque la rotation est supérieure à 30°, la normalisation géométrique n'est plus possible

Fig.I.16 : *Exemples de variation de poses.*

I.8.3 Expressions faciales

La déformation du visage qui est due aux expressions faciales est localisée principalement sur la partie inférieure du visage. L'information faciale se situant dans la partie supérieure du visage reste quasi invariable. Elle est généralement suffisante pour effectuer une identification. Toutefois, étant donné que l'expression faciale modifie l'aspect du visage, elle entraine forcement une diminution du taux de reconnaissance. L'identification de visage avec expression faciale est un problème difficile qui est toujours d'actualité et qui reste non résolu.

Fig.I.17 : *Exemples de variation d'expressions.*

I.8.4 Présence ou absence des composants structurels

La présence des composants structurels telle que la barbe, la moustache, ou bien les lunettes peut modifier énormément les caractéristiques faciales telles que la forme, la couleur, ou la taille du visage. De plus, ces composants peuvent cacher les caractéristiques faciales de base causant ainsi une défaillance du système de reconnaissance.

I.8.5 Les vrais jumeaux

Qui ont le même indicatif d'ADN, peuvent tromper les personnes qui ne les connaissent pas (les personnes familiers avec les jumeaux ont reçu une grande quantité d'information sur ces derniers et sont donc beaucoup plus qualifies à distinguer les jumeaux.). Il est peu probable que la vérification automatique de visage, ne pourra jamais détecter les différences très subtiles qui existent entre les jumeaux.

I.9 Conclusion

Dans ce chapitre, nous avons présenté les technologies utilisées dans les systèmes biométriques pour l'identification de personnes. Nous avons aussi donné un aperçu sur les techniques de mesure de leurs performances. Cette étude nous a permis de constater que la reconnaissance de visage suscite de plus en plus l'intérêt de la communauté scientifique, car elle présente plusieurs challenges et verrous technologiques. Enfin, nous avons mis en évidence les différentes difficultés inhérentes à la reconnaissance automatique de visages, ce qui nous a permis de bien définir les problématiques traitées dans ce mémoire. Les techniques utilisées aux différentes étapes de la reconnaissance de visage sont détaillées dans le chapitre suivant.

II.1 Introduction

Bien qu'il existe de nombreux algorithmes de reconnaissance du visage qui fonctionnent bien dans des environnements contraints. Divers changements au niveau des images présentent un grand défi face à un système de reconnaissance qui doit être robuste en ce qui concerne les grandes variabilités des images du visage comme les expressions faciales, la pose du visage et l'éclairage. Pour faire face à ce problème, il est important de choisir une représentation appropriée des images du visage. Cette représentation doit être compacte et significative.

Le but de ce chapitre est de donner un panorama des méthodes les plus significatives en reconnaissance de visages.

II.2 Analyse en Composantes Principales

L'algorithme PCA est né des travaux de MA. Turk et AP. Pentland au MIT Media Lab, en 1991[19,20].

L'idée principale consiste à exprimer les M images de départ selon une base de vecteurs orthogonaux particuliers '' les vecteurs propres '' contenant des informations indépendantes d'un vecteur à l'autre. Ces nouvelles données sont donc exprimées d'une manière plus appropriée à la reconnaissance du visage. Le but est d'extraire l'information caractéristique d'une image de visage en utilisant la KLT ou la DCT , pour l'encoder aussi efficacement que possible afin de la comparer à une base de données de modèles encodés de manière similaire [20].En termes mathématiques, cela revient à trouver les vecteurs propres de la matrice de covariance formée par les différentes images de notre base d'apprentissage. Donc, la PCA ne nécessite aucune connaissance à priori sur l'image et se révèle plus efficace lorsqu'elle est couplée à la mesure de distance Mah Cosine, mais sa simplicité à mettre en œuvre contraste avec une forte sensibilité aux changements d'éclairement, de pose et d'expression faciale [21].

Il exit plusieurs méthode qui basée sur la technique PCA comme la méthode « eigenface ». Son principe est le suivant : étant donné un ensemble d'images de visages exemples, il s'agit tout d'abord de trouver les composantes principales de ces visages. Ceci revient à déterminer les vecteurs propres de la matrice de covariance formée par l'ensemble des images exemples. Chaque visage exemple peut alors être décrit par une combinaison linéaire de ces vecteurs propres. Pour construire la matrice de covariance, chaque image de visage est transformée en vecteur. Chaque élément du vecteur correspond à l'intensité lumineuse d'un pixel.

Dans [22], les auteurs ont démontré que la matrice de covariance C peut s'écrire :

$$C = C_I + C_E$$

C'est-à-dire qu'elle est égale à la somme de la matrice de dispersion intra-personne C_I et la matrice de dispersion inter-personne C_E. Dans le cas d'un seul exemple d'apprentissage par personne, $C_I = 0$, et donc l'équation se réduit à C_E.

L'eigenspace estimé à partir de la matrice C_E seulement n'est pas fiable, parce qu'il ne peut pas différencier de manière efficace l'erreur d'identification des autres erreurs dues à la transformation et au bruit [22]. Pour illustrer l'influence du nombre d'exemples d'apprentissage par personne sur les performances de la reconnaissance, les auteurs ont utilisé la base de données ORL [23] comme base de test. La base de données ORL contient des images de 40 individus, chacun étant enregistré sous 10 vues différentes. Dans leur expérimentation, les auteurs ont fixé le nombre de visages de test. Par contre, ils ont fait varier le nombre de visages d'apprentissage. Ainsi, pour chaque personne, ils ont utilisé la dernière image (Figure II.1) pour le test et ont choisi aléatoirement les n premières images (n <= 9) pour l'apprentissage. Cette procédure a été répétée vingt fois.

Fig.II.1 : *Les dix vues d'une personne dans la base de données ORL.*

Dans le cas extrême, si seulement un exemple d'apprentissage par personne est utilisé, le taux d'identification moyen de l'eigenface tombe en dessous de 65 %. Ce taux atteint 95 % quand on utilise neuf exemples d'apprentissage par personne.

II.3 L'analyse Discriminante Linéaire (LDA)

L'algorithme LDA est né des travaux de Belhumeur et al. De Yale University (USA), en 1997[24]. Il est aussi connu sous le nom de « Fisherfaces ».Contrairement à l'algorithme PCA, celui de la LDA effectue une véritable séparation de classes. Pour pouvoir l'utiliser, il faut donc au préalable organiser la base d'apprentissage d'images en plusieurs classes : une classe par personne et plusieurs images par classe. La LDA analyse les vecteurs propres de la matrice de dispersion des données, avec pour objectif de maximiser les variations entre les images d'individus différents (interclasses) tout en minimisant les variations entre les images d'un même individu (intra-classes).

Cependant, lorsque le nombre d'individus à traiter est plus faible que la résolution de l'image, il est difficile d'appliquer la LDA qui peut alors faire apparaître des matrices de dispersions singulières (non inversibles).

Comme l'ACP ne prend pas en compte la discrimination des classes mais LDA résoudre ce problème, et que les méthodes basées sur LDA standard telles que Fisherfaces, appliquent en premier lieu l'ACP pour la réduction de dimension et puis l'analyse discriminante. Des questions appropriées au sujet de l'ACP sont habituellement liées au nombre des composantes principales (CP) utilisées et comment elles affectent la performance. Concernant l'analyse discriminante on doit comprendre les raisons de sur-ajustage de précision et comment l'éviter. Les réponses a ces deux questions sont étroitement liées. On peut réellement montrer qu'employer plus de CP peut mener a la diminution de la performance de l'authentification. L'explication de ce comportement est que les CP correspondantes aux vecteurs qui ont des petites valeurs propres correspondent aux composantes de hautes fréquences codent habituellement le bruit. En résulte, si les vecteurs propres correspondant aux petites valeurs propres sont employés pour définir le sous-espace réduit de PCA, le procède FLD s'accompagne aussi bien par le bruit et par conséquence le sur-ajustage de précision a lieu. Pour cette raison le modèle améliore du FLD (Enhanced FLD Model : EFM) est employé pour surmonter ces problèmes liés au sur-ajustage de précision, montrée en détail ci-dessous.

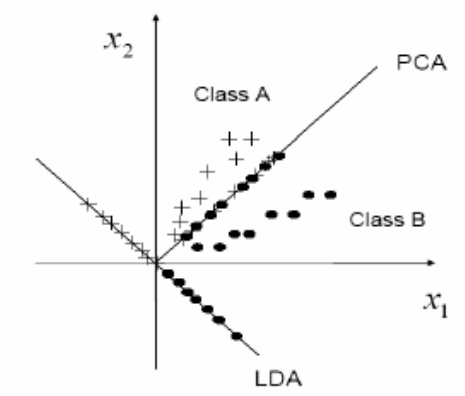

Fig.II.2 : *les projections ACP et LDA d'un ensemble de données.*

II.4 Analyse en composantes indépendantes

L'analyse en composantes indépendantes (ACI) a été introduite par les spécialistes du traitement de signal afin de trouver une solution au problème de séparation des sources lorsque la fonction de mélange F est inconnue. Le traitement consiste à extraire les composantes linéaires d'une observation multi variée afin qu'elles soient aussi indépendantes

que possible. Outre le traitement de signal, cette technique a été utilisée dans d'autres domaines, en l'occurrence les télécommunications et le traitement des signaux biomédicaux. Elle sert généralement à analyser les signaux issus de multiples capteurs pour lesquels la nature exacte des sources est inconnue, d'où vient son appellation de séparation aveugle de sources [27].

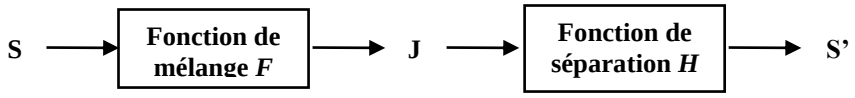

Fig.II.3 : *Modèle général du mélange et de la séparation de sources.*

Dans le cas considéré en reconnaissance de visages, la fonction de séparation H permet d'obtenir une estimation **S'** de la signature d'une image **J** selon **S'= H(J)**. Pour déterminer la fonction H, comme pour l'ACP, on part de la matrice de covariance C des images. Ensuite, plutôt que de diagonaliser cette matrice comme dans l'ACP, on cherche à la factoriser sous une forme qui autorise que les axes autour desquels se concentre l'information ne soient pas forcément orthogonaux [28, 29]. Cette factorisation, obtenue de façon itérative par des algorithmes variés, détermine conjointement la fonction de séparation H.

Cette approche a été utilisée par [30] pour la reconnaissance de visages. Il propose deux modèles différents de mélange des sources aboutissant à la formation de l'image J à partir des signatures (Fig.II.4). Dans chaque cas, il utilise une analyse en composantes indépendantes pour déterminer les fonctions de séparation. Les deux méthodes ont été testées sur la base de données FERET et ont donné de bons résultats (88% de taux de reconnaissance). Les tests effectués sur les bases Yale Faces et AT&T ont donné également des résultats satisfaisants (respectivement 96.36 % et 99.00 % de taux de reconnaissance) et ainsi prouvé l'efficacité de la méthode [31].

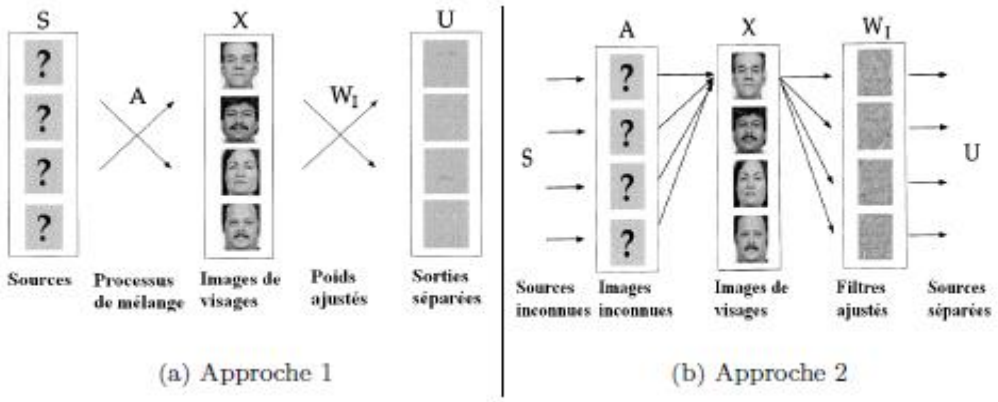

Fig.II.4 : *Le modèle de synthèse d'image de l'architecture d'ICA.*

Il faut également noter que de nombreuses variantes de l'algorithme d'ACI ont été proposées récemment. On trouve en particulier la technique rapide (Fast ICA), ou aussi FICA (FLD ICA) : la combinaison entre l'analyse en composantes indépendantes et l'analyse discriminante de Fisher [32]. Ces améliorations ont permis de remédier au problème du temps de calcul observé avec l'ACI classique. On trouve également des variantes basées sur la façon de traiter l'image originale, telle que la technique basée sur l'ACI par blocs [33]. Il s'agit ici de subdiviser l'image en ensemble de blocs et d'appliquer une ACI à chacun. En terme de comparaison, il a été démontré que l'ACI, ainsi que ses différentes variantes, est très performante par rapport à l'ACP. En effet, les composantes recherchées dans l'espace de représentation des images ne sont pas forcément orthogonales pour l'ACI, alors qu'elles le sont pour l'ACP.

II.5 Les réseaux de neurones (RNA)

Parmi les techniques non-linéaires d'extraction de signatures qui ont été largement utilisées pour la reconnaissance de visages, on trouve celles qui reposent sur un réseau de neurones artificiels (RNA). Ces derniers ont été initialement inspirés de la physiologie du système nerveux si parfaitement créée et conçue. Le neurone formel, introduit par J.Mc Culloch et W. Pitts dans les années quarante, constitue la base de l'architecture des RNA.

Un neurone formel est une fonction algébrique non-linéaire (paramétrée et à valeurs bornées) de variables réelles appelées entrées, qui tente de reproduire ce mode de fonctionnement. Un neurone formel effectue une somme pondérée des signaux d'entrée qui lui parviennent. Cette somme pondérée sert de paramètre à une fonction, souvent non linéaire, qui la transforme en nouveau signal transmis à la sortie (Fig.II.5).En référence au fonctionnement du neurone biologique, la fonction intervenant après la sommation des entrées est appelée fonction d'activation.

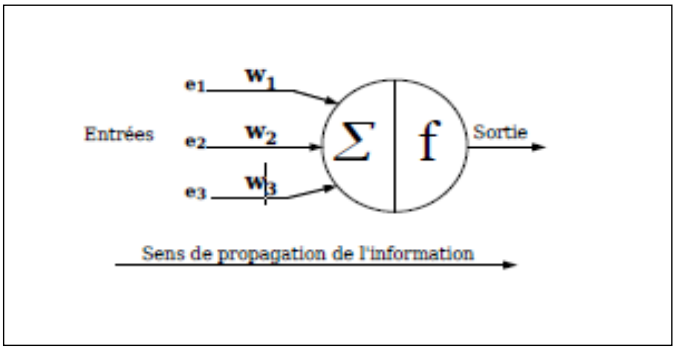

Fig.II.5 : *Neurone formel.*

Les RNA ont été utilisés dans nombreuses applications, particulièrement pour la classification de données, la modélisation de processus complexes et le traitement non-linéaire des signaux. Ces recherches ont engendré une panoplie d'architectures de réseaux dont chacune répond parfaitement à une application donnée. On note en particulier l'architecture MLP (Multi-Layer Perceptron, Perceptron Multicouches), l'architecture RBF (Radial Basis Function, Fonctions à base radiale) et l'architecture SOM (Self-Organizing Maps, Cartes auto organisatrices de Kohonen).

Dans le cas de la reconnaissance de visages, on constate que les réseaux de neurones ont été employés dans tous les modules intervenant dans la chaîne de traitements. Ils sont utilisés pour la détection de visages, pour l'extraction de signatures et pour la classification.

II.6 Machine à Vecteurs de Support (SVM)

C'est une technique qui a été proposée par V.Vapnik en 1995, elle est utilisée dans plusieurs domaines statistiques (classement, régression, fusion,… etc).

L'idée essentielle de cette approche consiste à projeter les données de l'espace d'entrée (appartenant à des classes différentes) non linéairement séparables, dans un espace de plus grande dimension appelé espace de caractéristiques, de façon à ce que les données deviennent linéairement séparables [25,26].

Dans cet espace, la technique de construction de l'hyperplan optimal est utilisée pour calculer la fonction de classement séparant les classes tels que :

- Les vecteurs appartenant aux différentes classes se trouvent de différents côtés de l'hyperplan.
- La plus petite distance entre les vecteurs et l'hyperplan (la marge) soit maximale.

Depuis son introduction dans le domaine de reconnaissance de formes, plusieurs travaux ont montré l'efficacité de cette technique, principalement en traitement d'images.

II.7 Modèle de Markov caché

Les modèles de Markov cachés *HMMs* sont massivement utilisés en reconnaissance de formes, en intelligence artificielle ou encore en traitement automatique du langage naturel. Les *HMMs* sont généralement employés pour la modélisation statistique de séries de vecteur de temps non stationnaire. En considérant l'information du visage comme étant une séquence variable dans le temps, le *HMM* peut être appliqué à la reconnaissance de visages [35]. Les caractéristiques faciales les plus significatives d'une image de visage frontale, à savoir les cheveux, le front, les yeux, le nez et la bouche, se présentent dans un ordre naturel de haut en

bas, même dans le cas où il y'a des petites rotations. En se basant sur cette observation, l'image d'un visage peut être modélisée en utilisant un *HMM* unidimensionnel en assignant à chacune de ces régions un état. Le *HMM* classifie une caractéristique par la propriété de la *chaîne de Markov*. Une séquence des valeurs des pixels forme une *chaîne de Markov*, si la probabilité que le système à l'instant n+1 soit à l'état *x n*+1 dépend uniquement de la probabilité que le système à l'instant n soit à l'état *x n*.

Dans une *chaîne de Markov*, la transition d'un état à un autre est probabiliste ce qui donne une distribution de probabilité de l'ensemble des sorties de chaque état. Ce résultat est employé pour faire la comparaison entre deux visages [35] [36].

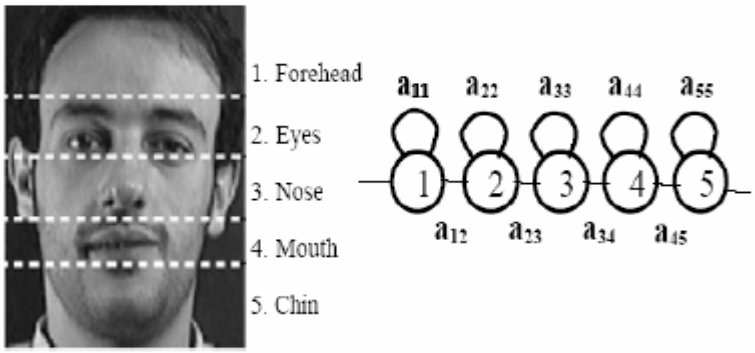

Fig.II.6 : *les 5 états du HMM (de haut en bas).*

Pour une image de visage d'une personne donnée de l'ensemble d'apprentissage, le but de l'étape d'apprentissage est d'optimiser les paramètres pour mieux décrire l'observation. La reconnaissance est effectuée en assortissant l'image de test contre chaque modèle d'apprentissage (chaque *HMM* représente une personne différente). Et dans la fin de cette procédure, l'image est convertie en une séquence d'observation et la probabilité est calculée pour chaque modèle enregistré.

Le modèle avec la probabilité la plus élevée indique l'identité de la personne inconnue [35] [34]. L'approche *HMM* à des performances de reconnaissance satisfaisantes, cependant il nécessite des calculs intenses ce qui augmente les temps d'exécution.

