République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Saad Dahlab Blida

Faculté des sciences

Département d'informatique

Mémoire Présenté par :

Benrachedi Sidahmed

En vue d'obtenir le diplôme de master

Domaine : Mathématique et informatique

Filière : Informatique
Spécialité : Informatique
Option : Ingénierie de logiciel

Sujet :

Détection automatique par application de la vidéosurveillance intelligente

Soutenu le :

Mme. BENBLIDIA Nadjia	Promotrice
Mme. REGUIEG F.Zohra	Encadrante
Mme. BOTOUMI . B	Président
Mme. REZOUG . N	Examinateur
Mr. ZAIR . M	Examinateur

Promotion
2014 / 2015

Remerciement

En premier lieu, je tiens à exprimer mon plus vifs remerciements à mon promotrice Mme BENBLIDIA Nadjia qui m'a guidés dans le choix du thème et qui suivi mon travail tout au long de son exécution malgré ses nombreuses charges. Sa compétence, sa rigueur scientifique.

Je tiens à remercier tous ceux qui ont contribué à ce travail parfois sans le savoir ou du moins sans mesurer la portée de leur influence.

Un grand merci aux membres du jury qui ont accepté d'évaluer et examiné mon travail.

Enfin, je remercier aussi tous les professeurs qui m'a soutenu durant mon formation à l'université, et tous ceux qui m'aidé à l'élaboration de ce mémoire

Dédicaces

A l'aide de DIEU tout puissant, qui trace le chemin de ma vie, j'ai pu arriver à réaliser ce modeste travail que je dédie:

A ma très chère mère celle a qui je souhaite une longue vie et bonne santé ;

A mon père qui n'a pas cessé de m'encourager

A mes Sœurs

Et

A mes frères

A ma famille et a tous mes amis

Sommaire

Introduction générale 1

Chapitre I : GENERALITES SUR LA BIOMETREIE --

I.1. Introduction 04

I.2 Caractéristiques Communes des Systèmes Biométriques 04

I.3 Les Techniques Biométrie 04

I.3.1 Biométriques physiologiques 05

I.3.2 Biométriques comportementales 05

I.4 Application de la Biométrie 05

I.5 Présentation des systèmes biométriques 05

I.5.1 Les systèmes basés sur l'analyse morphologique 06

I.5.2 Les systèmes basés sur l'analyse comportementale 11

I.6 Comparaison entre les systèmes biométriques 11

I.7 Systèmes de reconnaissance de visage 12

I.8 Mesure de performance d'un système biométrique 15

I.9 Conclusion 16

CHAPITRE II : TECHNIQUES DE DETCTION ET DE RECONNAISSANCE DE VISAGES --

II.1. Introduction 18

II.2. Détection de visages 18

II.3. Les Approches de la détection de visage 18

II.3.1. Approches basées sur l'apparence 18

II.3.2. Approches basées sur les connaissances acquises 19

II.3.3 Approches basées sur le « Template- matching » 20

II.3.4 Approches basées sur des caractéristiques invariantes 22

II.3.4.1 Méthodes basées sur les caractéristiques du visage 23

II.3.4.2. Méthodes basées sur l'analyse de la couleur de la peau 23

II.4. Les Approches de la reconnaissance de visage 24

II.4.1. Méthodes holistiques ou globales 24

II.4.1.1 Analyse en Composantes Principales 24

II.4.1.2 Analyse Discriminante Linéaire 25

II.4.1.3 Le réseau de neurones 25

II.4.1.4 Avantages et inconvénients des méthodes globales 25

II.4.2. Méthodes locales 26

II.4.2.1 Approches géométriques 26

II.4.2.2 Approches basées sur les graphes 27

II.4.2.3 Avantages et inconvénients des méthodes locales 27

II.4.3. Méthodes Hybrides 28

II.5 Conclusion 29

CHAPITRE III : CONCEPTION ET ARCHITECTURE DU LOGICIEL --

III.1 Introduction 31

III.2 Détection de visages sur le téléphone portable 31
III.3 Méthode de Viola et Jones 33
III.3.1 Caractéristiques pseudo-haar 34
III.3.2 Approche d'image intégrale 34
III.3.3 Algorithme AdaBoost 35
III.3.4 Algorithme en cascades de classifieurs 35
III.4 Reconnaissance des visages sur le téléphone portable 36
III.5 Des limites sur le téléphone portable 36
III.6 La structure du système 37
III.7 Vidéosurveillance intelligente : 37
III.8 Systèmes de vidéosurveillance avec caméras IP 38
III.9 Architecture des systèmes de vidéosurveillance intelligente 38
III.9.1 Architecture centralisée 38
III.9.2 Architecture distribuée 40
III.10 Communication dans les systèmes distribués 41
III.10.1 Protocoles TCP et UDP 41
III.10.2 Les sockets 42
III.11 Sécurité des réseaux 42
III.12 Définition du modèle client/serveur 43
III.12.1 Caractéristiques des systèmes client-serveur 43
III.12.2 La répartition des tâches 44
III.12.3 Les différents modèles de client/serveur 45
III.12.4 Présentation de l'architecture de système 45
III.13 Conception et Modalisation 47
III.13.1 Langage de modélisation 47
III.13.2 Diagramme de cas d'utilisation 47
III.13.3 Description du diagramme de cas d'utilisation 48
III.13.4 Diagramme de séquence 49
III.13.5 Diagramme de classes 51
III.13.6 Description des classes 51
III.14 Conclusion 52
CHAPITRE IV : IMPLEMENTATION --
IV.1 Introduction 54
IV.2 L'application sur le téléphone portable 54
IV.3 Environnement du travail 54
IV.3.1 Environnement matériel 54
IV.3.2 Environnement logiciel 55
IV.4 Interfaces graphique de l'application 58
IV.5 Résultats des expériences 63
IV.6 Conclusion 64
Conclusion Générale 66

Liste des figures

Figure I.1 : Acquisition de la forme de la main 6

Figure I.2 : L'iris d'œil 7

Figure I.3 : la rétine 8

Figure I.4 : Signal vocal 9

Figure I.5 : Empreinte digitale 10

Figure I.6 Signature 11

Figure I.7. Comparaison des différentes modalités selon quatre critères principaux : l'intrusivité, le pouvoir discriminant, le coût et l'effort [09] 12

Figure I.8: Système de reconnaissance..... 13

Figure I.9: Relation entre TFA et TFR 16

Figure II.1 Modèle de visage composé de 16 régions (les rectangles) associées à 23 relations (flèches) 21

Figure II.2 Différentes régions utilisées pour la phase de template matching..... 22

Figure III.1 : Schéma de la chaine de décision:..... 32

Figure III.2 : (a) Le classificateur simple en cascade ; (b) Le classificateur multiple en cascade ; (c) Le classificateur des arbres 33

Figure III.3: Exemples des caractéristiques pseudo-haar d'après [44,49]..... 34

Figure III.4: image intégrale : (a) la valeur de l'image intégrale à la position (u, v), (b) calcul de la somme des valeurs de pixels dans le rectangle Θ d'après [44,49]. 34

Figure III.5: La chaine de classifieurs en cascade..... 36

Figure III.6 : La structure générale du système ..... ;;..... 37

Figure III.7 : système centralisé à base de DVR [57].(Les fonctionnalités d'intelligence se situent dans le DVR). 39

Figure III.8 : système centralisé à base d'un PC serveur [57]. (Les fonctionnalités d'intelligence sont dans le serveur). 40

