Université SAAD DAHLEB BLIDA

Faculté des sciences

Département Informatique

Mémoire de fin d'étude pour l'obtention du diplôme Master en Informatique,

Spécialité Génie des systèmes informatiques

Reconnaissance faciale pour l'authentification basée sur les paramètres biométriques

Réalisé par :

- Cherbal Nasreddine
- Siahoui Karim

Supervisé par :

- Mr. Amine Cherif Zahar

Devant le jury composé de :

- Mr. Hadj Yahia Ouahid	Président
- Mr. Ferfera Sofiane	Examinateur
- Mr. Hammouda Mohamed	Examinateur

Année Universitaire

2014-2015

Remerciements

Avant tout on remercie Allah le Tout Puissant et Miséricordieux pour la force et la patience qu'il nous a données pour pouvoir réaliser ce travail.

Nos remerciements vont également aux deux familles Siahoui et Cherbal pour leurs soutiens et encouragement,

Nos professeurs pour leur patience, aide, conseils et encouragements pour la réalisation de ce projet de fin d'études.

Table des matières

Liste des figures

Introduction générale

Dans le monde d'aujourd'hui, la nécessité de maintenir la sécurité d'informations est de plus en plus à la fois importante et de plus en plus difficile, de temps en temps nous entendons parler des crimes de fraude par carte de crédit, piratage d'ordinateur dus à des failles de sécurité dans une entreprise ou un gouvernement. En 1998, une attaque cyber criminelle a causé plus de 100 millions de dollars de pertes. La plupart de ces crimes, exploite les défauts fondamentaux dans les systèmes de contrôle d'accès classiques, les systèmes ne donnent pas accès par «qui nous sommes», mais par "Ce que nous avons", tels que les cartes d'identité, clés, mots de passe, PIN numéros... Aucun de ces moyens nous définit vraiment, ils ne sont que des moyens qui nous permettent de s'authentifier, par exemple si une personne malveillante acquiert le mot de passe de l'ordinateur d'un collègue elle aura accès aux données de cet ordinateur. Récemment, plusieurs technologies sont devenues disponibles pour permettre la vérification d'identité d'un individu, ces technologies sont basées sur la "biométrie".

La biométrie est devenue une alternative aux anciennes solutions de sécurité comme les mots de passe, les cartes à puces pour vérifier l'identité d'un individu, elle se base sur les caractéristiques physiques qui sont uniques à chaque personne tel que l'empreinte digitale, l'iris, la forme de la main, l'ADN ou le visage.

On classifie le visage comme une donnée biométrique, ceci a donné l'idée de l'utiliser pour la réalisation d'un système de contrôle d'accès. Pour s'identifier, l'utilisateur doit placer son visage devant une caméra pour que le système puisse l'identifier.

Les ordinateurs portables, Smartphones ou tablettes sont des objets qu'on utilise tous les jours, la majorité des utilisateurs de ces appareils voudraient avoir un moyen plus sécurisé qu'un mot de passe, donc un système de reconnaissance de visage peut être la solution.

L'objectif de notre travail s'inscrit dans le contexte de développement d'une application de déverrouillage par reconnaissance faciale en utilisant une caméra, prenant en compte l'influence de la luminosité, la prise de vue etc...

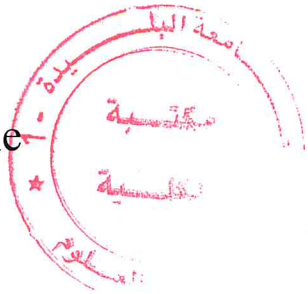
Organisation du mémoire

Ce mémoire est divisé en quatre chapitres :

- Chapitre 1 : Introduction à la Biométrie
- Chapitre 2 : Reconnaissance faciale
- Chapitre 3 : Conception d'un prototype
- Chapitre 4 : Expérimentation et test

Chapitre I
Introduction à la Biométrie

I. Introduction à la Biométrie



1. Introduction

Les systèmes d'information prennent de plus en plus une place stratégique au sein des entreprises. Ainsi la notion du risque lié à ces derniers devient une source d'inquiétude et une donnée importante à prendre en compte, ceci en partant de la phase de conception d'un système d'information jusqu'à son implémentation et le suivi de son fonctionnement.

Les exigences de la sécurité de l'information au sein des organisations ont conduit à deux changements majeurs au cours des dernières décennies. Avant l'usage généralisé d'équipements informatiques, la sécurité de l'information était assurée par des moyens physiques (classeurs fermés par un cadenas) ou administratifs (examen systématique des candidats au cours de leur recrutement). Avec l'introduction de l'ordinateur, le besoin d'outils automatisés pour la protection des fichiers et autres informations stockées est devenu évident. Ce besoin est accentué par un système accessible via un téléphone public ou un réseau de données, d'où la mise en place d'autres modèles de sécurité a eu lieu pour assurer la confidentialité. La première se repose sur la vérification de l'identité à l'aide d'un mot de passe, tandis que la deuxième se base sur l'utilisation d'une carte à puce ou un badge. Cependant, ces méthodes d'authentification sont aussi falsifiables car il est facile de voler un badge ou d'oublier un mot de passe.

La Biométrie quant à elle, entre comme une alternative aux méthodes précédentes, elle offre un niveau de sécurité plus élevé, elle consiste à identifier un individu à partir de ses caractéristiques physiques, biologiques ou comportementales qui peuvent le différencier des autres. Certains systèmes biométriques utilisent une seule caractéristique, d'autres combinent plusieurs afin de diminuer les taux d'erreurs et augmenter la sécurité.

Dans ce premier chapitre, nous allons présenter des notions générales sur la Biométrie, les modalités biométriques, la multi-modalité, le fonctionnement d'un système biométrique et la mesure de ses performances.

2. La biométrie

a) Définition et caractéristiques

Le mot biométrie désigne dans un sens très large l'étude quantitative des êtres vivants [WIK1], mais dans notre contexte plus précis de reconnaissance et d'identification d'individus, il existe deux définitions principales qui se complètent :

1. La biométrie est la science qui étudie à l'aide de mathématiques, les variations biologiques à l'intérieur d'un groupe déterminé [CLU].

2. Toute caractéristique physique ou trait personnel automatiquement mesurable, robuste et distinctif qui peut être employé pour identifier un individu ou pour vérifier l'identité qu'un individu affirme [RAN].

Le terme biométrie regroupe en fait ce que l'on appelle des *modalités biométriques*; contrairement à ce que l'on possède et que l'on peut donc perdre (une clé) ou ce que l'on sait et que l'on peut donc oublier (un mot de passe), les modalités biométriques représentent ce que l'on est et permettent de prouver notre identité. Pour que des caractéristiques collectées puissent être qualifiées de modalités biométriques, elles doivent être [BOU] :

– *universelles* : possédées par tout individu.
– *uniques* : propres à lui (permettent de différencier des autres individus).
– *permanentes* : ne doivent pas varier au cours du temps.
– *enregistrables*: facilement collectées (de manière précise et rapide).
– *Impossible à dupliquer* : c'est à dire, qu'elles ne sont pas vulnérables.
– *mesurables* : permettent une utilisation futur : permettent une utilisation futur

En pratique, une seule modalité ne possède pas toutes ces caractéristiques, ou du moins les possède avec des degrés différents. En réalité, aucune mesure ne se révèle être totalement exacte. Ce problème est dû à l'évolution de l'être humain par le temps (vieillissement, traumatismes, maladies), ce qui change les mesures.

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

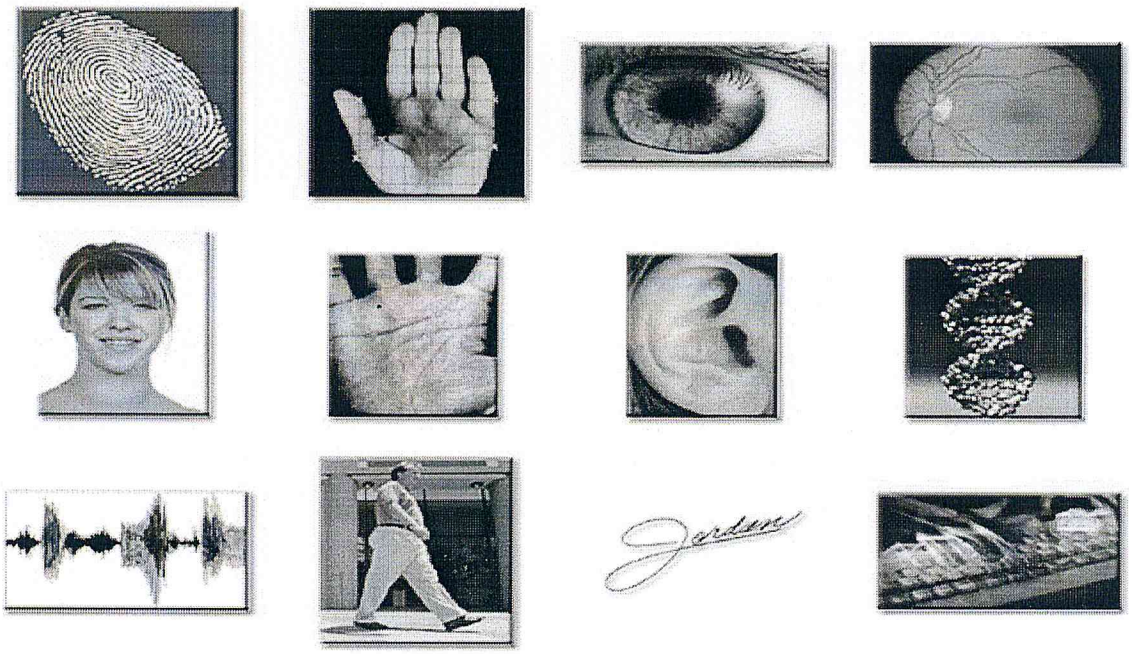


Figure I.1 : Différentes modalités biométriques

b) Technologies biométriques

Il existe trois catégories de technologies biométriques : l'analyse biologiques (odeur, sang, salive, urine, ADN…), l'analyse comportementale (dynamique de la signature, la façon d'utiliser un clavier d'ordinateur, la voix, la manière de marcher...) et l'analyse morphologique (empreintes digitales, formes de la main, traits du visage, dessins du réseau veineux de l'œil...) [GBI].

Ces éléments ont l'avantage d'être stables dans la vie d'un individu et ne subissent pas autant les effets du stress que l'on retrouve, par exemple, dans l'identification comportementale [GBI].

Odeur, sang, salive, ADN ses technologie constituent beaucoup de contraintes et demandent un certain effort. A titre d'exemple, pour avoir l'ADN d'une personne il faut avoir un cheveu, un peu de sang, mettre en œuvre un système de reconnaissance qui est utilisé fréquemment, ceci demande beaucoup de travail et comme inconvénient la perte de temps, c'est pour cela que ces caractéristiques sont utilisées dans les domaines médical et juridique dès lors qu'ils sont beaucoup plus fiables.

Les empreintes digitales, le visage, l'iris, la rétine ou la forme de la main, ses caractéristiques sont plus simples par rapport aux précédentes et demandent moins d'effort, on analyse une empreintes digitales en une seule seconde, on détecte un visage facilement

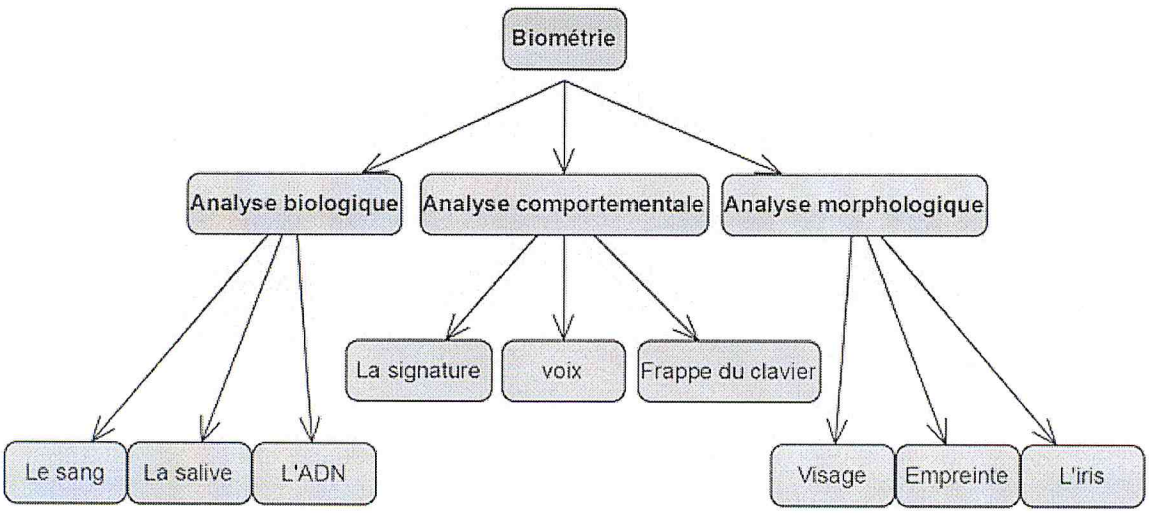


Figure I.2 : Les différents aspects de la Biométrie

c) Présentation de quelque technologie biométrique

i. 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 [DON99].

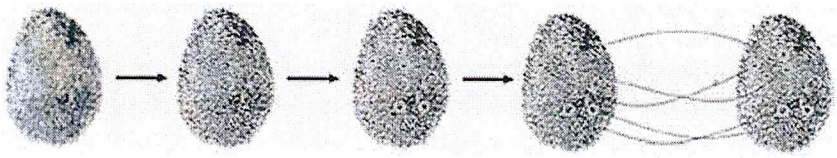


Figure I.3 : Le processus de reconnaissance par empreinte digitale.

ii. 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 [FIS36] [NIC06].

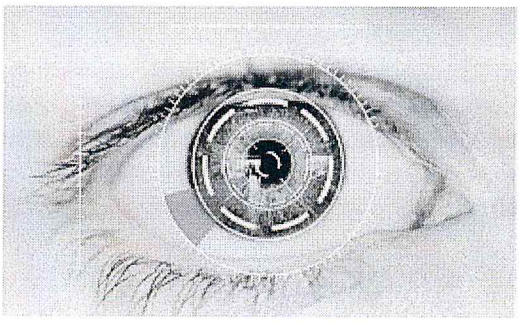


Figure I.4 : L'iris

iii. 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 doigts, 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 [HOL62].

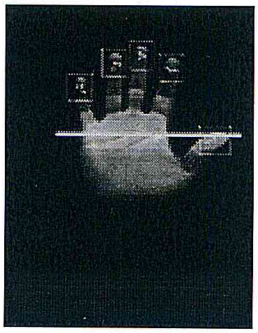


Figure I.5 : La reconnaissance pas la géométrie de la main

iv. 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 [HAR73].

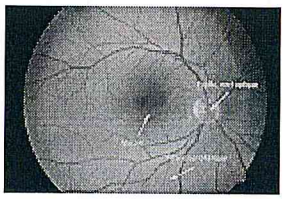


Figure I.6 : La rétine

v. 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 d'être corrompue par les bruits ambiants.

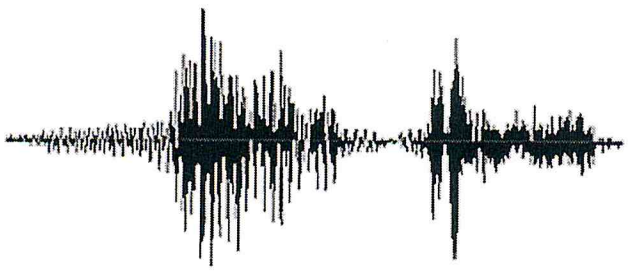


Figure I.7 : Spectre d'un signal voix.

vi. 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 varier selon le stress de l'utilisateur [CHO95].

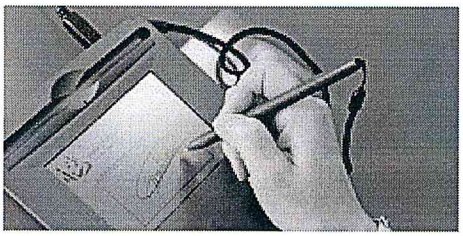


Figure I.8 : La signature numérique

vii. 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 dont à besoin le doigt de chaque personne pour effectuer une pression sur une touche et le temps où ce même 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 [DID92].

viii. 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.) [GOL89] [SIM76].

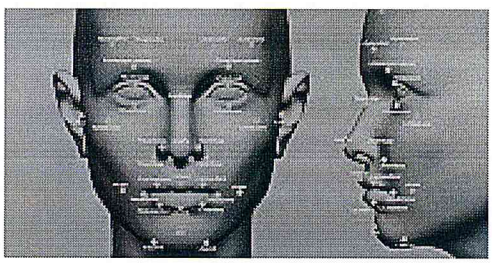


Figure I.9 : La reconnaissance du visage

d) Evaluation de différentes technologies

L'utilité de la biométrie varie d'une application à l'autre, pour déterminer son véritable avantage, il faut d'abord développer et comprendre les exigences opérationnelles de l'application. La biométrie peut fournir un moyen automatisé pour l'identification d'un individu ou de la

vérification d'une identité déclarée. Avant de prendre une décision, il faut assurer cette tâche, sa sera de répondre aux besoins opérationnels déterminés. La biométrie peut potentiellement fournir des économies de coûts grâce à la relocalisation des ressources en matière de sécurité ou de diminuer les frais liés à l'entretien de mot de passe, ou il pourrait entraîner des coûts supplémentaires en mettant en évidence les problèmes qui ont été précédemment manqués. Les avantages de coûts varient d'une application à une autre [AUT].

L'efficacité d'une technologie biométrique dépend de la façon dont elle est utilisée. Chaque modalité biométrique a ses propres forces et faiblesses qui doivent être évaluées par rapport à la demande avant la mise en œuvre. Les facteurs clés de décision pour la sélection d'une technologie biométrique comprennent l'évaluation de l'environnement, les besoins débit, taille de la population et la démographie, l'ergonomie, l'interopérabilité avec les systèmes existants, les considérations de l'utilisateur, etc. [AUT]. Par exemple, un système de contrôle d'accès dans une mine de charbon, où les individus auront des empreintes digitales usées et sales, ne sera pas un environnement approprié pour un lecteur d'empreintes digitales. L'évaluation attentive des facteurs clés de décision joue un rôle crucial dans le succès de la technologie choisie.

La « ***International Biometric Group*** », a fait une étude sur les caractéristiques des modalités les plus utilisées. Cette étude qui s'appelle « **Zephyr analysis** » a été faite selon quatre critères [TPE] :

-***Effort*** **:** L'effort fait par l'utilisateur lors de la mesure.
-***Cost*** **:** le cout nécessaire pour l'implémenter.
-***Accuracy*** **:** l'efficacité de la méthode.
-***Intrusiveness*** **:** les cas où l'utilisateur n'accepte pas la technologie.

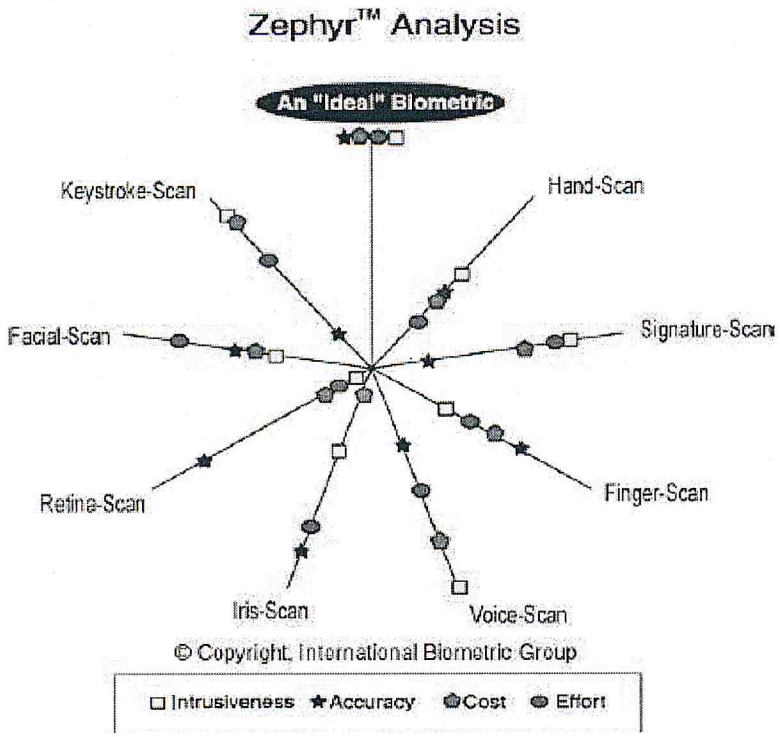


Figure I.10 : Zephyr Analysis: comaparaison entre modalités les plus utilisées selon quatre critères: l'effort, le cout, l'efficacité et l'intrusivité [TPE].

Selon le schéma ci-dessus (Figure 1.10), la meilleure technologie doit avoir des symboles à l'extrémité alors que la mauvaise a les symboles au centre du graphe. On peut constater que les technologies à base de l'iris et la rétine sont les plus efficaces, mais les plus couteuses. D'un autre côté, les modalités comportementales semblent les plus acceptées par les utilisateurs. Cependant, elles sont les moins efficaces. La forme de la main, l'empreinte digitale et la reconnaissance faciale représentent un compromis entre les quatre critères.

Le tableau ci-dessous, représente un comparatif entre les différentes technologies biométriques fait par CLUSIF (Club de la Sécurité des Systèmes d'Information Français) [TPE].

Techniques	Avantages	Inconvénients
Empreintes digitales	Coût, ergonomie moyenne, facilité de mise en place, taille du capteur	Qualité optimale des appareils de mesure (fiabilité), acceptabilité moyenne, possibilité d'attaques (rémanence de l'empreinte,...)
Forme de la main	Très ergonomique, bonne acceptabilité	Système encombrant, coût, perturbation possible par des blessures et l'authentification des membres d'une même famille

Visage	Coût, peu encombrant, bonne acceptabilité	Jumeaux, psychologie, religion, déguisement, vulnérabilité aux attaques
Rétine	Fiabilité, pérennité	Coût, acceptabilité faible, installation difficile
Iris	Fiabilité	Acceptabilité très faible, contrainte d'éclairage
Voix	Facilité	Vulnérable aux attaques
Signature	Ergonomie	Dépendant de l'état émotionnel de la personne, fiabilité
Frappe au clavier	Ergonomie	Dépendant de l'état physique de la personne

Tableau I.1 : Comparatif entre différentes modalités biométriques.