II.8 Template matching

Les templates peuvent être définis soit "manuellement", soit paramétrés à l'aide de fonctions. L'idée est de calculer la corrélation entre l'image candidate et le template. Ces méthodes rencontrent encore quelques problèmes de robustesse liés aux variations de lumière, d'échelle, etc. Sinha [37] [38] utilise un ensemble d'invariants décrivant le modèle du visage. Afin de déterminer les invariants aux changements de luminosité permettant de caractériser

les différentes parties du visage (telles que les yeux, les joues, et le front), cet algorithme calcule ainsi les rapports de luminance entre les régions du visage et retient les directions de ces rapports.

Yuille et al. [39] ont utilisé un template déformable pour modéliser les caractéristiques faciales. Ce template adapte un modèle élastique, connu a priori, aux caractéristiques faciales (e.g., yeux). Dans cette approche les caractéristiques faciales sont décrites par des templates paramétriques. Une fonction d'énergie est définie pour lier les contours, les sommets et les vallées dans l'image d'entrée aux paramètres correspondants dans le template. Le meilleur ajustement du modèle élastique est trouvé en minimisant une fonction d'énergie des paramètres. Bien que leurs résultats expérimentaux démontrent une bonne performance pour le suivi de caractéristiques non rigides, un inconvénient de cette approche est que le template déformable doit être initialisé dans la proximité de l'objet d'intérêt. Pour détecter les caractéristiques faciales pour la reconnaissance de visage, Brunelli et Peggio [40] ont utilisé, pour chaque région extraite, un détecteur approprié.

Fig.II.7 : *Différentes régions utilisées pour la phase de template matching.*

Pour les régions yeux, nez et bouche, ils utilisent la direction du gradient vertical et horizontal. La bouche et le nez sont localisés en utilisant des stratégies similaires. La position verticale est déterminée grâce aux standards anthropométriques. D'abord, une estimation fine de leur position réelle est obtenue en cherchant les pics de la projection horizontale du gradient vertical pour le nez, et les vallées de la projection horizontale de l'intensité pour la bouche.

La position des sourcils et leur épaisseur peuvent être trouvées par une analyse similaire. La recherche est une fois encore limitée à la fenêtre d'intérêt, juste au-dessus des yeux, et les sourcils sont trouvés en utilisant la carte du gradient vertical. Le détecteur du sourcil cherche les pairs de pics du gradient ayant des directions opposées.

II.9 Les Modèles Actifs d'Apparence

Les modèles actifs d'apparence (AAM) permettent de prendre en compte l'information de texture, en plus de celle de forme. Ils cherchent a minimiser la différence entre l'image originale et une image synthétique, construite à partir de la forme moyenne, de la texture moyenne et d'un vecteur de paramètres. Ils se basent sur l'ACP pour représenter conjointement les variations de forme et de texture présentes dans un ensemble d'apprentissage. le « Modèle Actif d'Apparence » présente un outil d'extraction des caractéristiques (signatures) représentant, à la fois, la forme et la texture des visages.

II.10 Approches basées sur les graphes

Plutôt que d'utiliser des méthodes purement géométriques, certains chercheurs ont choisi de représenter les caractéristiques locales du visage sous forme de graphes. Ils sont basée sur la décomposition en ondelettes de Gabor . La reconnaissance de visages est alors formulée comme un problème de mise en correspondance de graphes.

Cependant, une fois construit, le graphe topologique ne peut pas être modifié. Or, les images de visage changent facilement d'apparence en raison des différentes variations (illumination, expression, pose, etc.), et du coup un schéma de graphe topologique fixe n'est plus adéquat.

II.10.1 Elastic Graph Matching

L'algorithme d'*EGM* "*Elastic Graph Matching*" est décrit en *Architecture Dynamique De Lien DLA,* il représente des visages individuels par un graphe rectangulaire. Chaque nœud du graphe est étiqueté avec un ensemble de *coefficients complexes des ondelettes de Gabor* appelés *jets* différant en orientation et en échelle. Un *jet* est utilisé pour représenter les caractéristiques locales des images de visages en se basant sur *la transformée en ondelettes de Gabor*. Seulement les magnitudes des coefficients sont utilisées pour la reconnaissance.

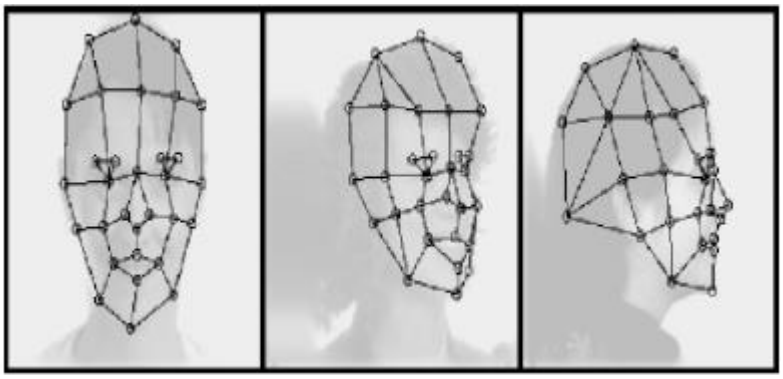

Fig.II.8 : *La représentation des visages par graphe rectangulaire.*

Pour la reconnaissance d'un nouveau visage, chaque graphe de la base de donnée est ajusté à ce nouveau graphe construit, et le bon ajustement indique la personne reconnue.

D'encouragent résultats sont obtenus lors d'utilisation de visages avec de large rotation d'angles. En général la *DLA* est bonne en terme de variation de rotation, cependant le processus de reconnaissance ou d'ajustement est coûteux en calcul.

L'*EGM* utilise la phase des *coefficients complexes des ondelettes de Gabor* pour réaliser une localisation plus précise des nœuds et pour différencier les modèles similaires en leurs coefficients de magnitude.

L'*EGM* emploi des *graphes adaptatifs d'objet* "*object adaptive graphs*", dont les nœuds référent aux *points de repère faciaux spécifiques,* ou les *points fiduciels* "*fiducial points*" dans le visage, à savoir les pupilles, les coins de la bouche et le bout du nez.

II.10 .2 ElasticBuch Graph Matching

Dans cette approche, on localise des points caractéristiques (coins des yeux, de la bouche, nez, etc.) à partir d'une image de visage, cette localisation peut se faire manuellement ou automatiquement à l'aide d'un algorithme. Un treillis élastique virtuel est ensuite appliqué sur l'image de visage à partir de ces points.

Chaque point représente un nœud labellisé auquel on associe un jeu de coefficients d'ondelettes complexes de Gabor, appelés Jet. Pour effectuer une reconnaissance avec une image test, on fait une mesure de similarité entre les différents Jets et les longueurs des segments du treillis de deux images.

La caractéristique de l'EBGM c'est qu'il ne traite pas directement les valeurs de niveaux de gris des pixels d'une image de visage, ce qui lui confère une plus grande robustesse aux changements d'éclairement, de pose et d'expression faciale. Cependant il est plus difficile à implémenter que les méthodes globales [19].

II.11 Les systèmes biométriques existants pour la reconnaissance des visages

Les systèmes biométriques de reconnaissance des visages se trouvent être de plus en plus répandus. Voici cités ci-dessous quelques systèmes mis en œuvre ainsi que les différents domaines d'utilisation de cette technologie en pleine expansion : Le 14 octobre 1998, le *Borough de Newham* de Londres mît en service un système qui a diminué le nombre de crimes et délits de 10 % en 6 mois, grâce à l'utilisation du logiciel de reconnaissance de visage appelé « Mandrake ». Le système alertait les opérateurs de caméra dès qu'il y avait 80 % de concordances entre l'image préalablement numérisée d'un délinquant et ce que captaient les

caméras. Les systèmes de reconnaissance des visages sont déployés dans le transport aérien, le système « Smart Gate » par exemple a été mis en œuvre afin d'effectuer une vérification automatique de l'identité pour l'équipage d'Aéronef traversant la frontière de l'Australie. Ce dernier effectue une comparaison entre le visage d'une personne à sa photographie de passeport [41] .

En Janvier 2002, « Visage Technology » le fournisseur de technologie et services de reconnaissance des visages a annoncé l'installation du premier système de reconnaissance des visages en Floride dans l'aéroport international St. Petersburg- Clearwater [42].

Cette technologie est aussi utilisée afin d'identifier les personnes recherchées en comparant les photos des passeports avec une base de personnes recherchées. Il existe encore toute une panoplie d'utilisations de la reconnaissance des visages. Aujourd'hui Les ATM's (Automatic Teller Machine : Distributeurs automatiques de billet mis en services par les banques ou autres institutions financières) identifient les utilisateurs non grâce à leurs numéros de carte bancaire, mais en se référant en plus à leur visage. En effet, l'ATM capture une image d'un visage et compare celle-ci avec la photo de la base afin de confirmer son identité. Plusieurs entreprises ont orienté leurs activités vers cette technologie, on retrouve par exemple L'Entreprise « Widget » qui a mis au point le système « Snappy Face» qui permet d'identifier le visage du propriétaire de l'ordinateur pour sécuriser son accès grâce à une webcam. ou encore « TitaniumTechnology Entreprise » basée à Pékin qui a développé un logiciel de reconnaissance automatique de visages pour la surveillance (Automatic Face Recognition Systems ou AFRS) nommé « ProFaceriDVR » [43].

II.12 Conclusion

Dans ce chapitre, nous avons présenté les principales techniques de reconnaissance de visages, Puis nous avons énoncé quelques systèmes commercialisés sur le marché. Cet engouement pour les systèmes de reconnaissance des visages est justifié par les nombreux avantages de cette approche. En effet cette technologie est peu couteuse, peu encombrante, elle est de surcroit peu contraignant pour les usagers.

I.1 Introduction

Parmi les différentes biométries, le visage est la caractéristique la plus utilisée par l'homme pour identifier un membre de son entourage. Afin de simuler ce comportement biologique, les chercheurs se sont mis à concevoir des systèmes de plus en plus performants. Dès lors, la reconnaissance des visages a connu un fort développement et reste un domaine qui suscite toujours des interrogations et un engouement par les chercheurs. Parmi toutes les méthodes présentées dans l'état de l'art, certaines demeurent plus avantageuses que d'autres et Les critères utilisés pour cette sélection reposent notamment sur les temps d'exécution et les taux de reconnaissance de cette dernière. Ce chapitre est divisé en deux parties : dans la première partie, nous décrivons en détail notre technique d'extraction de caractéristiques et réduction de dimension des données basée sur l'Analyse en Composantes Principales (ACP), ensuite nous présentons l'approche LBP (Local Binary Pattern).

III.2 Reconnaissance de visage Eigenface

III.2.1 Présentation de la méthode Eigenface

L'algorithme ACP, PCA en anglais (Principal Component Analysis) et aussi connu sous le nom d'Eigenfaces puisque il utilise des vecteurs propres et des valeurs propres. (respectivement *Eigenvectors* et *Eigenvalues* en anglais). Cet algorithme s'appuie sur des propriétés statistiques bien connues et utilise l'algèbre linéaire. Il est relativement rapide à mettre en œuvre mais il est sensible aux problèmes d'éclairages [20], de pose et d'expression faciale. Il est à la base de nombreux algorithmes globaux actuels.

L'idée principale consiste à exprimer les M images d'apprentissage selon une base de vecteurs orthogonaux particuliers, contenant des informations indépendantes d'un vecteur à l'autre. Ces nouvelles données sont donc exprimées d'une manière plus appropriée à la reconnaissance du visage.

Nous voulons extraire l'information caractéristique d'une image de visage, pour l'encoder aussi efficacement que possible afin de la comparer à une base de données de modèles encodés de manière similaire. En termes mathématiques, cela revient à trouver les vecteurs propres de la matrice de covariance formée par les différentes images de notre base d'apprentissage .Une image $I_{i\ (m,n)}$ est traitée comme un vecteur $\Gamma_{i(m\times n,1)}$ dans un espace vectoriel de grande dimension $(N = m \times n)$, par concaténation des colonnes.

$$\mathbf{I_1} = \begin{pmatrix} a_{1,1} & \dots & a_{1,m} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \dots & a_{n,m} \end{pmatrix} \quad \Rightarrow \quad \mathbf{\Gamma_1} = \begin{pmatrix} a_{1,1} \\ \vdots \\ a_{n,1} \\ \vdots \\ a_{1,m} \\ \vdots \\ a_{n,m} \end{pmatrix}$$

Fig.III.1 : *Passage d'une image vers un vecteur colonnes.*

Les coefficients $a_{i,j}$ représentent les valeurs des pixels en niveau de gris, codés de 0 à 255.

Après avoir rassemblé nos M images dans une unique matrice, nous obtenons une matrice d'images Γ, où chaque colonne représente une image Γ_i:

$$\mathbf{\Gamma} = \begin{pmatrix} a_{1,1} & b_{1,1} & \dots & z_{1,1} \\ \vdots & \vdots & \dots & \vdots \\ a_{n,1} & b_{n,1} & \dots & z_{n,1} \\ \vdots & \vdots & \dots & \vdots \\ a_{1,m} & b_{1,m} & \dots & z_{1,m} \\ \vdots & \vdots & \dots & \vdots \\ a_{n,m} & b_{n,m} & \dots & z_{n,m} \end{pmatrix}$$

On calcule ensuite l'image moyenne Ψ de toutes les images collectées.

Cette image peut être vue comme le centre de gravité du jeu d'images (Fig.III.2) :

$$\Psi = \frac{1}{M}\sum_{i=1}^{M} \Gamma_i \qquad \text{(III.1)}$$

On ajuste ensuite les données par rapport à la moyenne.

Fig.III.2: *Image moyenne.*

L'image moyenne est alors soustraite de chaque image avec la formule suivante:

$$\Phi_i = \Gamma_i - \Psi, \quad i = 1 \dots . M \qquad \text{(III.2)}$$

On calcule ensuite la matrice de covariance du jeu de données. Cette matrice peut être vue comme une matrice de moments d'ordre 2 :

$$C = \sum_{i=1}^{M} \Phi_i \Phi_i^T = AA^T \,, A = [\,\Phi_1, \Phi_2, \dots \dots \Phi_M] \qquad \text{(III.3)}$$

La prochaine étape consiste à calculer les vecteurs propres et les valeurs propres de cette matrice de covariance C de taille (N × N), c'est-à-dire de l'ordre de la résolution d'une image. Le problème est que cela peut parfois être très difficile et très long. En effet, si N > M (si la résolution est supérieure au nombre d'images), il y aura seulement (M -1) vecteurs propres qui contiendront de l'information [4] (les vecteurs propres restants auront des valeurs propres associées nulles). Par exemple, pour 50 images de résolution 180 × 200, nous pourrions résoudre une matrice L de 50 × 50 au lieu d'une matrice de 36000 × 36000 pour ensuite prendre les combinaisons linéaires appropriées des images Φ_i. Le gain de temps de calcul serait considérable, nous passerions d'une complexité de l'ordre du nombre de pixels dans une image à celle de l'ordre du nombre d'images.

Les étapes du processus qui nous permettent d'accélérer les calculs sont décrits ci-dessous :

Considérons les vecteurs propres e_i de $C = AA^T$, associés aux valeurs propres λ_iOn a :

$$Ce_i = \lambda_i e_i \tag{III.4}$$

Les vecteurs propres v_i de $L = A^T A$, associés aux valeurs propres $\mu_i$sont tels que :

$$Lv_i = \mu_i v_i \tag{III.5}$$

Soit :

$$A^T A v_i = \mu_i v_i \tag{III.6}$$

En multipliant à gauche par A des deux côtés de l'égalité, nous obtenons :

$$AA^T A v_i = A\mu_i v_i \tag{III.7}$$

Puisque $C = AA^T$, nous pouvons simplifier :

$$C(Av_i) = \mu_i (Av_i) \tag{III.8}$$

De (III.4) et (III.8), nous voyons que Av_i et μ_i sont respectivement les vecteurs propres et les valeurs propres de C :

$$\begin{cases} e_i = Av_i \\ \lambda_i = \mu_i \end{cases} \tag{III.9}$$

Nous pouvons donc trouver les valeurs propres de cette énorme matrice C en trouvant les valeurs propres d'une matrice L beaucoup plus petite. Pour trouver les vecteurs propres de C, il suffit juste de multiplier les vecteurs propres de L par la matrice A. Les vecteurs propres trouvés sont ensuite ordonnés selon leurs valeurs propres correspondantes, de manière décroissante. Plus une valeur propre est grande, plus la variance capturée par le vecteur propre

est importante. Cela implique que la majeure partie des informations est contenue dans les premiers vecteurs propres.

Une part de la grande efficacité de l'algorithme PCA vient de l'étape suivante qui consiste à ne sélectionner que les k meilleurs vecteurs propres (ceux avec les k plus grandes valeurs propres). On définit alors un espace vectoriel engendré par ces k vecteurs propres, que l'on appelle *l'espace des visages* E_v « *Face Space* ».

Les images originales peuvent être reconstituées par combinaison linéaire de ces vecteurs propres. Les représentations graphiques de ces vecteurs rappellent un peu des images fantômes, chacune mettant en avant une partie du visage, on les appelle *eigenfaces* (Fig.III.4).

Pratiquement, le choix de « k » peut se faire soit en fixant un certain pourcentage D tel que :

$$\frac{\sum_{i=K+1}^{n} \lambda_i}{\sum_{i=1}^{n} \lambda_i} < D \qquad \text{(III.10)}$$

Avec n représente le nombre total des valeurs propres on se basant sur le fait que la i^{ème} valeur propre est égale à la variance le long de la i^{ème} composante principale et on cherche, donc « k » le long du spectre des valeurs propres juste avant qu'il s'annule [20].

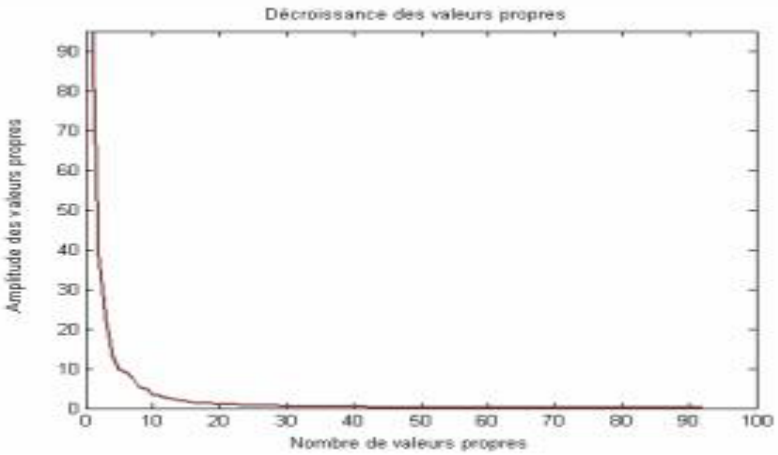

Fig.III.3 : *Décroissance des valeurs propres de la base de données utilisée en fonction du nombre de vecteurs propres retenu.*

Donc, les « k » premiers vecteurs propres correspondant aux « k » plus grandes valeurs propres sont un paramètre critique sur lequel dépend la performance du système de reconnaissance de visages (temps de calcul et taux de reconnaissance) et aussi un critère d'évaluation [20] des méthodes basées sur l'ACP.

A partir de là, on définit un espace vectoriel engendré par ces k vecteurs propres, que l'on appelle l'espace des visages E_v (Face Space). Les images originales peuvent être reconstituées par combinaison linéaire de ces vecteurs propres. Les représentations graphiques

de ces vecteurs rappellent un peu des images fantômes, chacune mettant en avant une partie du visage, on les appelle Eigenfaces (Fig.III.4).