Figure III.9 : système distribué, caméras IP [57]..... 41

Figure III.10 : Le modèle client/serveur 43

Figure III.11 : Architecture a 2 niveaux 46

Figure III.12 : Architecture a 3 niveaux 46

Figure III.13 : Diagramme de cas d'utilisation « Authentification » 47

Figure *III.14* : Diagramme de cas d'utilisation « administrateur » 48

Figure III.15 : Diagramme de cas d'utilisation « utilisateur »..... 48

Figure III.16 : Diagramme de séquence « Authentification »..... 49

Figure III.17 : : Diagramme de séquence « l'ajout d'une personne »..... 50

Figure III.18 : : Diagramme de séquence « Reconnaissance »..... 50

Figure III.19 : Diagramme de classes 51

Figure IV.*1 :* Une vue générale de librairie OpenCV [42] 56

Figure IV.*2 :* : La structure de la librairie OpenCV [43] 57

Figure IV.*3 :* Interface Login 59

Figure IV.*4 :* Interface Principale 60

Figure IV.*5 :* Interface de détection 60

Figure IV.*6 :* Interface de formulaire 61

Figure IV.*7 :* l'interface de Reconnaissance 62

Figure IV.*8 :* l'interface de La Base de données 63

CHAPITRE I

GENERALITES SUR LA BIOMETREIE

I.1 Introduction

L'identité est une notion qui existe depuis toujours. C'est une notion philosophique liée à l'âme et la personnalité de chaque individu. Les sociétés modernes ont besoin d'identifier les individus qui les composent, ce qui implique de disposer de "DESCRIPTEURS" de cette identité. L'identité est définie à la naissance par un nom et des données personnelles (date et lieu de naissance, famille, domicile, numéro de sécurité sociale ...) ; elle est de plus en plus vérifiée au cours de la vie d'un individu. Afin de sécuriser les transactions et les déplacements, chaque personne a pour besoin de déclarer et de laisser vérifier son identité à de nombreuses occasions (frontières, compte bancaire, accès à des endroits réservés ...). De nombreux moyens d'identification existent, ils étaient autrefois "humains", ils sont aujourd'hui devenus "numériques" et "automatiques". La **BIOMETRIE** est le moyen d'identification le plus complet car elle relie de plus en plus une identité à une personne physique au moyen de caractéristiques propres, qu'elles soient physiques ou comportementales.

I.2 Caractéristiques Communes des Systèmes Biométriques

La caractéristique commune à des systèmes biométrique est les suivantes :

- **Universalité :** chaque personne visée par le système doit avoir cette caractéristique.
- **Unicité :** unique pour chaque individu.
- **Permanence :** ne doit pas avoir un grand changement pour une période restreinte.
- **Mesurabilité :** les caractéristiques doivent être faciles à mesurer
- **Acceptation par le public :** la mesure des caractéristiques ne doit pas poser des problèmes aux utilisateurs.
- **La non-reproductibilité :** concerne la facilité ou non à falsifier une modalité biométrique.

I.3 Les Techniques Biométrie

Une des définitions de la biométrie est donnée par Roethenbaugh [24] : « La biométrie s'applique à des particularités ou des caractères humains uniques en leur genre et mesurables, permettant de reconnaître ou de vérifier automatiquement l'identité ». Mais Aucune modalité biométrique n'est en elle-même fiable à 100 %. Il existe des problèmes, liées aux dispositifs de capture des données, à l'utilisateur lui-même ou au condition lors de la capture, dans

lesquelles une modalité quelconque peut s'avérer défaillante. Parmi les principales modalités biométriques physiologiques et comportementales.

I.3.1 Biométriques physiologiques

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

I.3.2 Biométriques comportementales

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

I.4 Application de la Biométrie

Le champ d'application de la biométrie couvre potentiellement tous les domaines de la sécurité où il est nécessaire de connaître l'identité des personnes Aujourd'hui, les principales applications peuvent être divisées en trois groupes principaux :

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

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

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

I.5 Présentation des systèmes biométriques

Aucune biométrie unique ne pouvait répondre efficacement aux besoins de toutes les applications d'identification. Un certain nombre de techniques biométriques ont été proposées, analysées, et évaluées. Chaque biométrie à ses forces et ses limites, et en

conséquence, chaque biométrie est utilisée dans une application particulière. Pour les caractéristiques physiques, nous décrirons la reconnaissance de visage, les empreintes digitales, la géométrie de la main et l'iris. Pour les caractéristiques comportementales, nous décrirons les biométries basées sur la voix et la signature.

I.5.1 Les systèmes basés sur l'analyse morphologique

- La reconnaissance de la main

Ce type de mesure biométrique est très répondu, notamment aux Etats-Unis. Il représente 10% des applications, il s'appuie sur une image en trois dimensions de la main. Cela consiste à mesurer plusieurs caractéristiques de la main jusqu'à 90 attributs telles que sa forme, sa longueur, la largeur des doigts, les formes des articulations, etc.

Figure I.1 Acquisition de la forme de la main

Avantages

- Simplicité et facilité d'intégration.
- Bien acceptée par le public.
- Les capteurs ont connu une grande évolution depuis les lecteurs mécaniques jusqu'aux lecteurs en silicium qui capturent des images en 3D (Figure I.1).

Inconvénients

- La présence des bagues et des bandeaux influent sur les performances du système.
- Technologie sensible aux modifications de la forme de la main que peut provoquer le vieillissement ou encore le régime.
- Le capteur est quelque peu encombrant.

- La reconnaissance de l'iris

L'utilisation de l'iris comme caractéristique biométrique unique de l'homme a donné lieu à une technologie d'identification fiable et extrêmement précise. L'iris est la région, sous forme

d'anneau, située entre la pupille et le blanc de l'oeil, il est unique. L'iris a une structure extraordinaire et offre de nombreuses caractéristiques de texture qui sont uniques pour chaque individu. Les algorithmes utilisés dans la reconnaissance de l'iris sont si précis que la planète toute entière pourrait être inscrite dans une base de données de l'iris avec peu d'erreurs d'identification.

L'image de l'iris est généralement capturée à l'aide d'une caméra standard. Cependant, cette étape de capture implique une coopération de l'individu. De plus, il existe plusieurs contraintes liées à l'utilisation de cette technologie. Par exemple, il faut s'assurer que l'iris de l'individu est à une distance fixe et proche du dispositif de capture, ce qui limite l'utilisation de cette technologie.

Frank Burch est le premier ophtalmologiste ayant proposé cette solution en 1936 suivi par Flom et Safir qui ont montré que les iris (Figure I.2) de deux individus sont distinctifs [03]. En 1993, le premier système basé sur l'identification par l'iris a été mis en œuvre par Defence Nuclear Agency [04].

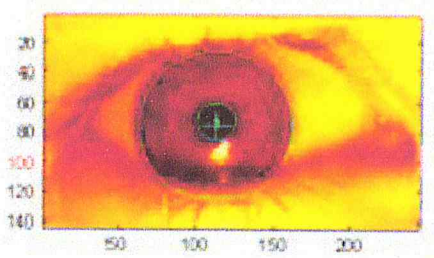


Figure I.2 L'iris d'œil

Avantages

- Donne un grand nombre de caractéristiques.
- Elle est très sécurisée (difficilement falsifiable).
- Les caractéristiques de l'iris sont inchangeables pendant toute la vie (après l'adolescence).
- Elle peut différencier entre les jumeaux et même l'oeil gauche de l'oeil droit.

Inconvénients

- Méthode intrusive.
- Très sensible à l'environnement, et nécessite une collaboration des utilisateurs.
- Les capteurs sont très couteux.

