BADJI MOKHTAR- ANNABA UNIVERSITY

UNIVERSITE BADJI MOKHTAR ANNABA

جامعة باجي مختار- عنابة

Année : 2016

Faculté: Sciences de l'ingéniorat
Département: Electronique

MEMOIRE
Présenté en vue de l'obtention du diplôme de : MASTER

Intitulé

Reconnaissance de visages par Analyse Discriminante Linéaire(LDA)

Domaine : Sciences et Technologie
Filière : Electronique

Spécialité: Télécommunications Avancées

Par : MERAMRIA Nabila

DEVANT Le JURY

Président :	**Saouchi . k**	**Grade M.C.A U. Annaba**
Directeur de mémoire :	**Zermi . N**	**Grade M.C.B U.Annaba**
Examinateur :	**Bouchaala . A**	**Grade M.A U. Annaba**

REMERCIEMENT

En premier lieu, je remercie "DIEU" de m'avoir donné tant de patience et de puissance de pouvoir réaliser ce modeste travail.

Je remercie tous qui m'apportés se l'aide tout ou long de la réalisation de notre travail, je tiens à exprimer tout particulièrement mon remerciement à :

- *Je voudrai remercier chaleureusement mon encadreur*

« « Dr ZERMI NARIMA » »

Qui m'éclairé avec ses conseils et suggestions et qui fut un soutient indispensable à l'accomplissement de mon travail

On n'omettra pas de remercier vivement tous les enseignants qu'on a eus tout le long de notre cycle du master
Et sur tout Mr Affifi.S
A Tout ..... je dis merci pour tout

Meramria Nabila

DEDICACE

Je dédie ce modeste travail aux être que sont les plus chère:

A l'espérés de ma mère que dieu le bénéfice

A ma sœur: Houda et à mon frère Salah Eddine,

A ma grand-mère Fatma

A mes petits poussins: Hadil, Seif Eddine Abd Alghani,
A mes chères Amis: Marwa, Soumaia, Fati, Ferial, Amira,

A qui j'ai passe avec mes meilleurs moments qui restent un bon souvenir pour toujours.
A tout mes collègues de la promotion de télécommunication avancée

2015/2016

Tous qui travail a département d'électronique.

A tous ..... je dis merci pour tout

Meramria Nabila

Sommaire

Chapitre III: Conception et implémentation

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 Eigen face 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.

-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 consacré à la partie conception et réalisation de notre système, où nous présenterons les bases de visages qui seront utilisées lors de la phase d'apprentissage et de test, aussi un ensemble de test est réalisées et nous montrant la suite des résultats obtenues toute en discutons ses résultats.

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

Chapitre I: Biométrie & systèmes de reconnaissance de visage

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) :

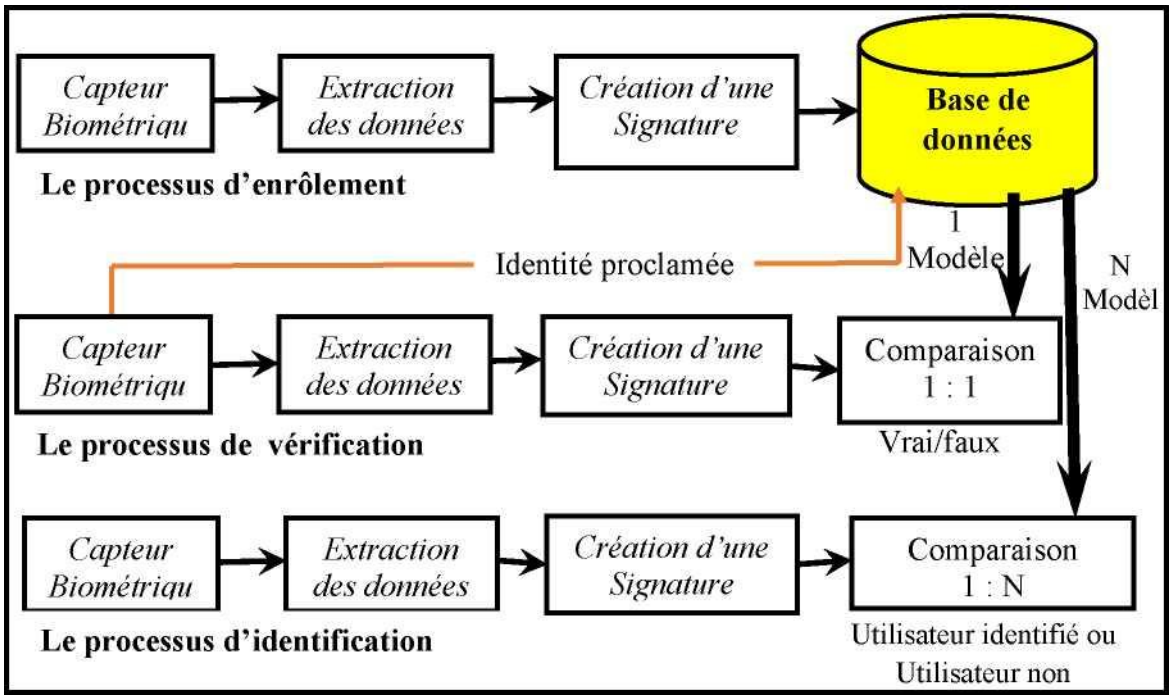

Fig.I.1 : Principaux modules d'un système biométrique ainsi que les différentes.

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, liés aux dispositifs de capture des données, à l'utilisateur lui-même ou 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.