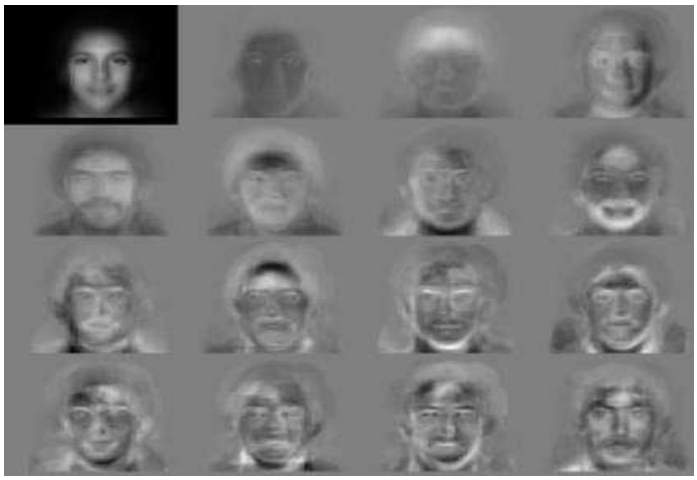

Fig.III.4 : *eigenfaces.*

III.2.2 Utilisation des Eigenfaces pour la classification des images visage

Nous allons maintenant projeter nos images de départ sur E_{v}. Une image Γ'_{i} est alors transformée en ses composantes Eigenfaces par une simple opération de projection vectorielle

$$\omega_K = e_K^T(\Gamma'_i - \Psi)\ , K = 1, \dots\ , M' \qquad \text{(III.11)}$$

Les vecteurs ω_K sont appelés vecteurs de poids et forment une matrice [44] Ω_T = $[\omega_1, \omega_2\ , \dots,, \omega_{M0}]$ qui décrit la contribution de chaque eigenface dans la représentation de l'image d'entrée. La matrice Ω_T est alors utilisée pour trouver quelle est, parmi un nombre prédéfini de classes, celle qui décrit le mieux une image d'entrée.

La méthode la plus simple pour déterminer quelle classe de visage fournit la meilleure description d'une image d'entrée est de trouver la classe de visage k qui minimise la distance Euclidienne.

$$\varepsilon_K^2 = \|\Omega - \Omega_K\|^2 \qquad \text{(III.12)}$$

Où Ω_K est un vecteur qui décrit la k^{ième} classe de visage.

Un visage appartient à une classe k quand le minimum ε_K est en dessous d'un certain seuil θ_ε Dans le cas contraire, le visage est classé comme étant inconnu et peut éventuellement être utilisé pour créer une nouvelle classe de visage. La création de la matrice de poids Ω^T est équivalente à la projection du visage original sur E_{v}. Puisque la distance ε entre l'image de visage et E_{v} est simplement le carré de la distance entre l'image d'entrée réajustée par rapport à la moyenne $\Phi = \Gamma' - \Psi$ et $\Phi_f = \sum_{i=1}^{M'} \omega_i e_i$, sa projection sur E_v est : $\varepsilon^2 = \|\Omega - \Omega_K\|^2$.

Il y a alors, quatre possibilités (Fig.III.5) pour une image d'entrée d'être reconnue ou non :

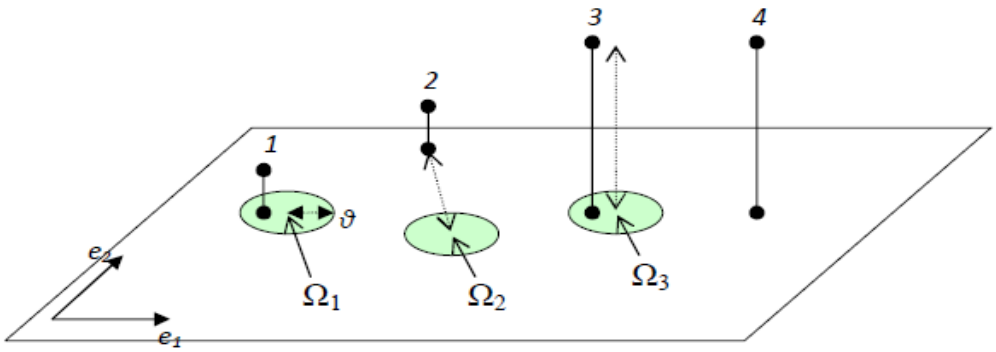

Fig.III.5 : *Illustration des cas possibles de classification d'une image.*

- ✓ Cas 1 : un individu est reconnu et identifié.
- ✓ Cas 2 : un individu inconnu du système est présent.
- ✓ Cas 3 et 4 : indiquent que l'image n'est pas une image de visage.

.

III.2.3 Principales étapes de la techniques d'eigenfaces

L'apprentissage des visages propres s'effectue selon les étapes suivantes :

1) Collecte des M images faciales et construction de la matrice T de taille M, par concaténation des colonnes des images faciales. Prétraitement des images collectées.
2) Calcul du visage moyen en sommant les colonnes de la matrice T et en divisant le vecteur résultant par le nombre d'image d'entrée (M).
3) Soustraction du visage moyen de la matrice T pour obtenir la matrice A ; où chaque élément représente la variance des valeurs d'intensité de chaque pixel.
4) Calcul de la matrice C', $C' = A^T A$.
5) Calcul des vecteurs propres de C' et les triés dans un ordre descendant selon les valeurs propres associées.
6) Calcul des vecteurs propres de la matrice de covariance C et obtention des visages propres en multipliant les vecteurs propres de C' par la matrice A.
7) Choix des K meilleur valeurs propres et les vecteurs propres associés.
8) Détermination du poids des images d'entrée en projetant chaque image dans l'espace visage.
9) Chaque visage est maintenant représenté par un vecteur qui est utilisé pour reconstruire les images. après on sauvegarde le visage moyen, les eigenfaces et la matrices de projection (de poids) des images.

Les neuf étapes décrites transformeront une base de données d'images faciales en un ensemble de projections dans l'espace visage (face space).

L'étape de reconnaissance peut être résumée comme suit :

- Prétraitement de l'image d'entrée et soustraction du visage moyen.
- Détermination du poids de l'image d'entrée par la projection de celle–ci dans l'espace visage en multipliant le vecteur résultant de l'étape (1) par les eigenfaces de la base de données.
- Comparaison des résultats obtenus en utilisant des métriques telles que la distance Euclidienne.

III.2.4 Mesures de Distance

Lorsqu'on souhaite comparer deux vecteurs de caractéristiques issus du module d'extraction de caractéristiques d'un système biométrique, on peut soit effectuer une mesure de similarité (ressemblance), soit une mesure de distance (divergence).

La première catégorie de distances est constituée de distances Euclidiennes et sont définies à partir de la distance de Minkowski d'ordre p dans un espace euclidien (déterminant la dimension de l'espace euclidien).

Considérons deux vecteurs $X = (x_1, x_2, \dots\dots, x_n)$ et $Y = (y_1, y_2, \dots\dots, y_n)$, la distance de Minkowski d'ordre p notée $L_p$est définie par :

$$L_p = \left(\sum_{i=1}^{n} (|x_i - y_i|)^p\right)^{1/p} \tag{III.13}$$

Nous allons présenter quelques mesures de distance dans l'espace original des images puis dans l'espace de Mahalanobis.

III.2.4.1 Distances Euclidiennes

A. Distance City Block (L1)

Pour p = 1, on obtient la distance City-Block (ou distance de Manhattan) :

$$L_1(x, y) = \sum_{i=1}^{n} |x_i - y_i| \tag{III.14}$$

B. Distance Euclidienne (L2)

Pour p = 2, on obtient la distance euclidienne :

$$L_2(x, y) = \sqrt{\sum_{i=1}^{n} |x_i - y_i|^2} \tag{III.15}$$

Les objets peuvent alors apparaître de façons très différentes selon la mesure de distance choisie (Fig.III.6).

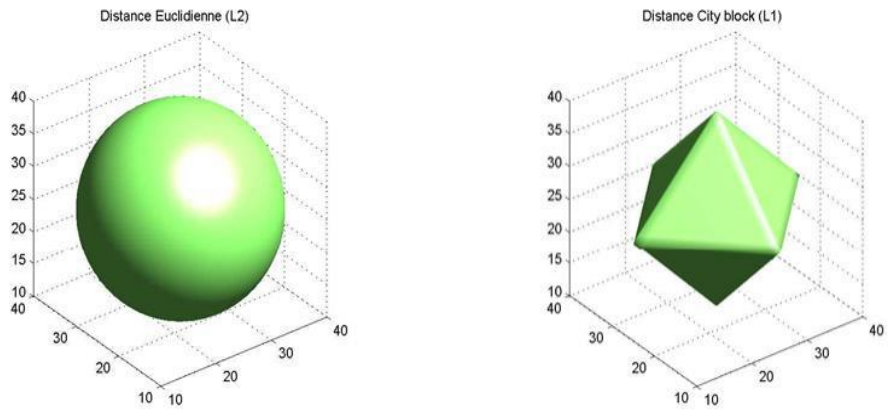

Fig.III.6 : *Représentation d'une sphère avec la distance euclidienne (III.2.4.1.B) et la distance City-Block (III.2.4.1.A).*

III.2.4.2 Distances dans l'Espace de Mahalanobis

A- De l'espace des images à l'espace de Mahalanobis

Avant de pouvoir effectuer des mesures de distance dans l'espace de Mahalanobis, il est essentiel de bien comprendre comment l'on passe de l'espace des images Im à l'espace de Mahalanobis $\mathcal{E}_{Mah}$.

En sortie de l'algorithme PCA, nous obtenons des vecteurs propres associés à des valeurs propres (représentant la variance selon chaque dimension). Ces vecteurs propres définissent une rotation vers un espace dont la covariance entre les différentes dimensions est nulle. L'espace de Mahalanobis est un espace où la variance selon chaque dimension est égale à 1. On l'obtient à partir de l'espace des images Im en divisant chaque vecteur propre par son écart-type correspondant.

Soit u et v deux vecteurs propres de I_m, issus de l'algorithme PCA, et *m* et *n* deux vecteurs de $\mathcal{E}_{Mah}$. Soit λ_i les valeurs propres associées aux vecteurs *u* et *v*, et σ_i l'écart-type, alors on définit $\lambda_i = \sigma_i$. Les vecteurs *u* et *v* sont reliés aux vecteurs *m* et *n* à partir des relations suivantes :

$$m_i = \frac{u_i}{\sigma_i} = \frac{u_i}{\sqrt{\lambda_i}} \text{ et } n_i = \frac{v_i}{\sigma_i} = \frac{v_i}{\sqrt{\lambda_i}} \qquad \text{(III.16)}$$

B- Mahalanobis L1 (MahL1)

Cette distance est exactement la même que la distance City-Block sauf que les vecteurs sont projetés dans l'espace de Mahalanobis. Ainsi, pour des vecteurs propres *u* et *v* de projections respectives *m* et *n* sur l'espace de Mahalanobis, la distance Mahalanobis L_1 est définit par :

$$Mah_{L1}(u,v) = \sum_{i=1}^{N} |m_i - n_i| \tag{III.17}$$

C- Mahalanobis L2 (MahL2)

Cette distance est identique à la distance euclidienne à part qu'elle est calculée dans l'espace de Mahalanobis. Ainsi, pour des vecteurs propres u et v de projections respectives m et n sur l'espace de Mahalanobis, la distance Mahalanobis L_2 est dénie par :

$$Mah_{L2}(u,v) = \sqrt{\sum_{i=1}^{N} |m_i - n_i|^2} \tag{III.18}$$

Par défaut, lorsqu'on parle de distance de Mahalanobis, c'est à cette distance que l'on doit se référer.

III.2.4.3 Cosinus de Mahalanobis (MahCosine)

Il s'agit tout simplement du cosinus de l'angle entre les vecteurs *u* et *v*, une fois qu'ils ont été projetés sur et normalisées par des estimateurs de la variance (Fig.III.7).

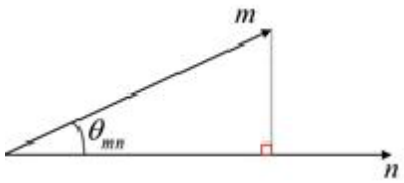

Fig.III.7 : *Les deux vecteurs m et n dans l'espace de Mahalanobis.*

Nous avons donc par définition :

$$S_{Mahcosine}(u,v) = \cos(\theta_{mn}) \tag{III.19}$$

De plus, on peut écrire :

$$\cos(\theta_{mn}) = \frac{|m||n|\cos(\theta_{mn})}{|m||n|} \tag{III.20}$$

D'où la formule finale de la mesure de similarité *MahCosine* :

$$S_{Mahcosine}(u,v) = \frac{mn}{|m||n|}, D_{Mahcosine}(u,v) = -S_{Mahcosins}(u,v) \tag{III.21}$$

où $D_{Mahcosine}(u,v)$ est la mesure de distance équivalente. On peut enfin noter qu'il s'agit principalement de la covariance entre les vecteurs dans l'espace de Mahalanobis.

III.2.4.4 Choix de la distance de similarité

Dans la communauté de la reconnaissance des formes, le choix d'une distance de similarité est souvent expliqué et argumenté par rapport à l'espace d'attributs et aux points de données utilisés. Nous avons remarqué entre autre, avec les mêmes vecteurs attributs Eigenfaces, que la distance Euclidienne fournit de meilleurs résultats d'identification des individus qu'avec la distance de Manhattan. Ces performances nous ont poussés à utiliser la distance Euclidienne dans ce dernier processus.

III.2.5 Organigramme détaillé de l'approche Eigenface

Notre organigramme se divise en trois parties : la première est le prétraitement suivi de la phase d'apprentissage et se termine par la phase d'identification où la distance euclidienne est retenue pour le calcul de la différence entre les poids de l'image à identifier et les images de base de données puis le programme affiche la plus proche.