- **La reconnaissance de 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 oeil face à un orifice de capture situé sur le dispositif d'acquisition. Un faisceau lumineux traverse l'oeil 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 oeil extrêmement près de la caméra [39].

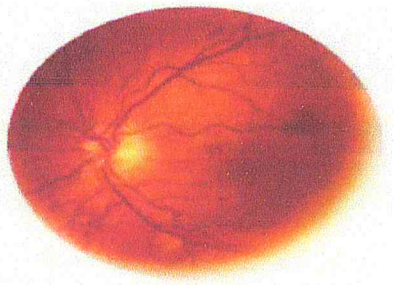


Figure I.3 la rétine

Avantages

- Donne de bonnes performances à cause de la stabilité du schéma sanguin.
- Il est presque impossible de la falsifier (destruction des vaisseaux sanguines trop rapidement après la mort).

Inconvénients

- La mesure est effectuée à petite distance (impossible d'effectuer une mesure à plus de trente centimètres).
- Mauvaise acceptation par le public.

- **La reconnaissance vocale**

C'est en 1962 que Lawrence Kersta, un ingénieur des Bell Laboratoires, a établi que la voix de chaque personne est unique et qu'il est possible de la représenter graphiquement. C'est dans les années 80 que les premiers systèmes de reconnaissance vocale apparaissent. En 2000, cette technique biométrique détenait 4,3% du marché international [05].

Figure I.4 Signal vocal

Avantages

- Technique facile à implémenter.
- C'est la seul technique qui nous permet une identification à distance sans la présence physique de la personne (réseau téléphonique).

Inconvénients

- Facile à falsifier par l'enregistrement.
- Sensible à l'environnement (bruit, qualité des capteurs, l'état physique et émotionnel de la personne).
- Ne donne pas toujours de bonnes performances.

- **La reconnaissance du visage**

Le visage est certainement la caractéristique biométrique que les humains utilisent le plus naturellement pour s'identifier entre eux. Le premier système semi-automatique a été développé aux années 1960 pour la localisation des caractéristiques du visage. En 1970, le premier système automatique pour l'identification a été mis au point par Golstein, Harmon et Lesken 1988 (www.ezinearticles.com). Une nouvelle approche (Eigen Faces) proposée par Kirby et Sirovich [06] a montré beaucoup d'avantages au niveau de la vitesse et de l'efficacité de la reconnaissance.

Avantages

- Méthode approuvée par les utilisateurs.
- Il y a une possibilité d'effectuer une identification à distance (petite distance).
- Possibilité d'effectuer une identification à partir d'une séquence vidéo.

Inconvénients

- Très sensible à l'environnement (éclairage, positionnement de la caméra, port des lunettes, arrière-plan, barbe, etc.).
- Des fois, il est impossible de différencier entre les jumeaux.
- Influence du vieillissement sur les performances des systèmes.

- La reconnaissance des empreintes digitales

La reconnaissance des empreintes digitales (Figure I.5) est la technique biométrique la plus ancienne et c'est l'une des plus matures. Galton est le premier qui a classé les dessins formés par les lignes papillaires (arrêts de lignes, bifurcations, lacs, ilots, branchements, crochets, ponts, etc.). La combinaison de ces classes donne un nombre infini de possibilités [03].

Figure I.5 Empreinte digitale

Avantages

- La Taille du capteur est petite ce qui facilite son intégration.
- Les capteurs sont moins couteux.
- Un bon compromis entre le TFR et le TFA.
- Le taux de ressemblance des empreintes peut atteindre 1/64 milliards [07].
- C'est la méthode la plus reconnue par le public.

Inconvénients

- Sensibilité à l'état du doigt (propre, humide ou sec, etc.).
- Peut-être falsifié en utilisant un doigt moulé (pour éviter ce problème, certains systèmes intègrent un module pour la détection du doigt vivant).
- Inadaptable pour les personnes qui travaillent avec des produits chimiques ou qui ont des blessures au niveau des empreintes.

I.5.2 Les systèmes basés sur l'analyse comportementale

- La reconnaissance de la signature

Il s'agit d'une analyse comportementale où différents éléments (mesure da la vitesse, ordre d'écriture, pression exercée, accélération…) sont mesurés lors de la signature. La falsification est possible en passant par une phase d'apprentissage, la signature peut carier selon le stress de l'utilisateur [40].

Figure I.6 Signature

- Frappe au clavier

L'utilisation de matériels informatiques a également suscité un intérêt pour la biométrie. Par exemple, les travaux de Monrose et Rubin [08] ont montré qu'il est possible de reconnaître une personne au rythme de sa frappe sur un clavier. Cette méthode présente l'avantage de permettre une identification continue de l'utilisateur et de détecter un changement d'utilisateur en temps réel et de façon transparente.

I.6 Comparaison entre les systèmes biométriques

La figure suivante résume une analyse comparative entre les systèmes biométriques selon la précision, l'indiscrétion, l'effort imposé à l'utilisateur et aussi le cout [09]. Les critères qui ont un grand pourcentage dans chaque système sont représentés à l'intérieur (approximation au point de centre).

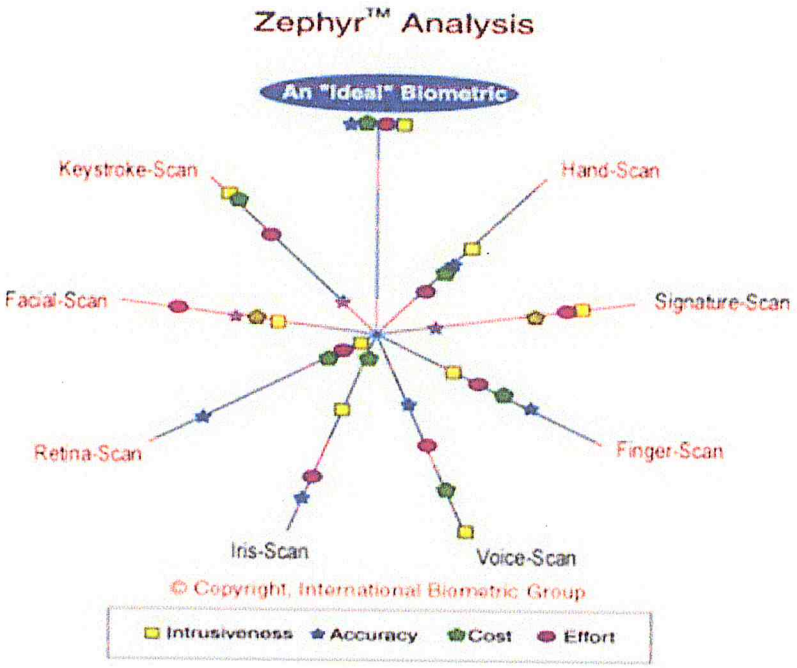


Figure I.7 Comparaison des différentes modalités selon quatre critères principaux : l'intrusivité, le pouvoir discriminant, le coût et l'effort [09]

I.7 Systèmes de reconnaissance de visage

Le système de reconnaissance exploite les caractéristiques du visage ainsi extraites pour créer une signature numérique qu'il stocke dans une base de données. Ainsi, à chaque visage de la base est associée une signature unique qui caractérise la personne correspondante.