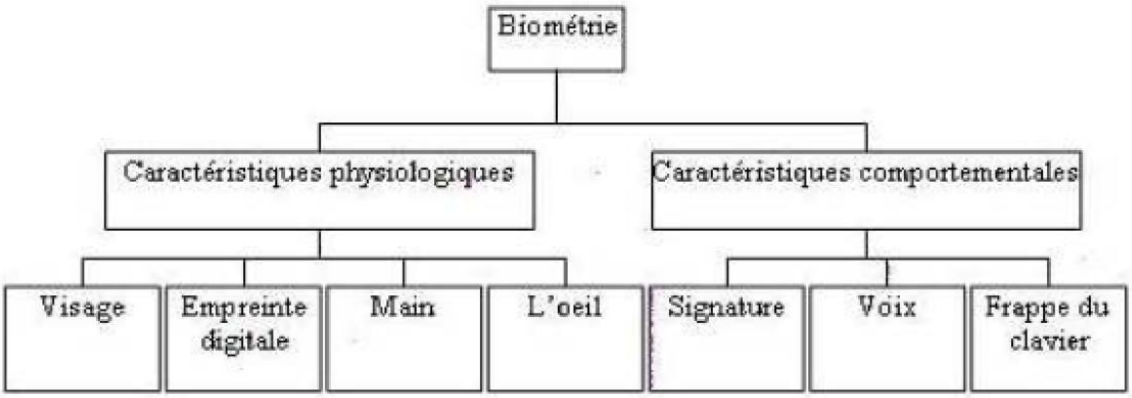

Fig.I.2 : La Classification De La Biométrie.

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].

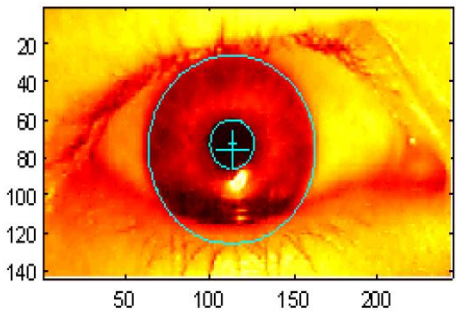

Fig.I.4 : Photo d'iris.

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].

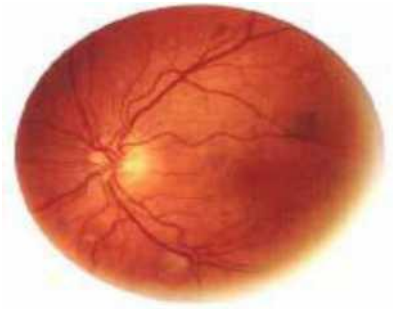

Fig.I.6 : Photo de rétine.

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.

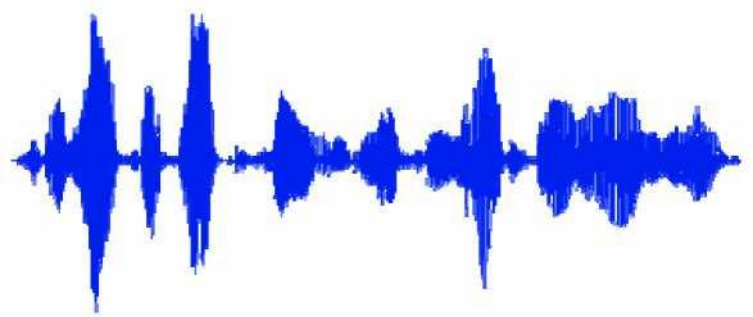

Fig.I.8 : Spectre d'un signal voix.

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
Ins	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 premium 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.

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

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.

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

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

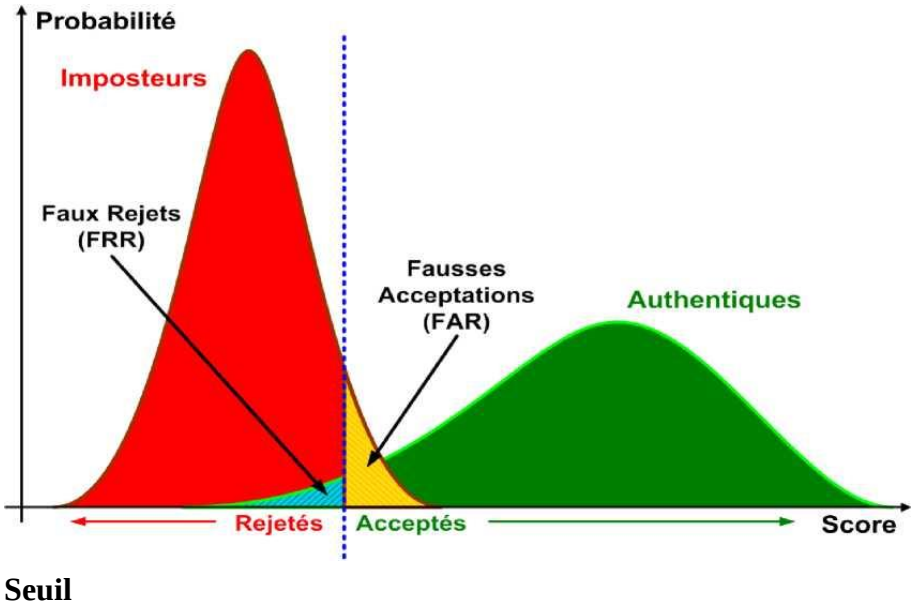

Fig.I.11 : Illustration du FRR et du FAR.

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, ...

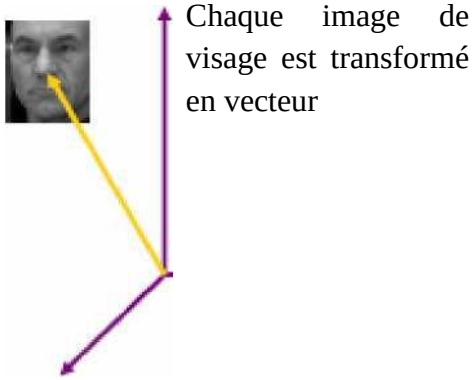

Fig.I.12 : le principe des méthodes globales.