III.2.5.1 Organigramme du prétraitement

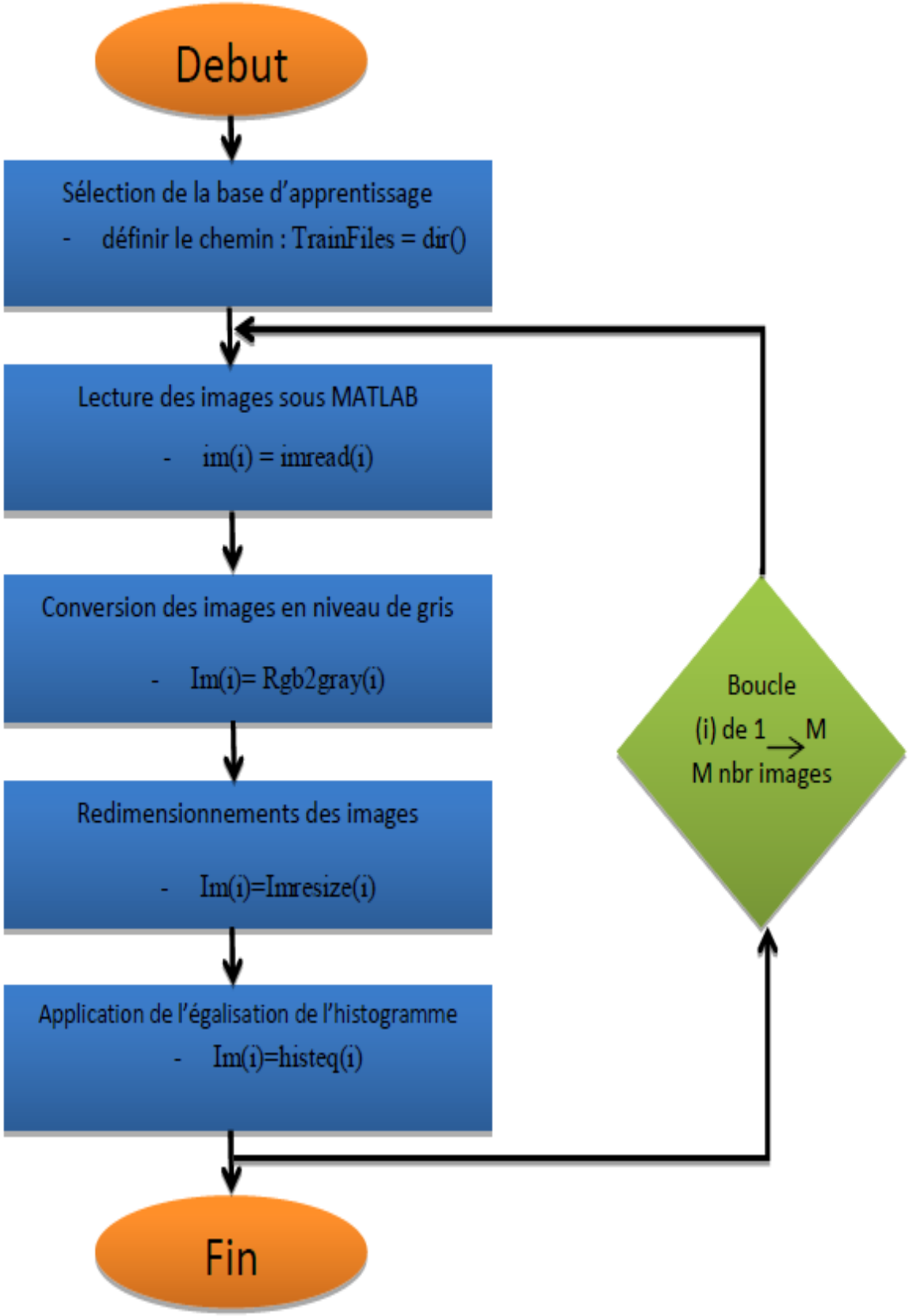

Fig.III.8 : *prétraitements.*

III.2.5.2 Organigramme de la phase d'apprentissage

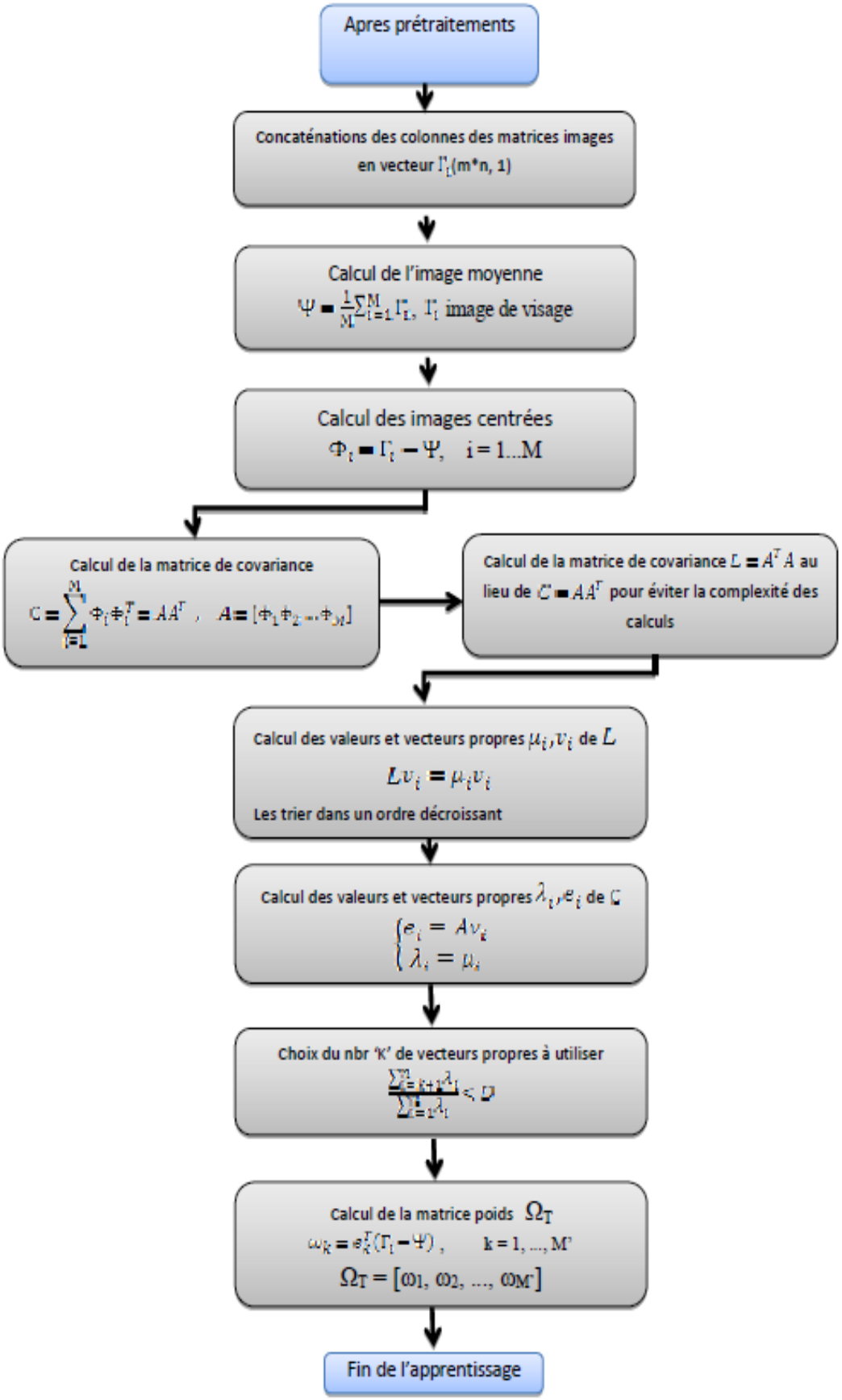

Fig.III.9 : *phase d'apprentissage.*

III.2.5.3 Organigramme de la phase d'identification

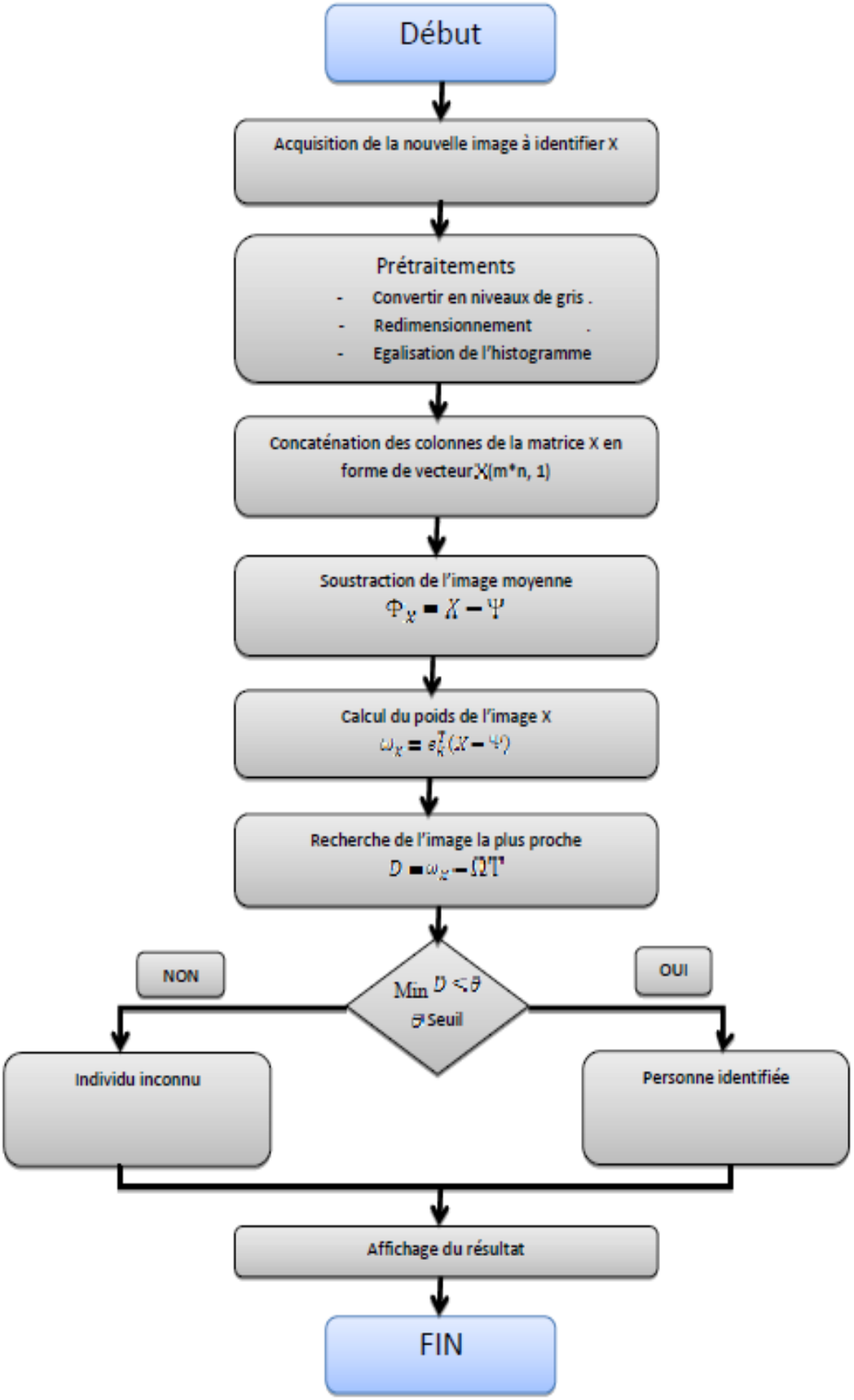

Fig.III.10 : *phase d'identification.*

III.3 Reconnaissance de visage par Local Binary Pattern (LBP)

III.3.1 Présentation

L'opérateur LBP a été proposé initialement par Ojala et al. [45] dans le but de caractériser la texture d'une image. Le calcul de la valeur LBP consiste pour chaque pixel à seuiller ses huit voisins directs avec un seuil dont la valeur est le niveau de gris du pixel courant. Tous les voisins prendront alors une valeur 1 si leur valeur est supérieure ou égale au pixel courant et 0 si leur valeur est inférieure (Fig.III.11). Le code LBP du pixel courant est alors produit en concaténant ces 8 valeurs pour former un code binaire. On obtient donc, comme pour une image à niveaux de gris, une image des valeurs LBP contenant des pixels dont l'intensité se situe entre 0 et 255.

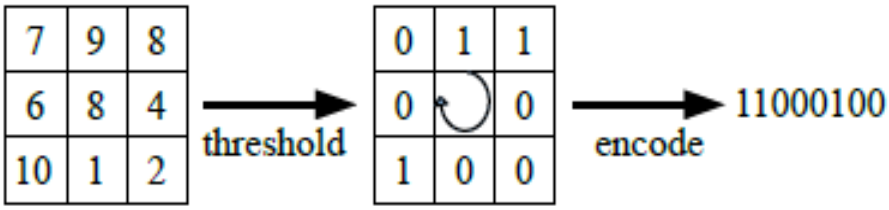

Fig.III.11: *Opérateur LBP.*

La technique LBP a été étendue ultérieurement en utilisant des voisinages de taille déférente. Dans ce cas, un cercle de rayon R autour du pixel central et Les valeurs des P points échantillonnés sur le bord de ce cercle sont prises et comparées avec la valeur du pixel central. Pour obtenir les valeurs des P points échantillonnés dans le voisinage pour tout rayon R, une interpolation est nécessaire. On adopte la notation (P, R) pour définir le voisinage de P points de rayon R d'un pixel. La Fig.III.12 (a), illustre trois voisinages pour des valeurs de R et P différentes.

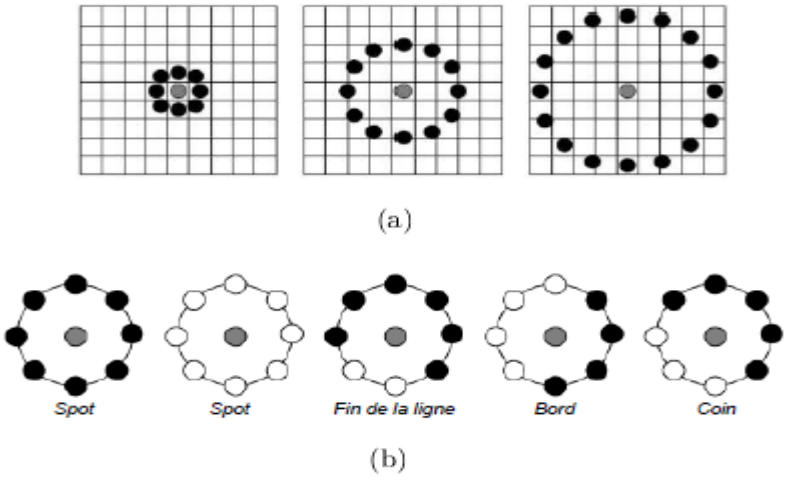

Fig.III.12 : *(a): Trois voisinages pour des R et P différents, (b) : Textures particulières détectées par* LBP^{u2}

Soient g_c le niveau de gris du pixel central, g_p $(P = 1 \ldots P)$ les niveaux de gris de ses voisins. L'indice LBP du pixel courant est calculé comme :

$$\mathrm{LBP}_{P,R}\ (x_c\ , y_c\ ) = \sum_{P=1}^{P} S(g_p\ , g_c\ )2^{P-1} \qquad \text{(III.22)}$$

Où

$$S(x) = \begin{cases} 1\ if\ x \geq 0 \\ 0\ if\ x < 0 \end{cases} \qquad \text{(III.23)}$$

Où $(x_c\ , y_c\ )$ sont les coordonnées du pixel courant, $\mathrm{LBP}_{\mathrm{P,R}}$ est le code LBP pour le rayon R et le nombre de voisins P. L'opérateur LBP obtenu avec P = 8 et R = 1 ($\mathrm{LBP}_{8,1}$) est très proche de l'opérateur LBP d'origine. La principale déférence est que les pixels doivent d'abord être interpolés pour obtenir les valeurs des points sur le cercle (voisinage circulaire au lieu de rectangulaire).

Une autre extension à l'opérateur d'origine est le LBP uniforme. Un code LBP est uniforme s'il contient au plus deux transitions de bits de 0 à 1 ou vice-versa lorsque la chaîne binaire est considérée circulaire. Par exemple, 00000000, 00011110 et 10000011 sont des codes uniformes. L'utilisation d'un code LBP uniforme, noté $\mathrm{LBP}^{\mathrm{u2}}$ à deux avantages. Le premier est le gain en mémoire et en temps calcul. Le deuxième est que $\mathrm{LBP}^{\mathrm{u2}}$ permet de détecter uniquement les textures locales importantes, comme les spots, les fins de ligne, les bords et les coins (Fig.III.12 .b), pour des exemples de ces textures particulières. En effet, Ojala et al ont montré que les LBPs uniformes contiennent plus de 90% de l'information d'une image.

La propriété importante du code LBP est que ce code est invariant aux changements uniformes globaux d'illumination parce que le LBP d'un pixel ne dépend que des différences entre son niveau de gris et celui de ses voisins.

III.3.2 LBP pour la reconnaissance de visages

Une fois le code LBP calculé pour tous les pixels de l'image, on calcule l'histogramme de cette image LBP pour former un vecteur de caractéristiques représentant l'image faciale. En réalité, afin d'incorporer plus informations spatiales au vecteur représentant le visage, on divise tout d'abord l'image codée par l'opérateur LBP en petites régions et l'histogramme est construit pour chaque région. Finalement, on concatène tous les histogrammes des régions afin de former un grand histogramme représentant l'image des caractéristiques faciales (voir Fig.III.13). L'efficacité du code LBP comme indice facial s'explique par le fait que le LBP permet de caractériser les détails d'un visage. Quand seules les LBPs uniformes sont utilisés, toutes les

codes LBPs non-uniformes sont étiquetés avec une étiquette unique, alors que chacun des codes uniformes est regroupé dans un histogramme unique. Par exemple, quand P = 8, nous avons 58 codes uniformes mais l'histogramme est de dimension 59. De même manière P = 6 produit un histogramme de dimension 33.

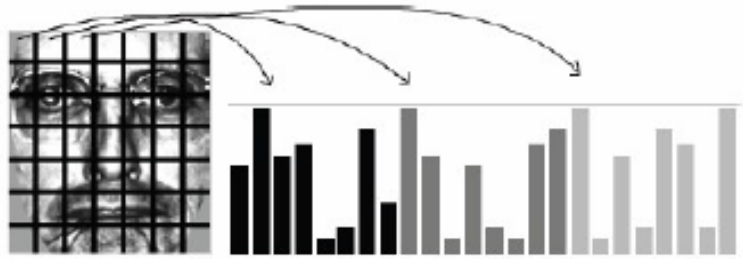

Fig.III.13: *Représentation d'un visage par les histogrammes du code LBP.*

Etant donnés deux histogrammes de LBP H^1, H^2 de deux visages, l'étape suivante est d'utiliser une métrique pour calculer la similarité entre ces deux histogrammes. En testant les trois métriques X^2, *Histogram intersection et Log-likelihood statistic,* Ahonen et al. [47] ont observé que la première métrique permet d'obtenir les meilleurs résultats :

$$X2(H^1, H^2) = \sum_i \frac{(H_i^1 - H_i^2)^2}{H_i^1 + H_i^2} \qquad \text{(III.24)}$$

III.3.3 Dernières avancées : Travail de Tan et Triggs

Leur travail [48] fait suite à celui de Ahonen et al. Il propose 3 nouveaux concepts qui permettent d'améliorer significativement les performances (plus de 40% sur la data base FRGC-104 selon leur publication). Ces trois concepts sont les Local Ternary Patterns (LTP), une méthode de prétraitement de l'image et enfin une méthode de mesure de distance pour la comparaison d'échantillons au format LBP ou LTP. Ces concepts sont détaillés ci-dessous.

III.3.3.1 Les local ternary patterns

Il s'agit de la généralisation des local binary patterns au système ternaire. Elle a été proposée par Tan et Triggs [48] comme solution au problème de sensibilité qu'éprouve le LBP face au bruit aléatoire et celui de quantification. Le principe est le suivant :

alors que les LBP appliquaient un seuil égal à la valeur du pixel central, la conversion en Local Ternay Patterns (LTP) attribue à la valeur 0 aux pixels dont la valeur se trouve dans un voisinage de la valeur du pixel central, 1 à ceux dont la valeur est au-delà de ce voisinage et -1 à ceux dont la valeur est en dessous. La formulation mathématique est la suivante pour u un pixel périphérique d'un entourage à convertir, IC la valeur du pixel central et t le voisinage :

$$S(u, i_c, t) = \begin{cases} 1 \; si \; u \geq i_c + t \\ 0 \; si \; |u - i_c| < t \\ -1 \; si \; u \leq \; i_c - t \end{cases} \quad \text{(III.25)}$$

Comme fait pour l'opérateur LBP basique, une illustration de l'opérateur LTP basique est faite à la Fig.III.14.

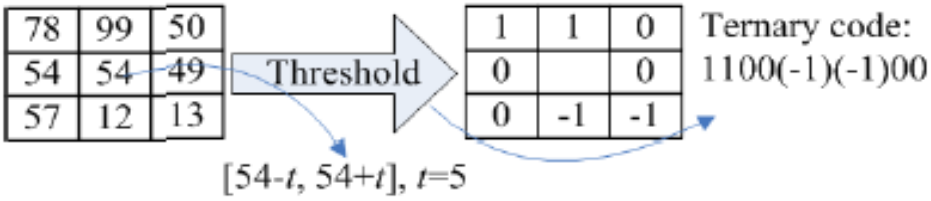

Fig.III.14: *Opérateur LTP basique.*

Ensuite, ce code ternaire peut être transformé soit en un nombre réel soit en code binaire pour passer à la phase suivante. Dans le premier cas on pourrait utiliser un code de valeurs 3^n similaire au code binaire2^n. Tan et Triggs ont quant à eux divisé le code ternaire en deux codes binaires traités séparément et rassemblés ensuite lors de la phase de comparaison. Cette méthode à l'avantage de garder le système simple d'élimination des patterns non-uniformes.

III.3.3.2 La méthode de préparation de l'image

Celle-ci s'effectué en trois étapes :

1. Correction Gamma. L'idée de base est que comme l'image réfléchie par un visage est le produit de la lumière qui l'atteint par la réflectance de la surface, une variation de la réflectance représentant un trait discriminatif aura une influence relative à l'illumination qu'elle subit, introduisant par la même un biais. La solution proposée est d'appliquer l'opérateur logarithmique par lequel ce produit deviendra une somme. Ainsi, pour une illumination locale uniforme, un saut de réflectance x provoquera la même incrémentation sur l'image réfléchie quelle que soit la valeur de l'illumination de départ. Néanmoins, selon Tan et al., un logarithme a tendance à trop amplifier le bruit dans les zones sombres. Pour cette raison, un exposant compris dans l'intervalle [0, 0.5] est utilisé à la place du logarithme. Ainsi la première étape se décrit par la relation mathématique :

$$I'(i,j) = I(i,j)^{\gamma}$$

où $I(i,j)$ est l'intensité du pixel de coordonnées (i,j) de l'image d'entrée etI' l'image issue de cette première étape de prétraitement.

2. Filtrage par différence de Gaussiennes. Il s'agit de l'implémentation d'un passe bande pour supprimer les basses fréquences contenant les effets non désirables des ombres et les hautes fréquences contenant l'aliasing et le bruit.
3. Egalisation des contrastes. Celle-ci s'effectue en trois étapes sur la région délimitant le visage.

$$I(x,y) \leftarrow \frac{I(x,y)}{(mean(|x',y'|^a))^{1/a}}$$

$$I(x,y) \leftarrow \frac{I(x,y)}{(mean(\min(T,|I(x',y')|)^a))^{1/a}}$$

$$I(x,y) \leftarrow Ttank(\frac{I(x,y)}{T}$$

où T est utilisé dans l'étape deux pour tronquer les grandes valeurs, a est un exposant inférieur à 1 réduisant l'effet des grandes valeurs. L'étape trois limites l'espace de l'image à l'intervalle$[-T,T\ ]$. Effectuer cette méthode sur une zone présentant plusieurs visages ne donnera pas le même résultat que l'application sur chacun des visages séparément. Par conséquent, si une étape de masquage doit être effectuée, il faut qu'elle le soit avant cette étape d'égalisation des contrastes. L'application de cette méthode à un même visage soumis à différentes conditions d'illumination est illustrée à la FIG.III.15.

Fig.III.15: *Illustration de l'application de la méthode de correction d'illumination proposée par Tan et Triggs.*

III.3.3.3 La métrique utilisée pour comparer deux histogrammes

La mesure de distance proposée par Tan et Triggs prend intrinsèquement compte de l'organisation spatiale des LTP distribués sur l'entièreté de l'image. Ici plus question d'histogramme non plus. Soit deux images à comparer X et . Pour chaque LTP (aussi nombreux que le nombre de pixels) de , la méthode va regarder parmi les LTPs de même valeur de X celui qui est le plus proche et utiliser la distance qui les sépare pour incrémenter proportionnellement la distance globale.

Concrètement, pour chaque valeur k possible de LTP, une matrice binaire b_x^k représentant la distribution des patterns k dans X est créée. Ensuite, les matrices de distances d_x^k sont compilées tel que l'élément (i,j) de d_x^k représente la distance entre (i,j) et la position du plus proche pixel de X dont la valeur est k. L'exemple d'une matrice b_x^k et de sa matrice d_x^k associée est présenté à la Fig.III.16.

Finalement le calcul de la distance entre deux images X et Y se fait comme suit :

$$D(X,Y) = \sum_{pixels(i,j)\ of\ Y} \omega\left(d_x^{kY(i,j)}(i,j)\right) \qquad \text{(III.26)}$$

où $\omega(d)$ est une fonction (à choisir) qui associe à une distance de pixel la pénalité correspondante. Tan et Triggs proposent la gaussienne $\omega(d) = exp^{-(d/\sigma)^2/2}$ et la troncation linéaire $\omega(d) = \min(d,T)$ et disent que leurs performances sont similaires.