La reconnaissance d'un visage requête est obtenue par l'extraction de la signature requête correspondante et sa mise en correspondance avec la signature la plus proche dans la base de données. La reconnaissance dépend du mode de comparaison utilisé : vérification ou identification. On peut représenter les systèmes de reconnaissance par la figure suivant

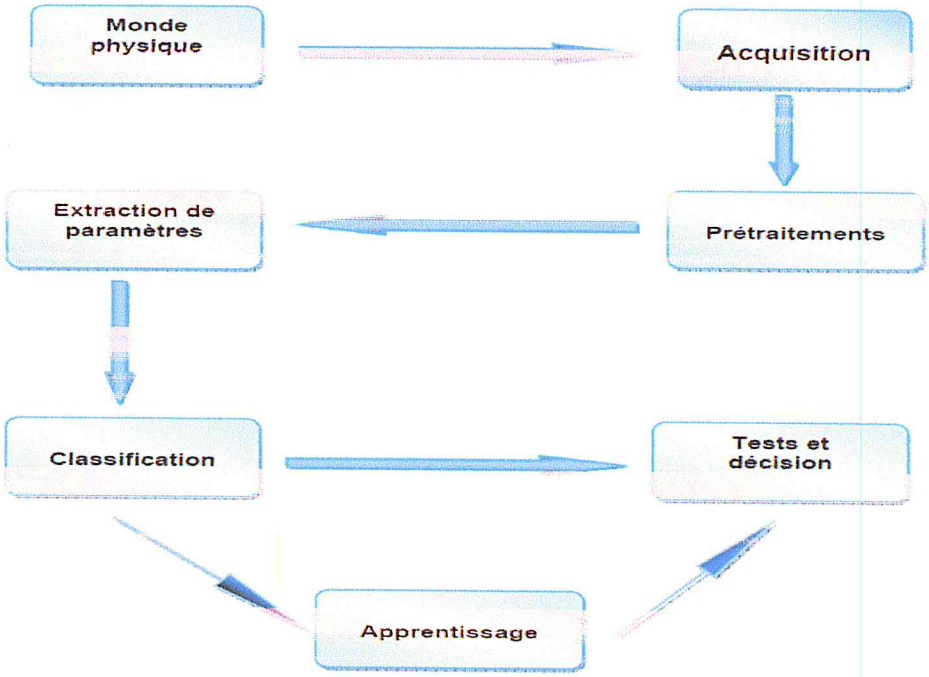


Figure I.8 : Système de reconnaissance.

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

- **Le monde physique (L'extérieur)**

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

- **L'Acquisition de l'image**

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

- **Les prétraitements**

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

- **L'extraction de paramètres**

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

- **La classification (Modélisation)**

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

- **L'apprentissage**

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

- **La décision**

C'est l'étape qui fait la différence entre un système d'identification d'individus et un autre de vérification. Dans cette étape, un système d'identification consiste à trouver le modèle qui correspond le mieux au visage pris en entrée à partir de ceux stockés dans la base de données.

I.8 Mesure de performance d'un système biométrique

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

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.

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

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.

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

3. Le troisième critère est connu sous le nom de taux d'erreur égale (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.

En fait, TFA et TFR sont des fonctions du seuil t de système ; si t est diminué pour rendre le système plus tolérant aux variations et au bruit d'entrée, alors TFA augmente. D'autre part, si t est augmenté pour rendre le système plus bloqué, TFR augmente en conséquence. Le diagramme dans la **figure I.9** montre la relation entre ces deux variables [09]

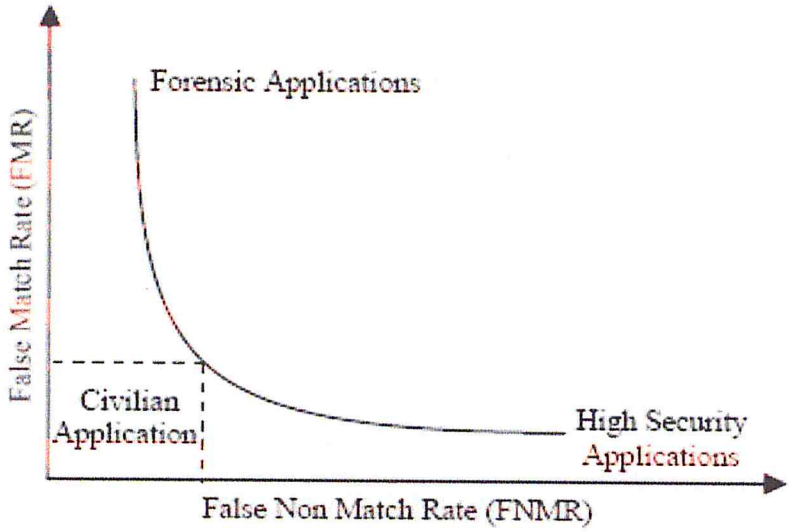


Figure I.9 Relation entre TFA et TFR [09]

I.9 Conclusion

Dans ce chapitre, nous avons présenté les différents types de la biométrie et les systèmes biométriques les plus utilisés ainsi que leurs caractéristiques. Dans la suite, on s'intéressera au système de la détection et reconnaissance de *visages.*

CHAPITRE II

TECHNIQUES DE DETCTION ET DE RECONNAISSANCE DE VISAGES

II.1. Introduction

Dans ce chapitre, nous présenterons un état de l'art sur les techniques de détection de visages et les différentes méthodes les plus connues de l a reconnaissance faciale

II.2. Détection de visages

La détection de visages est la première étape dans le processus de reconnaissance faciale. En effet, le processus de reconnaissance de visages ne pourra jamais devenir intégralement automatique s'il n'a pas été précédé par une étape de détection efficace.

.

II.3. Les Approches de la détection de visage

Il existe plusieurs méthodes pour la détection de visages. Elles peuvent être subdivisées en quatre différents types [12].

II.3.1. Approches basées sur l'apparence

Ces approches appliquent généralement des techniques d'apprentissage automatique. Ainsi, les modèles sont appris à partir d'un ensemble d'images représentatives de la variabilité de l'aspect facial. Ces modèles sont alors employés pour la détection. L'idée principale de ces méthodes est de considérer que le problème de la détection de visage est un problème de classification (visage, non-visage). Une des approches les plus connues de détection de visage est l'Eigenface [13]. Elle consiste à projeter l'image dans un espace et à calculer la distance euclidienne entre l'image et sa projection. En effet, en codant l'image dans un espace, on dégrade l'information contenue dans l'image, puis on calcule la perte d'information entre l'image et sa projection. Si cette perte d'information est grande (évaluée à partir de la distance, que l'on compare à un seuil fixé a priori), l'image n'est pas correctement représentée dans l'espace : elle ne contient pas de visage.

Cette méthode donne des résultats assez encourageants, mais le temps de calcul est très important. Dans Rowley et al. [14], les auteurs proposent un système de détection de visage basé sur la classification par des réseaux de neurones. Leur technique est divisée en deux étapes : la localisation des visages en utilisant un réseau de neurones et la vérification des résultats obtenus. Les auteurs ont construit un réseau de neurones qui, à partir d'une image prétraitée de 20x20 pixels, indique s'il s'agit d'un visage ou non. Le prétraitement consiste à égaliser l'histogramme. L'image est balayée avec des fenêtres de 20x20. Pour détecter les visages de différentes tailles, une analyse multi-résolutions est

effectuée. L'extension a aussi été proposée afin de déterminer un réseau de neurones indiquant le degré de rotation d'un visage. Ainsi, le système est capable de détecter des visages ayant subi des rotations dans le plan et de différentes échelles. L'un des avantages des réseaux de neurones est leur robustesse au bruit. Malheureusement, les réseaux de neurones, sont souvent difficiles à construire. Leur structure (nombre de couches cachées pour les perceptrons par exemple) influe beaucoup sur les résultats et il n'existe pas de méthode pour déterminer automatiquement cette structure.