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.

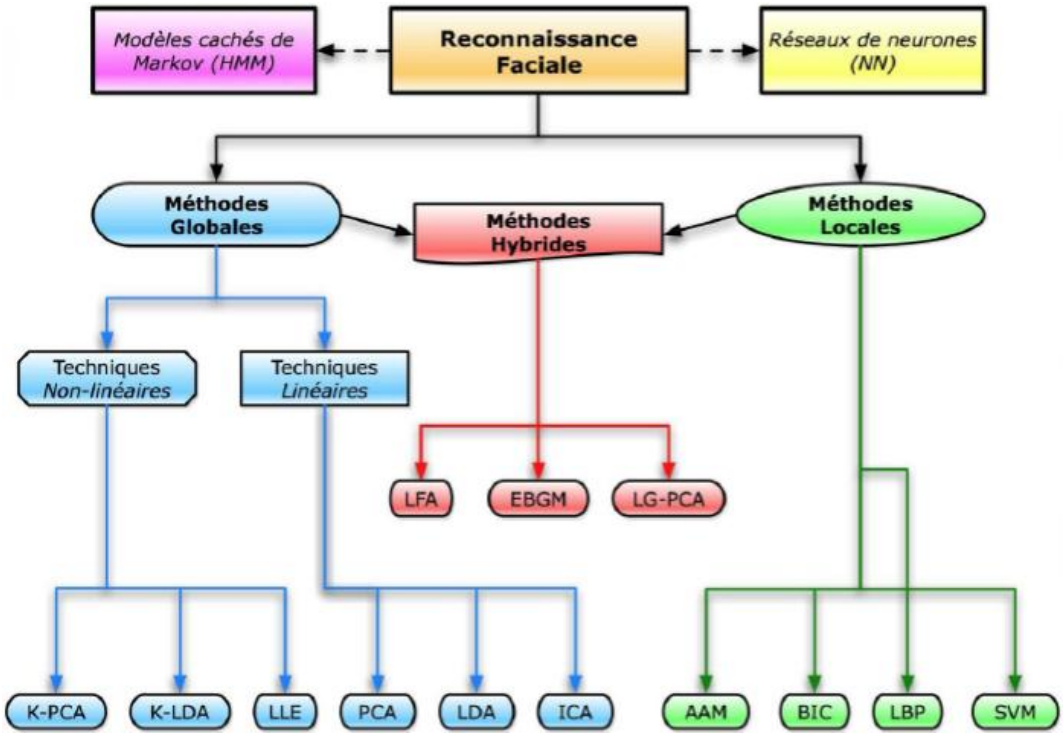

Fig.I.13 : Une classification des algorithmes principaux utilisés en reconnaissance faciale.

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 :

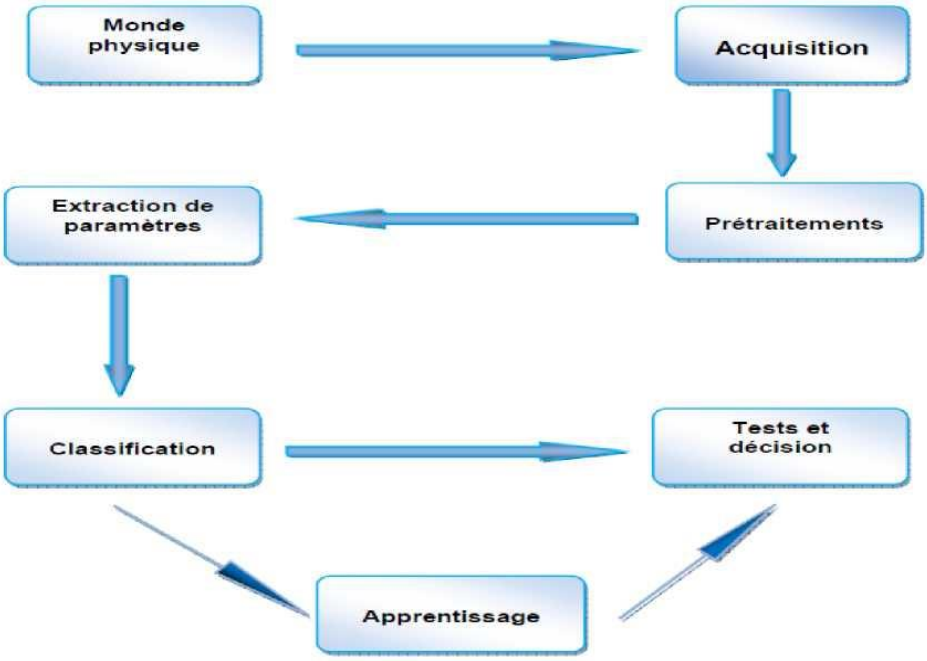

Fig.I.14 : Système de reconnaissance.

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.8.2 Variation 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.

Chapitre II: Etat de l'art des techniques de reconnaissance de visages

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 existe 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'Eigen face 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'Eigen face 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.

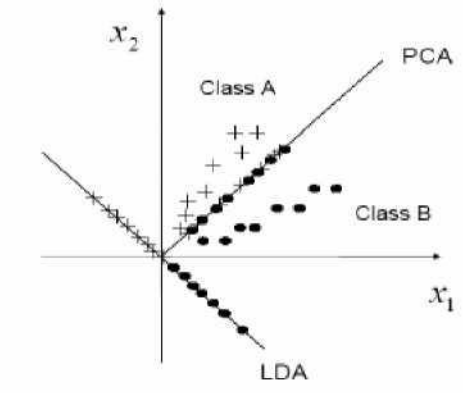

Fig.II.2 : les projections ACP et LDA d'un ensemble de données.

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].