Cette différence en termes de caractéristiques fait que les entreprises et les organismes préfèrent certaines technologies plus que d'autres.

e) La place de la reconnaissance faciale parmi les autres techniques biométriques

Les empreintes digitales sont les caractéristiques biométriques les plus communément utilisées pour la reconnaissance de criminels.

Le premier système automatique d'authentification utilisant les empreintes digitales a été commercialisé au début des années soixante. D'autres parts, plusieurs études ont démontré que l'iris est la caractéristique la plus fiable car la texture de l'iris reste stable au cours de la vie. Toutefois, ces méthodes présentent l'inconvénient majeur d'être intrusives, ce qui limite énormément leurs domaines d'applications. De plus, une méthode comme l'identification de l'iris reste contraignante pour les utilisateurs qui n'apprécient pas de placer leur œil devant un appareil [SOU11].

A l'inverse, des systèmes d'identification basés sur l'analyse des images de visage ne présentent aucune contrainte pour les utilisateurs. La reconnaissance faciale est une modalité qui peut être implémentée de manière indépendante des autres modalités biométriques, elle est souvent utilisée dans des applications de surveillance. La reconnaissance faciale offre plusieurs avantages : le système de capture est facile à installer, il est accepté dans les lieux publics ce qui permet d'avoir des bases de données de plus en plus grandes et ainsi d'améliorer les performances de la reconnaissance [SOU11].

Depuis quelques années, la reconnaissance faciale suscite un intérêt croissant auprès de la communauté scientifique, qui s'est notamment manifesté à travers l'organisation de conférences internationales spécialisées telle que « *The International Conférence on Audio and Video-based Biometric Person Authentication (AVBPA)* » depuis 1997, et « *The International Conference on Automatic Face and Gesture Recognition (AFGR)* » depuis1995 [SOU11].

Par ailleurs, les États-Unis ont mené depuis 1993 une série de tests de reconnaissance faciale dont les résultats sont accessibles au public. Ces tests sont désignés sous les noms de FERET, XM2VTS, FRVT 2000 et FRVT 2002.

Une analyse statistique des publications sur les techniques biométriques a été soumise et publiée dans un numéro spécial de la revue *IEEE Transaction on PAMI* (voir tableau 1.2) [SOU11].

Nous constatons que la reconnaissance faciale arrive largement en tête avec un pourcentage de 33% du nombre total de publications. Ceci démontre bien l'intérêt scientifique pour cette technique.

Article (%)	Visage	Empreintes digitale	Multimodale	Iris	Performance Evaluation	Autres
Soumission	33%	17%	16%	9%	4%	21%
Acceptation	33%	16%	16%	11%	5%	20%

Tableau I.2 : Répartition des articles sur les techniques biométriques soumis et acceptés dans la revue IEEE PAMI

3. Systèmes biométriques

a) Authentification ou Identification

Dans un système biométrique, nous pouvons distinguer deux modes de fonctionnement :

L'Authentification : Le processus d'identification d'un individu, généralement basée sur un mot de passe ou une empreinte digitale etc. Dans les systèmes de sécurité, l'authentification est distincte de l'autorisation, qui est le processus de donner aux particuliers l'accès aux objets du système en fonction de leur identité. L'authentification garantit simplement que la personne est bien celle qu'elle prétend être, mais ne dit rien sur les droits de l'individu d'accès.

L'identification : Dans un système de sécurité biométrique, le procédé consistant à comparer un échantillon de données biométriques à l'encontre de tous les systèmes à base de données des modèles de référence afin d'établir l'identité de la personne qui tente d'accéder au système.

b) Caractérisation et architecture d'un système biométrique

Un système biométrique typique peut être représenté par **quatre modules principaux** [NIC09]

Module d'acquisition (Mesure de la caractéristique) : est responsable de l'acquisition des données biométriques d'un individu (cela peut être un appareil photo, un lecteur d'empreintes digitales, une caméra de sécurité, etc.),

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

Module d'extraction de données : compare l'ensemble des caractéristiques extraites avec le modèle enregistré dans la base de données du système et détermine le degré de similitude (ou de divergence) entre les deux,

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

Il est à mentionner que les trois premiers modules (acquisition, prétraitement et extraction de données) sont utilisés dans deux phases :

a. Durant l'apprentissage : pour stocker les informations lors de l'ajout d'un nouvel utilisateur dans le système.

b. Durant la reconnaissance : pour déterminer l'identité de l'utilisateur, soit pour une identification ou une authentification.

Cependant, le dernier module (décision) est utilisé juste pour la reconnaissance d'un individu. La figure 1.11 représente l'architecture générale d'un système biométrique :

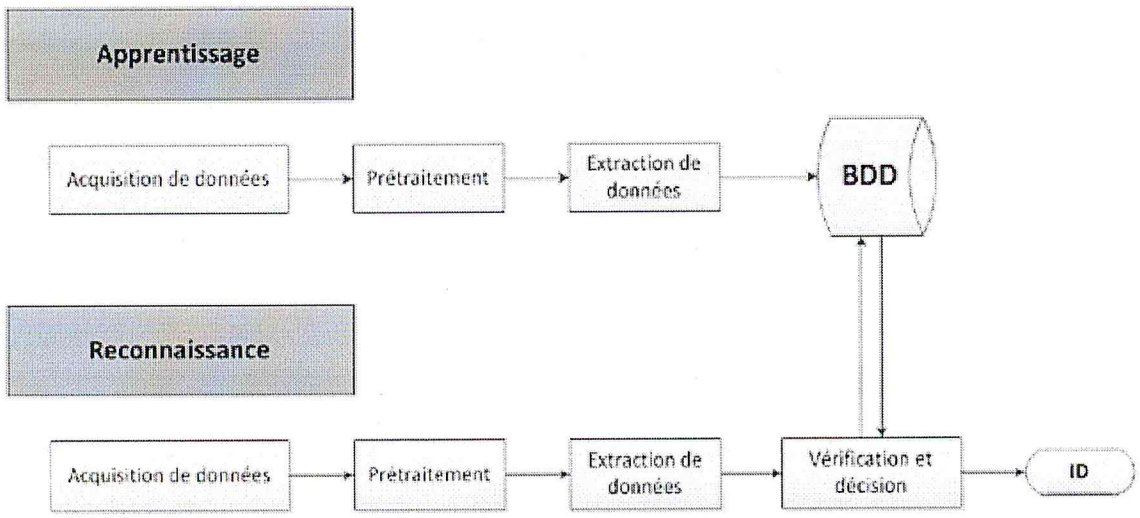


Figure I.11: Architecture générale d'un système biométrique

c) Système biométrique multimodale

Les systèmes biométriques multimodales utilisent plusieurs capteurs, algorithmes, caractéristiques biométriques… pour surmonter les limitations des systèmes biométriques uni modales. La reconnaissance par l'iris peut être compromise par le vieillissement, l'empreinte digitale peut être compromise par la brulure du doigt. On utilisant la multi modalité on réduit ses risques, les systèmes biométriques uni modales sont limités par l'intégrité de leur identifiant, il est peu probable que plusieurs systèmes uni modaux vont souffrir de limitations identiques [WIK3].

Selon la manière de combinaison des modalités, on peut distinguer cinq types de systèmes multimodaux [LOR09]:

- Multi-capteurs : lorsque plusieurs types de capteurs sont mis en place pour capturer la même modalité.
- Multi-instances : lorsque plusieurs instances de la même modalité sont prises.
- Multi-algorithmes : lorsque plusieurs algorithmes traitent les même informations acquises.
- Multi-échantillons : lorsqu'ils utilisent des échantillons différents de la même modalité, par exemple l'iris droite et gauche.
- Multi-biométries : lorsqu'ils se basent sur plusieurs modalités.

La figure 1.12 illustre les différents types de systèmes multimodaux qui existent

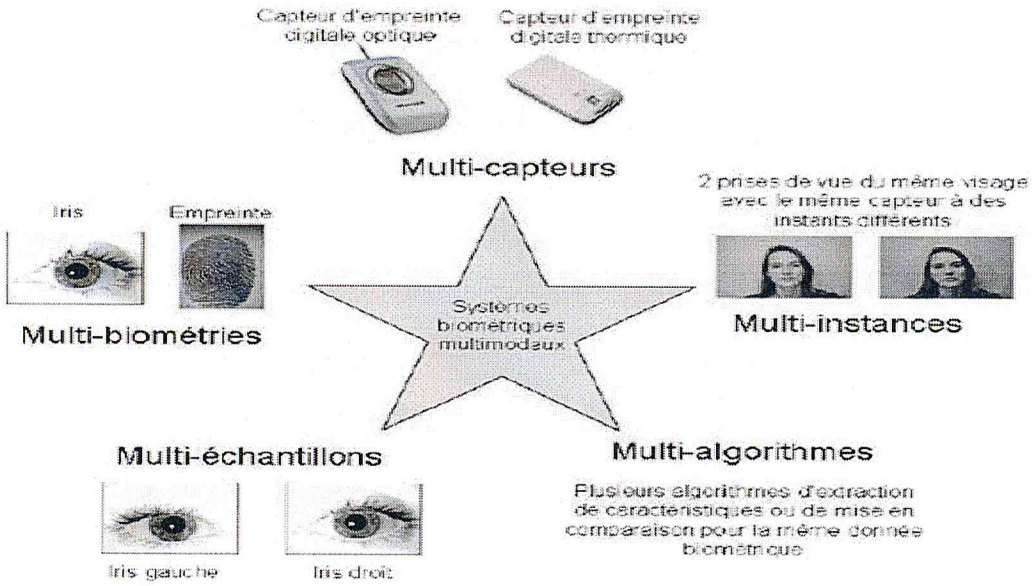


Figure I.12: Différents types de systèmes multimodaux.

Les systèmes multimodaux peuvent combiner plusieurs types. Le dernier type est très intéressant parce qu'il offre une solution aux problèmes des systèmes monomodaux comme la non-universalité. Cependant, les quatre premiers traitent des informations issues de la même modalité ce qui réduit seulement les problèmes liés à l'acquisition.

d) Mesure de la performance d'un système biométrique

Contrairement aux méthodes classiques (qui se basent sur l'utilisation d'un mot de passe ou d'une carte à puce) où une équivalence parfaite est obligatoire pour valider l'identité d'une personne, un système biométrique est exposé à plusieurs facteurs. En effet, des problèmes d'acquisition peuvent influencer les données, ce qui ne donnera certainement pas une ressemblance parfaite entre les données enregistrées durant l'apprentissage et celle collectées lors de la reconnaissance. En réalité, une ressemblance totale dans un système biométrique peut indiquer qu'une attaque est lancée sur le système. C'est pour cela que, pour mesurer les performances d'un système biométrique, il faut vérifier un certain nombre de conditions qui peuvent être plus au moins importantes à tester selon le domaine d'application. On peut citer : les capteurs utilisés, la facilité d'utilisation, le niveau de sécurité, le cout, le protocole d'acquisition, les taux d'erreur de reconnaissance, etc.

Pour faire l'évaluation, trois approches sont citées dans « La Biométrie multimodale » de Lorene Allano [LOR09] l'évaluation technologique, l'évaluation de scénario et l'évaluation opérationnelle.

L'évaluation technologique : elle ne s'intéresse qu'aux algorithmes utilisés pour extraire les données, faire la comparaison et donner la décision finale, par l'utilisation d'une base de données pré-acquise. Afin de faciliter l'étape de test, plusieurs bases de données sont disponibles, gratuites ou payantes, monomodales ou multimodales. Il existe en général trois types de bases de données qu'on utilise pour faire l'évaluation :

- Bases de données d'apprentissage des paramètres de fusion pour régler les paramètres de fusion et déterminer le seuil de décision.

- Bases de données de développement pour régler les paramètres des systèmes monomodaux.

- Bases de données de test pour évaluer les performances du système.

L'évaluation de scénario : outre que les algorithmes appliquées, ce type teste aussi les capteurs, l'environnement de l'application et l'ensemble des utilisateurs.

L'évaluation opérationnelle : elle teste le système complet en temps réel.
Dans un système biométriques, on trouve deux types de population : les utilisateurs qui sont autorisés à accéder au système, et les utilisateurs qui n'ont aucune autorisation mais qui vont essayer de rentrer, on parle d'imposteurs.
La différence entre les données préalablement enregistrées dans la base de données et les données de la personne voulant s'authentifier, nous mène à faire une étude de corrélation plutôt qu'une vérification, cela revient à calculer le degré de ressemblance [MAT05]. Ensuite, l'acceptation ou le refus est lié au domaine d'application. Cependant, en pratique, l'évaluation ne peut se faire qu'en se basant seulement sur cette étude car toutes les erreurs n'ont pas le même impact sur la fiabilité du système. En effet, deux types d'erreurs peuvent être commises par les systèmes de vérification :

- Accepter une personne qui doit être refusée, on parle de « Fausse Acceptation » ou « FA ».

- Rejeter une personne qui est authentifiée, on parle de « Faux rejet » ou « FR ».

Selon ces deux types d'erreurs, on peut distinguer trois critères d'évaluation : [NIC09]

1. Le premier critère s'appelle le taux de faux rejet ("*False Reject Rate*" ou FRR). Ce taux représente le pourcentage de personnes censées être reconnues mais qui sont rejetées par le système,

2. Le deuxième critère est le taux de fausse acceptation ("*False Accept Rate*" ou FAR).
Ce taux représente le pourcentage de personnes censées ne pas être reconnues mais qui sont tout de même acceptées par le système,

3. Le troisième critère est connu sous le nom de taux d'égale erreur ("*Equal Error Rate*" 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.

La figure 1.13 illustre le FRR et le FAR à partir de distributions des scores authentiques et imposteurs.

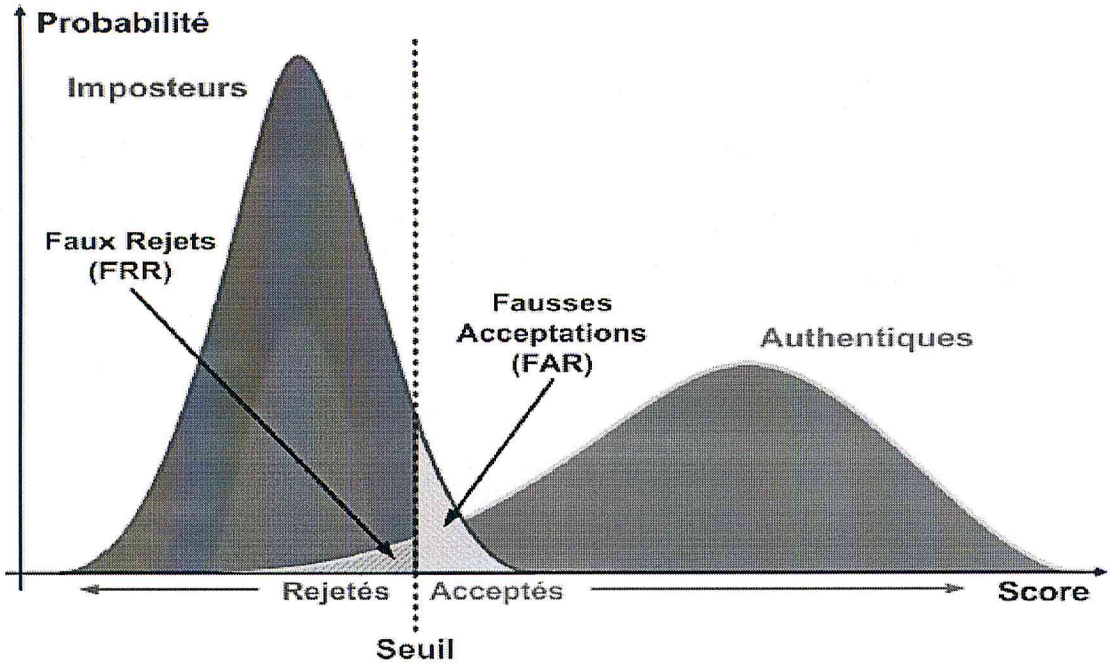


Figure I.13 : Illustration du FFR et FAR

Selon ces critères, on fixe le seuil de décision qui est lié au domaine d'application. En effet, les systèmes où le niveau de sécurité est un facteur très important demandent un FAR plus bas, alors que si le confort et la commodité sont prioritaires, un FRR bas est nécessaire. Le EER est utilisé pour faire une comparaison entre plusieurs systèmes biométriques, et plus il est bas, plus le système est fiable [BIO].

La liaison entre le FRR et le FAR pour différentes valeurs de seuil peut être représentée par deux courbes : la courbe ROC (*Receiver Operating Characteristics*) (figure 1.14) et la courbe DET (*Detection Error Trade-off*) (figure 1.14)[ACC12].

Les courbes ROC et DET représentent la variation du FRR en fonction du FAR lorsque le seuil varie. La différence entre ces deux courbes c'est que la courbe DET utilise une échelle logarithmique [ACC12].

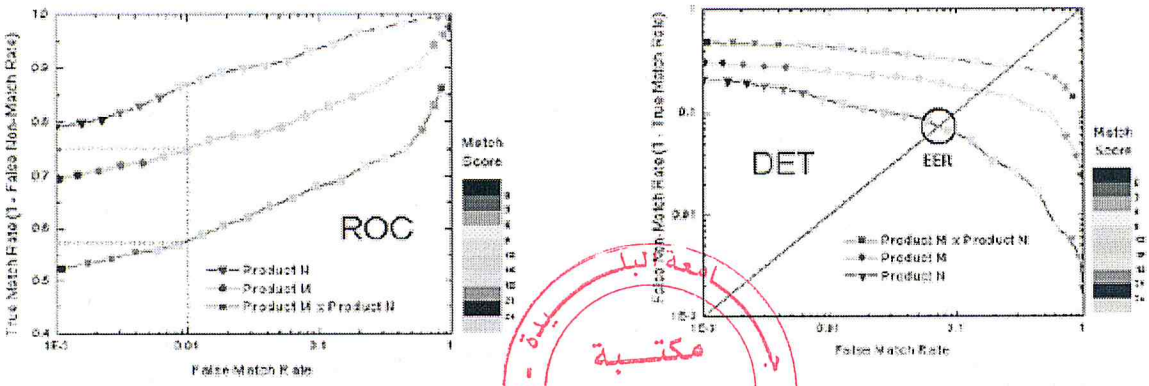


Figure I.14 : A gauche : Exemple de courbe ROC, à droite : Exemple de courbe DET.

4. Conclusion

Tout au long de ce chapitre, nous avons vu que la biométrie aide à surmonter plusieurs faiblesses des méthodes classiques et que les systèmes biométriques sont de plus en plus utilisés dans diverses applications. Cependant, il ne suffit pas de changer un login et un mot de passe par une mesure biométrique, il faut revoir l'architecture globale du système et la sécuriser. Le choix d'une modalité biométrique n'est pas arbitraire et dépend de plusieurs critères, surtout le domaine d'application.

Chaque modalité présente des avantages et des inconvénients, il n'existe pas une modalité parfaite. Ce dernier point a conduit à l'émergence de systèmes multimodaux qui sont plus fiables. La mesure des performances d'un système biométrique est une étape très importante, elle permet d'estimer la fiabilité du système en utilisant des indicateurs comme le taux de faux rejet et le taux de fausse acceptation.

Le marché de la biométrie est en pleine expansion et plusieurs entreprises sont en train d'investir dans ce domaine. Cela permet de prédire que la biométrie aura un avenir prometteur. Cependant, il faut admettre que son utilisation reste toujours limitée et un grand effort doit être fourni et des études doivent être faites afin de créer des systèmes biométriques plus performants qui dépassent les limites rencontrées.

Chapitre II
Reconnaissance faciale

II. Reconnaissance faciale

1. Introduction

La reconnaissance faciale fait partie des techniques biométriques qui permettent l'identification d'une personne à partir des caractéristiques de son visage. On remarque que dans la vie quotidienne chacun de nous identifie tout au long des journées différents visages. Ainsi lorsque nous rencontrons une personne, notre cerveau va chercher dans notre mémoire et vérifier si cette personne est répertoriée ou non. La difficulté de la reconnaissance de visage par ordinateur varie énormément suivant que les conditions d'acquisition, comme le vieillissement, l'éclairage, le changement d'expression du visage ou d'apparence et les problèmes génétiques tels que la similarité entre jumeaux, l'angle de la prise de vue et la détection de la présence ou l'absence de visage dans l'image

Plusieurs méthodes ont été développées pour la reconnaissance de visage. Cependant, elles présentent un certain nombre de limitations liées à l'orientation du visage ou à la pose, à l'éclairage, à l'expression faciale, aux occultations, etc.

Dans ce chapitre on va faire une étude des systèmes de reconnaissance de visage ainsi que l'état de l'art des principales méthodes de reconnaissance faciale.

2. La reconnaissance faciale

a) Psychologie de la reconnaissance faciale

La capacité des humains à reconnaître les visages tend vers deux extrêmes, d'une part, nous sommes extrêmement bon à la reconnaissance des visages qui nous sont familiers et nous pouvons le faire malgré les changements naturels des expressions, point de vue et coiffure ainsi que des manipulations d'images telles que l'inversion, cependant, quand il s'agit de visages que nous avons brièvement vus, là c'est totalement différent. Des témoins oculaires d'un crime trouvent très difficile à décrire et en particulier identifier l'auteur du crime et sont très sensibles à l'exposition des visages semblables et les instructions qui leur sont données. L'utilisation de témoignages oculaires peut également se révéler problématique dès lors que le témoin peut ainsi exprimer un niveau inapproprié de confiance dans sa décision. Bien sûr, un témoin oculaire se sert de sa mémoire pour reconnaitre un visage à qui il a été brièvement exposé, mais les choses ne semblent pas s'améliorer lorsque la tâche devient «purement perceptive » n'impliquant aucune charge mémorial. La recherche a constaté que les opérateurs donnent de mauvais résultats quand ils sont tenus de faire correspondre deux images faciales, comme cela est souvent le cas dans l'identification à partir d'images de surveillance ou de l'utilisation des cartes d'identité avec photo [IET20].