La phase d'apprentissage est difficile à mener puisque les exemples doivent être correctement choisis (en nombre et en configuration).

Méthode de détection de visage « Viola et Jones »

Une méthode bien connue de détection d'objets complexes tels que les visages est l'utilisation de « classifieurs de Haar » montés en cascade (boostés) au moyen d'un algorithme AdaBoost. Cette méthode est implémentée nativement dans la bibliothèque OpenCV [48] et a été présenté initialement dans Viola et Jones [49]. Le principe de cette méthode est obtenir un algorithme complexe de classification, composé de classifieurs élémentaires qui éliminent au fur et à mesure les zones de l'image qui ne sont pas compatibles avec l'objet recherché. Ces classifieurs binaires reposent sur des primitives visuelles qui dérivent des fonctions de Haar (Haar- like features).

Schneiderman et Kanade [45] utilise une information multi-résolution pour les différents niveaux de la transformée en ondelette. La classification en visage non linéaire ou bien en non visage est réalisée en utilisant les statistiques des produits d'histogrammes.

Ces derniers sont calculés à partir des exemples de visage et de non visage en utilisant la méthode « AdaBoost learning » [46] [47]. Adaboost est employé pour résoudre trois problèmes fondamentaux : 1) apprentissage effectif des caractéristiques à partir un grand ensemble de caractéristiques. 2) construction de classifieurs faibles, dont chacun est basé sur une des caractéristiques choisies ; et 3) le renforcement ou « boosting » des classifieurs faibles pour construire un classifieur fort. Le coût de calcul de cette technique est très élevé.

II.3.2. Approches basées sur les connaissances acquises

Ces méthodes sont basées sur la définition de règles strictes à partir des rapports entre les caractéristiques faciales. Elles s'intéressent aux parties caractéristiques du visage

comme le nez, la bouche et les yeux. Ces méthodes sont conçues principalement pour la localisation de

visage. Dans [15], Kotropoulous et Pitas utilisent une méthode à base de règles. Les caractéristiques du visage sont localisées à l'aide de la méthode de projection proposée par Kanade [16] pour détecter les contours d'un visage. Soit I(x,y) l'intensité de la luminance du pixel (x,y) de l'image m*n, les projections horizontale et verticale de cette image sont définies par l'équation suivante :

$$HI(x) = \sum_{y=1}^{n} I(x,y) \qquad VI(x) = \sum_{x=1}^{m} I(x,y)$$

Le profil horizontal de l'image originale est calculé en premier. Les deux minimas locaux sont déterminés, ils correspondent aux bords gauche et droit du visage. Ensuite, le profil vertical est à son tour calculé. Les minima locaux de ce profil vertical correspondent aux positions de la bouche, du nez et des yeux. L'inconvénient de cette méthode est qu'elle n'arrive pas à détecter le visage lorsque ce dernier se trouve sur un arrière-plan complexe. Yang and Huang [17] quant à eux, ont étudié les évolutions des caractéristiques du visage en fonction de la résolution. Quand la résolution de l'image d'un visage est réduite progressivement, par sous- échantillonnage ou par moyenne, les traits macroscopiques du visage disparaissent. Ainsi, pour une résolution faible, la région du visage devient uniforme. Yang et Huang se sont basés sur cette observation pour proposer une méthode hiérarchique de détection de visages.

En commençant par les images à faible résolution, un ensemble de candidats de visage est déterminé à l'aide d'un ensemble de règles permettant de rechercher les régions uniformes dans une image. Les candidats de visage sont ensuite vérifiés en cherchant l'existence de traits faciaux proéminents grâce au calcul des minimas locaux à des résolutions supérieures. Une caractéristique intéressante de cette technique « descendante » de recherche de zone d'intérêt (informations globales vers des informations plus détaillées) est de réduire le temps de calcul nécessaire par l'utilisation d'images sous-échantillonnées. Malheureusement, cette technique occasionne de nombreuses fausses détections et un taux faible de détection.

II.3.3 Approches basées sur le « Template- matching »

Les templates peuvent être définis soit "manuellement", soit paramétrés à l'aide de fonctions. L'idée est de calculer la corrélation entre l'image candidate et le template.

Ces méthodes rencontrent encore quelques problèmes de robustesse liés aux variations de lumière, d'échelle, etc. Sinha [18] utilise un ensemble d'invariants décrivant le modèle du visage. Afin de déterminer les invariants aux changements de luminosité permettant de caractériser les différentes parties du visage (telles que les yeux, les joues, et le front); cet algorithme calcule ainsi les rapports de luminance entre les régions du visage et retient les directions de ces rapports (par exemple, la région 1 est-elle plus claire ou plus sombre que la région 2). La figure II.1 montre un modèle prédéfini correspondant à 23 relations. Ces relations prédéfinies sont classifiées en 11 relations essentielles (flèches) et 12 relations confirmations (gris). Chaque flèche représente une relation entre deux régions (**figure II.1**). Une relation est vérifiée si le rapport entre les deux régions qui lui correspond dépasse un seuil. Le visage est localisé si le nombre de relations essentielles et de confirmation dépasse lui aussi un seuil.

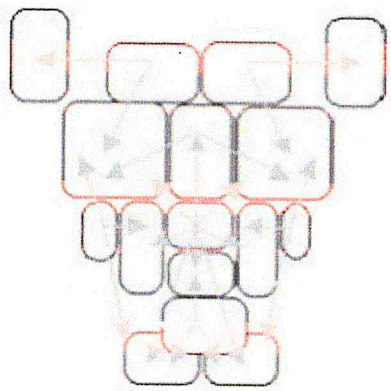


Figure II.1 : Modèle de visage composé de 16 régions (les rectangles) associées à 23 relations (flèches) [02]

Yuille et al. [19] ont utilisé un template déformable pour modéliser les caractéristiques faciales. Ce template adapte un modèle élastique, connu a priori, aux caractéristiques faciales (ex. yeux). Dans cette approche les caractéristiques faciales sont décrites par des templates paramétriques. Une fonction d'énergie est définie pour lier les contours, les sommets et les vallées dans l'image d'entrée aux paramètres correspondants dans le template. Le meilleur ajustement du modèle élastique est trouvé en minimisant une fonction d'énergie des paramètres. Bien que leurs résultats expérimentaux démontrent une bonne performance pour le suivi de caractéristiques non rigides, un inconvénient de cette approche est que le template déformable doit être initialisé dans la proximité de l'objet d'intérêt. Pour détecter les caractéristiques faciales pour la reconnaissance de visage,

Brunelli et Peggio [20] ont utilisé, pour chaque région extraite, un détecteur approprié. Ils se sont aussi inspirés de la méthode de Kanade.

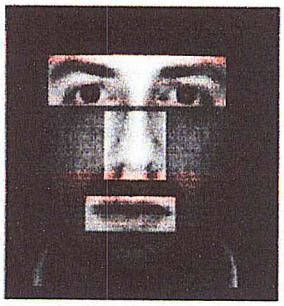


Figure II.2 : Différentes régions utilisées pour la phase de template matching

Pour les régions yeux, nez et bouche (figure II.2), ils utilisent la direction du gradient vertical et horizontal. La bouche et le nez sont localisés en utilisant des stratégies similaires. La position verticale est déterminée grâce aux standards anthropométriques. D'abord, une estimation fine de leur position réelle est obtenue en cherchant les pics de la projection horizontale du gradient vertical pour le nez et les vallées de la projection horizontale de l'intensité pour la bouche.