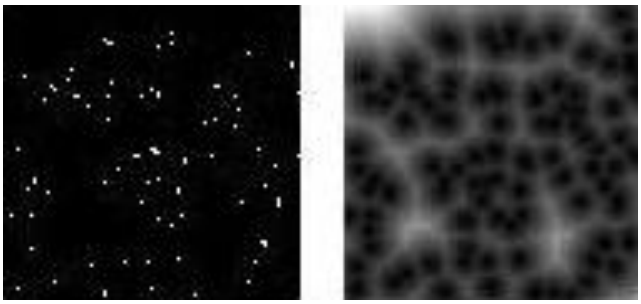

Fig.III.16 : *A gauche : Exemple de matrice binaire de distribution des patterns. A droite : Matrice de distances correspondante.*

III.4 Conclusion

Ce chapitre a été consacré à la présentation des deux méthode de reconnaissance faciale utilisée dans ce travail en l'occurrence de l'analyse en composante principale connue sous le nom «d' Eigenface » et la deuxième technique est basée sur l'utilisation du descripteur LBP, Ces technique permettent de diminuer le nombre de composantes toutes en gardant l'information caractérisant l'objet à analyser sans perte d'informations significatives.

Dans le chapitre suivant, nous testerons le système dans son environnement afin d'évaluer ses performances pour en déduire les paramètres optimaux qui garantissent une meilleure efficacité du système.

IV.1 Introduction

Pour évaluer l'efficacité des méthodes décrites dans la chapitre III, nous avons opté pour une validation sur des bases de données standard « ORL » et « FEI ». Notre travail consiste à concevoir un système d'identification biométrique de personnes par reconnaissance faciale se basant sur une analyse en composante principale et calcul de la valeur LBP qui peut être utilisée pour simplifier un ensemble de données, en réduisant sa dimension. Plusieurs étapes sont nécessaires, l'étape d'extraction des caractéristiques est la plus importante car les performances du système en dépendent (résultats et robustesse, un temps de latence acceptable pour des applications « temps réel »). Nous évaluerons dans ce chapitre les résultats obtenus sur les bases de données ORL et FEI sous différentes conditions et attributs des méthodes.

IV.2 Les bases de données de visage

Plusieurs bases de données contenant des informations qui permettent l'évaluation des Systèmes de reconnaissance de visages sont disponibles. Toutefois, ces bases de données sont généralement adaptées aux besoins de quelques algorithmes spécifiques de reconnaissance, chacune d'elle a été construite avec des conditions d'acquisition d'images de visages diverse (changements d'illumination, de pose, d'expressions faciales) ainsi que le nombre de sessions pour chaque individu.

IV.2.1 ORL

Les données utilisées pour réaliser les tests sur notre système proviennent de la base ORL [49]. Cette base a été collectée entre avril 1992 et avril 1994 par le laboratoire AT&T de L'université de Cambridge. La base contient 40 personnes, chacune étant enregistrée sous 10 vues différentes (figure IV.1). Les images sont de taille 112 × 92 pixels en format JPG et BMP *(portable format de gris*). Pour quelques sujets, les images ont été collectées à des dates différentes, avec des variations dans les conditions d'éclairage, les expressions faciales (expression neutre, sourire et yeux fermés) et des occultations partielles par les lunettes. Toutes les images ont été collectées sur un fond foncé. Les poses de la tête présentent quelques variations en profondeur par rapport à la pose frontale.

Fig.IV.1 : *Exemples d'images de visages de la base ORL.*

IV.2.2 FEI

La base de données de visage de FEI est une base de données brésilienne de visage qui Contient un ensemble d'images de visage prises entre juin 2005 et mars 2006 au laboratoire d'intelligence artificielle de FEI dans São Bernardo font Campo, São Paulo, Brésil. Elle contient des images de visage de 200 personnes, avec 14 images pour chacune d'entre elles, un total de 2800 images. Toutes les images sont en couleur et prises sur un fond blanc homogène en position frontale avec divers angles de pose de chaque personne, s'étendant du profil aux vues frontales. La variation d'éclairage est de 10% et la résolution de l'image est de 640x480 Pixel [50].

La Fig.IV.2 montre quelques exemples des variations d'image de la base de données de visage de FEI.

Fig.IV.2 : *Exemples d'images de visages de la base FEI.*

IV.2.3 Séparation des bases de données

Afin de développer une application de reconnaissance de visage, il est nécessaire de disposer de deux bases de données : une base pour effectuer l'apprentissage et une autre pour tester les techniques et déterminer leurs performances, mais Il n'y a pas de règle pour déterminer ce partage de manière quantitatif. Il résulte souvent d'un compromis tenant compte du nombre de données dont on dispose et du temps pour effectuer l'apprentissage.

Dans les séries de test que nous avons effectué la base a été scindée de la façon suivante :

• ***Images apprentissages*** **:** Les 6 premières images servent pour la phase d'apprentissage.

• ***Images Tests*** **:** Les 4 dernières images de chaque individu nous ont servies pour la réalisation des différents tests.

Le but est d'évaluer le taux de reconnaissance de différents algorithmes présenté, en suivant un protocole de test basé sur la mesure de taux de reconnaissance

$$Taux\ de\ reconnaissance = \frac{\text{nombre d'image de teste reconnues}}{nombre\ totale\ des\ images\ de\ teste}$$

IV.3 Environnement du travail

Dans cette section, nous présenterons les environnements matériel et logiciel de notre travail.

IV.3.1 Environnement matériel

Afin de mener à bien ce projet, il a été mis à notre disposition un ensemble de matériels dont les caractéristiques sont les suivantes :

Un ordinateur COMPAQ avec les caractéristiques suivantes :

– Processeur : Intel® Pentium® Dual CPU T3400 @ 2.16Ghz 2.17Ghz

– RAM : 2.00 Go de RAM

– Disque Dur : 250 Go

– OS : Microsoft Windows 7

IV.3.2 Outils de développement

Nous avons eu recours lors de l'élaboration de notre système à Matlab 7.12.0 que nous présenterons ci-dessous.

IV.3.2.1 Matlab 7.8.0 (R2009a)

Matlab et son environnement interactif est un langage de haut niveau qui permet l'exécution de tâches nécessitant une grande puissance de calcul et dont la mise en œuvre sera bien plus simple et rapide qu'avec des langages de programmation traditionnels tels que le C, C++. Il dispose de plusieurs boites à outils en particulier celle du traitement d'images « Image Processing ToolBox » qui propose un ensemble d'algorithme et d'outils graphiques de référence pour le traitement, l'analyse, la visualisation et le développement d'algorithmes de traitement d'images.

IV.4 Système de reconnaissance faciale : principes et expérimentations

Le problème de la reconnaissance de visages est défini comme suit : étant donnée une image de visage dont 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 image est associe 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 a comparer le vecteur de caractéristiques du visage a reconnaitre 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.

IV.4.1 Système de reconnaissance faciale basé sur ACP : Expérimentation et résultats

A partir du système de reconnaissance présenté en Fig.III.10 du chapitre III, différents tests ont été effectués en fonction de différents nombres de vecteurs propres. La base utilisée est l' Olivetti Research Laboratory aussi appelée ATT face database [49] a été scindée en deux sous bases, l'une pour l'apprentissage et l'autre pour le test.

Une étape de prétraitement est d'abord réalisée afin de rendre homogène les images à comparer. Ce prétraitement est effectué à la fois sur les images de la base de données d'apprentissage et sur l'image de question. Cela permet de convertir toutes les images dans un format identique pour assurer l'homogénéité des données.

Après avoir rassemblé les visages dans une unique matrice, nous obtenons une matrice regroupant tous les visages, On calcule ensuite le visage moyen de toutes ses images collectées. Cette image peut être vue comme le centre de gravité de toutes les matrices. On ajuste ensuite les données par rapport à la moyenne. L'image moyenne est alors soustraite de chaque image de la base de données (Fig. IV.3).

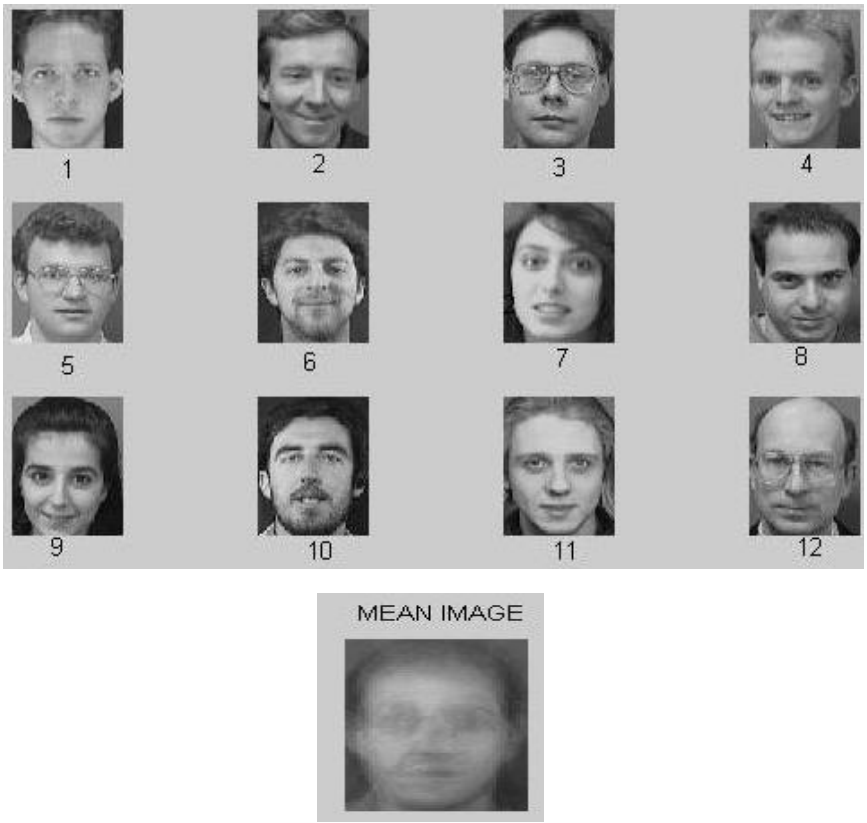

Fig.IV.3 : *visages de la base ORL normaliser et leurs visage moyen.*

La figure ci-dessous (Fig.IV.4) illustre la croissance des valeurs propres de la matrice de covariance des images de la base de visages ORL. On remarque sur la courbe qu'avec juste la moitie des valeurs propres de la matrice de covariance on peut représenter plus de 90% de l'information ce qui peut nous permettre de prendre une partie des vecteurs propres correspondant aux plus grandes valeurs propres.

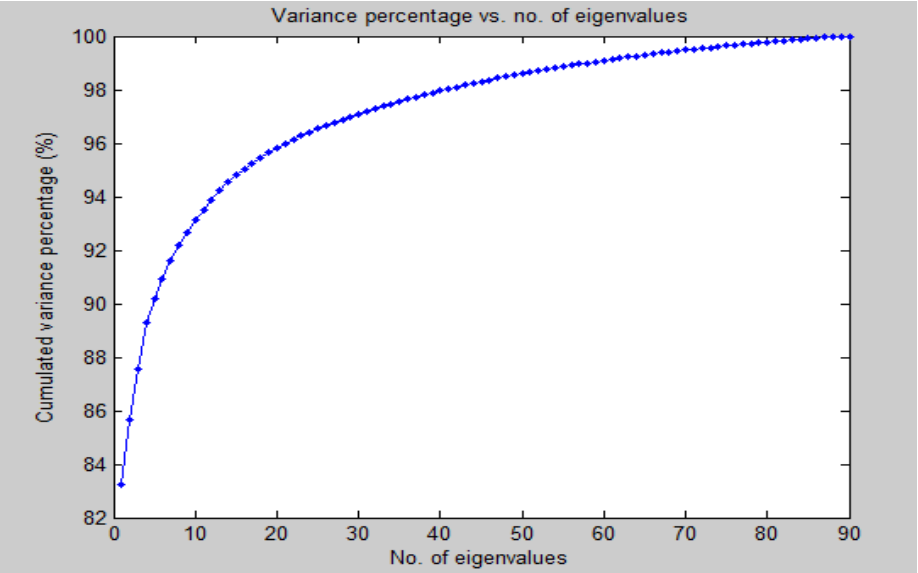

Fig.IV.4 : *Tracé des valeurs propres.*

Le nombre possible d'eigenfaces (Fig.IV.5) est égal au nombre d'images de visage de l'ensemble de la base d'apprentissage. Néanmoins les visages peuvent être approximés, en utilisant seulement les meilleurs Eigenfaces (ayant les plus larges valeurs propres qui représentent en fait, la plupart de variance dans l'ensemble d'images de visage), permettant ainsi de diminuer les calculs.

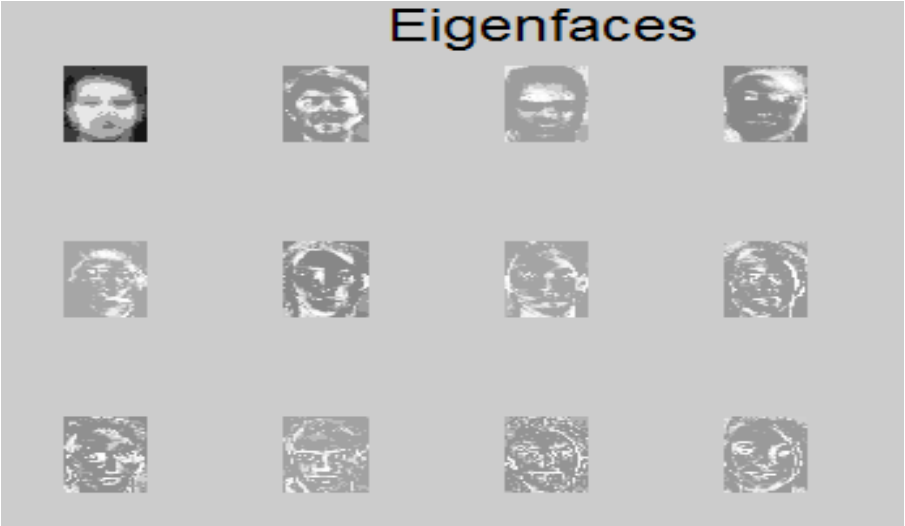

Fig.IV.5 : *Eigen faces.*

Après le calcul des vecteurs propres (eigenfaces), l'étape de classification est la phase dans laquelle le système de reconnaissance de visages assigne un visage test à une classe parmi celles de la base d'apprentissage selon un certain critère bien choisi. Dans notre cas on a utilisé la distance euclidienne.

❖ La première expérience consiste a prendre plusieurs galeries de la base ORL, chacune de ces galeries présente des variation due aux changement d'illumination, de pose , expression faciale ou la présence des composants structurels telle que le port des lunettes, ensuite on calcule Le taux de reconnaissance (%) de chacune comme illustré dans le Tab.IV.1.

Fig. IV.6 *: Exemple de changement d'illumination (galerie 1).*

Fig.IV.7 *: Exemple de changement d'expressions faciales (galerie 2).*

Fig.IV.8 : *Exemple de changement de pose (galerie 3).*

Fig.IV.9 : *Exemple d'individus neutre avec différent âges (galerie 4).*

Galeries	Nombre d'images d'entrainement	Nombre d'images de test	Taux de reconnaissance
Galerie 1	60	40	75 %
Galerie 2	60	40	82.25 %
Galerie 3	80	60	88.33%
Galerie 4	100	70	91.42 %

Tab.IV.1 *: Taux de reconnaissance (%) obtenus pour différentes galeries de la base ORL.*

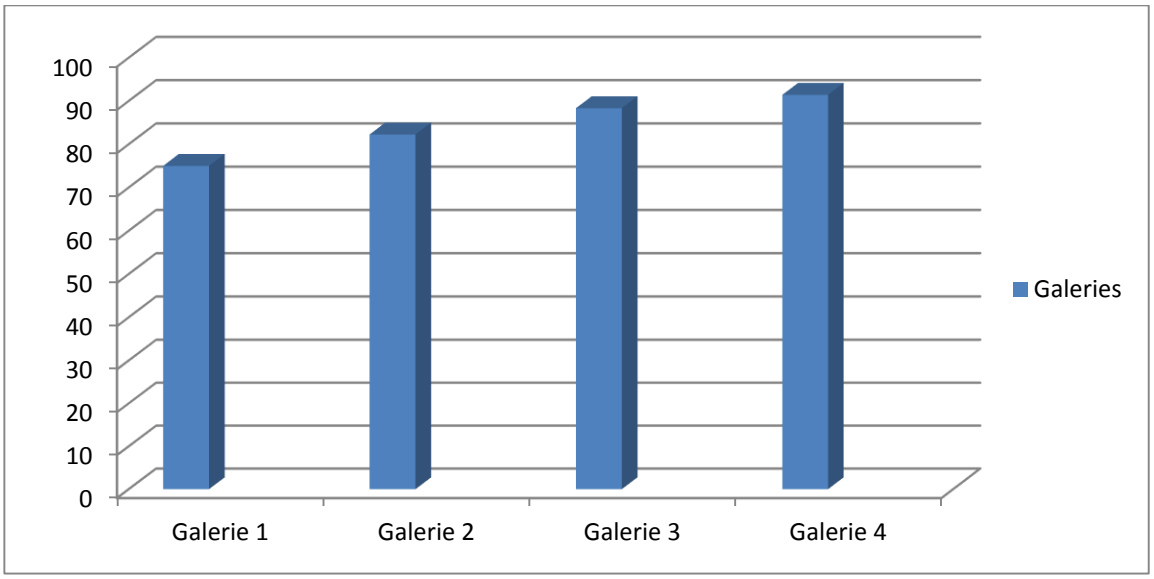

Fig.IV.10 *: Taux de reconnaissance obtenus pour différentes galeries.*

- L'expérience suivante consiste a prendre différents nombres de vecteurs propres (Eigenfaces) ce qui permet de reduire le temps de calcul pour ensuite evaluer le taux de reconnaissance (%) .Le Tab.IV.2 compare les resultats obtenus en utilisant différentes pourcentages des eigenfaces .

Pourcentage des Eigenfaces	40%	50%	60%	75%	100%
Taux de reconnaissance	28.5%	41.43%	48.56%	68.57%	91.42%

***Tab.IV.2** : Taux de reconnaissance (%) obtenus en fonction de différents nombres de vecteurs propres.*

- La troisième expérience illustre l'influence du nombre d'exemples d'apprentissage sur les performances de la reconnaissance. dans l'expérimentation, on a fixé le nombre de visages de test. Par contre, le nombre de visages d'apprentissage varie. Ainsi , pour chaque personne , on a utilise les deux dernières image pour le test et on choisi aléatoirement les n premières images (n<= 8) d'apprentissage.

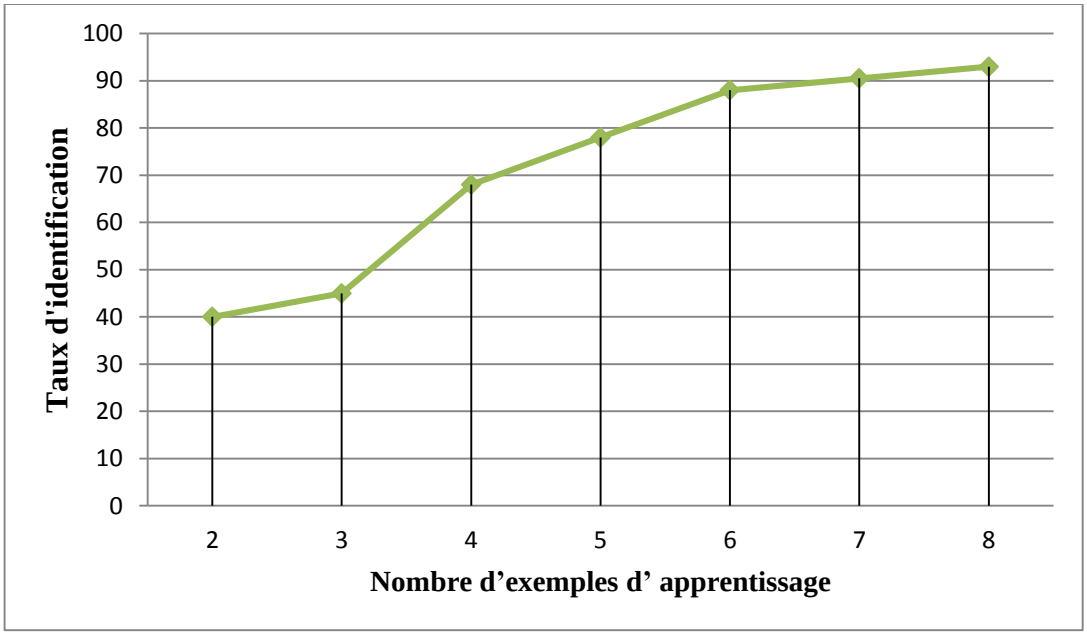

***Fig.IV.11** : Taux d'identification en fonction du nombre d'exemples d'apprentissage par personne (ACP).*

Depuis la Fig.IV.11 on remarque que la performance de la méthode des eigenfaces baisse avec la diminution du nombre d'exemples d'apprentissage pour chaque personne. Dans le cas extrême, si seulement un ou deux exemple d'apprentissage par personne est utilisé, le taux d'identification moyen de l'ACP tombe en dessous de 60 %. Par contre ce taux atteint 93 % quand on utilise huit exemples d'apprentissage par personne.