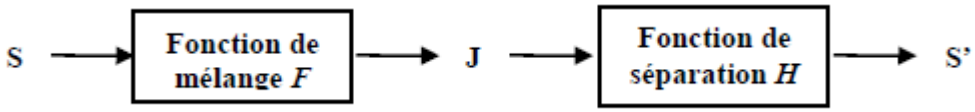

Fig.II.3 : Modèle général du mélange et de la séparation de sources.

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].

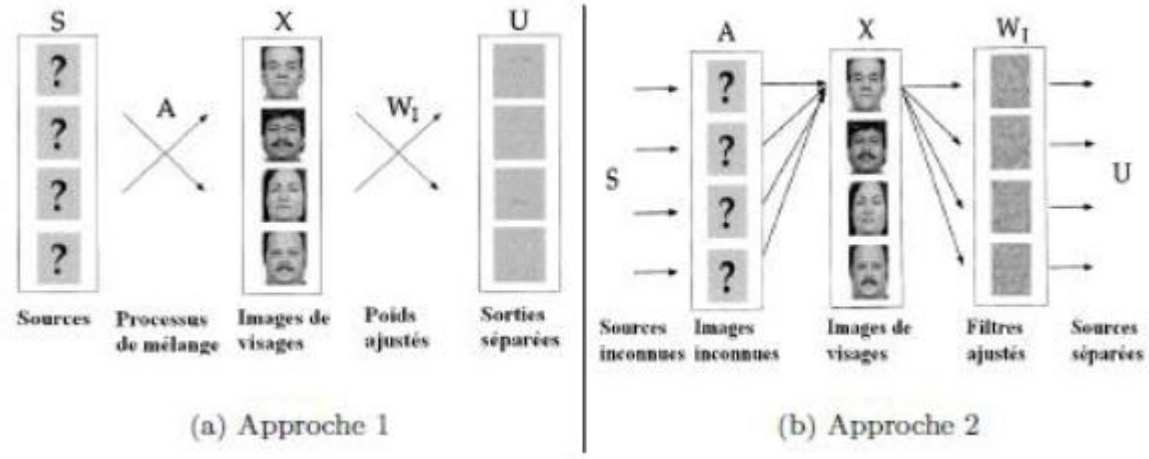

Fig.II.4 : Le modèle de synthèse d'image de l'architecture d'ICA.

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 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[34] .

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 [35].

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 « Titanium Technology 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 » [36].

II.6 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.

Chapitre III: Conception et implémentation

III.1 Introduction

Ce chapitre est consacré à la conception et réalisation de notre application. La première partie de ce chapitre est une présentation des détails ainsi que les approches théoriques utilisées dans le cadre de la conception de notre système de reconnaissance de visages à base de la LDA. Tandis que la seconde partie c'est l'implémentation de ce système et la présentation matériel et logiciel nécessaire à son fonctionnement.

III.2 Conception

La structure générale du système de reconnaissance de visages comporte deux phases :

1) **La phase d'apprentissage** : Comme son nom l'indique, c'est la phase où le système apprend la personne à partir d'une ou plusieurs images, elle s'effectue en utilisant l'algorithme de Fisher. A la fin de cette étape, on aura pour chaque personne un modèle unique qui le Caractérise.

2) **La phase de test :** Elle consiste à identifier une personne de la base de test à partir de celles qui se trouvent dans la base d'apprentissage.

III.2.1 Création de la base de données

On a utilisé une seule base de visages et c'est la base Yale. Elle se compose de 165 images frontales en niveau de gris de 40 personnes, avec 11 images pour chacune. On trouve trois angles d'éclairage différents : gauche, centre et droit, et il existe des images avec lunette et sans lunettes. La base offre des images incluant différentes expressions faciales : normale, triste, heureux, somnolant, étonnant, et clignotement de l'Sil.

Les limitations de cette base de données sont : le nombre limité de personnes, les positions exactes des sources d'éclairage ne sont pas indiquées, il n'y a aucune variation d'angle de pose et les facteurs environnementaux (tels que la présence de ou l'absence de la lumière ambiante) ne sont pas également décrits [37].

III.2.1.1 Base d'apprentissage

La base d'apprentissage est composée de 400 images de 40 individus différents, soit 7 images par individus dont les positions sont différentes par rapport à celle de la base de test.

Fig.III.1 **:** Quelques *exemples extraits de la base d'apprentissage Yale*

III.2.1.2 Base de test

La base de test est composée de 60 images de 15 individus différents, soit 4 images par individus dans des positions différentes à celle de la base d'apprentissage.

Fig.III.2 **:** *Quelques exemples extraits de la base de test Yale*.

La création de la base de données est l'étape initiale qui permet d'introduire les images d'apprentissage, cela est assuré dans notre application par la fonction *Acquisition*

III.2.2 Application de l'algorithme de Fisher

L'utilisation de l'image construite n'est pas assez pratique pour l'identification, il est nécessaire d'avoir une représentation compacte. Pour cela on doit y avoir besoin d'appliquer les opérations de l'Algorithme de Fisher (la LDA), grâce à la fonction *apprentissage* qui fait appelle à la fonction *Fisherface2*.

Les étapes suivantes ont été suivies pour l'implémentation de l'algorithme LDA :

- Dans un premier temps nous allons calculer la moyenne

m_database = mean(T, 2).

- Calcul de l'écart de chaque image par rapport à l'image moyenne.

A = T - repmat(m_database,1,P)

- Calcul de la matrice de covariance C=A*A' où A' est la matrice transposé de A et chaque colonne de cette dernière est un vecteur de différence.

- Calcul de L= A'*A le substitut de la matrice de covariance ou le calcul se limite à cause des dimensions élevées de C.

- Le tri et l'élimination des petites valeurs propres L_eig_vec = [L_eig_vecV(:,i)] pour i allant de 1 jusqu'au P.