Une synthèse des principaux résultats de recherche sur le système de reconnaissance faciale humain est faite par [PAW06], elle se résume dans les points suivants :

- Les êtres humains peuvent reconnaitre des visages familiers dans des images de faible résolution.
- La capacité de tolérer les dégradations s'améliore avec la familiarité.
- Les informations de hautes fréquences seules sont insuffisantes pour une bonne reconnaissance faciale.
- Les caractéristiques du visage sont traitées holistiquement.
- Les sourcils sont les caractéristiques faciales les plus importantes pour la reconnaissance.
- La forme du visage est codée de manière caricaturale.
- La pigmentation du visage est aussi importante que sa forme.
- La couleur joue un rôle important spécialement pour les formes dégradées.
- Il vaut mieux traiter l'identité faciale et les expressions séparément.

Ces résultats ont contribué à mieux comprendre le système de reconnaissances du visage humains et localiser les caractéristiques importantes du visage qui permettent sa reconnaissance, d'où la naissance des algorithmes de reconnaissance du visage que nous connaissons aujourd'hui.

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

b) Repère d'un visage

Des études en anthropométrie ont caractérisé la dimension du visage par des points spécifiques, on parle de « *landmarks* ». La figure 2.1 montre les différents *Landmarks* utilisés. Ces points servent à étudier et comprendre les caractéristiques du visage. Cependant, ils ne sont pas trop utilisés dans les systèmes de reconnaissance automatique car il est difficile de les détecter et différencier dans les images de mauvaise qualité.

Les caractéristiques du visage sont répertoriées dans trois catégories [ANI11]:

- **Catégorie 1** : les caractéristiques d'apparence permettant de connaitre le sexe, la race et la forme générale du visage.
- **Catégorie 2**: les caractéristiques essentielles pour établir l'identité de la personne, elles permettent d'avoir des informations sur les différentes zones du visage.

- **Catégorie3** : les caractéristiques nécessaires pour résoudre les ambiguïtés comme la distinction entre jumeaux. Elles permettent d'identifier les petites marques et cicatrices du visage.

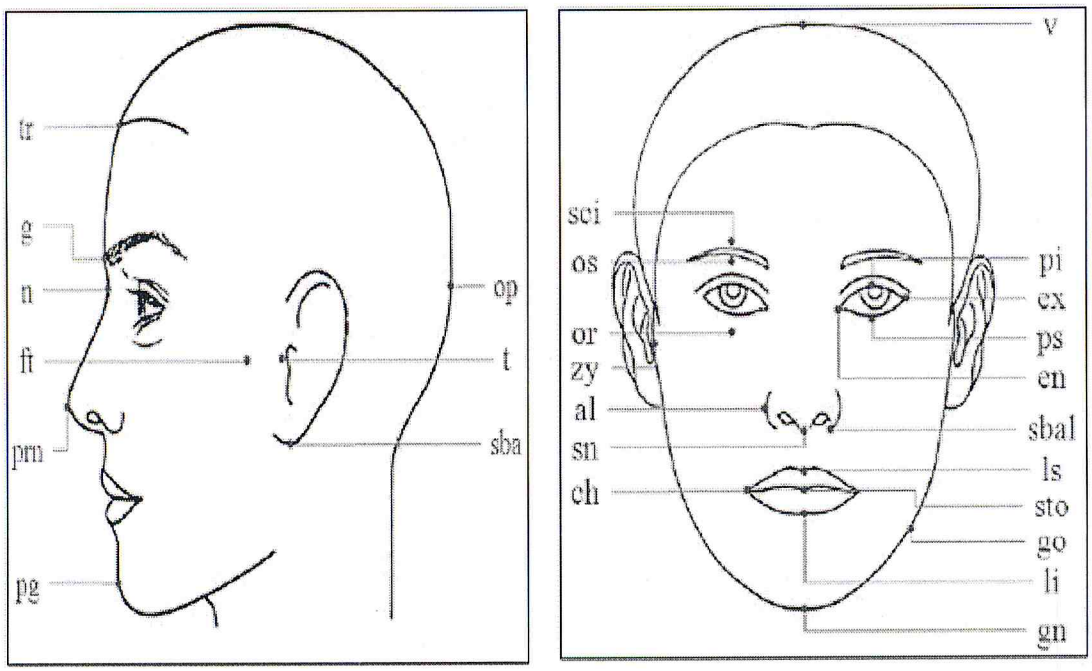


Figure II.1: Vue de profil et vue frontale du visage montrant les landmarks

c) Applications

La reconnaissance faciale connait aujourd'hui une large utilisation dans les affaires judiciaires, le contrôle d'accès et la vidéo surveillance. Tous les aéroports disposent aujourd'hui de caméras de surveillance pour identifier les criminels voulant s'enfuir, nous lisons plusieurs fois dans les journaux que des suspects ont été arrêtés après avoir été capturés par les caméras de surveillance. Aux Etats Unis et en France, la reconnaissance faciale est utilisée dans les casinos pour détecter les joueurs interdits. Elle est utilisée dans les stades pour refouler les supporteurs connus et dangereux, dans les magasins et grandes boutiques pour identifier les voleurs et dans les rues pour contrôler le respect de l'ordre public. La reconnaissance faciale est utilisée aussi pour gérer l'accès aux centres de recherches et laboratoires, mais souvent combinée à d'autres technologies biométriques comme la forme de la main, l'empreinte digitale ou l'iris.

3. Les systèmes de reconnaissance faciale

Un système de reconnaissance de visage passe par plusieurs étapes qui sont :

- Acquisition des images
- Prétraitement du visage
- L'extraction des informations relatives au visage
- La vérification et la décision de l'identité.

Dans l'acquisition, les images capturées peuvent être classées selon la technologie utilisée : visible, infrarouge ou thermique, ou selon la nature du flux de données : image 2D, image 3D ou vidéo. Dans le prétraitement, le système localise le visage dans l'image acquise et prépare les données afin de rendre l'extraction des informations plus efficace. Cependant, cette tâche devient délicate lorsque le fond d'image est encombré ou plusieurs visages existent dans la même image. La plupart des algorithmes existants traitent des images 2D vu la grande disponibilité des capteurs 2D. L'utilisation des images 3D vient pour résoudre les problèmes de luminosité, le changement de la pose et facilite la reconnaissance grâce au nombre important d'informations fournies dans le flux 3D. La troisième étape consiste à extraire des informations du visage détecté et les stocker dans une base de données dans le cas d'un nouvel utilisateur du système. La vérification est la comparaison entre les informations extraites et les données stockées dans la base de données afin de décider de l'identité de la personne. La figure 2.2 montre l'architecture globale d'un système de reconnaissance faciale.

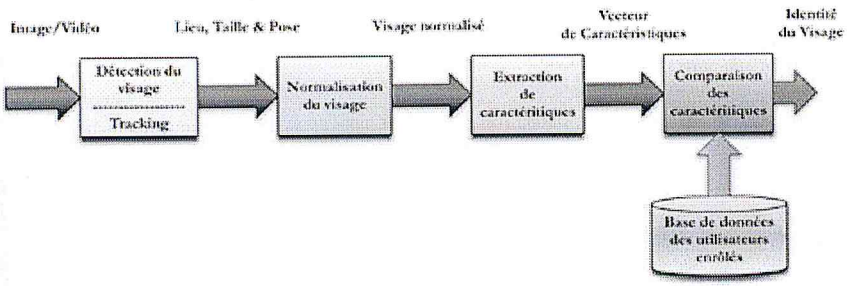


Figure II.2 : Principe de fonctionnement de base d'un système de reconnaissance faciale

a) Acquisition des images

L'acquisition est la première partie d'un système de reconnaissance du visage, la qualité des données capturées influence directement sur les performances du système, c'est pour cela qu'il est important de bien choisir le capteur approprié à l'environnement du travail, selon les moyens et le budget qui sont disponibles, mais aussi, connaitre les problèmes liés à chaque capteur et les capteurs en général.

Afin de les utiliser, les images doivent être sous format lisible par un ordinateur. Les formats les plus répandus sont : les images 2D, les images 3D et la vidéo. Il existe plusieurs capteurs et cameras pour acquérir les images. On distingue principalement deux types de capteurs :

Capteurs 2D

En général, la vue frontale du visage contient plus d'informations que la vue de profile. C'est pour cela qu'il est plus facile d'utiliser la vue frontale pour détecter un visage. Les Capteurs 2D permettent d'avoir une seule vue à la fois, ce qui entraine des problèmes de changement de la position. Pour remédier à ce problème, certains systèmes qui utilisent des capteurs 2D prennent plusieurs captures de visage de différentes poses. Ces systèmes sont aussi affectés par la variation de la luminosité et de la qualité d'image. Un autre problème est la portée des capteurs qui est, en général, entre un et deux mètres. Lorsqu'on dépasse la portée, on diminue la résolution de l'image. Pour améliorer les résultats, les entreprises ont créé des capteurs plus performants comme la camera PTZ (*pan-tilt-zoom*). La figure 2.3 montre quelques systèmes de capteurs 2D récents. [ANI11]

Figure II.3 : Quelques systèmes de capture 2D

b) Prétraitement des images

Le prétraitement ou préparation de données, est la deuxième étape dans le processus de reconnaissance faciale. Il consiste à éliminer les parties non utilisées des données initiales et ne garder que les parties utiles pour les prochaines étapes. C'est une étape très importante qui améliore les performances du système. Le prétraitement comporte la détection du visage, l'amélioration et la correction des données acquises, la segmentation et la normalisation du visage.

c) Extraction des données

Le module d'extraction exploite les visages prétraités pour en extraire des données utiles pour la reconnaissance. Ensuite, à partir de ces données, il crée une signature numérique qu'il stocke dans une base de données. Ainsi, à chaque personne inscrite dans le système, on associe une signature numérique qui lui est propre. Le stockage de la signature numérique dans la base de données est lié au mode de fonctionnement du système : apprentissage ou reconnaissance.

Les méthodes d'extraction de données se distinguent les unes des autres selon le type de données : 2D ou 3D. Ainsi, à chaque type de données, il existe plusieurs méthodes.

d) Vérification et décision

Ce module va comparer entre deux modèles de visage et décider si ce sont des modèles d'une même personne. Cela revient à calculer la similarité ou la di similarité entre les deux visages en utilisant une méthode de calcul comme la distance euclidienne, la distance khi deux ou la méthode probabiliste.

4. Les performances d'un système de reconnaissance du visage

Les systèmes biométriques doivent être évalués pour pouvoir envisager leur déploiement. Les performances d'un système de reconnaissance du visage sont liées à plusieurs facteurs qui agissent sur plusieurs niveaux. Parmi ces facteurs nous trouvons :

- L'environnement de l'acquisition.
- La qualité des capteurs utilisés.
- La position des capteurs.

- La mauvaise utilisation des capteurs.
- Les algorithmes utilisés.

L'évaluation du système comprend plusieurs aspects qui ont une importance différente selon l'application. On cite :

- La facilité d'utilisation pour les utilisateurs.
- La sécurité d'utilisation et de données.
- Le cout de réalisation.
- La fiabilité du système.
- Les pannes et la nécessité de maintenance.
- Et surtout les taux d'erreurs de reconnaissance (TFR, TFA, EER).

5. Les méthodes de reconnaissance du visage

La majorité des méthodes de reconnaissance faciale traitent des données 2D, vue la grande disponibilité des capteurs dédiés. Les méthodes de reconnaissance faciale peuvent être classées en deux grandes approches : les approches globales et les approches locales.

a) Méthodes Globales

Les approches globales basées sur l'apparence globale considèrent le visage dans son ensemble. En général, lorsqu'on prend tout le visage, on aura une grande quantité de données. Les méthodes **ACP**, **LDA** et **ICA** sont les plus utilisées pour réduire la dimension des descripteurs (données originales) en gardant uniquement les éléments pertinents sous une nouvelle représentation (un nouvel espace).

1 - Analyse Composante Principales ACP (*Eigenface*)

C'est l'une des premières méthodes proposées pour la reconnaissance faciale et les plus connues. Son principe est le suivant : étant donné un ensemble d'images de visages, 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 [SOU11]. 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 [ANI11]. L'ACP est une technique rapide, simple et populaire dans l'identification de modèle, c'est l'une

des meilleures techniques. Les projections de l'ACP sont optimales pour la reconstruction d'une base de dimension réduite. Cependant, l'ACP n'est pas optimisé pour la séparabilité (discrimination) de classe. Une alternative qui est l'analyse discriminante linéaire LDA tient compte de ceci.

2 - Analyse Discriminante Linéaire ADL (*Fisherface*)

C'est une extension de la méthode *eigenfaces* qui se base sur l'analyse discriminante linéaire. L'objectif de la plupart des algorithmes basés sur l'ADL, est de trouver les directions de projection les plus discriminantes dans l'espace propre, en maximisant le ratio entre les variations interpersonnelles et les variations intra-personnelles. Comme les variations intra-personnelles peuvent être petites (notablement quand il n'y a pas beaucoup d'images par individu), ce ratio est difficile à maximiser puisque il est déjà grand [ANI11] [AND10]. Ce problème est encore appelé *Small Sample Size*. Pour l'éviter, on peut utiliser tout d'abord l'ACP et ensuite l'ADL, et cette méthode est appelée *Fisherfaces*. Voilà pourquoi les méthodes basées sur l'ADL ne fonctionnent bien que lorsque beaucoup d'images par personne sont disponibles dans la base d'apprentissage. En revanche, quand il n'y a pas beaucoup d'images par personne, les méthodes basées sur l'ADL marchent moins bien que celles basées sur l'ACP [SOU11].

3 - Analyse en composantes indépendantes (ACI)

Contrairement à l'ACP, au lieu de trouver un sous-espace où l'erreur de reconstruction est minimale, les méthodes basées sur l'ACI cherchent une meilleure représentation des données en gardant les sources indépendantes entre eux.

L'ACI essaye de générer des composantes statistiquement indépendantes entre eux, ce qui donne les coefficients les plus indépendants possible. De plus, les images de base développées par l'ACP dépendent que des statistiques du second ordre. Par contre, l'ACI généralise ce concept aux modèles statistiques d'ordre supérieur. Une comparaison plus complète entre l'ACI et l'ACP est faite dans [DRA03].

b) Méthodes locales

Les approches locales sont basées sur la détection des zones spécifiques du visage telles que les yeux, le nez, les sourcils et la bouche, ainsi que les propriétés et relations géométriques entre les différentes caractéristiques du visage comme les coins des yeux et les coins de la bouche. Les méthodes locales se divisent en deux catégories : les approches basées sur les caractéristiques locales du visage et les approches basées sur les apparences locales du visage.

1 - Les méthodes basées sur les caractéristiques locales

Les approches basées sur les caractéristiques locales subdivisent en deux catégories : les approches géométriques et les approches basées sur des graphes [SOU11].

- **Les approches géométriques :**

Les approches géométriques sont basées sur la localisation des éléments caractérisant le visage (le nez, les yeux, la bouche). Ces éléments sont représentés par leurs positions géométriques relatives. Ces méthodes se différencient par le nombre d'éléments à extraire et la méthode de similitude. Ces approches ont l'avantage d'utiliser un faible espace de stockage de données. Cependant, elles présentent quelques inconvénients comme la non-exploitation de plusieurs caractéristiques du visage comme le niveau de gris des images. De plus, en général, ces caractéristiques sont difficiles à détecter surtout dans un environnement non contrôlé.

- **Les approches basées sur des graphes :**

Dans cette approche, les caractéristiques détectées sont représentées sous forme d'un graphe basé sur les ondelettes de Gabor 2, d'où, la comparaison entre les visages est devenue un problème de similitude entre graphes. La méthode basique qui utilise un graphe topologique fixe présente plusieurs inconvénients. En effet, le graphe topologique fixe ne peut pas être modifié, contrairement aux visages qui changent en raison de la variation de pose et d'expression. Cela a mené à la naissance de nouvelles variantes dont la plus connue est ***Elastic Buch Graph Matching*** **(EBGM)**. Cette dernière consiste à construire un graphe topologique élastique qui peut s'adapter aux changements d'expression et d'orientation. Le graphe élastique donne des informations sur la structure des variations attendues. Les arrêtes du graphe représente la forme géométrique des objets, tandis que chaque nœud du graphe contient plusieurs coefficients de Gabor nommés « jets » qui représentent les différentes variations possibles (œil ouvert, œil fermé, etc.). Bien que l'EBGM soit robuste, elle demande un temps de calcul important par rapport aux autres méthodes.

Les méthodes basées sur les caractéristiques locales sont très efficaces mais leur grand inconvénient est la difficulté de détecter les caractéristiques du visage dans les environnements non contrôlés.

2 - Les méthodes basées sur les apparences locales

La plupart de ces méthodes sont des versions modulaires de méthodes globales comme l'ACP et ADL modulaires, l'approche probabiliste locale ou les modèles de Markov cachés modulaires. Une fois qu'on applique la méthode sur chaque région du visage, un modèle global peut être construit en combinant tous les modèles locaux. Les régions sont définies selon la forme ou la taille. La division en régions a l'avantage de séparer les problèmes (variations) de chaque région du visage. Par exemple, la bouche est la plus affectée par la variation du sourire. Cela permet de traiter les problèmes de façon modulaire. Parmi les techniques les plus utilisée dans cette approche, on cite ***Local Binary Pattern*** **(LBP).**
Le LBP a été utilisée pour la reconnaissance des formes en général y inclut le visage.

- ***Local Binary Pattern*** **(LBP)**

Il existe plusieurs méthodes pour extraire le plus de fonctionnalités utiles du visage pour effectuer une reconnaissance de visage. L'une des méthodes d'extraction est le *Local Binary Pattern*, cette nouvelle approche a été introduite en1996 par Ojala et al. Avec LBP il est possible

de décrire la texture et la forme d'une image numérique, c'est fait en divisant une image en plusieurs petites régions dont les caractéristiques sont extraites (Figure 2.5)

Figure II.4 : une photo devisée en 64 régions

Ces caractéristiques consistent en des configurations binaires qui décrivent les environs des pixels dans chaque région, les caractéristiques obtenues à partir des régions sont enchaînés en un seul histogramme de caractéristique, qui forme une représentation de l'image. Les images peuvent être comparées en mesurant la similitude (distance) entre les histogrammes. Selon plusieurs études la reconnaissance de visage en utilisant la méthode LBP offre de très bons résultats, tant en termes de vitesse et performances de discrimination. En raison de la façon dont la texture et la forme d'images est décrite, la méthode semble être assez robuste contre les images de visage avec différentes expressions faciales, allégement différente conditions, rotation d'image et le vieillissement des personnes [ANT13].

- **Principe de *Local Binary Pattern***

  L'opérateur de LBP originale a été introduit par Ojala et al. Cet opérateur fonctionne avec les huit voisins d'un pixel, en utilisant la valeur de ce pixel central en tant que seuil. Si un pixel voisin a un gris plus élevé que la valeur du pixel central (ou la même valeur de gris) alors 1 est affectée à ce pixel, sinon il obtient un zéro. Le code LBP pour le pixel central est alors produit par la concaténation des huit un ou des huit zéros à un code binaire (Figure 2.6)

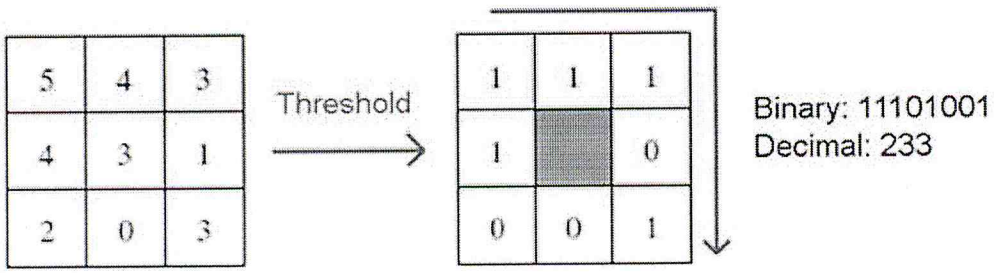


Figure II.5 : L'opération LBP originale

Ensuite, l'opérateur LBP a été étendu à utiliser des voisins de différentes tailles. Dans ce cas, un cercle est fait avec le rayon R du pixel central, échantillonnage de points P sur le bord de ce cercle sont prises et comparée à la valeur du pixel central. Pour obtenir les valeurs de tous les points d'échantillonnage dans le voisinage pour n'importe quel rayon et n'importe quel nombre de pixels, l'interpolation est nécessaire. On a l'annotation (P, R) qui est utilisé pour le voisinage. La Figure 2.7 illustre trois-ensembles voisins pour différentes valeurs de P et R [ANT13].