IV.4.2 Système de reconnaissance faciale basé sur LBP : Expérimentation et résultats

La méthode de reconnaissance faciale LBP (Local Binary Patterns) consiste à visualiser la valeur d'un pixel (moyenne des trois composantes RGB) par rapport aux pixels voisins. Pour commencer, l'image est divisée en groupe de pixels. Chaque groupe de pixels correspond à une matrice carrée contenant les valeurs des pixels. Puis, le pixel placé au centre de la matrice est choisi comme valeur de référence. Ensuite, toutes les valeurs de la matrice sont remplacées soit par 0, soit par 1 en fonction de leur valeur. Nous attribuons la valeur 0 si la valeur du pixel est inférieure à la valeur du pixel de référence, 1 sinon. Après cette opération, chaque pixel du groupe est pondéré avec un poids plus ou moins fort (le pixel en haut à gauche a le poids le plus faible, tandis que le pixel en bas à droite a le poids le plus fort). Ainsi, nous obtenons un nombre binaire qui donne une certaine valeur en base 10. Tous les groupes de l'image sont soumis à ce processus pour finalement obtenir un histogramme de l'image. Enfin, il ne reste plus qu'à faire la différence entre deux histogrammes pour comparer deux images.

L'operateur LBP basique prend comme entrée un carré de 9 pixels et a pour sortie un nombre binaire 8 bits. La motivation qui nous a poussée a utilisé cet operateur est qu'un visage peut être vu comme un assemblage de micro-patterns dont la description par LBP est a la fois bonne, robuste face aux variations de gris et rapide a générer. Cet operateur simple a été étendu pour rester fiable a différentes échelles.

Ainsi, P points décrivent le nombre binaire et ceux-ci sont distribues le long d'un cercle de rayon R. Cet entourage sera note (P;R). Comme ces P points ne tombent pas nécessairement au centre d'un pixel de l'image, leurs valeurs sont obtenues par interpolation bilinéaire. Ceci est illustré dans la Fig.IV.12.

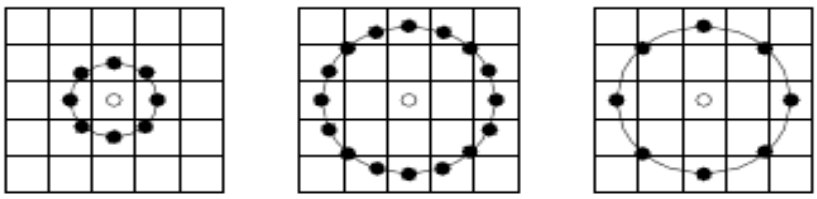

Fig.IV.12 : *l'operateur LBP basique. Les entourages (8,1), (16,2), (8,2) sont Représentés.*

Ensuite ne sont gardés que les patterns 'uniformes' ne présentant au plus que deux transitions 1-0 ou 0-1 lorsqu'ils sont regardés comme des cercles. Ainsi 00110000 et 10000001 sont uniformes tandis que 10010001 et 11011101 ne le sont pas.

En pratique, la conversion d'un pattern non uniforme donne le résultat 0. On se rend compte ainsi que 90% des patterns (8; 1) appartiennent a la catégorie des uniformes. Cette extension permet l'interpréter les LBP en termes de coins et arrêtes inclinées.

Ensuite pour inclure une information quant a la disposition spatiale des textures et éviter de se limiter a une description holistique des textures qui sourirait des limitations connues des méthodes de ce type, l'image convertie est divisée en plusieurs sous-regions pour lesquelles autant d'histogrammes LBP seront faits. Ainsi pour 4 sous-regions, 4 histogrammes seront générés. Ces derniers seront concaténés pour former une matrice a 2 dimensions appelée 'histogramme spatialement amélioré. Notons que les sous-régions peuvent se recouvrir et ne doivent pas nécessairement être rectangulaires.

La comparaison de deux histogrammes spatialement améliorés suppose d'une part d'établir une méthode de mesure de distance entre deux histogrammes simples et d'autre part l'utilisation de poids pour rassembler les distances obtenues pour chaque sous-région.

(P;R)	(8,1)	(8,2)	(16,1)	(16,2)
Taux de reconnaissance	**75%**	**84.5%**	**83%**	**94.5%**

Tab.IV.3 : *Taux de reconnaissance (%) obtenus en utilisant LBP.*

Dans cette partie, nous avons expérimenté la méthode de reconnaissance de visage basé sur les descripteurs LBP. cette expérience consistait à observer les taux de reconnaissance en fonction du nombre d'images présentes dans la base de données et les différentes valeurs du couple (P , R) et de comparer le pourcentage de réussite. Cela pour voir la robustesse de la méthode, c'est-à-dire si elle marchait également pour des cas particuliers.

IV.4.3 Discussion

Dans cette partie, on a présenté en premier lieu un système de reconnaissance de visage basé sur une approche qui a eu le plus de succès dans ce domaine : la PCA (Principal Component

Analysis) connue sous le nom de « Eigen Face », qui est une technique rapide, simple et populaire dans l'identification des visages. Les projections de PCA sont optimales pour la reconstruction d'une base de dimension réduite. Nous avons testé les performances des cette techniques sur la base de données ORL en fonction de différentes galeries et nombres des Eigen faces où il s'est avéré que le taux de reconnaissance est maximale en utilisant la totalité des eigenfaces . Le choix principal de cette base de données est sa grande taille, et sa popularité puisqu'elle est devenue une norme dans la communauté biométrique de vérification d'identité.

Dans la deuxième partie l'application de la technique ('local binary patterns') pour la reconnaissance de visages convertit les images en modèles binaires locaux, les divise en plusieurs sous-régions et détermine l'identité d'un visage en comparant leurs histogrammes de sous-régions.

La méthode d'authentification, basée sur une représentation LBP de l'image. Elle offre une meilleure robustesse aux conditions de lumière et une procédure d'entrainement plus simple et rapide.

Bien que les méthodes holistiques en l'occurrence de la méthode des eigenfaces aient eu beaucoup de succès, leur inconvénient majeur réside dans le fait qu'elles utilisent uniquement des photos 2D d'apparence faciale. Or, on sait qu'une telle représentation est sensible aux changements d'expression, d'illumination et de poses. Une manière d'éviter ce problème consiste à utiliser des représentations faciales locales. En effet, les caractéristiques locales ne sont généralement pas aussi sensibles aux changements d'apparence que les caractéristiques globales.

Le premier point notable de ces expériences est que l'apprentissage de l'ACP pose un problème de généralisation, retrouvé dans toutes les méthodes de reconnaissance par réduction d'espace. Sachant que si l'espace de réduction est construit à partir de personnes qui ne sont pas dans la base d'évaluation ORL, les performances sont dégradées de façon significative. On remarque aussi que la variabilité des personnes est moins importante que la variabilité des situations environnementales. Cette technique souffre aussi d'un grand temps de calcul. Sachant que l'évaluation d'un système de reconnaissance se fait essentiellement par rapport à deux paramètres qui sont : la robustesse et le temps d'exécution, elle n'est pas dédié à des applications temps réel, et n'est pas optimisée pour la séparabilité (discrimination) de classe.

IV.5 Principe du système de reconnaissance

On peut définir notre système et son rôle en deux parties :

- Mode vérification
- Mode identification

IV.5.1 Mode vérification

Ce mode consiste à comparer une image à une autre stocké dans la base de donnés.

- Importer une image de la base de test.
- Importer une l'image de la base de donné d'apprentissage.
- Effectuer une reconnaissance.

IV.5.2 Mode identification

Dans cette phase on compare une image avec toutes les images de la base de donnes d'apprentissage.

- Importer une image de la base de test.
- Comparer cette image avec ceux stocké dans la base de donnes

IV.6 Présentation de l'application

On présente dans cette section les différents aspects du notre système de reconnaissance.

IV.6.1 Interface de Présentation du projet

C'est une interface destinée aux utilisateurs, elle est simple et permet d'illustrer les principaux processus du système de reconnaissance (identification, visage moyen, reconstruction de l'image, visage propre). Ces opérations sont effectuées sur les bases de données (ORL et FEI) décrites dans ce chapitre .

Fig.IV.13 : *Interface graphique de notre application.*

- la première interface contient deux boutons :
  - ✓ **'Start' :** pour démarrer le programme.
  - ✓ **'close' :** pour quitter le programme.

Pour lancer le programme on clique sur le bouton 'Start ' :

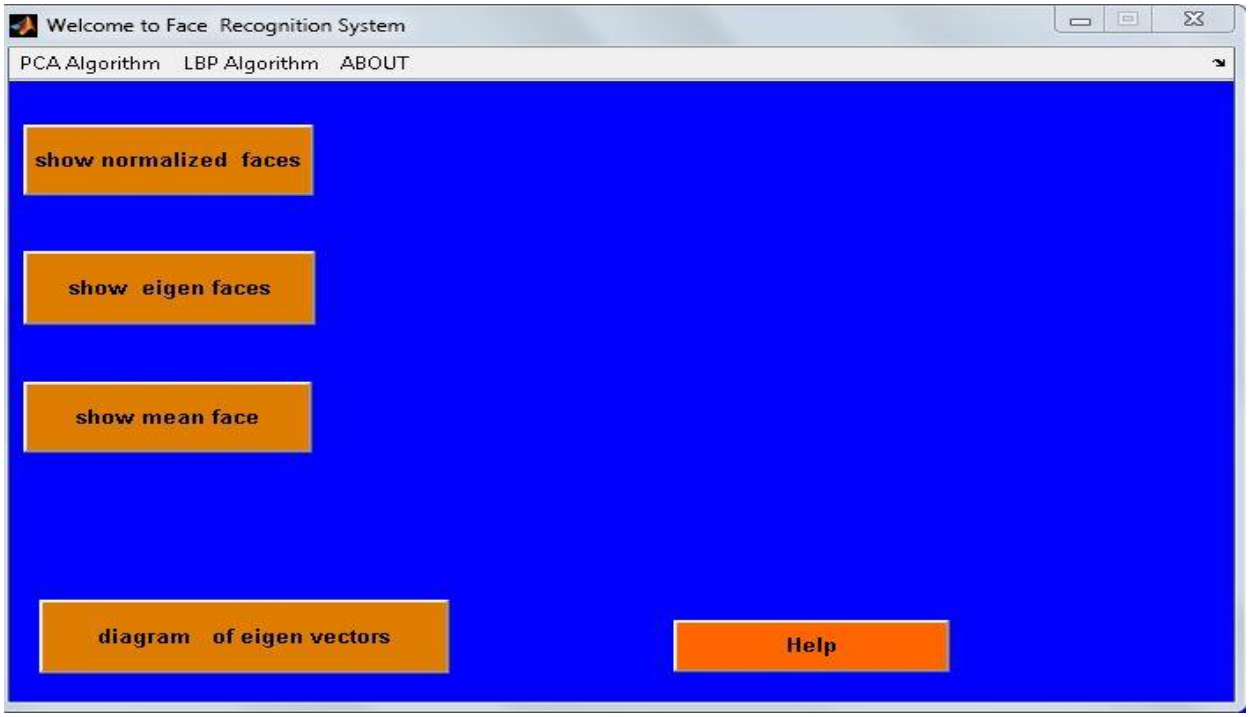

Fig.IV.14 : *L'interface graphique de reconnaissance faciale.*

La 2ième interface est construite en trois menus :

1. L'interface de PCA Algorithme.(regroupe deux menus ou chaque menu représente deux phases : ORL data base et FEI data base).
2. L'interface de LBP Algorithme. (regroupe deux menus ou chaque menu représente deux phases : ORL data base et FEI data base).
3. L'interface d'ABOUT présente un guide d'information sur notre système

IV.6.2 L'interface PCA Algorithme de reconnaissance faciale

L'interface PCA Algorithme contient 5 boutons et un axe pour l'affichage :

A- Le bouton « show normalized face » : le programme affiche les visages normalise dans l'axe.

Fig.IV.15 : *les visages normalisés.*

B- le boutons « show mean face » : après la normalisation des visages de la base de donnes notre programme calcule le visage moyenne ensuite représente ce dernier dans l'axe d'affichage.

Fig.IV.16 : *Le visage moyen.*

C- Le boutons « show eigen faces » : Dans ce cas le programme calcule les vecteurs propre pour chaque image et afficher les eigenfaces dans l'axe.

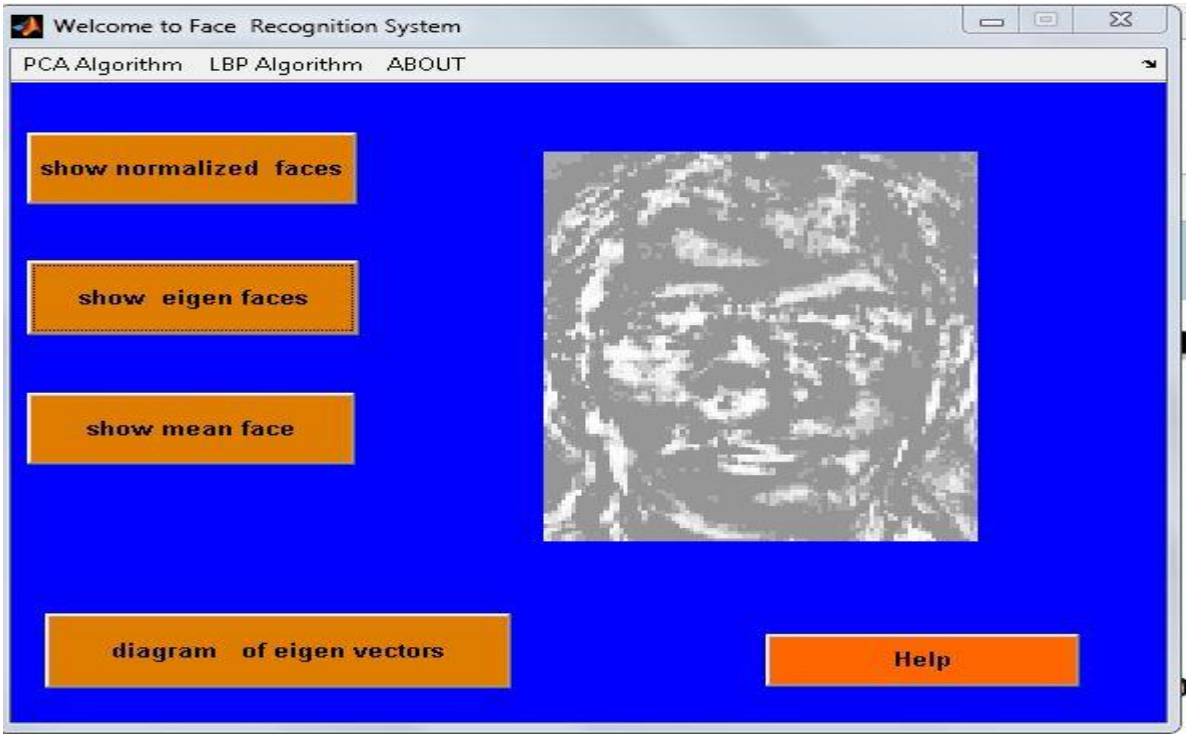

Fig.IV.17 : *Eigenfaces.*

D- le boutons « diagram of eigen vectors » : donne le diagramme de traçage des valeurs propre.

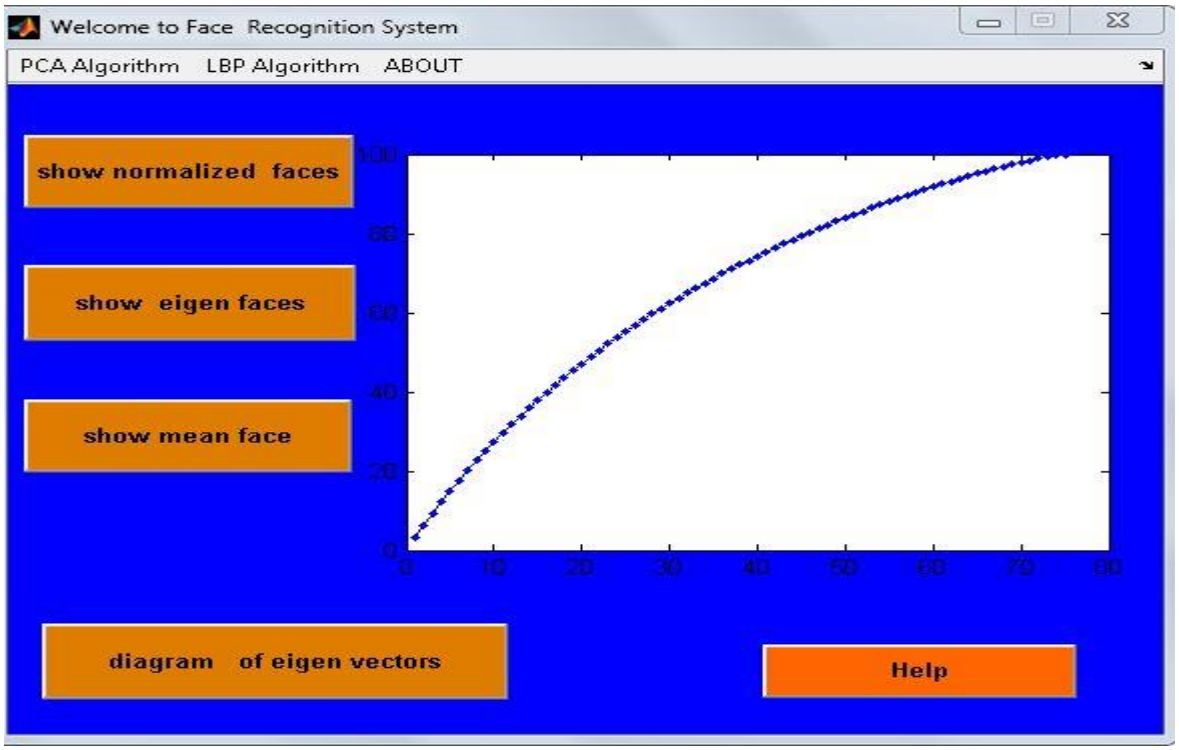

Fig.IV.18 : *Tracé du diagramme le des vecteurs propres .*

E- le bouton « help » : donne plus d'information sur notre application.

Pour effectuer les test on choisira dans le menu la technique ACP ou LBP .