- Calcul des vecteurs propres de la matrice de covariance 'C ' V_PCA=A *L_eig_vec.

- Calcul de la moyenne de chaque classe en espace propre.

- Initialisation de la matrice de dispersion intra-classe (withinScatter matrix Sw) et la matrice de dispersion inter-classe (BetweenScatter matrix Sb).

- Calcule de la matrice de dispersion totale S= Sb+Sw .

- La maximisation de Sb tout en minimisant Sw, Ainsi, une fonction de coût J est défini, de sorte que cette condition est remplie.

- La projection d'images dans l'espace de Fisher.

III.2.3 Reconnaissance

Dans cette étape on compare deux faces en projetant les images dans FaceSpace et mesure la distance euclidienne entre l'image de test et toutes les images de la base de d'apprentissage, la personne en entrée est affecté à la classe avec laquelle il à une distance euclidienne plus petite.

III.3 Réalisation

Dans cette partie nous allons décrire l'aspect implémentation de l'application réalisée. Parler de l'implémentation revient à détailler l'aspect matériel, l'environnement de développement et les différents modules qui composent le système.

III.3.1 Aspect matériel

Notre projet a été développé sur un micro bureau:

- Processeur : Intel(R) Core (TM) i5-2540M CPU Ø Capacité Mémoire (RAM) :4.00 Go

- Vitesse d'horloge : 2.60 Ghz

- Capacité disque dur : 256 Go

- Système d'exploitation : Windows 8.1

III.3.2 Outils de développement

Pour la réalisation de notre système nous avons choisi le langage de programmation MATLAB Version 8.0 (R2012b). MATLAB est un environnement de calcul scientifique et de visualisation de données. Sa facilité d'apprentissage et d'utilisation (due à une syntaxe très claire) en ont fait un standard adapté pour les divers problèmes l'ingénierie.

Parmi les raisons qui nous ont poussés à l'utiliser, on trouve :

" Ses très nombreuses fonctions prédéfinies et prêtes à l'emploi.

" Sa simplicité à l'implémentation et rapidité de calculs.

" Sa fiabilité et sa robustesse.

MATLAB offre un certain nombre de fonctionnalités pour la documentation et le partage du travail. On peut intégrer le code MATLAB avec d'autres langages et applications, et distribuer les algorithmes et applications MATLAB.

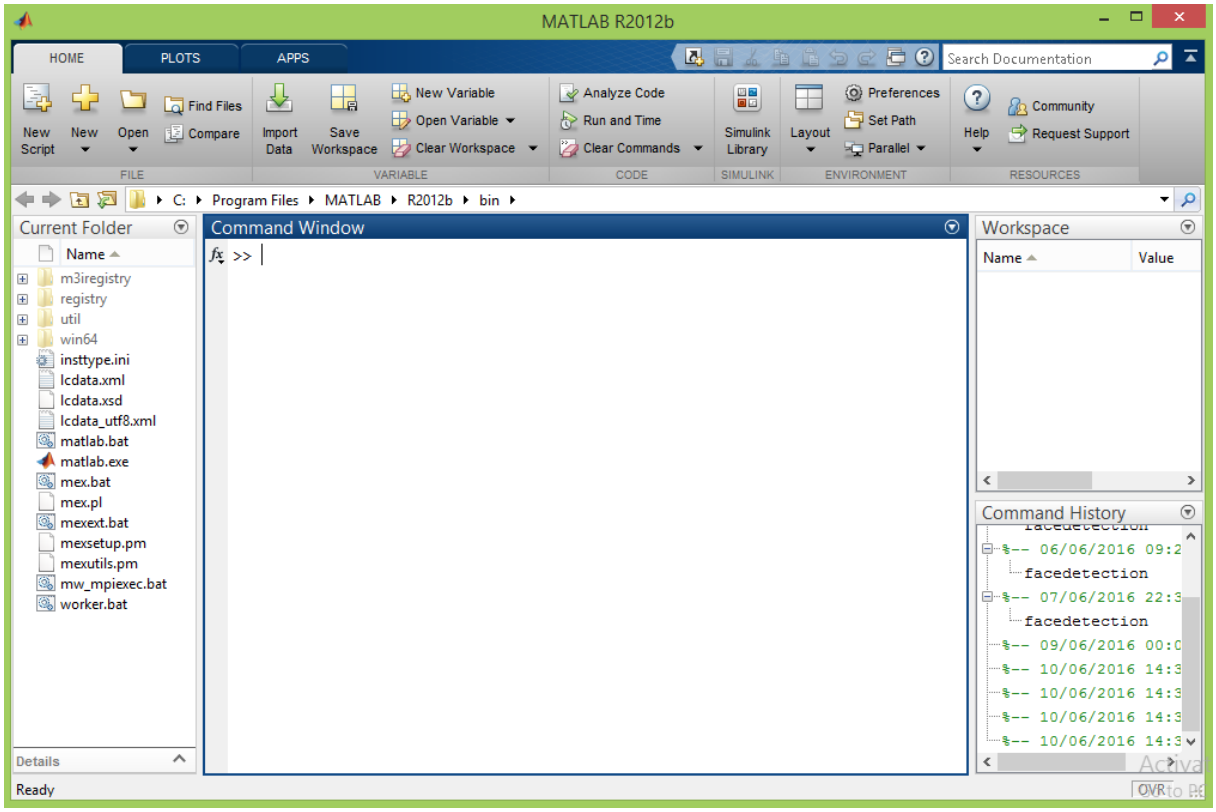

Fig.III .3 : Fenêtre principale de MATLAB

III.3.3 Différents fonctions de l'application:

Notre application comporte un ensemble de fonctions qui assure les points discutées dans la partie conception, dans ce qui suit nous donnerons une description de ces fonctions :

- La création de la base de données est l'étape initiale qui permet d'introduire les images d'apprentissage, cela est assuré dans notre application par la fonction *Acquisition*.