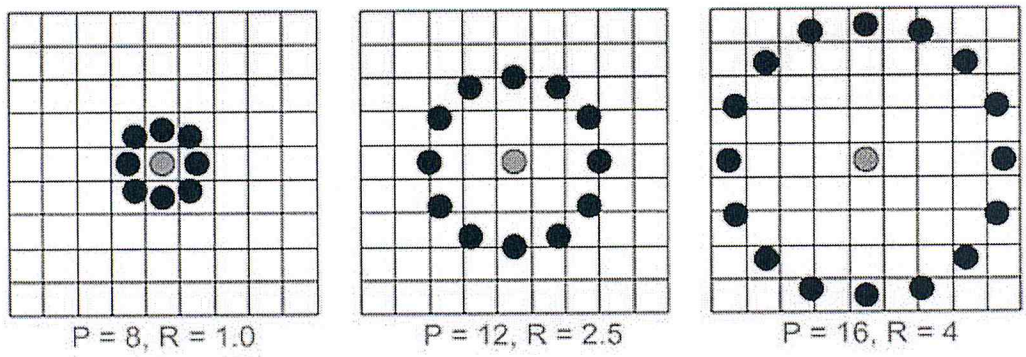


Figure II.6 : Trois ensembles voisins avec différentes valeurs de P et R

Si les coordonnées du pixel central sont (x_c, y_c) et les coordonnées de ses voisins de P(x_p, y_p) sur le bord du cercle de rayon R peut être calculée avec sinus et cosinus:

$$x_p = x_c + R\cos(2\pi p / P)$$

$$y_p = y_c + R\text{SIN}(2\pi p / P)$$

Si la valeur de gris du pixel central est g_c et la valeurs de gris de ses voisins sont g_p, avec p =0, ...,p-1 alors la texture T dans le voisinage local de pixels (x_c, y_c) peut être définie comme:

$$T = t(g_c, g_0, \ldots, g_{p-1})$$

Une fois que ces valeurs sont obtenues des points il est également possible de décrire la texture d'une autre manière, cela se fait en soustrayant la valeur du pixel central à partir des valeurs des points sur le cercle. Dans cette direction la texture locale est représentée par une distribution conjointe de la valeur du pixel central et les différences : $T = t(g_c, g_0 - g_c, \ldots, g_{P-1} - g_c)$

Depuis t (g_c) décrit la luminance globale d'une image qui n'est pas liée à la texture de l'image locale, il ne fournit pas d'informations utiles pour la texture analytique. Par conséquent, la plupart des informations à propos de la caractéristique de texture dans la distribution conjointe d'origine sont conservées dans la distribution de la différence commune :

$$T \approx (g_0 - g_c, \ldots, g_{P-1} - g_c)$$

Bien que l'invariant par rapport aux changements d'échelle de gris, les différences sont affectés par l'extension. Atteindre l'invariant par rapport à toute transformation monotone de l'échelle

de gris, seuls les signes des différences sont considérés. Cela signifie que dans le cas d'un point sur le cercle a une valeur de gris plus élevé que le pixel central (ou la même valeur), un 1est affecté à ce moment-là, sinon il prend un zéro : T ≈ (s(g0 –gc), . . . , s(gP-1–gc)) avec :

$$s(x) = \begin{cases} 1, & x \geq 0 \\ 0, & x < 0 \end{cases}$$

Dans la dernière étape pour produire le LBP pour le pixel (xc, yc) un poids binomiale 2^p est affecté à chaque signes (gp -gc). Ces poids binomiales sont additionnés :

$$\text{LBP P,R (xc,yc)} = \sum \text{« p=0, p-1 »} (s(gP - gc)2^p)$$

Le *Local Binary Pattern* caractérise la texture de l'image autour (xc, yc). L'opérateur d'origine LBP la figure 2.6 est très similaire à cet opérateur avec P=8etR = 1,ainsi$LBP_{8,1}$. La principale différence entre ces opérateurs est que dans $LBP_{8,1}$les pixels doivent d'abord être interpolées pour obtenir les valeurs des points du cercle [ANT13].

- ***Local Binary Pattern* uniforme**

Local Binary Pattern est appelé uniforme s'il contient au plus deux transitions de bits0-1ou vice versa. En fait, cela signifie qu'un motif uniforme n'a pas de transitions ou deux transitions. Une Seule transition n'est pas possible, puis que la chaîne binaire doit être considérée circulaire. Les deux modèles avec des passages par zéro, par exemple huit bits, 00000000et11111111, Autre exemple de modèles uniformes avec huit bits et deux transitions sont 00011100et11100001.Pour les modèles avec deux transitions ils ont P(P-1) Combinaison possible. Pour les modèles uniformes avec P points d'échantillonnage et de rayon r la notion la notion LBPu2-p,r est utilisée [ANT13].

En utilisant seulement *Local Binary Pattern* uniforme à deux avantages importants. Le premièr est qu'il permet d'économiser de la mémoire. Avec des motifs non uniformes, et il y'a 2^P combinaisons possibles [ANT13].

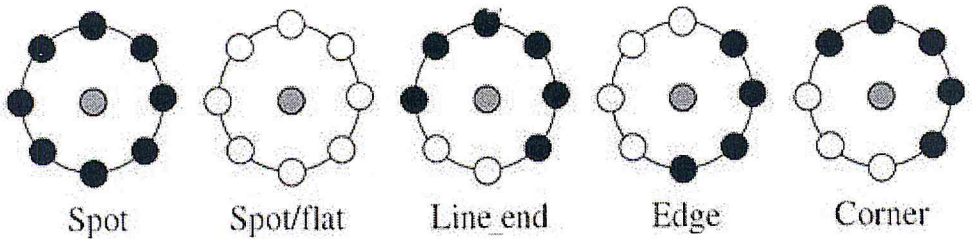


Figure II.7 : Différentes primitives de texture détectés par le LBPu2 p,r

- **Reconnaissance faciale avec *Local Binary Pattern***

Nous avons expliqué comment la méthode LBP peut être appliquée sur des images pour extraire des caractéristiques qui peuvent être utilisées pour obtenir une mesure de la similitude entre ces images. L'idée principale est que pour chaque pixel d'une l'image le code LBP est calculé. L'apparition de chaque motif possible de l'image est maintenue. L'histogramme de ces modèles, aussi appelés étiquettes, forme un vecteur de caractéristique, et est donc une représentation pour la texture de l'image. Ces histogrammes peuvent ensuite être utilisés pour mesurer la similitude entre les images, par le calcul de la distance entre les histogrammes [ANT13].

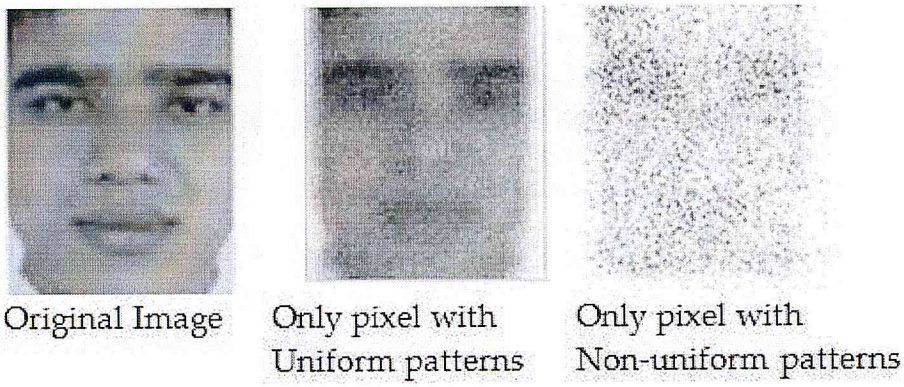


Figure II.8 : Image de visage divisé en une image avec seulement de pixels avec des motifs uniformes et d'une image avec seulement des motifs non uniformes

Figure 2.9 montre une image qui est divisée en une image avec seulement de pixels avec des motifs uniformes et une image avec seulement des motifs non uniformes. Ces images sont créées en utilisant l'opérateur LBP16,2. Il arrive que l'image avec seulement de pixels avec des motifs uniformes contienne encore une quantité considérable de pixels, à savoir99% de l'image originale. Ainsi, 99% des pixels de l'image ont des modèles uniformes. Une autre chose frappante est le fait que, en prenant seulement les pixels avec des motifs uniformes, le fond est également préservé. C'est parce qu'à l'arrière-plan, les pixels ont tous la même couleur (même valeur de gris) et donc leurs modèles contiennent zéro transitions. Il semble également que la plupart des pixels autour de la bouche, le nez et les yeux (surtout les sourcils) ont des modèles uniformes [ANT13].

6. Les 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 [BET14].

a) 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 [BET14].

b) 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 [BET14].

c) 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 [BET14].

d) 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 [BET14].

e) 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 [BET14].

7. Base de données

Il existe plusieurs bases de données contenant des informations qui permettent l'évaluation des systèmes de reconnaissance faciale. Par ailleurs la plupart de ces base de données sont adapté aux besoins de quelques algorithmes spécifique de reconnaissance chacune de ses base de données a été créé sur des conditions d'acquisition d'image de visage tel que le changement d'illumination, de pose ou des expressions faciales. On trouve des base de données anciennes tel que ORL et Yale qui ont été les plus utilisé et on trouve d'autres plus récentes tel FERET, FRGC, CVL et AR qui contiennent un plus grand nombre d'exemple de personne et sont donc utiles pour des évaluations à plus grande échelle.

Bien qu'il existe de nombreuses bases de données en cours d'utilisation actuellement, le choix d'une base de données appropriée à utiliser doit être fait sur la base de la tâche donnée (vieillissement, les expressions, l'éclairage, etc.). Une autre façon est de choisir l'ensemble spécifique à la propriété à tester des données (par exemple, comment l'algorithme se comporte lorsqu'on lui fournit des images avec des changements d'éclairage ou des images avec différentes expressions faciales). Si, d'autre part, un algorithme doit être formé avec plus d'images par classe (comme LDA), la base de données Yale est probablement plus appropriée que FERET.

On détaillera par la suite quelques bases de données qui sont les plus utilisées et qui s'adaptent à l'algorithme qu'on a vu dans le chapitre précédent.

a) La Base de données FERET

Le programme FERET avait pour but d'établir une grande base de données d'images faciales qui ont été recueillies indépendamment par les développeurs de l'algorithme. Le Dr Harry Wechsler à l'Université George Mason a été choisi pour diriger la collecte de cette base de données. La collection de la base de données est un effort de collaboration entre le Dr Wechsler et le Dr Phillips. Les images ont été recueillies dans un environnement semi-contrôlée [FER].

Pour maintenir un degré de cohérence tout au long de la base de données, la même configuration physique a été utilisée pour chaque session de photographie. Parce que l'équipement devait être remonté pour chaque session, il y avait une certaine variation mineure dans les images recueillies à des dates différentes. La base de données a été recueillie en 15 séances entre Août 1993 et Juillet 1996 [FER].

La base de données contient 1 564 ensembles d'images pour un total de 14 126 images qui comprend 1 199 individus et 365 ensembles d'images en double. Un ensemble en double est un second ensemble d'images d'une personne qui est déjà dans la base de données et a été généralement pris un autre jour. Pour certaines personnes, plus de deux ans se sont écoulés entre les premières et dernières séances, avec quelques sujets photographiés à plusieurs reprises. Ce laps de temps est important car il a permis aux chercheurs d'étudier, pour la première fois, des changements dans l'apparence d'un sujet qui se produisent au cours d'une année [FER].

Pour chaque individu, on dispose d'une vue faciale régulière **fa** et une vue faciale alternative **fb** prise un peu après **fa** Pour quelques personnes de la base, on dispose d'autres vues duplicates

collectées dans des conditions similaires à **fa** et fb mais dans des sessions ultérieures. Aucune contrainte n'est imposée sur la date de la prise de vue de l'image duplicate I. par contre, la vue duplicate II a été collectée au moins 540 jours après la première prise de vue [PHI20].

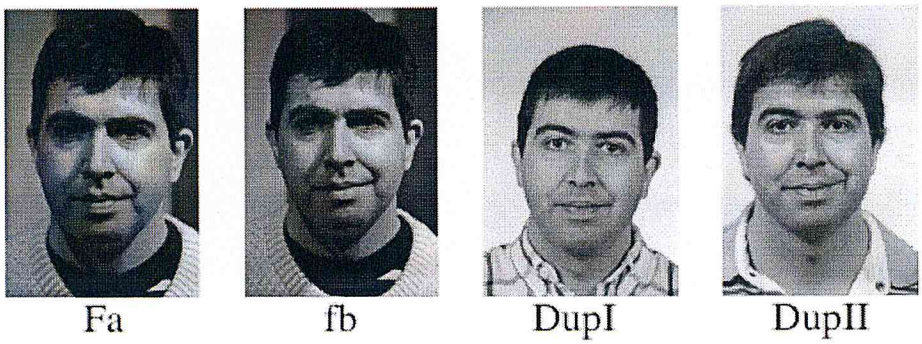


Figure II.9 : Extrait de la base de données FERET : Les images sont transformées en niveau gris.

b) La Base de données XM2VTS

Au début c'était la base de données M2VTS (Multimodal Face *Data Base*) [MES99] qui est constituée à partir de 37 visages différents et fournit 5 photos pour chaque personne. Ces images ont été prises à une semaine d'intervalle ou lorsque des changements de visage drastiques survenus dans l'intervalle. Au cours de chaque tir, les gens ont été invités à compter à partir de «0» à «9» dans leur langue maternelle (la plupart des gens parlent français), faire tourner la tête de 0 à -90 degrés, de nouveau à 0, puis à 90 et retour à 0 degrés. En outre, ils ont été invités à faire tourner la tête une fois de plus sans lunettes, s'ils en portaient.

Après c'est devenu une base de données plus étendue d'où son nom XM2VTS (*Extended Multimodal Face Data Base*) Contient quatre enregistrements de 295 sujets pris sur une période de quatre mois. Chaque enregistrement contient photo du visage en parlant et photo du visage en rotation. Des séries de données prises à partir de cette base de données sont disponibles, y compris des images de haute qualité de couleur de 32 kHz, 16 bits des fichiers audio, des séquences vidéo et un modèle 3D [MES99].

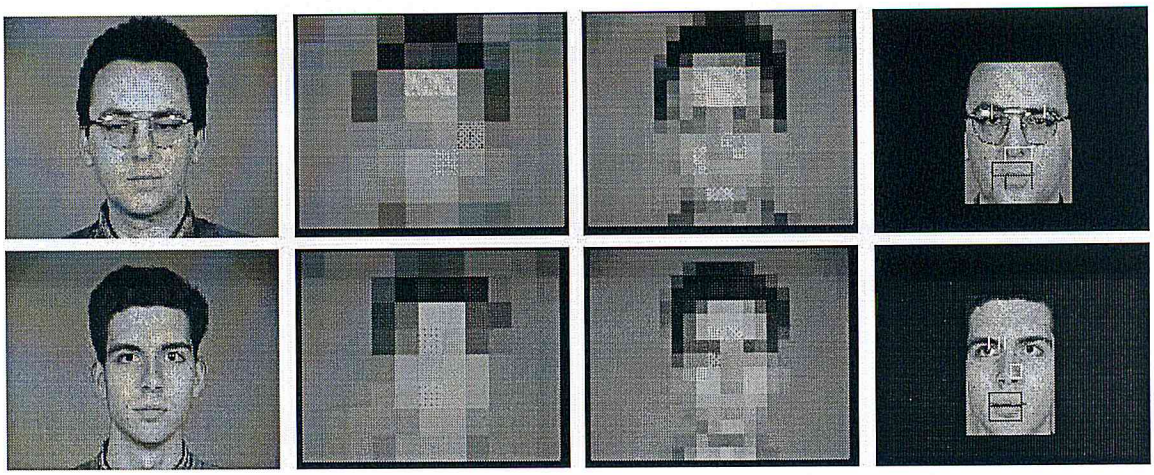


Figure II.10 : Deux images de face frontale de la base de données M2VTS

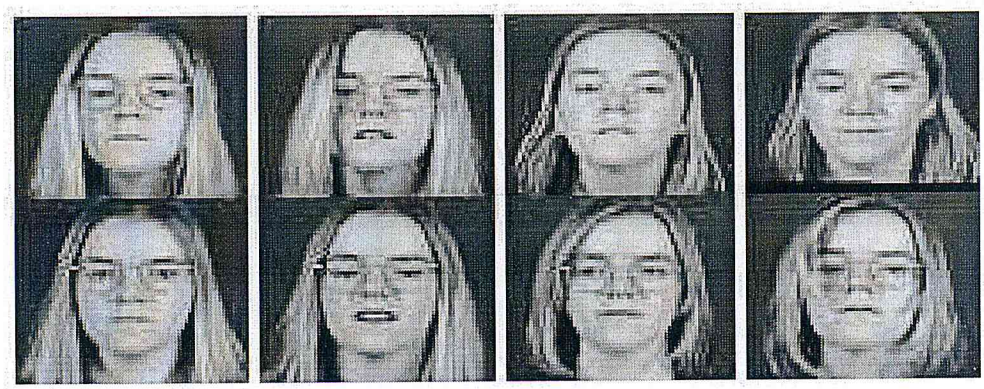


Figure II.11 : Extrait de la base de données XM2VTS

c) La Base de données Yale

The Yale Face Database : Contient 165 images en niveaux de gris au format GIF de 15 personnes. Il y'a 11 images par sujet, chaque une avec une expression de visage différente ou configuration différente : centre-lumière, avec lunettes, heureux, à gauche, la lumière avec ou sans lunettes, lumière du coté droit, lumière normale, triste, somnolent, surpris, et clin d'œil.

The Yale Face Database B : Contient5760 avec une seule source de lumière de 10 sujets chacun vu sous576 conditions de visualisation (9 poses x64 conditions d'éclairage). Pour chaque sujet dans une pose particulière, une image avec un éclairage ambiant a également été capturée [YAL].

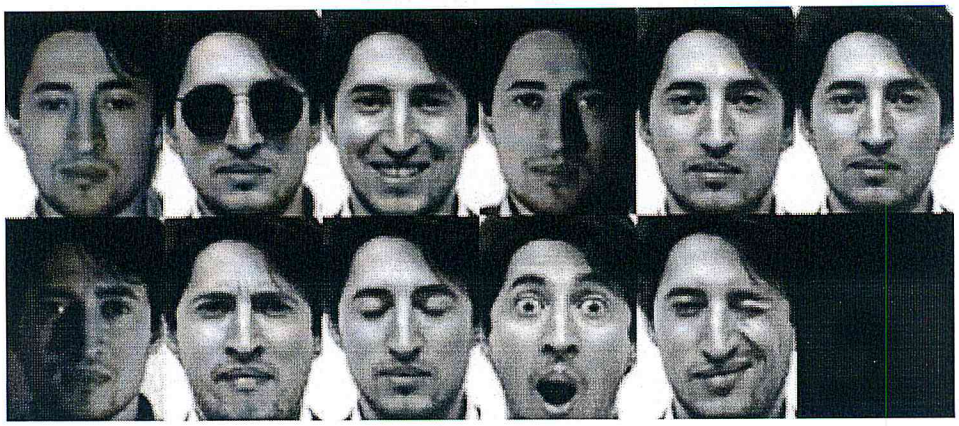


Figure II.12 : Exemple de la base de données Yale

d) La base de données FRAV

Il existe deux types de base de données FRAV une pour les images 2D (FRAV2D) et une autre qui traite le fichier 2D, 2.5D et 3D (FRAV3D) [FAC].

i. FRAV2D Database

Cette base de données est formée par 109sujets (75 hommes et34 femmes), avec 32 images en couleur par personne. Chaque image a une résolution de 320 x 240 pixels, avec le visage occupant la majeure partie de l'image dans une position verticale. Pour une seule personne, toutes les photos ont été prises le même jour, bien que le sujet a été obligé de se lever et de se rasseoir pour changer de pose et de geste [FAC]. Dans tous les cas, le fond est clair et bleu foncé. Les 32 images ont été classées en six groupes selon les conditions de pose et d'éclairage : 12 images frontales, 4 images détournées de 15 degrés, 4 images tournées de 30 dégrées, 4 images avec des gestes, 4 images avec traits du visage occlus et 4 images frontales avec un changement de l'éclairage. Cette base de données est livrée gratuitement exclusivement à des fins de recherche.

ii. FRAV3D Data base

Cette base de données contient 106 sujets, dont environ une femme sur quatre. Les données ont été acquises avec un scanner Minolta VIVID 700, qui fournit des informations de texture (image 2D) et un fichier VRML (image 3D). Si besoin, les données de la plage d'image correspondantes (2,5D) peuvent être calculées à l'aide du fichier VRML. Par conséquent, elle est une base de données multimodal (2D, 2,5D y 3D). Au cours de tous les temps, un protocole d'acquisition stricte a été suivi, avec des conditions d'éclairage contrôlées. La personne est assise sur un tabouret réglable en face du scanner et en face d'un mur bleu. Les lunettes, les chapeaux ou les foulards n'ont pas été autorisés. Un total de 16 captures par personne ont été prises à chaque séance, avec différentes poses et conditions d'éclairage, en essayant de couvrir toutes les variations possibles, y compris les tours dans des directions différentes, les gestes et les

changements d'éclairage. Dans tous les cas un seul paramètre a été modifié entre deux captures. Cette base de données est livrée gratuitement exclusivement à des fins de recherche [FAC].

e) La Base de données ORL

Conçu par AT&T laboratoires de l'université de Cambridge en Angleterre, la base de Donnée ORL *(Olivetti Research Laboratory)* est une base de donnée de référence pour les systèmes de reconnaissances automatique des visages. En effet tous les systèmes de reconnaissances de visages trouvés dans la littérature ont été testés par rapport à l'ORL.

Dix images différentes de chacun des 40 sujets distincts. Pour certains sujets, les images ont été prises à des moments différents, variant l'éclairage, les expressions du visage (yeux ouverts / fermés, souriant /pas sourire) et les détails du visage (lunettes / sans lunettes). Toutes les images ont été prises sur un fond sombre homogène avec les sujets dans une position frontale verticale (avec tolérance pour un mouvement de côté) [CAM].

Figure II.13 : Base de données ORL

Figure II.14 : Exemple de changements d'orientations du visage

Figure II.15 : Exemple de changements d'éclairage

8. Conclusion

Dans ce chapitre, des généralités sur la reconnaissance faciale sont abordées. Nous avons vu que le visage est la partie du corps la plus utilisée pour s'exprimer et s'identifier. Pour comprendre le système de reconnaissance humain, les chercheurs ont essayé de comprendre la psychologie de la reconnaissance faciale, ce qui a permis de déterminer les caractéristiques essentielles du visage qui permettent de différencier entre un humain et un autre.

Dans la deuxième partie, nous nous sommes concentrés sur les systèmes de reconnaissance du visage et leurs architectures. Cette dernière se divise généralement en quatre modules : acquisition, prétraitement, extraction de données et décision.
Une grande partie de ce chapitre a été consacrée aux différentes méthodes de reconnaissance du visage.

Chapitre III
Conception d'un prototype

III. Conception d'un prototype

1. Introduction

Les documents de recherche sur les systèmes de reconnaissance de visage sont étudiés et l'état courant de la technologie, ils sont examinés et résumés dans le chapitre précédent, dont le résultat va nous guider pour concevoir une application de reconnaissance faciale.

Une enquête a révélé que ces différentes méthodes et leurs combinaisons peuvent être appliquées dans le développement d'un nouveau Système de reconnaissance faciale. Parmi les nombreuses approches possibles, nous avons décidé d'utiliser la méthode de *Viola and Jones* pour la partie détection de visage et la méthode *Principal Component Analysis* (PCA) connue aussi sous le nom *Eigenface* pour la partie de reconnaissance du visage. La principale raison de cette sélection est leur bonne applicabilité et fiabilité.

2. La partie Acquisition

La partie acquisition est une condition préalable pour notre application de reconnaissance de visage. L'opération d'acquisition d'image est effectuée dans cette partie. Les images en direct capturées sont converties en données numériques pour effectuer des calculs de traitement d'image. Ces images capturées sont envoyées à l'algorithme de détection de visage. C'est la caméra frontale d'un Smartphone ou d'une tablette qui va s'occuper de la capture d'images.