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

II.3.4 Approches basées sur des caractéristiques invariantes

Ces approches sont utilisées principalement pour la localisation de visage. Les algorithmes développés visent à trouver les caractéristiques structurales existantes même si la pose, le point de vue ou la condition d'éclairage changent. Puis, ils emploient ces caractéristiques invariables pour localiser les visages. Il y a deux familles de méthodes : Les méthodes basées sur la couleur de la peau et les méthodes basées sur les caractéristiques de visage. Elles consistent à localiser les cinq caractéristiques (deux yeux, deux narines, et la jonction nez/lèvre) pour décrire un visage typique.

II.3.4.1 Méthodes basées sur les caractéristiques du visage

L'algorithme développé par De Silva et al. [21] utilise tout d'abord une hypothèse sur la position du haut du visage ensuite l'algorithme de recherche parcourt le visage de haut en bas afin de trouver l'axe des yeux caractérisé par une augmentation soudaine de la densité de contours (mesurée par le rapport noir/blanc le long des plans horizontaux). La longueur entre le haut du visage et le plan de l'œil est alors utilisée comme une longueur de référence pour construire un « template » facial flexible. Ce « template » couvrant des caractéristiques telles que les yeux et la bouche est initialisé à partir de l'image d'entrée. La forme initiale du « template » est obtenue en utilisant la longueur anthropométrique en respectant la longueur de référence.

Le template flexible est alors ajusté par rapport aux positions finales des caractéristiques en utilisant un algorithme de réglage fin qui emploie une fonction de coût basée contour.

Bien que ces algorithmes réussissent à détecter les caractéristiques d'ethnies différentes puisqu'ils ne se basent pas sur les informations de niveaux de gris et de couleur, ils n'arrivent pas cependant à détecter correctement ces caractéristiques si l'image du visage contient des lunettes ou bien si les cheveux couvrent le front.

II.3.4.2. Méthodes basées sur l'analyse de la couleur de la peau

Dans cette approche, la couleur de peau humaine a été employée comme un dispositif efficace pour la détection de visage, et les applications reliées. Bien que la couleur de peau diffère d'un individu à un autre, plusieurs études ont prouvé que la différence principale existe dans l'intensité plutôt que la chrominance, Plusieurs espaces de couleur ont été employés pour marquer des pixels de peau comprenant RVB (RGB), HSV [41]

Quoique l'information de couleur semble être un outil efficace pour identifier des secteurs faciaux, les modèles de couleur de peau peuvent échouer quand le spectre (la température corrélée de couleur) de la source lumineuse change de manière significative. En outre, les caractéristiques du dispositif d'acquisition (équilibre spécifiquement blanc) effectueront également la transformation de couleur entre l'environnement et l'image.

Après avoir vue quelques algorithmes de détection de visage, nous passerons à la phase suivante qui est la reconnaissance. Avant d'arriver à cette dernière, nous devons passer par une étape transitoire de prétraitement qui est la normalisation de l'image de

visage détecté dans le but de minimiser les effets du bruit engendré durant la chaine d'acquisition de l'mage.

II.4. Les Approches de la reconnaissance de visage

Dans cette partie de ce chapitre, nous allons présenter les approches de la reconnaissance de visage les plus connues. Les approches globales, les approches locales et les approches hybrides.

II.4.1. Méthodes holistiques ou globales

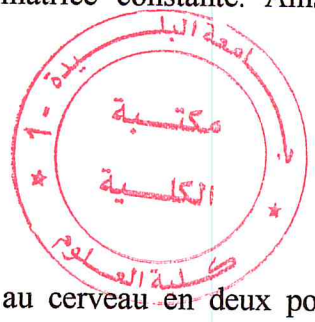
Ces méthodes identifient un visage en utilisant l'image entière de ce dernier comme entrée du système de reconnaissance. Chaque image de visage de dimension (n,m) est représentée par un vecteur simple de dimension n m, en concaténant les valeurs du niveau de gris de tous les pixels de l'image du visage. L'espace I contenant tous les vecteurs images de visages est appelé espace images. L'avantage de cette représentation est qu'elle préserve implicitement les informations de texture et de forme nécessaire pour la reconnaissance de visages. De plus, elle permet une meilleure capture de l'aspect global du visage que les représentations locales [22]. Toutefois, son inconvénient majeur réside dans la dimension très grande de l'espace image qu'elle nécessite [23, 24, 25], ce qui rend très difficile la classification.

II.4.1.1 Analyse en Composantes Principales

Une des techniques les plus utilisées dans l'identification de visage, est la méthode « eigenface » [26, 27]. Son principe est le suivant : étant donné un ensemble d'images de visages exemples, il s'agit tout d'abord de trouver les composantes principales de ces visages. Ceci revient à déterminer les vecteurs propres de la matrice de covariance formée par l'ensemble des images exemples. Chaque visage exemple peut alors être décrit par une combinaison linéaire de ces vecteurs propres. Pour construire la matrice de covariance, chaque image de visage est transformée en vecteur. Chaque élément du vecteur correspond à l'intensité lumineuse d'un pixel

II.4.1.2 Analyse Discriminante Linéaire

Les méthodes basées sur l'Analyse Discriminante Linéaire (ADL) déterminent les directions de projection les plus discriminantes dans l'eigenspace. Pour cela, elles maximisent les variations inter-personnes par rapport aux variations intra-personne. Cependant, si un seul exemple d'apprentissage par personne est utilisé, c'est-à-dire si les variations intra classes sont nulles, alors les performances de l'ADL deviennent faibles par rapport à celles qui sont données par l'eigenface [28]. Afin de remédier à ce problème, Zhao et al. [29] ont proposé de remplacer la matrice de dispersion intra-personne par une matrice constante. Ainsi, la méthode basée ADL se réduit alors à la méthode eigenface.



II.4.1.3 Le réseau de neurones

D'après Haykin [30] un réseau de neurones ressemble au cerveau en deux points : l'acquisition d'une connaissance est le résultat d'un processus d'apprentissage et la mémorisation d'une connaissance prennent fait des poids de connections entre les neurones. L'avantage de la technique des réseaux de neurones réside dans sa capacité d'apprendre, de mémoriser et de généraliser pour mieux classer de nouvelles données.

Zhang et *al.* [31] utilisent les réseaux de neurones pour le problème de reconnaissance des visagess faciales. Ils marquent sur le visage 34 points dites points d'intérêts et calculent 18 coefficients d'ondelettes de Gabor à chaque point pour fabriquer un ensemble de caractéristiques (ces dernières forment les entrées du réseau) de type position géométrique et de type filtre de Gabor. Les chercheurs développent un perceptron à deux couches et ils l'entrainent par Rprop (Resilient propagation). La première couche effectue une réduction non linéaire de la dimension des entrées et la seconde met une décision statistique tout en se basant sur un jeu de fonctionnalité des unités cachées.

II.4.1.4 Avantages et inconvénients des méthodes globales

Les méthodes globales présentent quelques avantages et/ou inconvénients dont :

Avantages

- Le problème de la reconnaissance faciale automatique est transformé en un problème d'analyse de sous–espaces de visages, pour lequel de nombreuses méthodes statistiques existent.
- Les méthodes globales sont souvent appliquées à des images basses résolutions ou de mauvaises qualités.