L'interface de test est représentée dans la figure suivante :

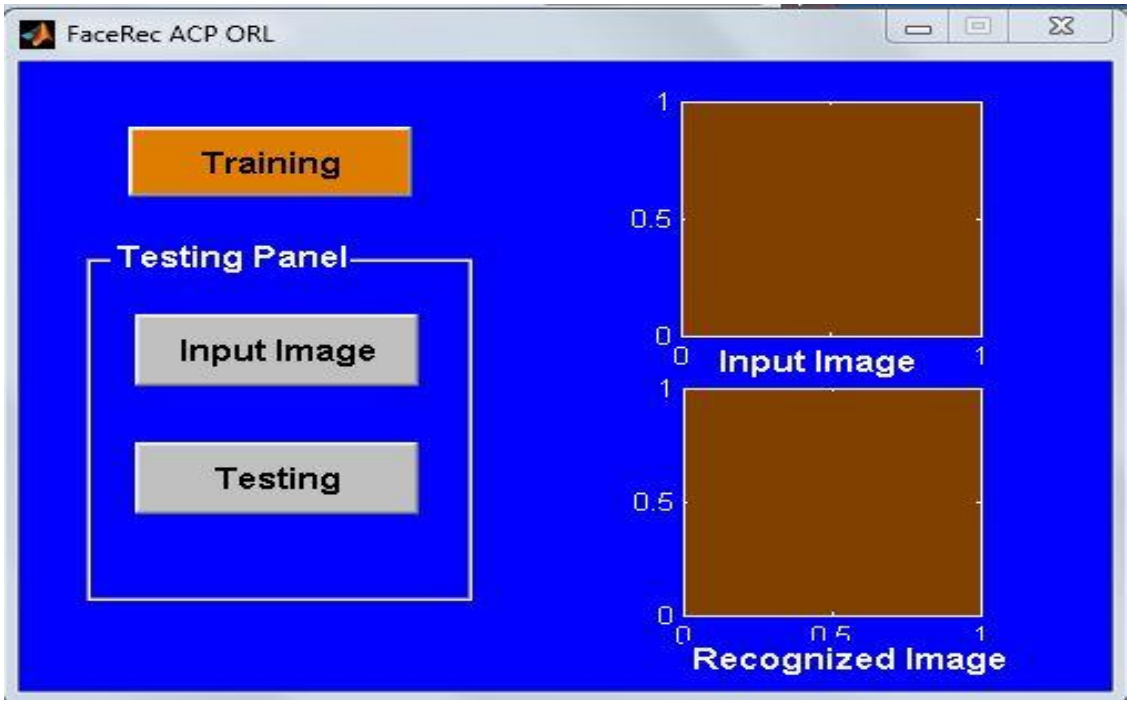

Fig.IV.19 : *interface ACP test.*

Test sur la base ORL

On click sur le bouton training : dans ce cas le programme crée et sauvegarde la matrice de projection. quand le programme est terminer on reçoi un message box .

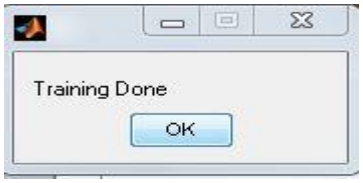

Fig.IV.20 : *message fin training.*

Ensuite on sélectionne le bouton input image pour entrer le chemine d'image de test.

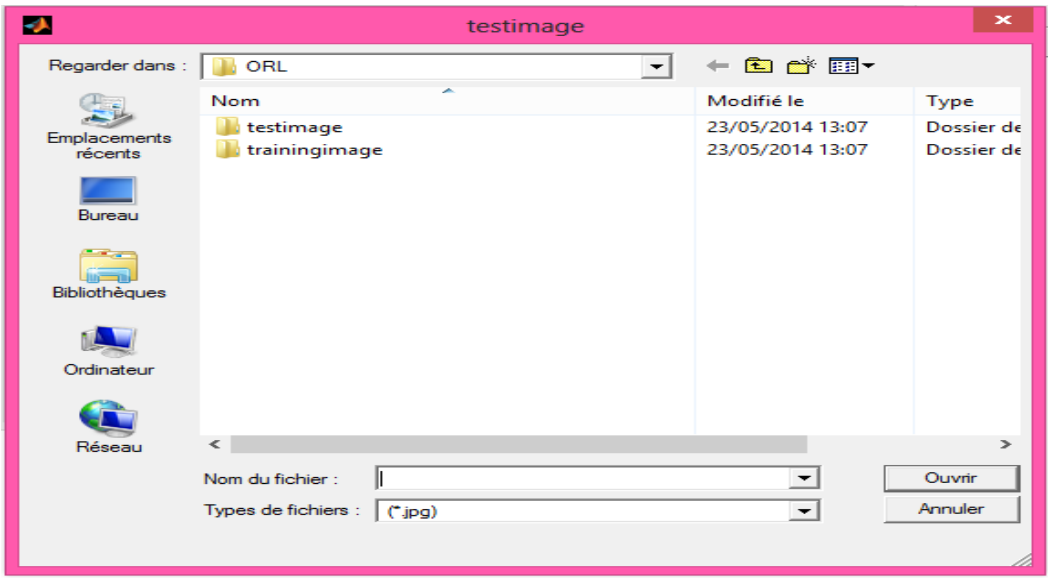

Fig.IV.21 : *chois de chemine d'image test.*

Après le bouton testing permet de visualiser le visage reconnue par le système.

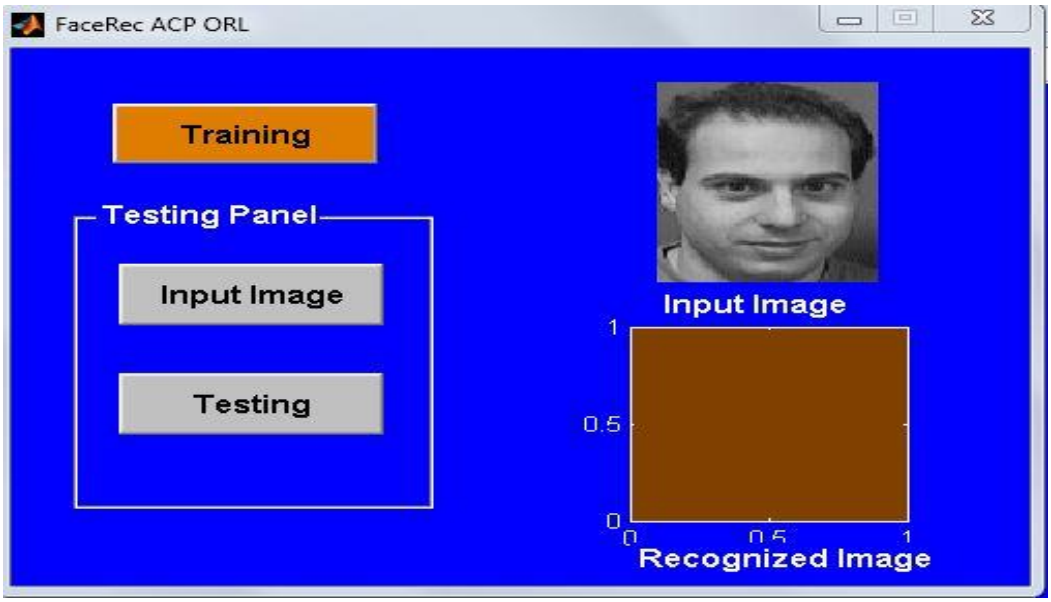

Fig.IV.22 : *l'affichage d'image de test.*

Dans ce cas le programme est lire et comparer avec les images trainning .

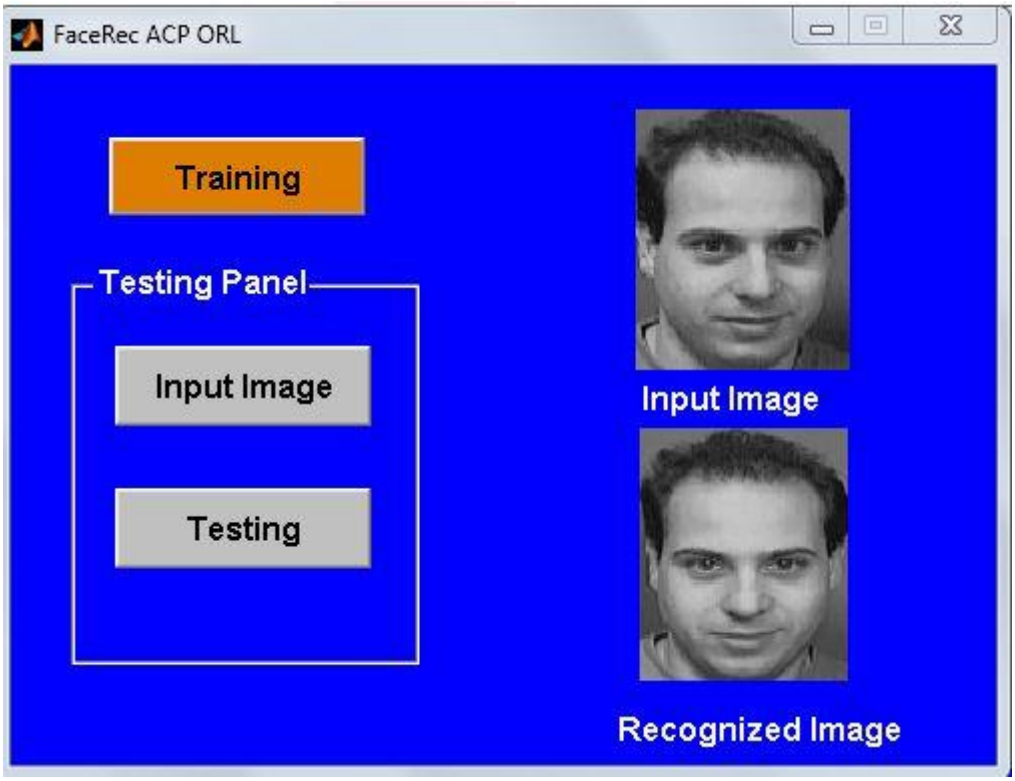

Fig.IV.23 : *fin étape de test.*

IV.6.3 Expérimentations

A. Base ORL

Dans cette partie l'algorithme ACP est appliqué sur la base ORL, cette dernière est scindé en deux sous base , la première qui s'appelle « trainingimage » c'est une base d'apprentissage elle contient 100 image .et la deuxième s'appelle « testimage » c'est une base de test elle contient 70 image .Après l'exécution:

- Le nombre d'image test qui notre système connue =64 image.
- Le nombre d'image test qui notre système inconnue =6 image.
- Le nombre totale d'image test =70.

Taux de reconnaissance pour la base ORL par algorithme ACP = 91.42 %.

B. Base FEI :

Dans cette partie l'algorithme ACP est appliqué sur la base FEI qui est séparé comme suit :

Une sous base qui s'appelle « traifei » (contient 114 image) pour la base d'apprentissage, une autre sous base qui s'appelle « testfei » (contient 74 image) pour la base de test.

Après l'exécution :

- Le nombre d'image test qui notre système connue = 61 image.
- Le nombre d'image test qui notre système inconnue = 14 image.
- Le nombre totale d'image test =75.

Taux de reconnaissance pour la base FEI par algorithme ACP = % 81.33.

IV.6.4 L'interface de LBP Algorithme

Dans cette interface la technique 'local binary pattern ' est utilisé pour la reconnaissance de visage, on choisira la base de donné pour appliqué le test par l'algorithme LBP dans le menu LBP Algorithme

Si on choisir LBP ORL alors que il y a une nouvelle interface qui se présente dans la figure.

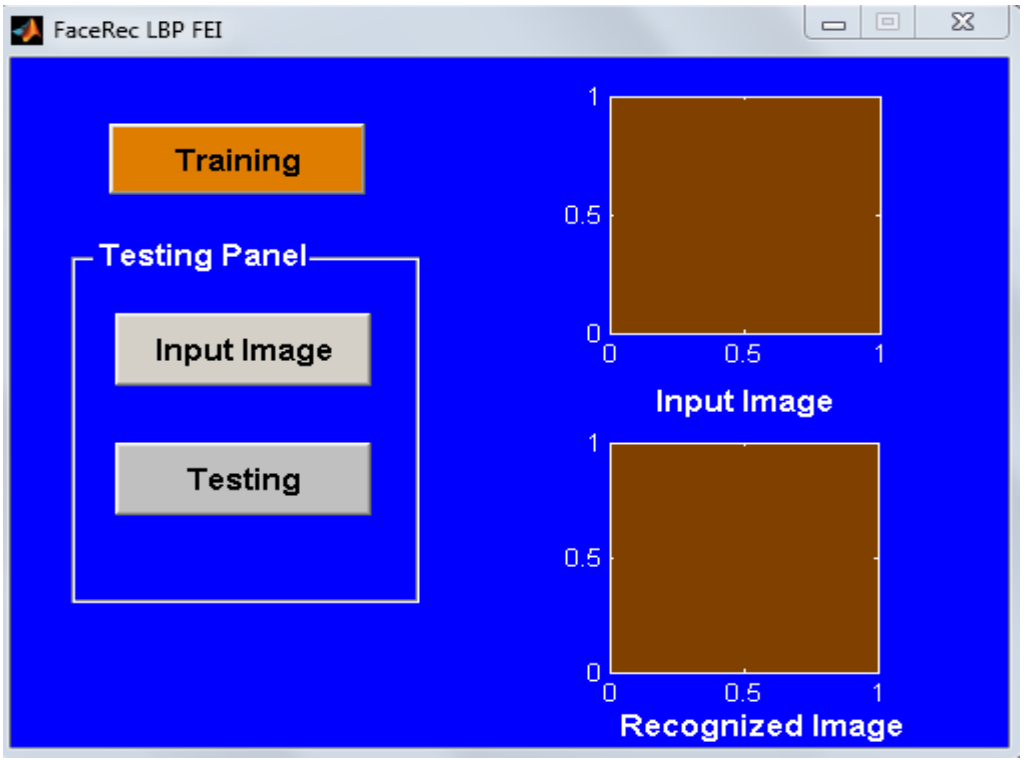

Fig.IV.24 : *l'interface test pour LBP de la base FEI.*

1. On click sur le bouton training

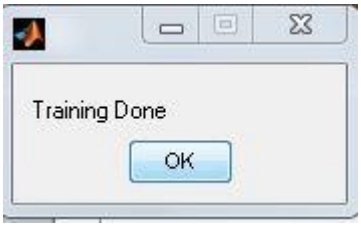

Fig.IV.25 : *Message de fin training.*

2. On click sur le bouton input image pour sélectionner l'image test

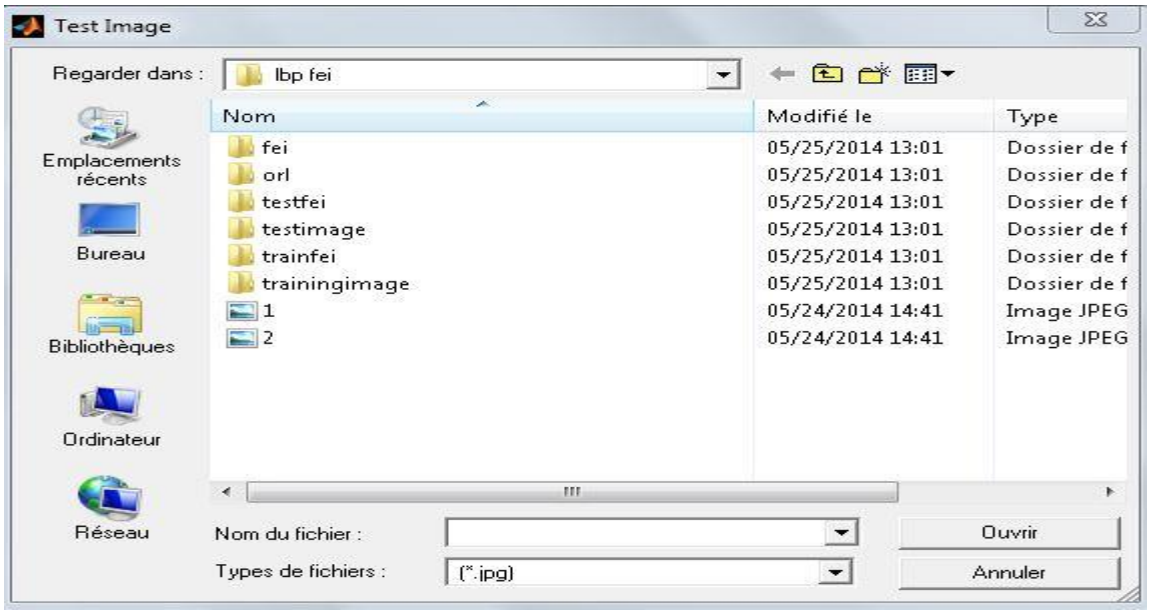

Fig.IV.26 : *le choix de l'image test pour la base FEI.*

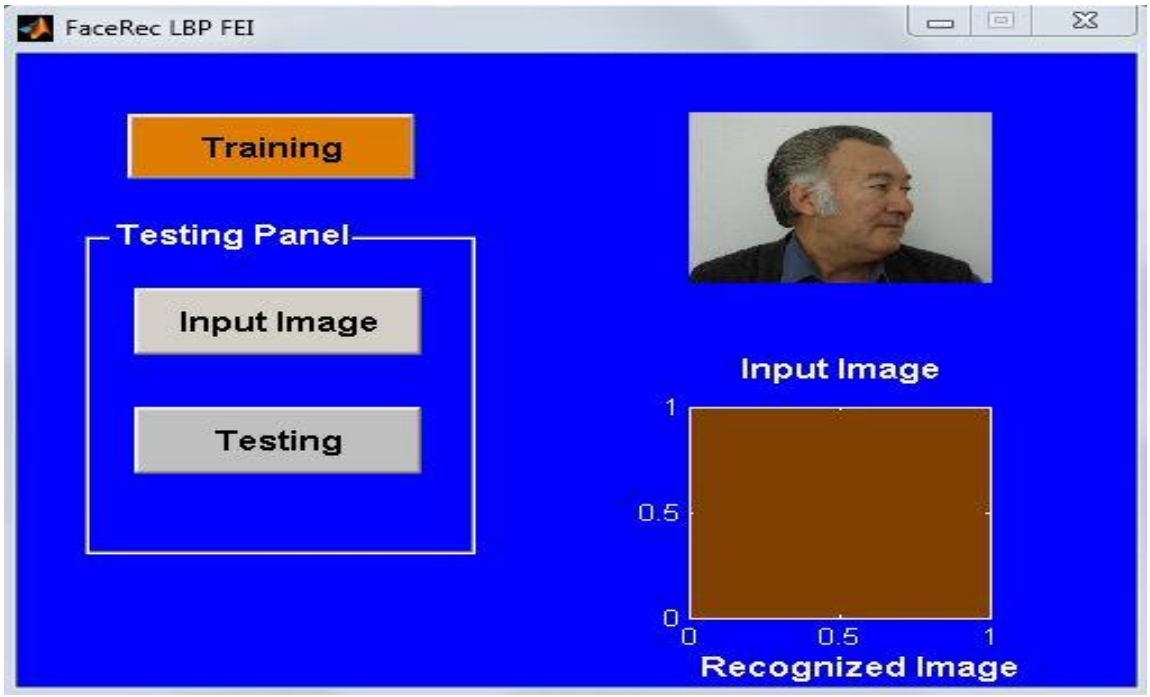

Fig.IV.27 : *l'affichage de l'image test.*

3. On click sur « testing » pour l'idetification de l'image test:

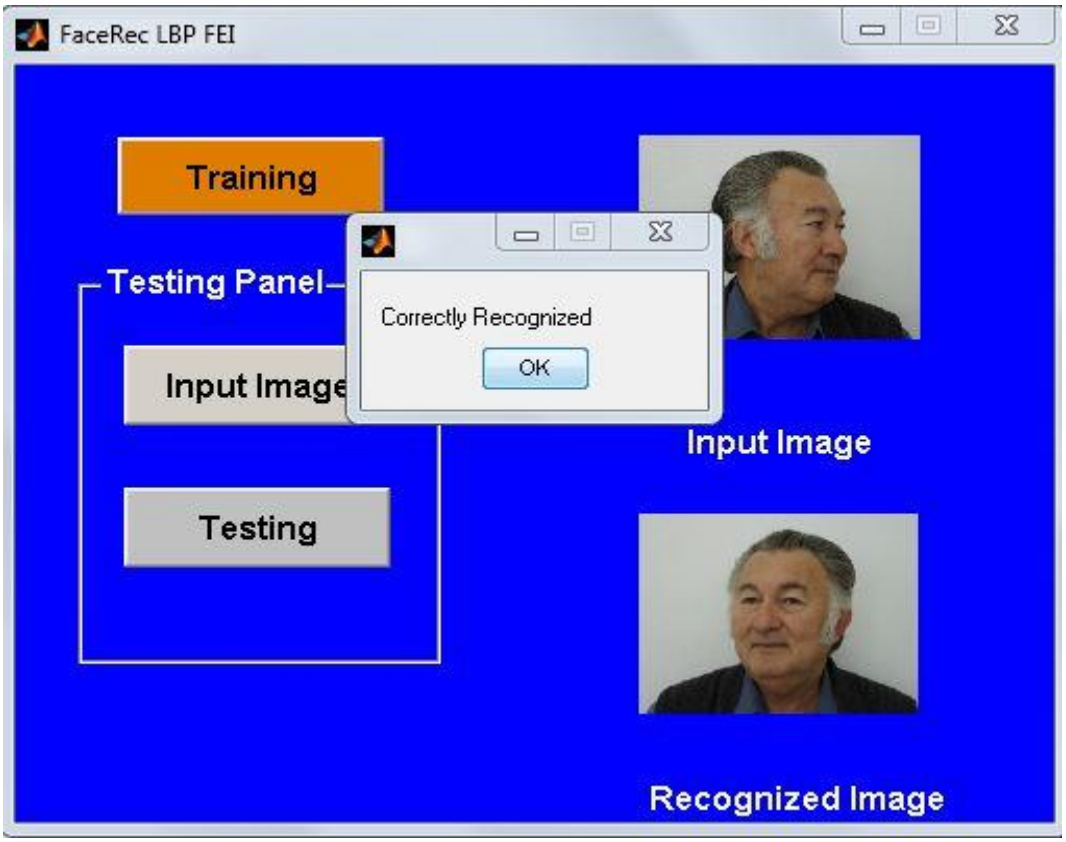

Fig.IV.28 : *fin de l'étape test.*

IV.6.5 Résultats

1) Taux de reconnaissance pour la base ORL

On a appliqué l'algorithme LBP sur la base ORL, cette dernière contient 400 images de 40 personnes différentes. Chaque individu est représenté par un ensemble de 10 images, les 6 premières images on été sélectionner pour faire l'apprentissage et les 4 restantes pour faire faire le différent test.