3. La partie détection de visage

La partie détection de visages effectue la localisation et l'extraction de visage d'une image pour notre système de reconnaissance faciale.

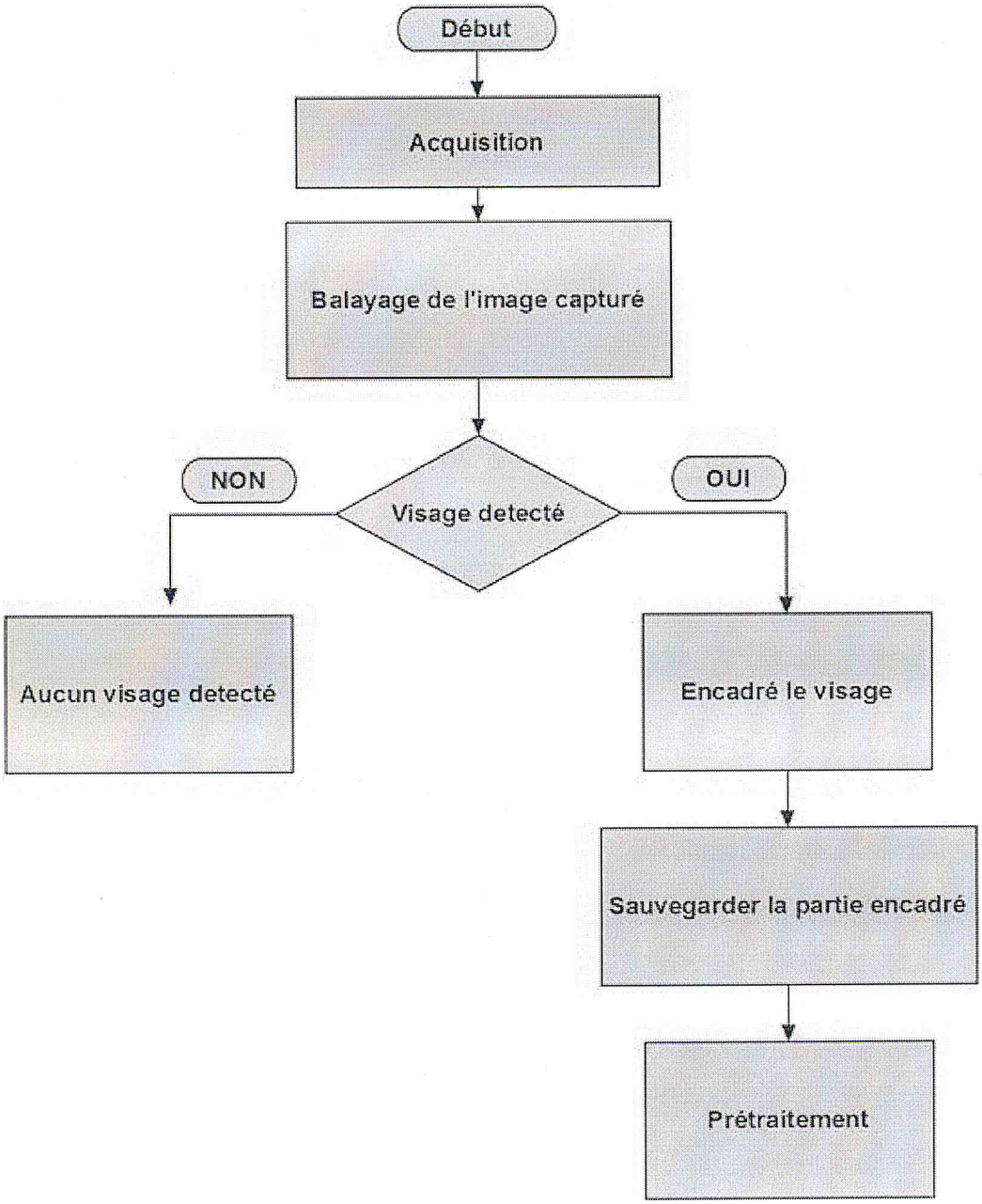


Figure III.1 : Organigramme de détection de visage

C'est l'algorithme de *Viola and Jones* qui a été choisie pour cette partie, cette méthode consiste à balayer une image à l'aide d'une fenêtre de détection de taille initiale 24px par 24px (dans l'algorithme original) et de déterminer si un visage y est présent ou non. Lorsque l'image a été parcourue entièrement, la taille de la fenêtre est augmentée et le balayage recommence, jusqu'à ce que la fenêtre fasse la taille de l'image. L'augmentation de la taille de la fenêtre se fait par un facteur multiplicatif de 1,25 qui peut être modifié [DIY13].

Le balayage, quant à lui, consiste simplement à décaler la fenêtre d'un pixel. Ce décalage peut être changé afin d'accélérer le processus, mais un décalage d'un pixel assure une précision maximale.

Cette méthode est une approche basée sur l'apparence, qui consiste à parcourir l'ensemble de l'image en calculant un certain nombre de **caractéristiques** dans des zones rectangulaires qui se chevauchent. Elle a la particularité d'utiliser des caractéristiques très simples mais très nombreuses [DIY13].

Une caractéristique est une représentation synthétique et informative, calculée à partir des valeurs des pixels. Les caractéristiques utilisées ici sont les **caractéristiques *pseudo-haar***. Elles sont calculées par la différence des sommes de pixels de deux ou plusieurs zones rectangulaires adjacentes [WIK].

Prenons un exemple. Voici deux zones rectangulaires adjacentes, la première en blanc, la deuxième en noire :

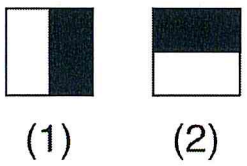


Figure III.2 : deux caractéristiques rectangulaires

Les caractéristiques seraient calculées en soustrayant la somme des pixels noirs à la somme des pixels blancs.

Les caractéristiques sont calculées à toutes les positions et à toutes les échelles dans une fenêtre de détection de petite taille, typiquement de 24x24 pixels ou de 20x15 pixels. Un très grand nombre de caractéristiques par fenêtre est ainsi généré, Viola et Jones donnant l'exemple d'une fenêtre de taille 24 x 24 qui génère environ 160 000 caractéristiques [DIY13].

L'image précédente présente des caractéristiques *pseudo-haar* à seulement deux caractéristiques mais il en existe d'autres, allant de 4 à 14, et avec différentes orientations.

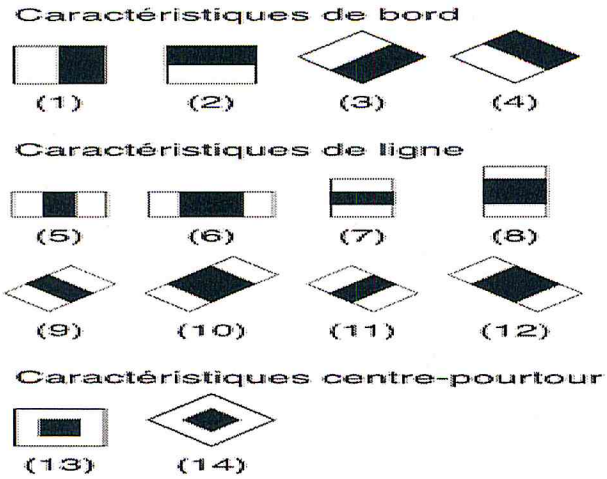


Figure III.3 : Quelques caractéristiques Pseudo Haar

Etant donné une image ou une vidéo, l'algorithme identifie tous se qui se trouve dans cette image et le classifier comme un visage ou un non visage.

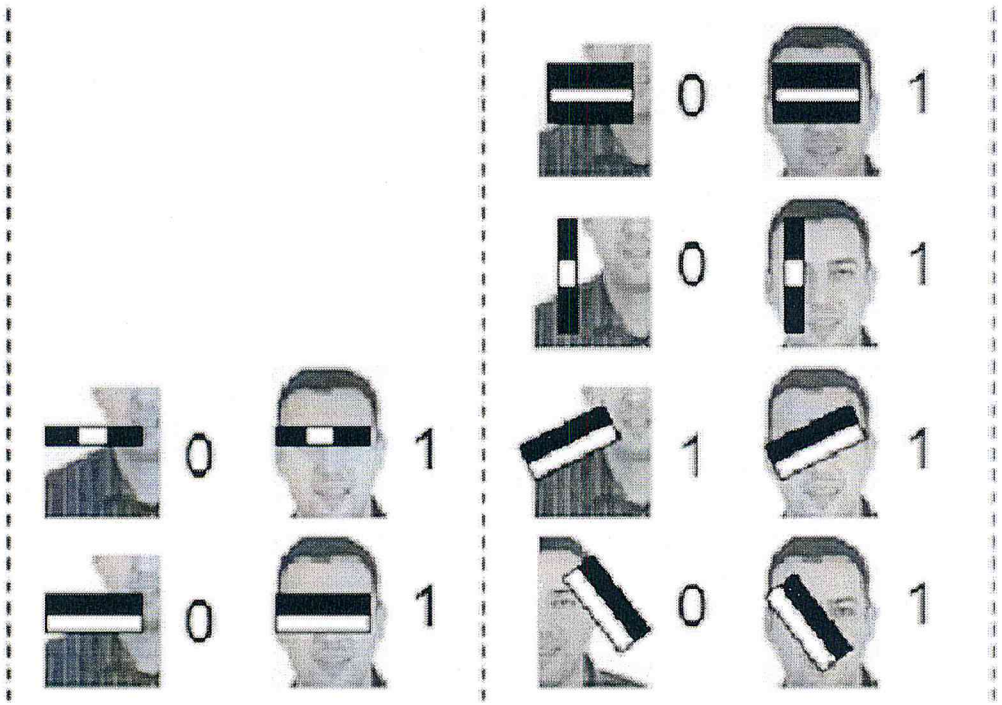


Figure III.4 : Exemple de l'application de quelques caractéristiques

Après avoir détecté le visage on extrait la partie visage seulement, c'est cette partie qui nous intéresse pour la reconnaissance faciale. Cette image va subir différents prétraitements avant de la sauvegardé dans la base de données du système, ce prétraitement consiste en la conversion en niveau de gris, l'égalisation d'histogramme et le redimensionnement de notre image.

4. La partie prétraitement

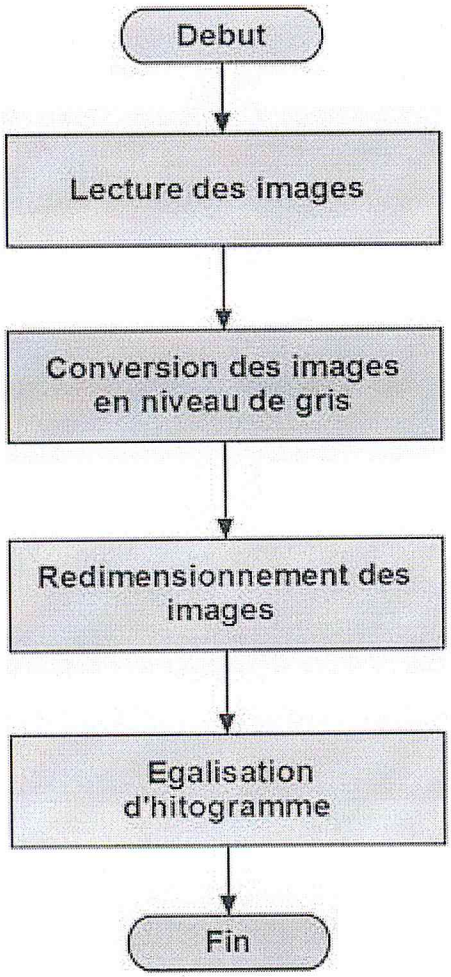


Figure III.5 : Organigramme du prétraitement

a) Transformation en niveau de gris

Image en niveaux de gris est une image dans laquelle la valeur de chaque pixel est un échantillon unique, cet échantillon exerce seulement une information d'intensité. Les Images de ce genre, aussi connu comme le noir et blanc, sont composées exclusivement de nuances de gris, variant du noir à la plus faible intensité de blanc. Les avantages de cette transformation par rapport aux images RVB (en couleur) :

- Pour de nombreuses applications de traitement d'image, les informations de couleur ne nous aident pas à identifier des bords importants ou d'autres caractéristiques. Il y'a des exceptions, s'il y a une arête (une nouvelle étape dans la valeur de pixel) en teinte qui est difficile à détecter dans une image en niveaux de gris, ou si nous avons besoin d'identifier des objets de teinte connue (fruits orange en face de feuilles vertes), là les informations de couleur pourront être utiles. Si on n'a pas besoin de couleur, alors nous pouvons considérer les couleurs comme obstructives.

- Complexité du code. Si nous voulons trouver des bords sur la base de luminance et de chrominance, nous aurons plus de travail devant nous. Ce travail supplémentaire est une perte de temps et est difficile à justifier si les informations de couleur ne sont pas utiles pour l'application.

- Avec les ordinateurs modernes, et avec la programmation parallèle, il est possible d'effectuer un traitement d'une image méga pixels simples pixel par pixel en millisecondes. La reconnaissance faciale, OCR, la segmentation de décalage moyenne, et d'autres tâches peut prendre beaucoup plus que cela. Quel que soit le temps de traitement nécessaire pour manipuler l'image ou d'extraire quelques données utiles, la plupart des clients / utilisateurs veulent que ça aille plus vite. Si nous faisons l'hypothèse à la main que le traitement d'une image couleur à trois canaux prend trois fois plus de temps que le traitement d'une image en niveaux de gris a un seul canal ou peut-être quatre fois plus longtemps, puisque l'on peut créer un canal de luminance séparé, ce n'est pas un problème si nous voulons traiter des images vidéo ou chaque image peut être traitée en moins de 1/30eme ou 1/25eme de seconde. Mais si nous analysons des milliers d'images à partir d'une base de données, le temps augmentera beaucoup.

b) Egalisation des Histogrammes

L'histogramme d'une image, c'est une représentation graphique de la distribution d'intensité d'une image. On quantifie le nombre de pixels pour chaque valeur d'intensité considérée.

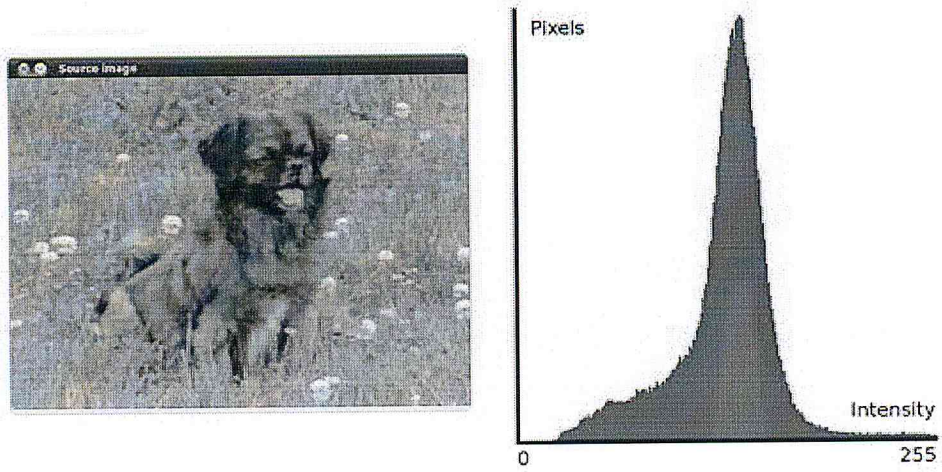


Figure III.6 : A gauche Image en niveau de gris, A droite l'histogramme de cette image

L'égalisation d'histogramme : Elle porte sur un procédé qui permet d'améliorer le contraste d'une image, afin d'étendre la gamme d'intensité, pour le rendre plus clair, à partir de l'image ci-dessus, nous pouvons voir que les pixels semblent regroupés autour du milieu de la gamme disponible des intensités. Ce que fait l'égalisation d'histogramme est l'étirassions de cette gamme. Les cercles verts dans la figure 3.7indiquent les intensités sous-peuplées. Après l'application de l'égalisation, nous obtenons un histogramme comme la figure dans le centre. L'image résultante est représentée sur à droite.

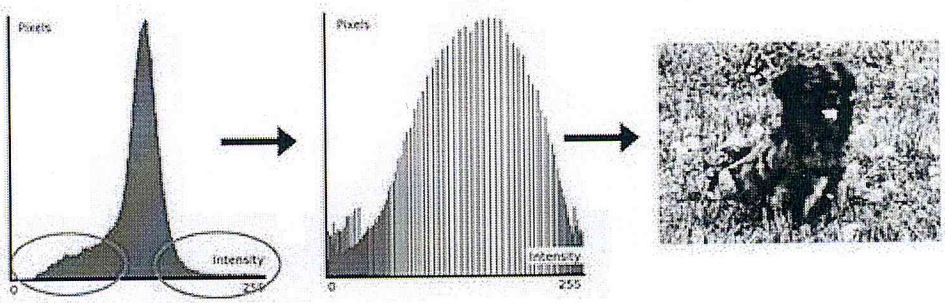


Figure III.7 : Exemple d'histogramme après égalisation

L'égalisation implique une cartographie de distribution (l'histogramme de donnée) à une autre distribution (une distribution plus large et plus uniforme des valeurs d'intensité) de sorte que les valeurs d'intensités ont éparpillées sur toute la gamme.

c) Redimensionnement d'images

Après l'application de l'égalisation d'histogramme, l'image d'entrée doit être similaire aux visages dans la base de données, là il manque qu'une étape le redimensionnement de notre image, supposant que l'image faciale acquise est de taille de 240*270 pixels faudrait la redimensionner pour qu'elle soit de même taille avec les images de notre base de données.

Figure III.8 : Exemple de redimensionnement d'une image

Maintenant qu'on a terminé le traitement de notre image on va la sauvegardé dans notre base de données avec les autres images qui s'y trouve déjà, là on aura toutes nos images de même taille.

5. La partie Reconnaissance du visage

Maintenant que la partie détection de visage est terminé on passe à la partie Reconnaissance de visage nous avons nos images faciale prétraitées, nous pouvons appliquer la méthode PCA pour la reconnaissance faciale

a) Principal Component Analysis

Principal Component Analysis ACP(PCA) a été inventé en 1901 par Karl Pearson. PCA est une procédure de réduction de variable et elle est utile lorsque les données obtenues ont une certaine redondance.

Le But de l'ACP est de réduire la dimension des données en retenant autant que possible les variations dans notre ensemble de données d'origine. Mais la réduction de la dimension implique la perte d'information. Le meilleur espace à petite dimension peut être déterminé par les meilleures composantes principales.
Le principal avantage de l'APC est qu'il utilise l'approche de visage propre *Eigenfaces* qui contribue à réduction de la taille de la base de données.

Les images sont stockées en tant que vecteurs de caractéristiques dans la base de données. PCA est appliquée sur l'approche *Eigenfaces* pour réduire la dimensionnalité d'un grand ensemble de données.

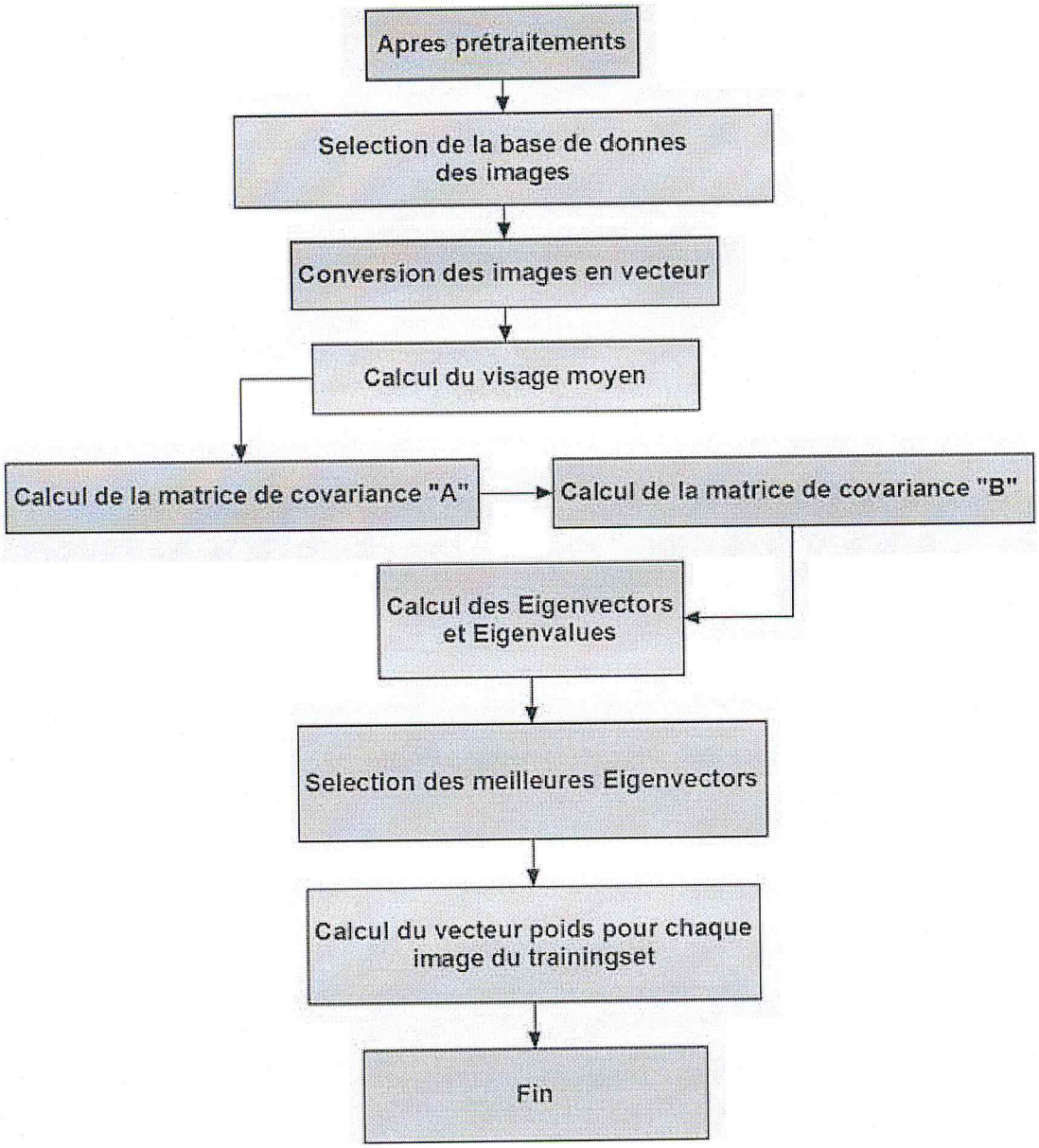


Figure III.9 : Organigramme du calcul des Eigenfaces

Une grande partie des travaux antérieurs sur la reconnaissance faciale a ignoré la question quels sont seulement les aspects de la relance du visage qui sont importants pour la reconnaissance faciale. Ceci suggère l'utilisation d'une approche de la théorie de l'information de codage et de décodage des images de visage, en insistant sur les caractéristiques locales et mondiales importantes. Tel fonctions peuvent ou ne peuvent pas être directement liées à notre notion intuitive de traits du visage tels que les yeux, le nez, les lèvres et les cheveux.