Inconvénients

- Il est nécessaire de disposer de suffisamment de données représentatives des visages.
- Il n'y a pas d'a priori sur le physique d'un visage.
- Ces méthodes ne sont robustes qu'à des variations limitées (pose, illumination, expression).

II.4.2. Méthodes locales

Les méthodes locales utilisent les caractéristiques faciales locales pour la reconnaissance de visage. Elles sont relativement matures comparées aux méthodes holistiques [32, 33, 34, 35, 36]. Dans ces méthodes, le visage est représenté par un ensemble de vecteurs caractéristiques de dimensions faibles, plutôt que par un seul vecteur de grande dimension.

Les approches basées sur l'extraction de points caractéristiques peuvent être subdivisées en deux catégories : les approches géométriques et les approches basées sur les graphes.

II.4.2.1 Approches géométriques

Elles sont basées sur l'extraction de la position relative des éléments qui constituent le visage (tel que le nez, la bouche et les yeux). La plupart des approches géométriques utilisent des points d'intérêt (comme les coins de la bouche et des yeux). Au début des années 1990, Brunelli et Poggio [33] ont décrit un système de reconnaissance faciale qui extrait automatiquement 35 caractéristiques géométriques du visage. La similitude est calculée à l'aide de classifieurs de Bayes. Un taux d'identification de 90 % sur une base de données de 47 sujets a été rapporté par les auteurs. Le coût de stockage des techniques géométriques est

très bas comparé à celui des autres techniques. Toutefois, les approches purement géométriques présentent quelques inconvénients :

- les caractéristiques géométriques sont généralement difficiles à extraire, surtout dans des cas complexes : illumination variable, occultations, etc.

- les caractéristiques géométriques seules ne suffisent pas pour représenter un visage, tandis que d'autres informations utiles comme les niveaux de gris de l'image ne sont pas du tout exploitées.

II.4.2.2 Approches basées sur les graphes

Plutôt que d'utiliser des méthodes purement géométriques, certains chercheurs ont choisi de représenter les caractéristiques locales du visage sous forme de graphes. Manjunath et al. [35] ont proposé une méthode de détection de caractéristiques locales du visage, basée sur la décomposition en ondelettes de Gabor [37]. La reconnaissance de visages est alors formulée comme un problème de mise en correspondance de graphes. L'efficacité de cette méthode a été validée sur un ensemble de données de visage de 86 sujets, contenant des variations d'expression et de pose, Un taux de reconnaissance de 90% en moyenne a été rapporté démontrant la robustesse de cette approche. Cependant, une fois construit, le graphe topologique ne peut pas être modifié.

Or, les images de visage changent facilement d'apparence en raison des différentes variations (illumination, expression, pose, etc.), et du coup un schéma de graphe topologique fixe n'est plus adéquat.

II.4.2.3 Avantages et inconvénients des méthodes locales

Les méthodes locales présentent elles aussi certains avantages et/ou inconvénients dont :

Avantages

Le modèle créé possède des relations intrinsèques bien définies avec les visages réels.

- Les modèles créés peuvent prendre en compte explicitement les variations telles que la pose, l'illumination ou les expressions. La reconnaissance est ainsi plus efficace dans le cas de fortes variations.

- La connaissance a priori sur les visages peut être intégrée aux modèles afin d'améliorer leur efficacité.

Inconvénients

- La construction du modèle, reposant souvent sur la détection de points caractéristiques faciaux, peut être laborieuse.
- L'extraction des points caractéristiques peut être difficile dans le cas de variations de pose, d'illumination, d'occlusion . . .
- Les images doivent être de relativement de bonne qualité, et/ou être de résolution suffisante afin de pouvoir extraire les points caractéristiques.

II.4.3. Méthodes Hybrides

Les méthodes hybrides sont des approches qui combinent les caractéristiques holistiques et locales afin d'améliorer les performances de la reconnaissance de visages. En effet, les caractéristiques locales et les caractéristiques globales ont des propriétés tout à fait différentes. On peut espérer pouvoir exploiter leur complémentarité pour améliorer la classification. Le tableau 1 récapitule qualitativement la différence entre les deux types de caractéristiques [38].

Facteurs de variations	Caractéristiques locales	Caractéristiques globales
Illuminations [19]	Très sensible	Sensible
Expressions [28][64]	Pas sensible	Sensible
Pose [49]	Sensible	Très sensible
Bruit [65]	Très sensible	Sensible
Occlusion [28][64]	Pas sensible	Très sensible

Tableau II.1. Comparaison des méthodes basées sur les caractéristiques locales ou globales [38]

Nous pouvons voir que les caractéristiques locales et globales réagissant différemment sensibles aux facteurs de variation. Par exemple, les changements d'illumination peuvent avoir plus d'influence sur les caractéristiques locales, tandis que les changements d'expression ont plus d'impact sur les caractéristiques holistiques. Ainsi, les méthodes hybrides peuvent constituer une approche efficace pour réduire la complexité des classifieurs et améliorer leur capacité de généralisation.

II.5 Conclusion

Dans ce chapitre, nous avons passé en revue les principales techniques les plus connues de la détection de visages. Par la suite, nous nous sommes focalisés sur les principales approches de la reconnaissance faciale, qui se divisent en trois catégories à savoir les méthodes globales, locales et hybrides. Chaque méthode a été décrite en présentant leurs avantages et leurs inconvénients.

CHAPITRE III

CONCEPTION ET ARCHITECTURE DU LOGICIEL

III.1 Introduction

Dans ce chapitre, on va présenter les solutions que nous avons choisi de développer sur le téléphone portable. Ensuite, nous allons découvrir la structure du notre programme avec un système d'exploitation Android et nous allons terminer par la conception et la modélisation du système à concevoir

III.2 Détection de visages sur le téléphone portable

Pour objectif la conception et la réalisation d'un système de détection et reconnaissance de visages en temps réel, on a choisi l'approche de Paul viola et Michael Jones en 2001 [44,49]. Cette méthode est implantée dans la librairie OpenCV. Le détecteur de visages d'OpenCV a été initialement proposé par Paul Viola. Tout d'abord, un classificateur (c'est-à-dire une cascade de classificateurs augmentés qui fonctionne avec des caractéristiques Haar) est formé avec des centaines d'échantillons d'un visage, appelé exemples positifs, qui ont la même taille (par exemple, 40x40), et des exemples négatifs qui sont des images arbitraires de la même taille. Après le classificateur est formé, il peut être appliqué à une région d'intérêt (de la même taille que celle utilisé lors de l'apprentissage) dans une image d'entrée. Le classificateur délivre un "1" si la région contient un visage, et «0» sinon. Pour rechercher l'objet dans toute l'image, nous pouvons déplacer la fenêtre de recherche sur l'image et vérifier chaque emplacement en utilisant le classificateur. Le classificateur est conçu de telle manière qu'il peut facilement changer sa taille afin de trouver les objets d'intérêt avec des tailles différentes, ce qui est plus efficace que le changement de la taille de l'image. Ainsi, pour trouver un objet d'une taille inconnue dans l'image, la procédure de recherche doit être fait à plusieurs différentes échelles.