- Le nombre totale d'images de test 40*4 =160.
- Le nombre d'images connu par notre programme est 160.
- Le nombre d'images inconnu par notre programme est zéro.

Alors :

Taux de reconnaissance pour la base ORL par algorithme LBP = 97 %.

2) Taux de reconnaissance pour la base FEI :

On a appliqué l'algorithme LBP sur la base FEI qui contient 10 images pour chacun des 21 individus, soit un total de 210 images.

- Le nombre totale d'images égale à 21*10 = 210.
- Le nombre d'images connu par notre système est 200.
- Le nombre d'images inconnu par notre système est 10.

Alors :

Taux de reconnaissance pour la base FEI par algorithme LBP = % 95.23

IV.7 Tableau de comparaison entre les algorithmes

	algorithme ***ACP***	Algorithme ***LBP***
Base de données ***ORL***	***91.42 %***	***97 %***
Base de données ***FEI***	***81.33 %***	***95.23 %***

Tab.IV.4 : *Tableau de comparaison entre les algorithmes.*

IV.8 Conclusions

Dans ce chapitre, nous avons présenté une application de reconnaissance faciale basée sur les algorithmes ACP et LBP, on a présenté aussi les différents résultats obtenus pour chaque algorithme. Notre système de reconnaissance de visages face recognition system, est appliquée sur deux bases de donné de visages ORL et FEI. Pour conclure, Nous pouvons noter qu'Eigenface devient de plus en plus lent à mesure que le nombre d'images dans la base de données augmente ainsi que les expérimentations ont montré que la méthode de reconnaissance faciale LBP est la plus efficace que l'ACP. Cependant, nous avons également vu que de nombreux facteurs extérieurs influent sur la qualité de la reconnaissance.

Conclusion générale

La biométrie est un domaine à la fois passionnant et complexe. Elle tente, par des outils mathématiques souvent très évolués, de faire la distinction entre des individus, nous obligeant à travailler dans un contexte de très grande diversité. Cette diversité se retrouve également dans le nombre considérable d'algorithmes qui ont été proposés en reconnaissance faciale.

Dans ce mémoire, nous nous sommes intéressés au problème de reconnaissance faciale. Notre travail consiste à la mise au point d'un algorithme robuste destiné à reconnaître un individu par son visage en utilisant deux méthode parmi les méthodes la plus utilisé dans ce domaine la premier technique est « Eigenface » qui se base sur une analyse en composante principale(ACP). L'ACP est une méthode mathématique qui peut être utilisée pour simplifier un ensemble de données, en réduisant sa dimension. Elle est utilisée pour représenter efficacement les images de visages, qui peuvent être approximativement reconstruites à partir d'un petit ensemble de poids et d'une image de visage standard. La seconde technique utilisé est LBP (local Binary Pattern),c'est une méthode mathématique dont son but consiste à caractériser la texture d'une image par calcule le code LBP pour tous les pixels d'image ensuit on calcule l'histogramme de cette image LBP pour former un vecteur de caractéristiques représentant l'image faciale.

Nous avons souligné durant ce travail l'influence néfaste sur le taux de reconnaissance du système et pour cela nous avons proposé quelques solutions qui ont été évaluées durant la phase de test. Malgré tous les progrès qui ont été réalisés, les problèmes de pose et d'éclairage pour l'identification dans des environnements extérieurs restent des challenges qui susciteront les efforts des chercheurs. L'ACP reste une méthode efficace et simple pour gérer ce type de problème. C'est pour toutes ces raisons que nous avons opté pour cette approche de reconnaissance du visage.

Nous estimons avoir réalisé un système répondant à l'objectif que nous nous sommes fixés au départ, à savoir la mise en œuvre d'un système permettant la reconnaissance d'individus et le contrôle d'accès.

En guise de perspectives, dans un premier temps une extension de ce travail peut être envisager par l'étude et la réalisation d'un système de détection et de localisation du visage avec des performances assez hautes , une autre consiste à appliquer ce système sur d'autres bases de visages présentant de fortes variations dans l'éclairage et de la pose ainsi que d'envisager la possibilité d'employer une approche basée sur les éléments locale du visage. Ensuite, un des grands challenges serait de pouvoir mieux maîtriser les variations

d'environnement, qui perturbent encore trop les systèmes de reconnaissance, Les dernières avancées de la technologie de capture 3D des images de visage ont permis de mettre en place des systèmes de reconnaissance assez robustes par rapport à la 2D.

Si la biométrie est un enjeu important au niveau économique, la recherche, en particulier dans le domaine de la reconnaissance Des visages offre encore un champ d'investigations très ouvert.

Bibliographie

[1] G. Roethenbaugh. “An Introduction to Biometrics and General History”, Biometrics Explained, Section 1, 1998.

[2] M. Donias, « *Caractérisation de Champs d’Orientation par Analyse en Composantes Principales et Estimation de la Courbure : Application aux Images Sismiques* », Thèse de doctorat, Université Bordeaux I, France, Janvier 1999.

[3] R. A. Fisher, « *The use of multiple measurements in taxonomic problems* », *Annals of Eugenics*, Vol. 7, pp. 179-188, 1936.

[4] Cherng Jye Liou, “A Real Time Face Recognition System”, DSP/IC Design Lab, Department of Electrical Engineering, National Taiwan University, June 1997.

[5] John Holland, « *Outline for a logical theory of adaptive systems* », Journal of the Association of Computing Machinery, 3, 1962.

[6] D.E. Goldberg, « *Genetic Algorithms in Search, Optimization and Machine Learning* », Reading MA AddisonWesley, 1989.

[7] E. Diday, J. C. Simon, « *Cluster Analysis* », dans Digital Pattern Recognition, (K. S. FU edition), pp. 47-94, Springer – Verlag, Berlin, 1976.

[8] R. O. Duda, P. E. Hart, « *Pattern Classification and Scene Analysis* », John Wiley and Sons, New York, 1973.

[9] T. W. S. Chow, G. Fei, « *Three phase induction machines asymmetrical faults identification using bispectrum* » IEEE Transactions on Energy Conversion, Vol. 10, Issue 4, pp. 688-693, December 1995.

[10] E. Didelet, « *Les arbres de neurones avec rejet d’ambiguïté. Application au diagnostic pour le pilotage en temps réel du réseau téléphonique français* », Thèse de doctorat, Université de Technologie de Compiègne, 1992.

[11] R.P. Wildes, « *A system for automated iris recognition* », Proc. of 2nd IEEE Workshop on Applications of Computer Vision, pp. 121-128, Décembre 1994.

[12] CNN World News. Schiphol Backs Eye Scan Security. Available at http://www.cnn.com/2002/WORLD/europe/03/27/schiphol.security/, March 27, 2002.

[13] J. Daugman. Recognizing Persons by Their Iris Patterns. In A. K. Jain, R. Bolle, and S. Pankanti, editors, Biometrics: Personal Identification in a Networked Society, pp. 103-121, Kluwer Academic Publishers, 1999.

[14] E. Hjelmås and B.K. Low. Face detection : A survey. Computer Vision and Image Understanding, 83(3) :236–274, 2001.

[15] M-Y. Yang, D.J. Kriegman, and N. Ahuja. Detecting faces in images : A survey. IEEE Transactions on Pattern Analysis and Machine Intelligence, 24(1) :34–58, 2002.

[16] X.G. Lu, D. Colbry, and A.K. Jain. Three-dimensional model based face recognition. In International Conference on Pattern Recognition, pages 362–366, Cambridge, UK, 2004.

[17] T. Kanade. “Picture Processing Systemby Computer Complex and Recognition of Human Faces”. In : *Doctoral dissertation, Kyoto University*, November 1973.

[18] S. Arca, P. Campadelli, and R. Lanzarotti. “A Face Recognition SystemBased On Automatically Determined Facial Fiducial Points”. *Pattern Recognition*, Vol. 39, No. 3, pp. 432–443, 2006.

[19] Nicolas MORIZET, Thomas EA, Florence ROSSANT, Frédéric AMIEL et Amara AMARA. "Revue des algorithmes PCA, LDA et EBGM utilisés en reconnaissance 2D du visage pour la biométrie" P1-11. Institut Supérieur d’Electronique de Paris (ISEP), département d’Electronique, 2006.

[20] M. Turk, A. Pentland, Eigenfaces for Recognition, Journal of Cognitive Neurosicence,Vol. 3, No. 1, 1991, pp. 71-86

[21] Moad Benkiniouar, Mohamed Benmohamed. "Méthodes d’identification et de reconnaissance de visages en temps réel basées sur AdaBoost" Article P2-3,2005.

[22] X. Wang, X. Tang, Unified subspace analysis for face recognition, Proceedings of the Ninth IEEE International Conference on Computer Vision, 2003, pp. 679–686.

[23] F. Samaria, A. Harter, Parameterisation of a stochastic model for human face identification, in: F.L. Sarasota (Ed.), Proceedings of Second IEEE

[24] K. Etemad, R. Chellappa, Discriminant Analysis for Recognition of Human Face images, Journal of the Optical Society of America A, Vol. 14, No. 8, August 1997, pp. 1724-1733

[25] W.Zhao, R.Chellappa, P.J.Phillips, « ACM Computing Surveys », Vol. 35, No. 4, December 2003, pp. 399–458.

[26] G. Guo, S.Z. Li, K. Chan, Face Recognition by Support Vector Machines, Proc. of the IEEE International Conference on Automatic Face and Gesture Recognition, 26-30 March 2000, Grenoble, France, pp. 196-201

[27] J.-F. Cardoso. Analyse en composantes indépendantes. Dans Journées de Statistique, JSBL 2002, Bruxelles-Belgique, mai 2002.

[28] P. Comon. Independent Component Analysis, a new concept. Signal Processing, Elsevier, 3(287-314), avril 1994. Special issue on Higher-Order Statistics.

[29] C. Liu et H. Wechsler. Comparative assessment of independent component analysis (ICA) for face recognition. Dans Second International Conference on Audio- and Video-based Biometric Person Authentication, pages 211– 216, Washington D.C., USA, mars 1999.

[30] N. Kwak, C.-H. Choi, et N. Ahuja. Face recognition using feature extraction based on independent component analysis. Dans Proceedings of the IEEE International Conference on Image Processing (ICIP'02), volume 2, pages 337–340, Rochester, NY, USA, septembre 2002.

[31] K.-C. Kwak et W. Pedrycz. Face recognition using an enhanced independent component analysis approach. IEEE Transactions on Neural Networks, 18(2) :530 – 541, mars 2007.

[32] M. Bartlett, J. Movellan, et T. Sejnowski. Face recognition by independent component analysis. IEEE Transactions on Neural Networks, 13(6) :1450 – 1464, novembre 2002.

[33] L. Zhang, Q. Gao, et Z. D. Block independent component analysis for face recognition. Dans 14th International Conference on Image Analysis and Processing, 10.1109/ICIAP.2007.4362782, pages 217 – 222, septembre 2007.

[34] A. S. Tolba, A.H. El-Baz, and A.A. El-Harby, "Face Recognition: A Literature Review", INTERNATIONAL JOURNAL OF SIGNAL PROCESSING VOLUME 2 NUMBER 2 2005 ISSN 1304-4494.

[35] Wen Gao, Shiguang Shan, Face Verification for Access Control, "Biometrics Solutions for Authentication in an E-World", Edited by David Zhang, Kluwer Academic Publishers, Chapter 13, pp339-376, 2002.

[36] L. Png, "Morphological Shared-Weight Neural Network For Face Recognition", A dissertation submitted to the University of Manchester Institute of Science and Technology for the degree of MSc, August 2004.

[37] P.Sinha,"Object Recognition via Image Invariants: A Case Study," Investigative Ophthalmology and Visual Science, vol. 35, no. 4, pp. 1735- 1740, 1994.

[38] P. Sinha, “Processing and Recognizing 3D Forms,” PhD thesis, Massachusetts Inst. of Technology, 1995.

[39] A. Yuille, P. Hallinan, and D. Cohen, “Feature Extraction from Faces Using Deformable Templates,” Int’l J. Computer Vision, vol. 8, no. 2, pp. 99-111, 1992.

[40] R. Brunelli, T. Poggio. Face recognition: features versus templates. IEEE Trans. Pattern Anal. Mach. Intell, pp-1042–1062, 1993.

[41] Emily Hammon FACCI, « Australia Locks in High Technology », Sydney CURITY.

[42] www.i-cube.co.za/50_plus_face_recognition_uses.htm.

[43] MESSER Kieron ; KITTLER Josef , « Face authentication competition on the BANCA database » ; 2004.

[44] A. K. Jain, L. Hong, S. Pankanti, « Biometrics : Promising Frontiers for Emerging Identification Market », Communications of the ACM, pp. 91-98, February 2000.

[45] T. Ojala, M. Pietikainen, and T. Maenpaa. Multiresolution gray-scale and rotation invariant texture classi_cation with local binary patterns. IEEE Trans. PAMI,24(7) :971_987, 2002.

[46] T. Ahonen, A. Hadid, and M. Pietikainen. Face recognition with local binary patterns. In ECCV, pages 469_481, 2004.

[47] T. Ahonen, A. Hadid, and M. Pietikainen. Face recognition with local binary patterns. In ECCV, pages 469_481, 2004.

[48] Xiaoyang Tan and Bill Triggs. Enhanced local texture feature sets for face recognition Under difficult lighting conditions. In Analysis and Modelling of Faces and Gestures, volume 4778 of LNCS, pages 168 ,182. Springer, oct 2007.

[49] http://web.mit.edu/emeyers/www/face_databases.html#orl (consulté le 03 /05/2014)

[50] http://cswww.essex.ac.uk/mv/otherprojects.html(consulté le 03 /05/2014)

Résumé

Au cours de ces dernières années, on observe un intérêt croissant autour de la biométrie. La reconnaissance faciale en tant qu'une technologie biométriques de base, a pris une part de plus en plus importante dans le domaine de la recherche, du fait de son caractère non intrusif et sans contact. Mais malgré les nombreuses approches et méthodes qui ont été proposées pour résoudre le problème de reconnaissance du visage humains, il demeure un problème extrêmement difficile, ceci est dû au fait que le visage de personnes différentes ont généralement la même forme et varie du fait des conditions d'éclairage, de la variation de pose, et des expressions faciales. De nos jours les systèmes de vérification d'identité apparaît être un vecteur intéressant à exploiter, vu la multitude des applications qui leurs font appel contrôle d'accès aux sites sensibles, télésurveillance...etc.

Le travail effectué dans le cadre de ce mémoire porte sur l'identification automatique de visages avec deux méthodes de reconnaissance faciale en utilisant l'analyse en composantes principales (ACP) et local binnary pattern (LBP). Les résultats, obtenue ont montré que LBP donne nettement des meilleurs résultats par rapport à l'ACP .Pour validé ce travail nous avons testé ces techniques sur des images frontales de les bases de données ORL et FEI.

Mots-clés:

Reconnaissance de visages, Biométrie, ACP, LBP, extraction de caractéristiques, eigenfaces.

ملخص

خلال السنوات الأخيرة , هناك اهتمام متزايد حول المقاييس الحيوية. وقد أخذ نظام التعرف على الوجه - كقاعدة التكنولوجيا الحيوية - أهمية متزايدة في مجال البحوث ، بسبب عدم التدخل والتماس. لكن على الرغم من الكثير من النهج والأساليب التي تم اقتراحها لحل المشاكل المتعلقة بالتعرف على الوجه البشري، فإنها لا تزال مشاكل صعبة للغاية، وهذا يرجع إلى حقيقة أن الناس على اختلافهم يمتلكون عموما نفس الشكل ويختلف بسبب ظروف الإضاءة، واختلاف الوضعيات، وتعابير الوجه. في الوقت الحاضر تعتبر نظم التحقق من الهوية مجالا هاما لاستغلال، و هذا بالنظر إلى العديد من التطبيقات التي تستخدم فيها لتحكم في الوصول إلى المواقع الحساسة، والرصد عن بعد ... الخ.

يركز العمل الذي نقوم به كجزء من هذه الأطروحة على تحديد وجه التلقائي مع أسلوب "مختلط" للتعرف علي وجه بإستخدام طريقتين للتعرف على الوجه وهما تحليل المكون الرئيسي(آسيبي) و النموذج الثنائي المحلي (ال بي بي) .النتيجة المحصل عليها تبين أن ال بي بي تعطي أفضل نتيجة مقارنة ب الآسيبي. لللتحقق من صحة هذا العمل قمنا بإختبار هاتين التقنيتين على الصور من قاعدة البيانات "أو آرآل"و"اف او اي".

كلمات البحث:

التعرف على الوجوه، القياسات الحيوية،تحليل المكونات الأساسية، النموذج الثنائي المحلي ، استخراج الخصائص ، القيم الفردية.

Abstract

In recent years, there has been a growing interest around biometrics. Facial recognition, as a biometric technology, has played an increasingly important role in the field of research, because of its non-intrusive and contactless. However, despite of the many approaches and methods that have been proposed to solve the problem of human face recognition, it remains an extremely difficult problem. this is due to the fact that different people faces have generally the same shape and vary due to the lighting conditions , variation of pose , and facial expressions. Nowadays, identity verification systems appears to be an interesting domain to exploit, given the multitude of applications that utilize their controlling access to sensitive sites, remote monitoring ... etc.

The work done as part of this thesis is focused on identifying automatic face with two methods for face recognition principal component analysis(PCA) and local binary pattern(LBP). The results, of LBP compared with the PCA, provide a significant improvement in performance. For the validation of this work, we tested this technique on frontal images of the database ORL and FEI .

Keywords:

Face recognition, Biometrics, PCA,LBP , feature extraction, eigenfaces.