Dans le langage de la théorie de l'information, les informations pertinentes dans un visage sont extraites et codées aussi efficacement que possible, et ensuite comparées à une base de données de modèles codés de manière similaire. Une approche simple pour extraire les informations contenues dans une image de visage est de capturer quelque sorte la variation dans une collection d'images de visage, indépendamment de tout jugement de fonctionnalités, et l'utilisation de cette information pour coder et comparer les images de visage individuels.

En termes mathématiques, les principales composantes de la distribution de visage, ou les vecteurs propres (*Eigenvectors*) de la matrice de covariance de l'ensemble des images de visage, traitement d'une image en tant que point (ou vecteur) dans un espace dimensionnel très élevé est difficile.

Les *Eigenvectors* (vecteurs propres) sont ordonnés, chacun d'eux représente une quantité différente de la variation entre les images de visage. Ces *eigenvector*s peuvent être considérés comme un ensemble de fonctionnalités qui, caractérise la variation entre les images de visage. Chaque emplacement d'image contribue plus ou moins à chaque *eigenvector*, de sorte qu'il est possible d'afficher ses *eigenvectors* comme une sorte d'image de visage fantomatique (*ghostly face*) qui est appelé un « *Eigenface* » [ABH12].

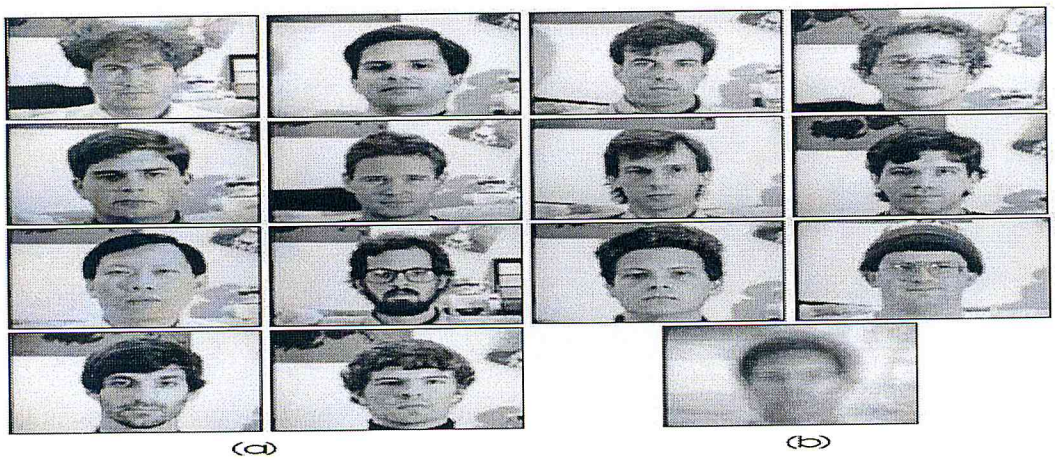


Figure III.10 : Quelques images de visage (a) et leur visage Moyen (b)

Figure III.11 : Les eigenfaces correspondant à l'ensemble des visages de la figure III.12

Chaque visage d'individu peut être représenté exactement en termes de combinaison linéaire de ses *Eigenfaces*. Chaque visage peut aussi être estimé à l'aide seulement des meilleurs *Eigenfaces* ceux qui ont les plus grandes *eigenvalue*. Les meilleurs M *eigenfaces* couvrent un sous-espace de M- dimension appelé l'espace visage de toutes les images possibles.

Kirby et Sirovich [SIR87] ont développé une technique pour représenter efficacement des photos de visages à l'aide d'analyse en composantes principales. A partir d'un ensemble d'image de visages d'origine, ils ont calculé un système pour coordonner au mieux la compression d'image, où chaque coordonnée est en fait une image qu'ils ont appelé une "*Eigenpicture*". Ils ont fait valoir qu'au moins en principe, n'importe quelles collections d'images de visage peuvent être reconstruites en stockant environ une petite collection de poids pour chaque visage, et une petite série de photos standards (les *eigenpictures*). Les poids décrivant chaque visage se trouvent en projetant l'image de visage sur chaque *eigenpicture*.

Dans ce travail, nous avons suivi la méthode qui a été proposée par M. Turk et A. Pentland [MAT91] pour développer un système de reconnaissance de visage basée sur l'approche *Eigenfaces*. Ils ont fait valoir que, si une multitude d'images de visage peut être reconstruite par la somme pondérée d'une petite collection de caractéristiques ou *eigenpictures*, ceci peut-être un moyen efficace pour apprendre et reconnaître les visages, la mise en place des caractéristiques sera par expérience au fil du temps et la reconnaissance des visages particuliers sera en comparant les poids nécessaires pour les reconstruire avec les poids associés à des individus connus. En conséquence, chaque individu est caractérisé par un petit ensemble de poids nécessaire pour pouvoir le décrire et le reconstruire.

Soit une image de visage I (x, y)à deux dimensions NxN. Une image peut également être considéré comme un vecteur de dimension N^2, de sorte qu'une image de taille 256 x 256 devient un vecteur de dimension 65 536, ou de façon équivalente un point dans l'espace de 65 536 dimensions. Les Images de visages, étant similaires dans leur configuration globale, ne seront pas réparties de façon aléatoire dans cet immense espace de l'image et peut donc être décrite par un faible sous-espace dimensionnel. L'idée principale de l'analyse de composante principale (ou l'expansion de Karhunen-Loève) est de trouver les meilleurs vecteurs qui comptent pour la distribution d'images de visage à l'intérieur de l'espace de l'image entière [MAT91].

Ces vecteurs définissent le sous-espace des images de visages, que nous appelons «*face space* ». Chaque vecteur est de longueur N^2, décrit une image de Nx N en une combinaison linéaire des images de visage originales. Étant donné ces vecteurs sont *les eigenvectors* de la matrice de covariance correspondante aux images de visages d'origine, et parce qu'ils sont en apparence comme des visages, nous nous référons à eux comme *eigenfaces*.

b) *Eigenvectors* et *Eigenvalues*

Définition

Une matrice A de taille NxN est dite d'avoir un *eigenvecteur* X, et correspondant à une *eigenvalue* λ si [ABH12]:

$$AX = \lambda X. \quad 3.1$$

Evidemment, l'équation précédente ne peut tenir que si :

$$\det|A - \lambda I| = 0 \quad 3.2$$

Si cette équation est étendue, ça sera un polynôme de degré N dont les racines sont les *eigenfaces*. Cela prouve qu'il y'a toujours N (non nécessairement distinctes) *eigenfaces*.

Une matrice est appelée symétrique si elle est égale à sa transposée:

$$A = A^T \text{ or } a_{ij} = a_{ji} \quad 3.3$$

Elle est appelée orthogonale si sa transposée est égale à son inverse :

$$A^T A = AA^T = I \quad 3.4$$

Une matrice réelle est dite normale si elle commute ave csa transposée :

$$AA^T = A^T A. \quad 3.5$$

Après avoir donné un aperçu sur les conditions qui vont être utilisées dans l'évaluation des *eigenfaces*, nous pouvons concentrer pour trouver ces *eigenfaces* [ABH12].

Que le *trainingset* des images de visages soit Γ1, Γ2,…, ΓM et la moyenne du *trainingset* (visage moyen) définie par :

$$\Psi = \frac{1}{M}\sum_{n=1}^{M}\Gamma_n \qquad 3.6$$

Chaque visage diffère du visage moyen par :

$$\Phi_i = \Gamma_i - \Psi \,. \qquad 3.7$$

Un exemple du *trainingset* est illustré à la figure3.10-a, avec le visage moyen Y figure 3.10-b.

Cet ensemble de très grands vecteurs est alors soumis à une analyse de composante principale, qui cherche un ensemble de M vecteurs orthonormés, U_n, qui décrit le mieux la répartition des données. Le vecteur k-ième,U_k, est choisi de telle sorte que :

$$\lambda_k = \frac{1}{M}\sum_{n=1}^{M}(u_k^T \Phi_n)^2 \qquad 3.8$$

$$u_l^T u_k = \delta_{lk} = \begin{cases} 1, & \text{if } l = k \\ 0, & \text{otherwise} \end{cases} \qquad 3.9$$

Les vecteurs U_k et scalaires $\lambda_k$sont les *eigenfaces* et les *eigenvalues*, respectivement de la matrice de covariance.

$$C = \frac{1}{M}\sum_{n=1}^{M}\Phi_n\Phi_n^T = AA^T \,. \qquad 3.10$$

Ou la matrice A= [ϕ1, ϕ2,…, ϕM], la matrice de covariance par contre est une matrice réelle symétrique de taille $N^2 \times N^2$, et pour déterminer les N^2 *eigenvectors* et *eigenvaluesest* une tâche insurmontable pour les tailles typiques d'images. Nous avons besoin d'une autre méthode de calcul pour trouver ces *eigenvectors.*

Si le nombre de points de données dans l'espace de l'image est inférieure à la dimension de l'espace ($M<N^2$), il y aura seulement M-1, plutôt que de N^2, *eigenvectors* significatifs. Les *eigenvectors* restants seront associé à une *eigenvalue* = 0. Nous pouvons résoudre les *eigenvectors* de dimensions N^2 dans ce cas par la résolution d'abord des *eigenvectors* d'une matrice Mx M tels que la résolution d'une matrice de taille de 16x16 matrice demande moins de calcul plutôt qu'une matrice16 384x16 384, puis prendre les combinaison linéaire des images de visage ϕi [ABH12].

Considérons les *eigenvectors*VideA^TA tel que :

$$A^T A v_i = \mu_i v_i \quad 3.11$$

On multipliant à des deux côtés par A, on aura :

$$AA^T A v_i = \mu_i A v_i \quad 3.12$$

À partir de laquelle nous voyons que Av_i sont *les eigenvectors* de$C=AA^T$.

Suite à ces analyses, nous construisons la matrice $L = A^TA$ de taille M x M, $L_{mn}=\phi^T_m\phi_n$, et trouver les M *eigenvectors* Vi, de L. Ces vecteurs détermineront les combinaisons linéaires de M images de visage du *trainingset* pour former les *eigenfaces* U_i.

$$u_l = \sum_{k=1}^{M} v_{lk} \Phi_k , \qquad l = 1,\ldots,M \quad 3.13$$

Avec cette analyse, les calculs sont considérablement réduits, de l'ordre du nombre de pixels dans les images (N^2) à l'ordre du nombre d'images dans l'ensemble de la formation *Trainingset* (M). En pratique, l'ensemble de formation des images de visages sera relativement petit ($M << N^2$), et les calculs deviennent tout à fait gérable. La *eigenvalue* associées nous permet de classer les *eigenvectors* en fonction de leur utilité pour caractériser la variation entre les images [ABH12].

Le succès de cet algorithme est basé sur l'évaluation des *eigenvalue* et des *eigenvectors* de la matrice symétrique réelle L qui est composé des images du *Trainingset*.

c) L'utilisation d'Eigenfaces pour classifier une image

Les *eigenfaces* calculées à partir des *eigenvectors* de L, couvrent un ensemble de base avec lequel on peut décrire des images de visage. Sirovichet Kirbyont évalué une version dans ce cadre sur un ensemble de M =115 images d'homme de race blanche, et ont constaté que M'=40 *eigenfaces* étaient suffisant pour une très bonne description des images de

visage. Dans la pratique, une plus petite valeur M 'peut être suffisante pour l'identification, car une reconstruction précise de l'image n'est pas obligatoire, pour une précision maximale, le nombre de *eigenfaces* doit être égal au nombre d'images dans le *trainingset* [ABH12].

Les *eigenfaces* couvrent un sous-espace de dimension M' de l'espace image originale N^2. Les M' *eigenvectors* significatifs de la matrice de L sont choisis comme ceux qui ont la plus grande *eigenvalue* associées.

Une nouvelle image de visage est transformée en composant *eigenfaces* par la simple opération suivante :

$$W_k = U_k^T (\Gamma - \Psi) \quad 3.14$$

Les poids forment un vecteur de caractéristique :

$$\Omega^T = [W_1 W_2 \ldots W_{M'}] \quad 3.15$$

Ceci décrit la contribution de chaque visage propre pour représenter l'image de visage en entrée, les visages propres (*eigenfaces*) sont traités comme un ensemble de base pour les images de visage. Le vecteur de caractéristiques est ensuite utilisé dans un algorithme de reconnaissance de modèle standard pour trouver un certain nombre de classe de visage prédéfinies, le cas échéant, qui décrit mieux le visage. Les classes de visage Wi peut être calculée en faisant la moyenne des résultats de la représentation du visage propre au cours d'un petit nombre d'images de visages de chaque individu.

Le classement se fait en comparant les vecteurs de caractéristiques du visage d'un membre de la base de données avec le vecteur de caractéristiques de l'image de visage en entrée. Cette comparaison est basée sur la distance euclidienne entre les deux éléments pour qu'elle soit plus petite du seuil défini par l'utilisateur ϵ_k. Elle est donnée dans l'équation (3.16). Si la comparaison tombe dans le seuil défini par l'utilisateur, alors le visage est classé comme «connu», sinon, il est classé comme "inconnu" et peut être ajouté à la base de données avec son vecteur de caractéristique pour une utilisation ultérieure, rendant ainsi le système à reconnaître de nouveau visages [ABH12].

$$\frac{\|\Omega - \Omega_k\|}{\|\Omega_k\|} \leq \varepsilon_k \quad 3.16$$

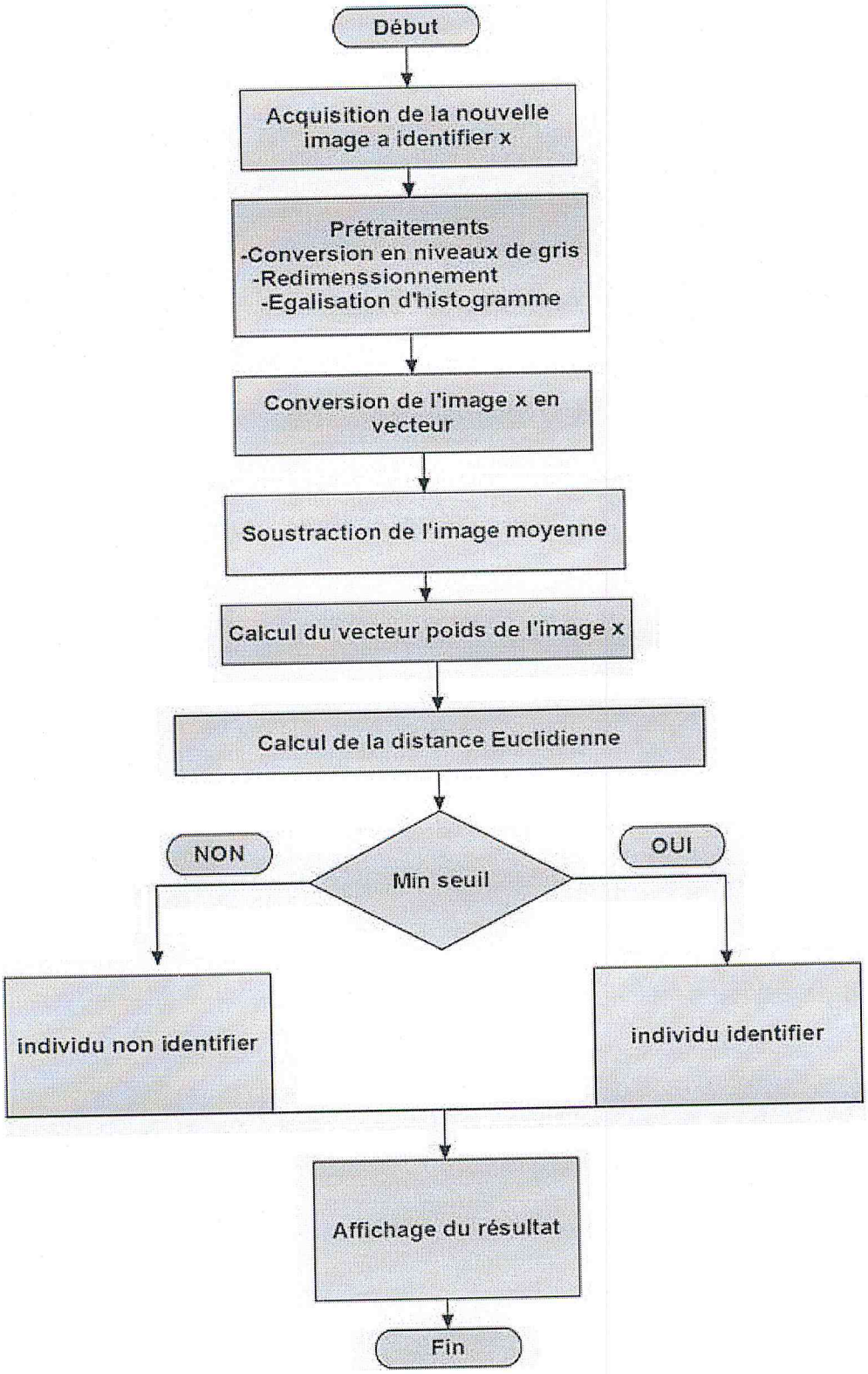


Figure III.13 : Organigramme d'identification

d) La reconstruction d'une image de visage avec *Eigenfaces*

Une image de visage peut être reconstruite approximativement en utilisant son vecteur de caractéristiques et les *eigenfaces*.

$$\Gamma' = \Psi + \Phi_f \quad 3.17 \qquad \Phi_f = \sum_{i=1}^{M'} w_i u_i \quad 3.18$$

Ou ϕ_f est l'image projeté.

Eq (3.17) nous dit que l'image du visage est reconstruite en ajoutant chaque visage propre avec une contribution de w_i (poids) Eq(3.18) au visage moyen du training set. Le degré de l'ajustement ou le taux d'erreur de la reconstruction peut être exprimé au moyen de la distance euclidienne entre l'image originale et l'image du visage reconstruite telle que donnée dans l'équation (3.19).

$$\text{Ratio des erreurs de reconstruction} = \frac{\|\Gamma' - \Gamma\|}{\|\Gamma\|} \quad 3.19$$

Il a été observé que, le ratio des erreurs de reconstruction augmente à mesure que les membres du *trainingset* diffèrent fortement les uns des autres. Cela est dû à l'addition du visage moyen. Lorsque les éléments sont différents les uns des autres (en particulier dans le fond d'image) l'image moyenne du visage devient plus compliquée et cela augmente ce rapport d'erreur. Il est possible de réduire ce taux d'erreur par l'utilisation de Eq 3.18 avec :

$$\frac{\|\Phi - \Phi_f\|}{\|\Phi_f\|} \leq \phi_k \quad 3.20$$

Où ϕ_k est un seuil défini par l'utilisateur des images de visage d'entrée appartenant à k-ième classe visage.

e) Résumé de la procédure de reconnaissance par *Eigenface*

Les étapes de l'approche *Eigenfaces* pour la reconnaissance du visage peut être résumées dans ce qui suit:

- Former une base de données de visage qui se compose des images de visages d'individus connus.

- Choisissez un *trainingset* qui comprend un certain nombre d'images (M) pour chaque personne avec une certaine variation dans l'expression et à la lumière.
- Calculer la matrice L M x M, trouver ses vecteurs et valeurs propres (*eigenfaces*, *eigenvalues*), et choisir M' vecteurs propres avec les valeurs propres les plus élevé.
- Combiner le *trainingset* d'images selon l'équation. (3.13) pour générer M' eigenfaces. Conservez ces visages propres pour une utilisation ultérieure.
- Pour chaque membre dans la base de données, calculer et stocker un vecteur de caractéristiques selon l'Eq. (3,15).
- Choisir un seuil ϵ selon l'équation (3.16) distance maximale de n'importe quelle classe de visage
- Pour chaque nouvelle image de visage à identifier, calculer son vecteur caractéristique selon l'Eq. (3,15) et le comparer avec les vecteurs de caractéristiques mémorisées de la base de données. Si la comparaison répond à la condition donnée dans l'équation. (3.16) pour au moins un membre, classer cette image de visage comme «connu», sinon la classer comme "inconnu" et ajoutez ce membre à la base de données de visage avec son vecteur caractéristique.

6. Conclusion

Dans ce chapitre nous avons vu comment notre prototype va être implémenté par la méthode *Eigenfaces* en se basant sur une analyse en composante principale, les principales étapes à suivre pour pouvoir mettre en œuvre un système de reconnaissance faciale.

Dans le chapitre suivant nous essayerons d'implémenter un système de reconnaissance faciale en se basant sur la méthode étudiée « *Eigenfaces* », tout en effectuent quelques tests sur notre système pour évaluer les performances de notre système et essayerons de les améliorer.

Chapitre IV
Expérimentation et test

IV. Expérimentation et Test

1. Introduction

Ce dernier chapitre est consacré à l'implémentation de notre application de reconnaissance faciale, le programme de reconnaissance faciale sera codé en JAVA avec l'utilisation d'autre utilitaire tel qu'*OpenCV*.

Le but de l'application sera d'identifier une personne à partir d'une image de visage capturé d'une webcam (ou capturer d'une caméra frontale dans le cas d'une application pour *Android*) et de la comparer aux images se trouvant dans une base de données l'aide de la méthode PCA.