- La fonction *Acquisition* utilise la variable*« AppDatabasePath »* comme entrée et retourne *« T »* une matrice contenant tous les images transformée en vecteur colonne. Cette fonction transforme toutes les images de la base d'apprentissage en un vecteur colonne 1D,

- Chaque colonne de la matrice *« T »* est une personne de la base d'apprentissage qui est a été remodelée.

- La fonction *Fisherface2* a comme entré la matrice *« T »* et retourne la moyenne des images d'apprentissage *«m_databse »*, les vecteurs propres *«V_PCA »* de la matrice de covariance, les vecteurs propres *« V_Fisher »* de la matrice de projection et la variable *« Projected Images_Fisher »* qui est la projection de toutes les images dans l'espace de Fisher.

- Pour la reconnaissance on fait appel à la fonction *Recognition* qui a 5 entrées, *« TestImage »*

qui est l'une des images qu'on cherche à identifier, elle est extraite de la base de teste, *« m-database »*, *« V_PCA »*, *« V_Fisher »*, et *«Projected Images_Fisher »* qu'on a vu précédemment. Et elle retourne *«équivalent Image »* qui est l'image équivalente à l'image de test dans la base d'apprentissage, en outre c'est l'image qui a la distance la plus petite avec l'image test.

III.3.4 Interface graphique

III.3.4.1 Fenêtre d'accueil

Voici la fenêtre d'accueil telle qu'elle apparait lors du lancement de l'application depuis MATLAB.

C'est la fenêtre à partir de laquelle on démarre notre système, elle comporte deux boutons, le bouton suivant permettant de passer à la fenêtre principale d'apprentissage et de reconnaissance, et un bouton quitter permettant de quitter l'application, la figure suivante montre cette fenêtre :

Fig.III.4 : Fenêtre d'accueil de l'application

1 Permet d'entrer à la fenêtre principale.

2 Permet de quitter l'application

III.3.4.2 fenêtre principale

En cliquant sur le Bouton suivant de la fenêtre d'accueil une autre fenêtre s'ouvre : c'est la fenêtre principale de l'application

Fig.III.5 : fenêtre principale de l'application

1 Permet d'afficher les 105 images d'apprentissages de la base Yale.

2 Permet de choisir une des phases.

3 Permet d'accéder à l'aide concernant l'application

4 Permet de quitter l'application.

5 Permet de revenir à l'accueil.

Et cliquant sur le bouton apparaissent, on choisissant la phase apprentissage on obtient la figure suivante :

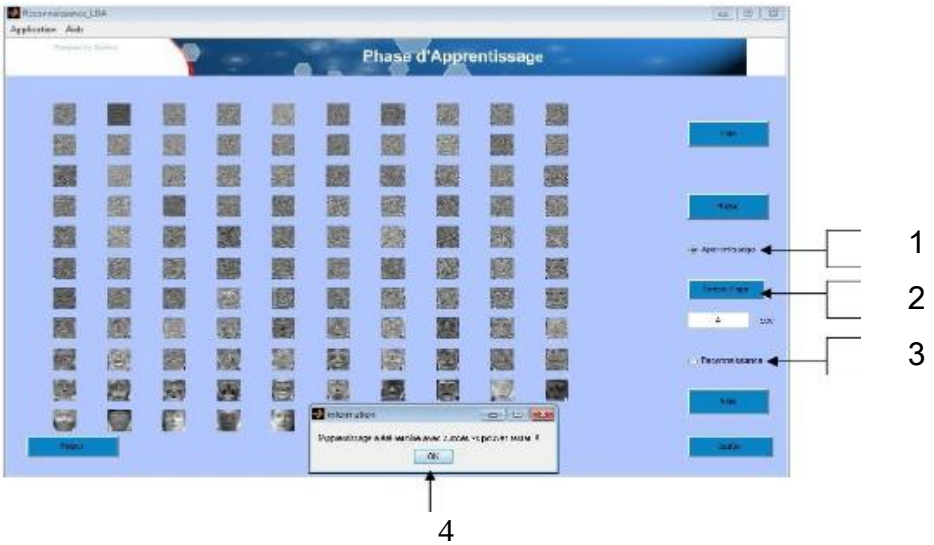

Fig.III.6 : Phase d'apprentissage

1. Permet de lancer l'apprentissage.

2. Permet d'afficher le temps d'apprentissage.

3. Permet d'accéder à la fenêtre de reconnaissance ou de lancer le test.

4. Permet d'accéder à la fenêtre de reconnaissance ou de lancer le test.

III.3.4.3 fenêtre de reconnaissance (phase de test)

En choisissant la phase reconnaissance, une autre fenêtre s'ouvre et on obtient la figure suivante :