2. Environnement de Travail

Le but de ce projet est de développer une application de reconnaissance faciale en utilisons une caméra, l'ensemble du matériel et logiciel utilisé est le suivant :

Processeur : Intel ® Core ™ i5-2430M CPU 2.40 Ghz

RAM : 4.00 GO DDR3

OS : Microsoft Windows 7

Eclipse Luna

OpenCV

a) OpenCV

OpenCV est publié sous une licence BSD et donc il est gratuit pour une utilisation à la fois académique et commerciale. Il possède des interfaces C++, C, Python et Java et prend en charge Windows, Linux, Mac OS, iOS et Android (OpenCV4Android). OpenCVa été conçu pour l'efficacité de calcule avec un fort accent sur les applications en temps réel. Écrit C / C++, la bibliothèque peut prendre avantage de traitement multi-core. Activé avec OpenCL, il peut profiter de l'accélération matérielle de la plate-forme de calcul hétérogène sous-jacent. Adopté dans le monde entier, OpenCV a plus de 47mille personnes de la communauté des utilisateurs et le nombre estimé de téléchargements dépassant 9 millions. Les plages d'utilisation de l'art interactif, à l'inspection des mines, cartes de couture sur le web ou par la robotique de pointe [OCV].

OpenCV propose la plupart des opérations classiques en traitement bas niveau des images:

- lecture, écriture et affichage d'une image.
- calcul de l'histogramme des niveaux de gris ou d'histogrammes couleurs.
- lissage, filtrage.
- seuillage d'image (méthode d'Otsu, seuillage adaptatif).
- segmentation (composantes connexes, *GrabCut*).
- morphologie mathématique.

b) Eclipse

Eclipse est un environnement de développement intégré (IDE). Il contient un espace de travail de base et un système de plug-in extensible pour la personnalisation de l'environnement. Écrit principalement en Java, Eclipse peut être utilisé pour développer des applications par le biais de divers plug-ins, Eclipse peut également être utilisé pour développer des applications dans d'autres langages de programmation : Ada, ABAP, C, C ++, COBOL, Fortran, Haskell, JavaScript, Lasso, Lua, naturel, Perl, PHP, Prolog, Python, R, Ruby (y compris Ruby on Rails *framework*), Scala, Clojure, Groovy, Scheme, et Erlang. Il peut également être utilisé pour développer des forfaits pour le logiciel Mathematica. Les environnements de développement comprennent les outils de développement Eclipse Java (JDT) pour Java et Scala, Eclipse CDT pour C / C ++ et PHP pour Eclipse PDT, entre autres.

Le code source initial provient d'IBM VisualAge. Le kit de développement Eclipse (SDK), qui comprend les outils de développement Java, est destiné aux développeurs Java. Les utilisateurs peuvent étendre leurs capacités par l'installation de plug-ins écrits pour la plateforme Eclipse, tels que les outils de développement pour d'autres langages de programmation, et peuvent écrire et contribuer leurs propres modules de plug-in.

Eclipse SDK est un logiciel libre et open source (même si elle est incompatible avec la GNU General Public License). Il était l'un des premiers IDE pour fonctionner sous GNU Classpath et il fonctionne sans problème sous IcedTea [WIK2]

c) Configuration d'OpenCV avec Eclipse

Après l'installation d'*OpenCV* sur notre plateforme Windows, on passe à sa configuration pour notre projet sous Eclipse, la premiere étape l'installation de Plugin CDT pour Eclipse car les classe d'*OpenCV* sont implémentées en C/C++, ce plugin nous permet de compiler les codes C/C++, La prochaine étape c'est d'ajouter les fichiers jar et dll nécessaires au fonctionnement d'*OpenCV*.

OpenCV/Build/JAVA/opencv-2410.jar
OpenCV/Build/JAVA/x64/opencv-2410.dll

3. Comment détecter un visage à l'aide d'*OpenCV*

Comme nous l'avons déjà mentionné au part avant la premier étape de notre système de reconnaissance faciale est la détection de visage, à l'aide de la bibliothèque *OpenCV* on a pu détecter des visages dans un flux vidéo, et ceci par l'utilisation du Haar Cascade (connu comme la méthode de *Viola-Jones*).

Etant donné un fichier ou une vidéo en direct, le détecteur de visage examine chaque emplacement de l'image et classifie comme visage ou non visage, le classifieur va utiliser des données se trouvant dans des fichiers XML pour pouvoir détecter différents objets selon le type d'objet (voiture, rectangle, visage…) dans notre cas ça sera le fichier contenant les informations de visage. *OpenCV* propose différents classifieurs pour la détection de visage dans des poses frontales, dans des poses de profil, la détection du haut du corps ou du corps complet, la détection des yeux …

Nous allons créer notre classifieur avec la commande Cascade_Classifier () et lui donné en paramètre l'un des classifieur Haar_Cascade contenant les informations nécessaires pour la détection d'un certain objet, l'objet en question dans ce cas sera le visage.

Pour la détection de visage en pose frontal *OpenCV* offre quatre classifieurs :

- haarcascade_frontalface_default.xml
- haarcascade_frontalface_alt.xml
- haarcascade_frontalface_alt2.xml
- haarcascade_frontalface_alt_tree.xml

Après une séries de tests sur une base d'images contenant au total 400 photos de visages. Voici les résultats obtenus par les cascades de type frontalface

	Bonnes détections		Mauvaise détections	
	Nombre	Pourcentage	Nombre	Pourcentage
Frontalface_alt	365	91,25%	35	8,75%
Frontalface_alt2	343	85,75%	57	14,25%
Frontalface_alt_tree	341	85,25%	59	14,75%
Frontalface_default	328	81,25%	72	18,75%

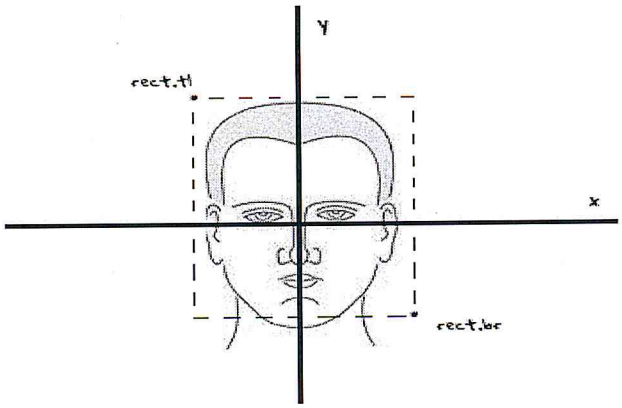
Tableau IV.1 : Résultat des détections de visage

on a conclu que le *haarcascade_frontalface_alt* est celui qui nous convient le mieux dans l'implémentation de notre application suivant les résultats du tableau 3.1 et aussi qu'avec les trois autres on a eu quelques problème ou il détecte des objets ressemblant à des visages mais qui ne le sont pas.

Maintenant on passe à la capture d'images, on a utilisé pour cela la webcam d'un ordinateur, la classe *Videocapture* nous permet de faire une capture vidéo depuis une caméra.

Il reste qu'à faire la détection de nos visages qui se trouvent dans les images capturées depuis notre webcam pour cela ces images vont passer par notre classifieur avant d'être projeté à l'écran, et retourné le nombre de visage détecté dans chaque image.

Pour savoir où se trouve les visages que notre détecteur à détecter et enregistrer que la partie du visage seulement car c'est ce qui nous intéresse, on va faire entourer les visages détecter d'une ellipse mais le problème qui s'est posé c'est que après avoir extrait le visage de notre image en se servant d'une ellipse c'est qu'on perd quelques caractérises qui sont importantes pour notre algorithme de reconnaissance faciale. Donc on a opté pour un cadre rectangulaire, le problème du cadre rectangulaire c'est comment savoir les limites de notre visage en hauteur et en largeur, la classe Rect de OpenCV fournit deux point le Rect.tl() et Rect.bl(), Rect.tl représente le point haut à gauche (top left) et le Rect.bl le point bas à droite (bottom right)



Avec ces deux points on a pu sélectionner le visage dans sa totalité la figure suivante montre un visage détecté encadré par un rectangle.

4. Comment faire le prétraitement des images faciales

Maintenant que nous avons réussi faire la détection de visage, on peut utiliser cette image de visage pour la reconnaissance faciale, mais si on fait directement une reconnaissance sur une image normale on aura un résultat inférieur à 10%, donc il est nécessaire de faire passer cette image par divers techniques de prétraitement pour standardiser les images que nous fournissant à notre système de reconnaissance faciale.

La majorité des algorithmes de reconnaissance faciale sont sensible a plusieurs facteur tel que la luminosité, l'algorithme aura du mal à reconnaitre une personne si sa photo qui se trouve dans la base de données était prise dans un milieu a un niveau de luminosité très grand, et que la photo à reconnaitre a été prise dans un milieu sombre.

Il y'a d'autres problèmes tel que la position du visage, elle doit être dans une position cohérente de l'image, émotion, sourire, colère … c'est pourquoi il est important d'appliquer un prétraitement avant l'étape de reconnaissance.

Notre système de reconnaissance faciale est basé sur l'algorithme PCA *(Eigenfaces)* cet algorithme traite des images en niveau de gris, donc les images acquises RVB (en couleur) vont être convertit en des images en niveau de gris, et ensuite redimensionner chaque images pour que chaque images de visage, que ce soit celle d'entrée ou qui se trouvent dans la base de données soit de même taille.

Enfin l'égalisation d'histogramme pour standardiser automatiquement le contraste et la luminosité des images.

La bibliothèque OpenCV offre plusieurs fonctions dont une pour la transformation d'une image en couleur en une image en niveau de gris la méthode `cvCvtColor`de la classe ImgProc et une autre pour l'égalisation d'histogramme `equalizeHist`de la même classe.

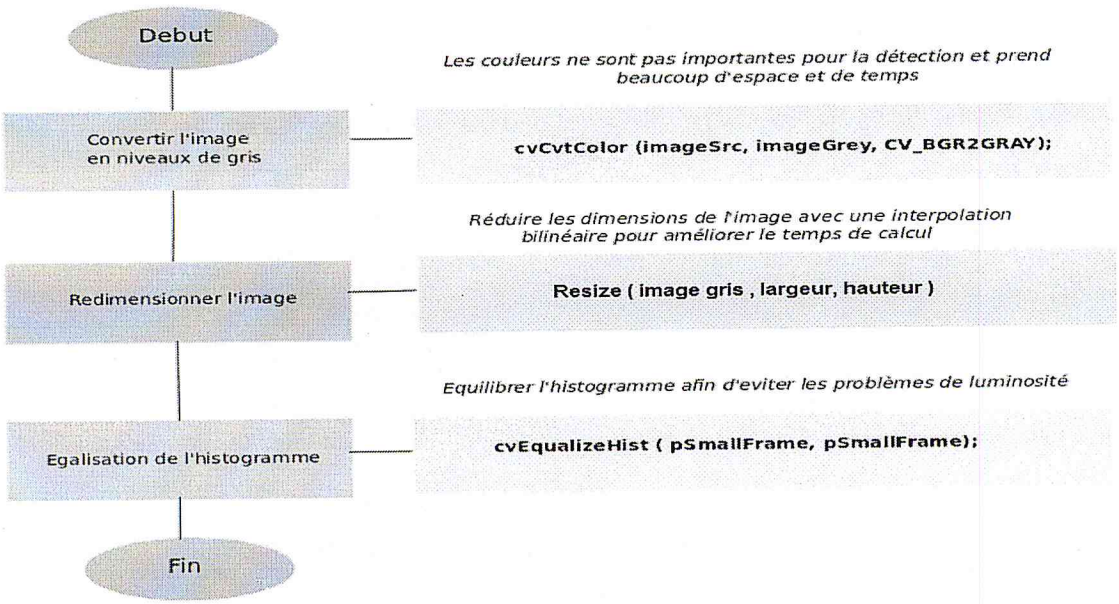


Figure IV.1 : Etapes et fonctions du prétraitement

5. Comment réaliser la reconnaissance faciale

Le problème de la reconnaissance faciale peut être défini comme suit : prenons une image de visage dont on souhaite déterminer l'identité de la personne correspondante. Pour ce faire, il est indispensable d'avoir des images de références avec lesquels on compare, ces images la vont former 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 est obtenue par la comparaison du vecteur de caractéristiques du visage à 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.

On prend un ensemble d'images de la base de données dans notre cas on a utilisé la base de données Yale qui contient différente prise pour chaque personne (9 images/personne) avec lunettes, sans lunette, souriant, en colère … ces images vont être transformé en vecteur

Figure IV.2 : Exemple du visage moyen, le premier eigenface et le dernier eigenface

Nous avons maintenant nos *eigenfaces, eigenvalues* et l'image du visage, ses données vont être stocké dans fichier XML avec la méthode `save()` avec en paramètre un chemin ou nous voulons mettre notre fichier, ce fichier `dataface.xml` représentera notre training set avec lequel on va faire la comparaison de nos images et nous permet aussi de ne pas refaire le calcul des *eigenfaces* à chaque fois qu'on relance le processus de reconnaissance qui diminue les performance. Dans le cas d'ajout d'une nouvelle personne à la base de données la méthode `Update ()` nous le permet sans recalculer tous les *eigenfaces*.

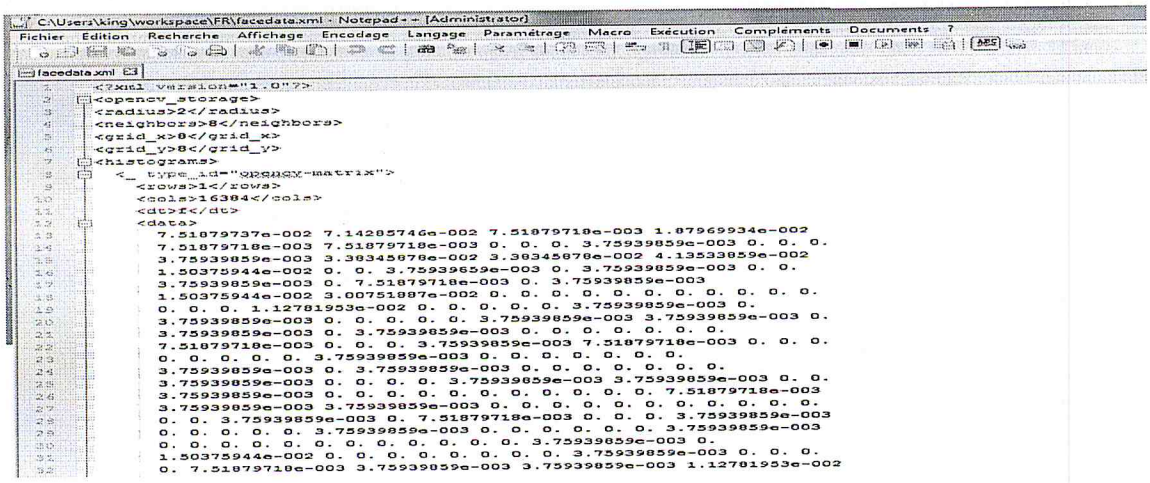


Figure IV.3 : Fichier XML dataface

Chaque image de visage sera associé à une chaine de caractère qui contient le nom de la personne comme sa on faisant la comparaison avec une image d'un individu X on dira que c'est la personne Y qui se trouve dans la base de données.

On fait l'apprentissage avec la fonction `Train()`en chargeant notre fichier dataface.xml et aussi le tableau contenant les nom des personne dans notre base de données

L'identification d'un nouveau individu se fait par le calcul de la distance euclidienne, fondamentalement, il vérifie le degré de similarité de l'image d'entrée avec chaque image de l'apprentissage et trouve la plus proche. La méthode `predict()` prend en paramètre l'image du visage de la personne à identifier et calcule la distance euclidienne par rapport aux autre visage et retourne l'image qui correspond le mieux.

6. Présentation de l'interface graphique

L'interface graphique de notre application contient le flux capturé par la webcam et deux buttons c'est une interface destinée aux utilisateurs, elle est simple et permet d'illustrer les Principaux processus de notre système de reconnaissance

Button Capture : Capture l'image du visage et l'enregistre dans la base de données.
Button Identifier : Identifier le visage de l'image capturé.
Button SelectDB : Sélectionner une base de données
Button SelectImg : Sélectionner une image a identifié

Dans notre Application il existe deux modes de reconnaissance, « Mode capture » capture le visage d'une personne se trouvant devant la caméra, ou par la sélection d'une image, après le lancement de notre application on remarque dans la figure suivante que le visage a bien été détecté, en cliquant sur « Capture » le système va prétraiter l'image capturé du visage détecté et l'enregistre dans un répertoire de test « Test Set ».

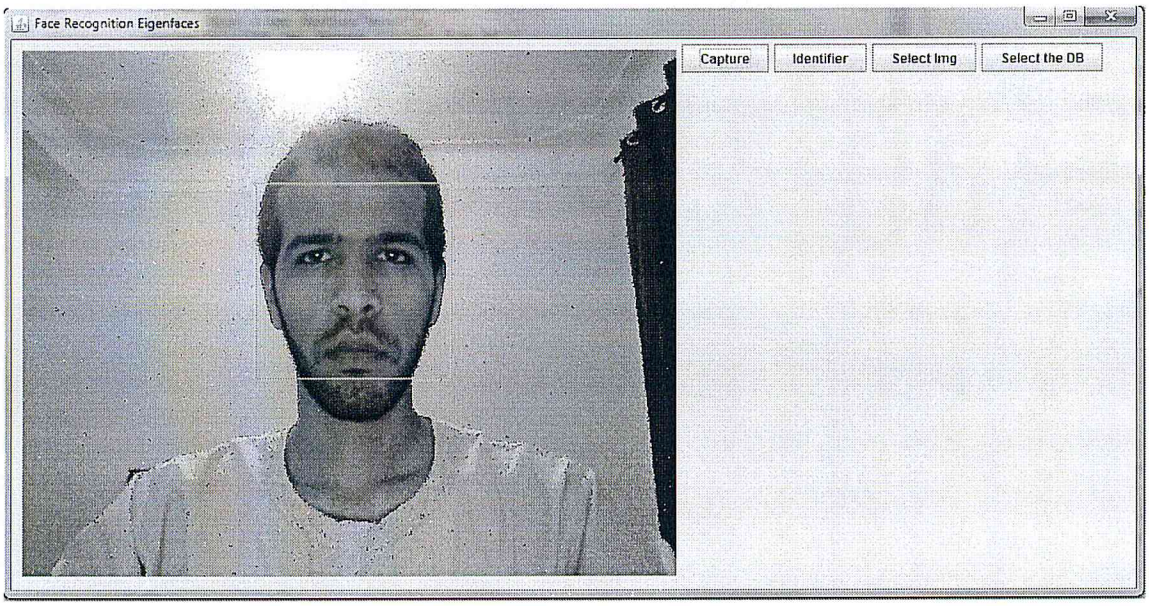


Figure IV.4 : Mode Capture

On passe au deuxième mode le « mode Select » Sélectionner une image de visage par le button « SelectImg » comme le montre la figure 4.5.

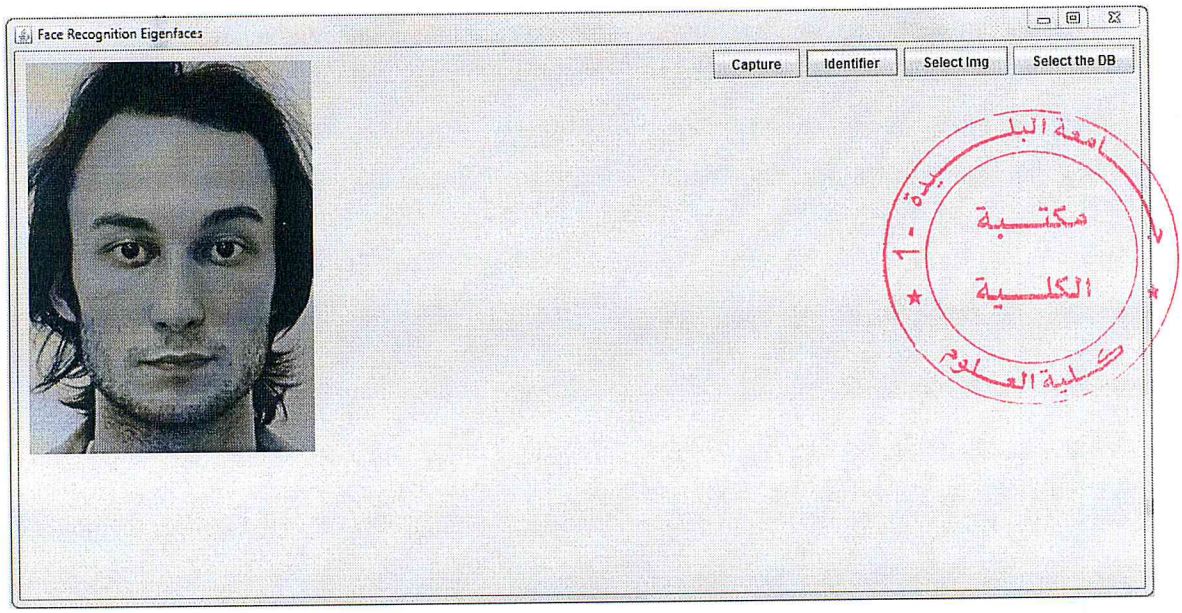


Figure IV.5 : Mode Select

Pour l'identification on a le button « Identifier » on cliquant dessus le programme affiche l'image correspondante a la personne à identifier qui se trouve dans la base de données.

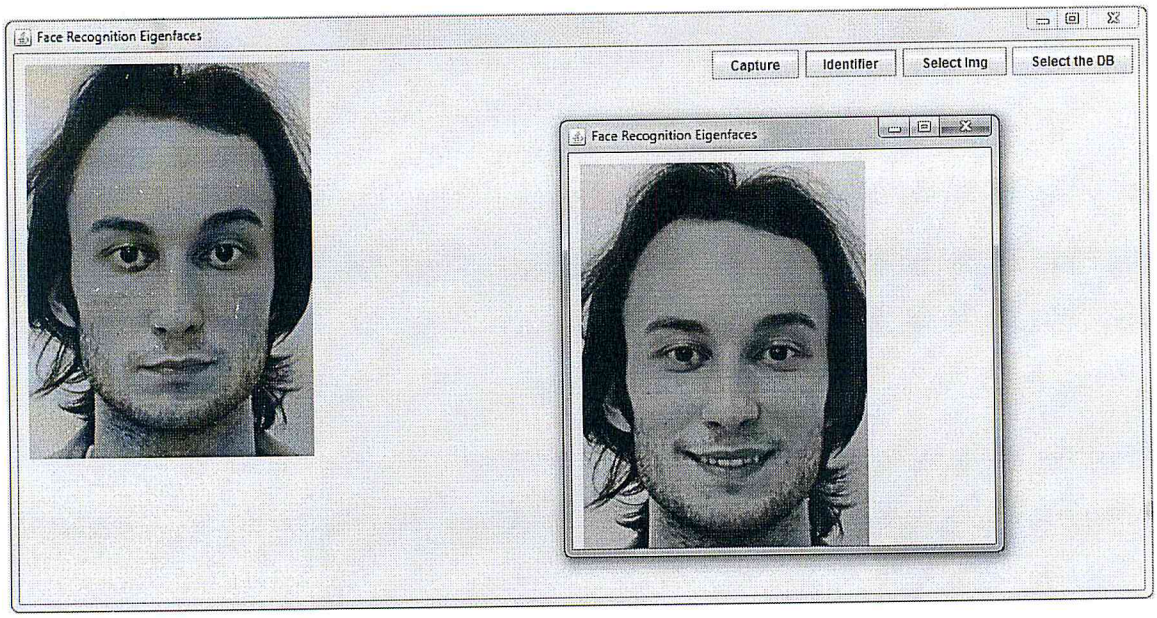


Figure IV.6 : Personne à identifier et l'image correspondante dans la base de données

Lorsque la personne à identifier n'a pas une image qu'il lui correspond dans la base de données le programme affiche une personne inconnu.

Figure IV.7 : Personne non identifié

7. Test et Resultat

Dans cette partie la base de données utilisée est la FEI face Database, est une base de données de visage qui contient un ensemble d'images de visage prises entre Juin 2005 et Mars 2006 au Laboratoire d'Intelligence Artificielle du FEI à São Bernardo do Campo, São Paulo, Brésil. Il existe14 images pour chacun des 200 individus, un total de 2800 images. Toutes les images sont colorées et prises sur un fond blanc homogène dans une position frontale droite avec profil rotation jusqu'à environ 180 degrés. L'Échelle peut varier d'environ 10% et la taille d'origine de chaque image est de 640x480 pixels. Tous les visages sont principalement représentés par les étudiants et le personnel de la FEI, entre 19 et 40 ans avec une apparence distincte, coiffure, et orne. Le nombre de sujets mâles et femelles est le même et égale à 100 [FEI].

a) Changement d'expression faciale

Pour la partie test changement d'expression faciale de notre application on s'est servis de la base de données FEI-1 de 400 images de 200 personnes (2 images/personne) taille 260*360chaque personne a 2 images une en souriant et l'autre sérieux on divise cette base de données en deux groupe, le premier contient les visages sérieux et le deuxième contient les visages souriant, le premier sera notre *TestSet* et l'autre sera le *TrainingSet*. La répartition des images : 240 images dans le Test Set, 160 images dans TrainingSet, 40 images de 20 personnes qui se trouve dans le *TestSet* n'ont pas de correspondance dans *TrainingSet* ceci pour pouvoir étudié le Faux accepté.

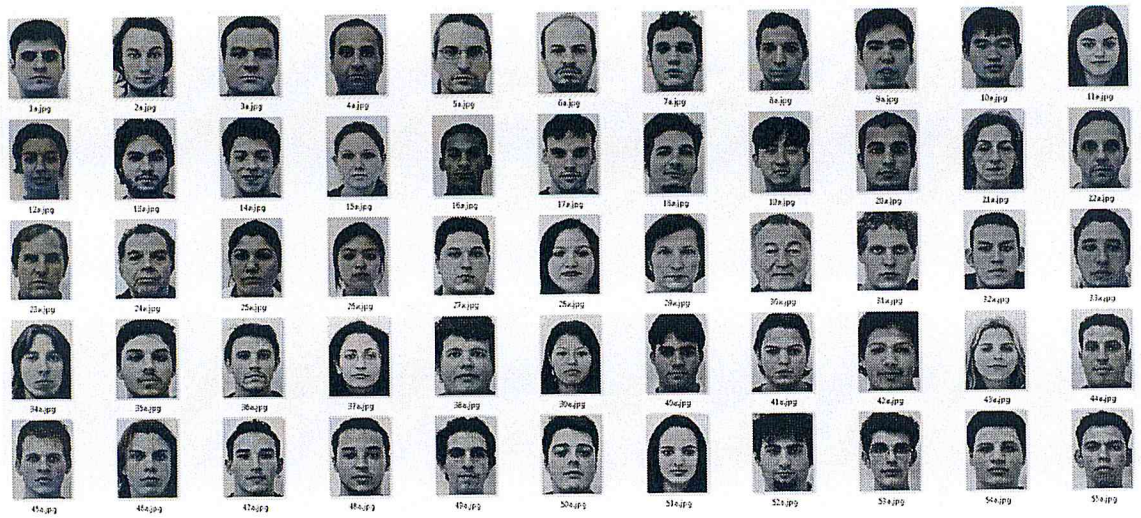


Figure IV.8 : Quelques images du TestSet(Base FEI-1)

Figure IV.9 : Quelques images du TrainingSet (base FEI-1)

Après la réalisation du 1er test de ces images-là, les résultats obtenus sont les suivant :

Base de données	Temps d'apprentissage	Temps de reconnaissance	Faux rejet	Faux accépté
FEI-1	9 sec	5 sec	0/220	34/40

Ces résultats ne reflètent pas un bon système de reconnaissance faciale, Après le changement du seuil de la distance euclidienne le meilleur résultat obtenu qui est équilibré entre le Faux rejet et le faux accepté est le suivant :

Base de données	Temps d'apprentissage	Temps de reconnaissance	Faux rejet	Faux accepté
FEI-1	9 sec	5 sec	26/220	9/40

Le test avec la base de données FEI-1 a donnée de bons résultats, seulement cette base de données ne détermine pas à elle seule que ce système est un bon système de reconnaissance car comme on le voit dans la figure 4.8 et la figure 4.9 cette base de données contient une seule différence faciale sérieux ou souriant, il reste les problèmes liée aux prises de vue.

b) Changement de pose

Pour cela on va utiliser une autre base de données qu'on appellera FEI-2 qui contient 50 personnes et différente poses pour chaque personne, dans cette partie on va effectuer deux tests, identification simple avec un seul exemple (rotation de 30 dégrée à gauche) de chaque personne dans le *TraningSet* et une identification multiple avec 6 exemples (rotation 30, 60,90 gauche et droite) de chaque personne.

Figure IV.10 : TrainingSet de l'identification Simple

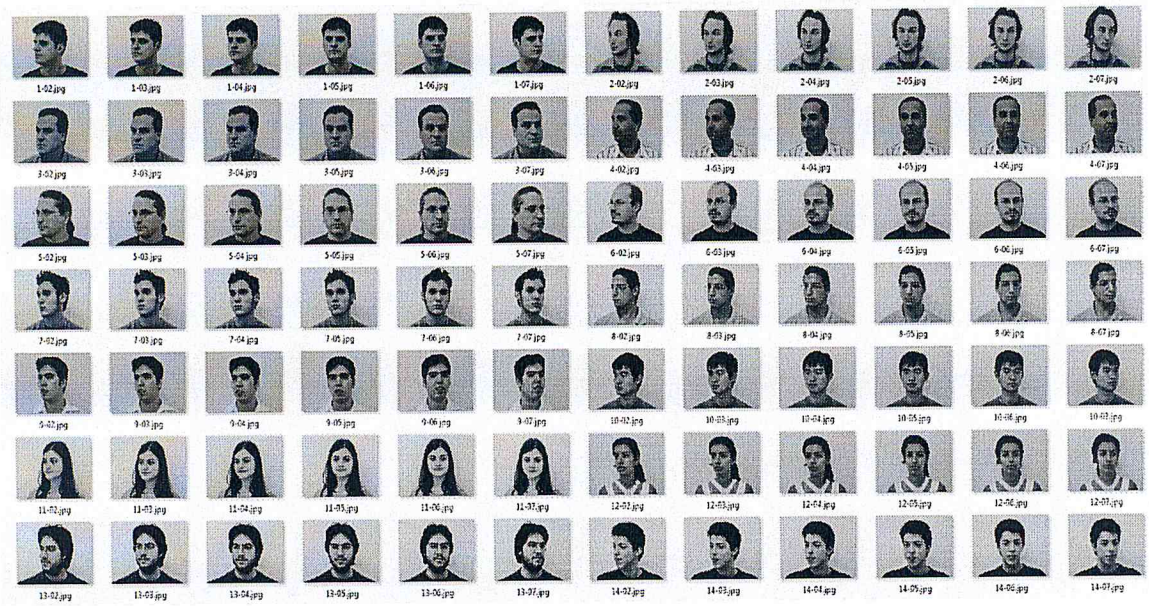


Figure IV.11 : TrainingSet de l'identification multiple

Base de données	Identification Simple	Identification multiple
FEI-2	65,7%	90,1%

On a remarqué que si le visage dépasse les 30 dégrée de la pose frontale avec une identification simple, la reconnaissance retourne toujours personne non reconnu alors qu'elle existe dans la base de données.

Avec l'identification multiple on a de très bon résultat sauf que l'inconvénient avec l'identification multiple c'est qu'on se retrouve avec une base de données importante d'où une augmentation dans le temps de calcul.

8. Conclusion

Dans ce chapitre nous avons vu l'implémentation d'une application de reconnaissance faciale, les outils utilisés tel qu'*OpenCV* qui offre plusieurs fonctionnalités intéressantes pour la vision par ordinateur. Peu de test ont été appliqué, Les tests réalisés montrent que la reconnaissance faciale a besoin plus d'étude et de travail pour améliorer les résultats obtenus.

Conclusion Générale

La biométrie est un domaine très intéressant et complexe. A l'aide de mathématique évolué elle nous permet de faire une distinction entre individus que ce soit par l'empreinte digitale, iris, ou le visage ce qui nous oblige 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.

L'objectif de ce travail est l'implémentation d'une application de reconnaissance faciale en utilisant les paramètres biométriques, pour y arriver nous avons utilisé la méthode de *viola and Jones* pour la détection de visage avec laquelle nous avons obtenu un taux de détection de 92,77%, concernant la reconnaissance de visage on a utilisé la méthode *Principal Compenent Analysis* qui se base sur les *eigenfaces*, une méthode connue par sa simplicité et son efficacité.

Les tests appliqués ont été effectués à l'aide de la base de données FEI, qui contient différentes images pour chaque personne, chaque image diffère d'une autre soit par un changement d'expression faciale ou changement de pose. Le meilleur résultat obtenu concernant le changement d'expression est un faux rejet de 11,8% et un faux accepté de 22,5%, en ce qui concerne le changement de pose nous avons effectué deux tests le premier par identification simple et le deuxième par identification multiple, on a obtenu un meilleur résultat avec l'identification multiple avec un taux de 90,1% d'identification exacte

Ces résultats restent acceptables en prenant en compte les inconvénients de cette technologie la prise de vue, le changement d'expression et la luminosité. De bons résultats ont été obtenus avec l'identification multiple mais l'inconvénient de l'identification multiple est le temps de calcul qui devient assez important 45 seconde pour l'apprentissage et 28 secondes pour la reconnaissance, ce temps peut être réduit par la diminution du nombre d'image de la base de données et plus important aussi par la réduction du nombre d'exemplaire d'images pour chaque personne. En ce qui concerne la variation de la luminosité peu de test ont été appliqués et ont donné de mauvais résultats.

Pour améliorer ce projet on propose l'idée de développer de nouvelles méthodes de prétraitement pour améliorer la qualité des données et rendre le module de prétraitement plus efficace concernant le changement de luminosité.

Ce projet nous a permis d'approfondir nos connaissances dans le domaine du développement d'une application complexe et aussi l'étude d'un algorithmere connu. Le but de ce travail est d'implémenter un prototype pour l'environnement *Android*, l'étape qu'on n'a pas réalisé ceci est due à une mauvaise décision de notre part c'est de développer une application pour l'environnement Windows et passer ensuite à l'environnement *Android*. Le principe et les outils utilisés pour le développement de notre application sont les même pour l'environnement *Android*, nous aurions aimé avoir plus de temps pour l'implémentation dans cet environnement, réaliser plus de test et également pour affiner l'interface de notre application Windows.

Bibliographie

[DON99] 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.

[FIS36] R. A. Fisher, « The use of multiple measurements in taxonomic problems », Annals of Eugenics, Vol. 7, p. 179-188, 1936.

[NIC06] 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), department d'electronique, 2006.

[HOL62] John Holland, « Outline for a logical theory of adaptive systems », Journal of the Association of Computing Machinery, 03/1962.

[AND10] Andre Bouchier « L'analyse Discriminente linéaire: LDA »

[HAR73] R. O. Duda, P. E. Hart, « Pattern Classification and Scene Analysis », John Wiley and Sons, New York, 1973.

[CHO95] 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, 12/1995.

[DID92] 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.

[GOL89] D.E. Goldberg, « Genetic Algorithms in Search, Optimization and Machine Learning », Reading MA Addisonn Wesley, 1989.

[SIM76] E. Diday, J. C. Simon, « Cluster Analysis », dans Digital Pattern Recognition, (K. S. FU edition), P 47-94, Springer – Verlag, Berlin, 1976.

[CLU12] CLUB DE LA SECURITE DES SYSTEMES D'INFORMATION FRANÇAIS « Technique de contrôle d'accès par biométrie » (2012).

[IBG12] International Biometric Group: « Summary description of and future projections for the biometrics industry » (2012)

[MES99] K. Messer, J. Matas, J. Kittler, J. Luettin, and G. Maitre. XM2VTSDB: « The Extended M2VTS Database ». In Proceedings, International Conference on Audio- and Video-Based Person Authentication. P 72–77, 1999.

[NIC09] Nicolas Morizet : « Reconnaissance Biométrique par Fusion Multimodale du Visage et de l'Iris ». Paris, France, l'Ecole Nationale Supérieure des Télécommunications, 2009.

[LOR09] Lorene Alano : « La Biométrie multimodale : stratégies de fusion de scores et mesures de dépendance appliquées aux bases de personnes virtuelles ». Paris, France, INSTITUT NATIONAL DES TELECOMMUNICATIONS, 2009.

[MAT05] Matthieu Wirotius : « Authentification par signature manuscrite sur support nomade ». France, Université François Rabelais Tours, 2005

[OUA12] OUAMANE Hanane, « Identification de reconnaissance faciale avec des expressions » Mémoire de Fin d'Etudes Master Université Mohamed Khider Biskra, 07/06/2012

[PHI20] P. J. Philips, H. Moon, S. A. Rizvi, P. J. Rauss, « The FERET evaluation methodology for face-recognition algorithms », IEEE Trans. On Pattern Analysis and Machine Intelligence, vol. 22, no.10, pp.1090-1100, 2000.

[SIR87] L. Sirovitch and M. Kirby « Low dimensional procedure for characterization of human faces »03/1987, 519-524.

[BRU03] Bruce A. Draper,Kyungim Baek,Marian Stewart Bartlett,and J. Ross Beveridge « Recognizing faces with PCA and ICA », 11/02/2003

[MAT91] Matthew Turk and Alex Pentland « Eigenfaces for Recognition » in "Journal of cognitive science" Vol. 3, Num 1, Massachusetts Institute of Technology, 1991.

[ABH12] Abhishek Singh, « Face Recognition Using PCA and Eigen Face Approach » Bachelor of Technology degree project, 2012.

[SOU11] SOUHILA GUERFI « Authentification d'individus par reconnaissance de caractéristiques biométriques liées aux visages 2D/3D » 13/09/2011.

[IET20] IET, Visual Biometrics (Ref. No. 2000/018), Pages : 11/1 - 11/6, 2000.

[ANT13] Md. Abdur Rahim, Md. Najmul Hossain, Tanzillah Wahid & Md. ShafiuAzam « Face Recognition using Local Binary Patterns » (LBP) Pabna University of Science and Technology, Bangladesh 2013.

[PAW06] Pawan Sinha, Benjamin Balas, Yuri Ostrovsky, and Richard Russell « Face Recognition by Humans: Nineteen Results All Computer Vision Researchers Should Know About»

[ANI11] Anil K. Jain, Arun Ross and Salil Prabhakar « An Introduction to Biometric Recognition », 2011

[MIC11] Michael Zollhöfer, Michael Martinek, Günther Greiner, Marc Stamminger, Jochen Süßmuth « Automatic Reconstruction of Personalized Avatars from 3D Face Scans »2011

[BET14] BETTAHAR Abdessettar, SABER Fathi, « Extraction des caractéristiques pour l'analyse biométrique d'un visage » Université Kasdi merbah Ouergla 15/06/2014

[DIY13] Face tracking : implémentation de la méthode de Viola & Jones en C++ http://www.firediy.fr/article-18.html 15/03/2013

[CLU] Claudine Guerrier, Laure-Anne Cornelie, CLUSIF (CLUB de la Sécurité des systèmes d'Information Français.) « Les aspects juridiques de la biométrie ».

[RAN] Woodward J.D. & al, RAND Public Safety and Justice, « Biometrics, a Look at Facial Recognition ».

[AUT] Authentication technologies http://biometrics.pbworks.com/w/page/14811351/Authentication%technologies

[BIO] www.biometrie-online.net : « Les Technologies Biométriques : principe de fonctionnement ». http://www.biometrie online.net/technologies/fonctionnement

[FER] Le site web de la base de données Color FERET « http://www.nist.gov/humanid/colorferet ».

[YAL] Le site web de la base de données Yale « http://vision.ucsd.edu/content/extended-yale-face-database-b ».

[FAC] Face Recognition Home Page. « http://wwww.face rec.org/databases/ ».

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

[OCV] OpenCV site officiel « opencv.org ».

[ACC12] Jean François Mainguet « Accurancy / Précision » 13/04/2012 http://fingerchip.pagesperso-orange.fr/biometrics/accuracy.htm

[WIK] Article de l'encyclopédie libre Wikipedia La method de Viola and Jones http://fr.wikipedia.org/wiki/ Méthode_de_Viola_et_Jones.

[WIK1] Article de l'encyclopédie libre Wikipedia La biométrie http://fr.wikipedia.org/wiki/Biométrie

[WIK2] Article de l'encyclopédie libre WikipediaEclipse (projet) fr.wikipedia.org/wiki/Éclipse.

[WIK3] « Article de l'encyclopédie libreWikipediaMultimodal Biometric System » http://en.wikipedia.org/wiki/Biometrics#Multimodal_biometric_system.

[GBI] Groupe BIOSÉCUR Inc. Qu'est-ce que la biométrie http://groupebiosecur.com/index.php/biometrie

[BOU] Boudjellal Sofiane, « Détection et identification de personne par méthode biométrique » Mémoire en Electronique Magister, Université Mouloud Maameri, Tizi Ouzou UMMTO

[TPE] Biométrie TPE 02/02/2009 http://biometrie-tpevh.blogspot.co.uk/

[FEI] http://fei.edu.br/~cet/facedatabase.html

Résumé

Au cours des dernières années, beaucoup de personne s'intéressent à la biométrie et ce qu'ils peuvent faire avec. La biométrie se divise en trois catégories selon le type de données biométrique, catégorie biologique, comportementale et morphologique, à l'aide de l'une de ses technologies biométriques est née l'idée de la reconnaissance faciale.

La reconnaissance faciale présente un problème difficile dans le domaine de l'analyse d'image et la vision par ordinateur, et en tant que telle, elle a reçu beaucoup d'attention au cours des dernières années en raison de ses nombreuses applications dans divers domaines. Il existe beaucoup de méthodes pour réaliser un système de reconnaissance faciales, ses méthodes se divisent en deux, méthodes global et méthodes locales, l'une de ses méthodes globales est la méthode ACP, dans ce document on a étudié d'autres méthodes mais on s'est basé sur la méthode ACP, comment elle fonctionne et l'implémentation d'un prototype en s'en servant de cette méthode.

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 les visages de personnes différentes ont généralement la même forme et varient du fait des conditions d'éclairage, de la variation de pose, et des expressions faciales.

Abstract

In the last years, many people are interested in biometrics and what they can do with it. Biometrics is divided into three categories according to the biometric data type, biological category, behavioural and morphological; using one of this biometrics technology was born the idea of facial recognition.

Facial recognition presents a difficult problem in the field of image analysis and computer vision, and as such, it has received much attention in recent years because of its many applications in various fields. There are many ways to make a facial recognition system, its methods are divided into two, global methods and local methods, one of its global methods is the PCA method, in this paper, we will study other methods but we will base on the PCA method, how it works and the implementation of a prototype using this method.

Despite the many approaches and methods that have been proposed to solve the human face recognition problem, it remains an extremely difficult problem, this is due to the fact that the face of different people generally have the same shape and varies due to the conditions lighting, the change in pose, and facial expressions.

ملخص

في السنوات الأخيرة، العديد من الناس مهتمون في القياسات الحيوية وما يمكن أن تفعله حيال ذلك .وتنقسم القياسات الحيوية إلى ثلاث فئات وفقا لنوع البيانات البيومترية، الفئة البيولوجية والسلوكية والمورفولوجيا، وباستخدام واحدة من التقنيات البيومترية ولدت فكرة التعرف على الوجه.

يقدم التعرف على الوجه مشكلة صعبة في مجال تحليل الصور والرؤية الحاسوبية، وعلى هذا النحو، أنها تلقت الكثير من الاهتمام في السنوات الأخيرة بسبب العديد من التطبيقات في مختلف المجالات.هناك العديد من الطرق لتطوير نظام التعرف على الوجه، وتنقسم الطرق إلى قسمين، الطرق الشاملة وطرق الموضعية، واحدة من الأساليب الشاملة هو الأسلوب اي سي بي، في هذه المذكرة درسنا طرقا أخرى وقد اعتمدنا في ذلك على أسلوب اي سي بي، وكيف يعمل وتنفيذ نموذج باستخدام هذا الأسلوب.

على الرغم من العديد من الأساليب والطرق التي تم اقتراحها لحل مشكلة التعرف على الوجوه البشرية، فإنه لا يزال يمثل مشكلة صعبة للغاية، ويرجع ذلك إلى حقيقة أن مواجهة مختلف الناس عموما لديهم نفس الشكل وتختلف نظرا لظروف الإضاءة، وتغيير في الوقفة، وتعبيرات الوجه .