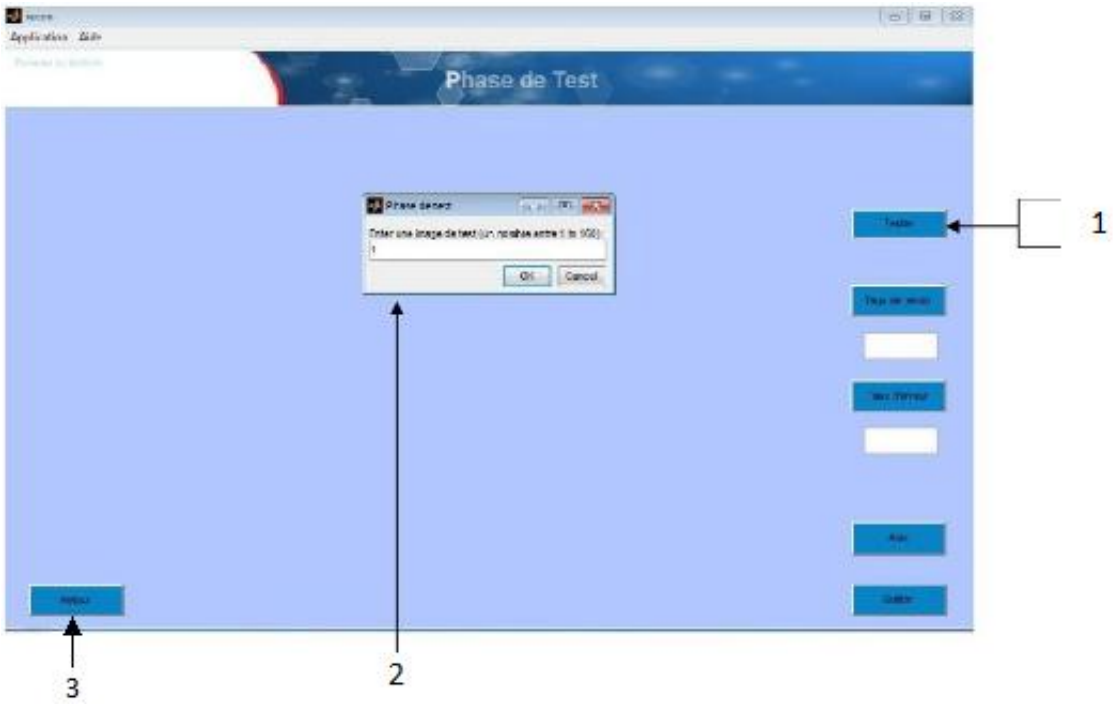

Fig.III.7 : fenêtre de la phase de test

1. Permet d'afficher une boite de dialogue

2. Permet d'enter une image test.

3. Permet de revenir à la fenêtre précédente (celle de l'apprentissage).

III.3.4.4 Exemple sur la base Yale

Nous avons présentée dans ce qui suit deux exemples sur la base Yale, un exemple de test qui donne un résultat positif et un autre exemple qui donne de résultat négatif, le premier sera représenté par la *Fig.III.8* , et le seconde par la *Fig.III.9*

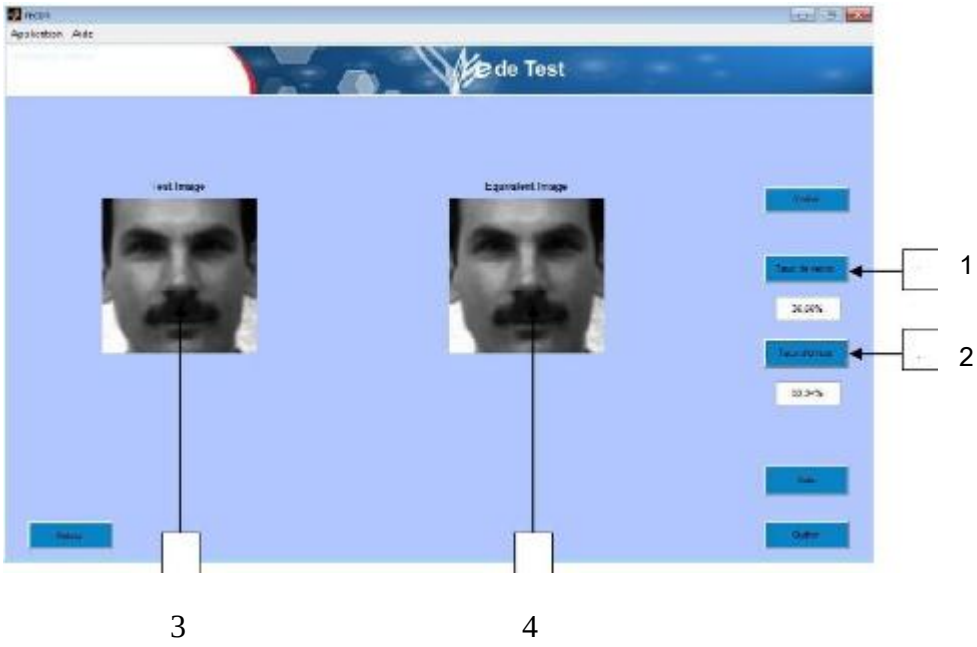

Fig.III.8 : Résultat d'un test positif

1. Permet d'afficher le taux de reconnaissance

2. Permet d'afficher le taux d'erreur.

3. L'image test

4. L'équivalent de l'image de test (image reconnu).

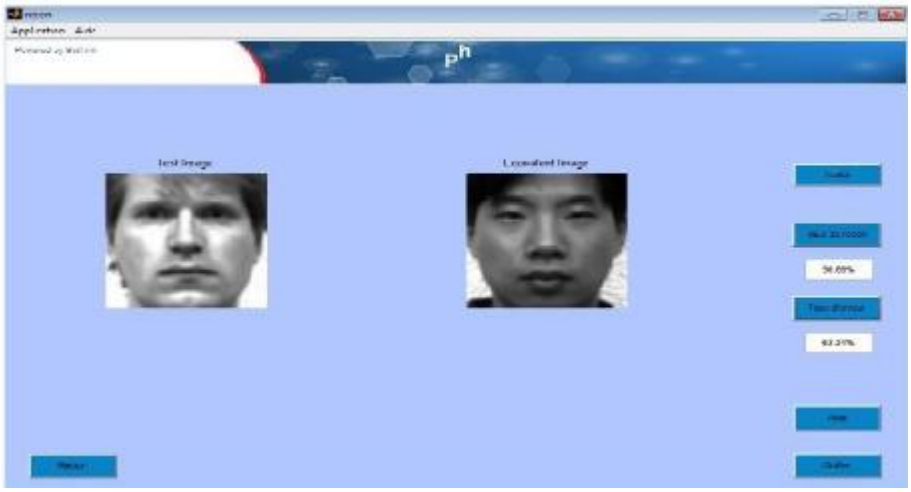

Fig.III.9 : Résultat d'un test négatif

III.3.5 Test et Evaluation

Pour tester l'efficacité de notre système nous avons créé deux nouvelles bases de test et d'apprentissage à partir de la base Yale, cette création c'est une simple sélection de visages à partir de la base originale (Yale data base) :

- La première base est composée de 105 images d'apprentissages et 60 pour le test et cela a conduit à des résultats qui sont illustrés dans le tableau suivant :

Temps d'apprentissage = 3sec	Taux de reconnaissance (%)	Taux d'erreur(%)
Base d'apprentissage (105 visages)	100%	0%
Base de test (60 visages)	36,66%	63,44%

TableauIII-1 : Résultat obtenu sur la 1^{ere} base de donnée

- La deuxième base est composée de 20 images d'apprentissages et 10 pour le test, les résultats sont illustrés dans le tableau suivant

Temps d'apprentissage= 1sec	Taux de reconnaissance (%)	Taux d'erreur(%)
Base d'apprentissage (20)	100%	0%
Base de test (10)	60%	40%

Tableau III-2 : Résultat obtenu sur la2^{eme} base de donnée

III.3.6 Discussion des résultats

La méthode LDA que nous avons appliqué donne de bons résultats quand le nombre d'images d'apprentissages est limité (*Tableau III-2)*, et donne de mauvais résultats lorsque le nombre d'images d'apprentissages augmente (*Tableau III-1*).

Ce problème est souvent reconnu en littérature sous le nom SSS (Small Sample Size).

III.4 Conclusion

Dans ce chapitre, nous avons illustré l'architecture globale de notre système de reconnaissance de visages basé sur la LDA et les détails des fonctions qui le composent, ainsi que le langage qui assure son fonctionnement. Et à travers les tests obtenus on peut dire que la performance du système repose sur un critère, qui est le bon choix des images d'apprentissages.

Conclusion Générale et perspectives

Vu la nécessité d'utiliser des applications de contrôle d'accès, la reconnaissance de visages a émergé comme un secteur actif de recherches, enjambant des disciplines telles que le traitement d'images, l'identification de modèle, et la vision par ordinateur.

Dû à sa nature facile à utiliser, la reconnaissance de visages restera un outil puissant malgré l'existence d'autres méthodes biométriques de reconnaissance.

Durant ses dernières années de nombreuses méthodes ont été proposé, dont plusieurs ont été appliqué avec succès. Le choix d'une méthode doit être basé sur les conditions spécifiques de chaque application. Parmi toutes ces méthodes, l'algorithme LDA reste une des approches les plus fiables mais complexe.

A travers les tests effectués, le fait d'avoir un nombre suffisant de données d'apprentissage conduit à une mauvaise classification.

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

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. 103121, Kluwer Academic Publishers, 1999.

[14] E. Hjelmâs 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 (ICTP'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] Emily Hammon FACCI, « Australia Locks in High Technology », Sydney CURITY.

[35] www.i-cube.co.za/50 plus face recognition uses.htm.

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

[37]: A. Mellakh «*Reconnaissance des visages en conditions dégradées* », thèse de doctorat a l'Ecole National Supérieur de télécommunication, France, 2009.

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.

Comme toute tâche de reconnaissance de formes, le processus de reconnaissance automatique de visages se décompose en deux étapes : l'extraction d'éléments caractéristiques et la classification de ceux-ci. Pour cela on va utiliser la méthode LDA (Linear Discriminent Analysis) qui utilise le critère de réduction qui se base sur la notion de séparabilité de classe. Cette méthode comporte deux étapes aussi : la réduction de l'espace d'origine par l'ACP, puis les vecteurs de l'espace de projection final « Fisherfaces » sont calculés sur le critère de séparabilité des classes mais dans l'espace réduit.La classification avec LDA est également utilisée avec succès mais couteuse en temps de calcul quand les dimensions de l'image sont hautes et la taille de l'échantillon d'apprentissage est grande.

Mots-clés:

Reconnaissance de visages, Biométrie, LDA, extraction de caractéristiques, Eigen faces.

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.

مثل أي عملية التعرف على الأنماط ، تتكون عملية التعرف التلقائي على الوجوه من خطوتين : إستخراج الميزات و تصنيف ا لهذا سوف نستخدم طريقة تحليل التمايز الخطي (ل د ا) بإستعمال معيار الحد الذي يستند على مفهوم إنفصال الطبقات .هذه

الطريقة في حد ذاتها تتضمن خطوتين : أولها الحد من المساحة الأصلية من قبل(ا س ب) ، ثم يتم إحتساب ناقلات مساحة الإسقاط النهائي" فيشرفكس "على معيار إنفصال الطبقات ولكن في مساحة صغيرة. أُستخدم أيضا التصنيف بطريقة(ل د ا) بنجاح إلا أنه يكلف الوقت ، عندما تكون أبعاد الصورة كبيرة و حجم العينة كبير.

كلمات البحث:
التعرف على الوجوه، (ل د ا) ، 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.

Like any shape recognition task, the automatic face recognition process is broken down into two steps: The features extraction and the classification of these features. For this we will use the LDA method (linear discriminate analysis) using the reduction criterion which is based on the notion of class separability. This method involves two steps as well: The reduction of the original space by the ACP, and the vectors of the final projection space "Fisherfaces" are calculated on the separability criterion classes but in the reduced space. The classification with LDA is also successfully used but expensive in calculation time when the image dimensions are high and the size of the training set is large. keywords:LDA,Fisher faces

Keywords:
Face recognition, Biometrics, LDA , feature extraction, Eigen faces.