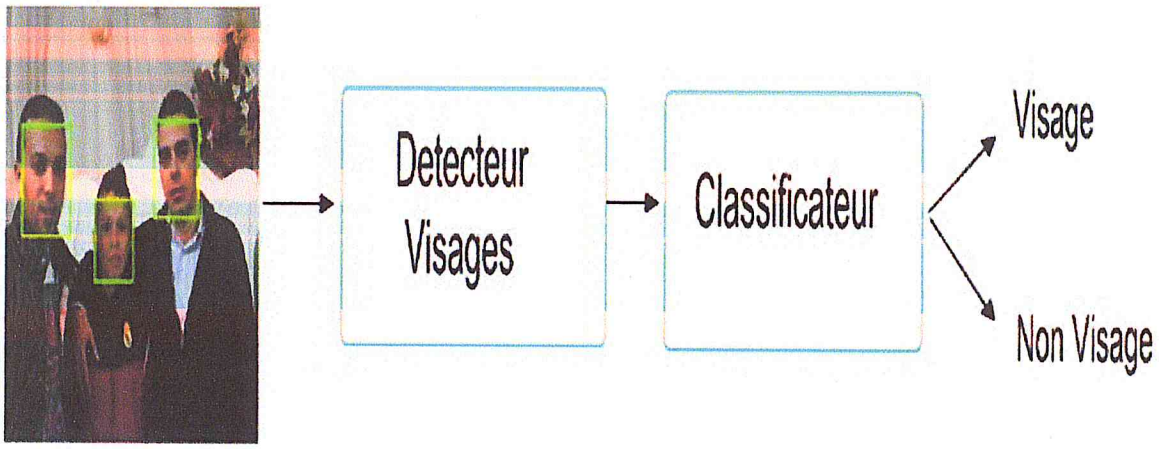
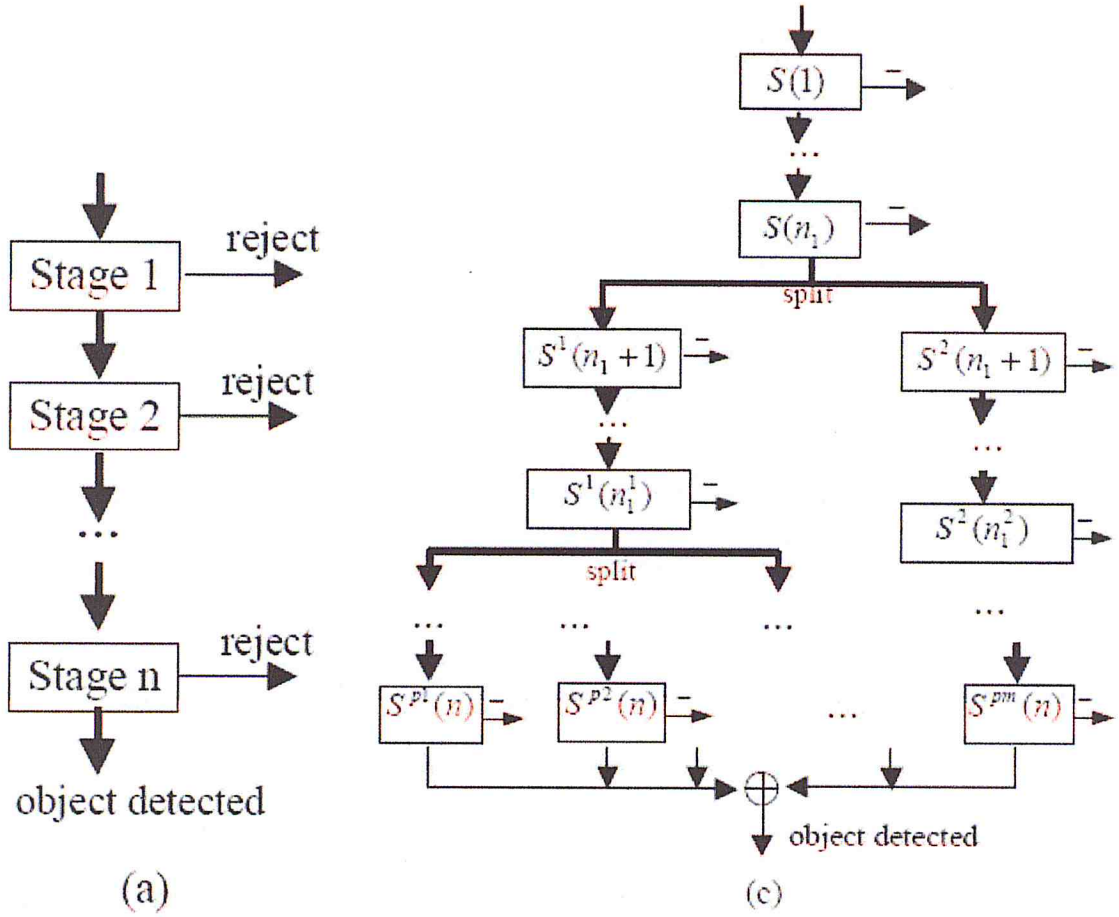


Figure III.1 : Schéma de la chaine de décision



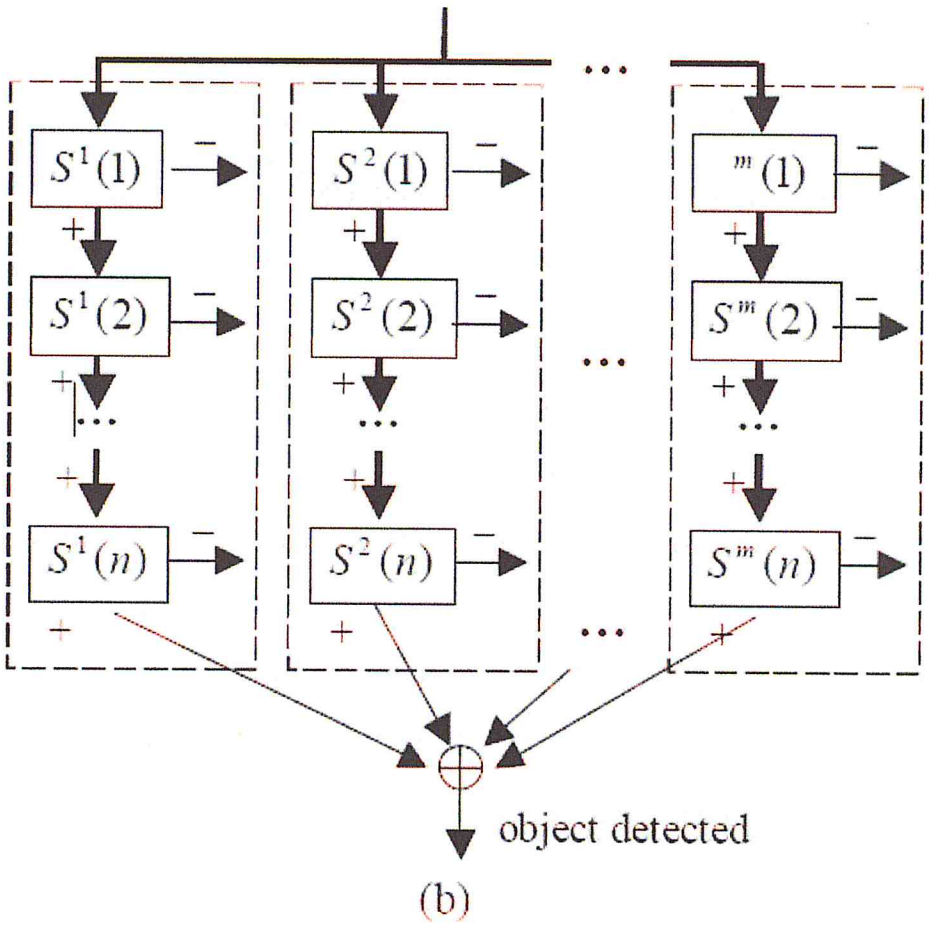


Figure III.2: (a) Le classificateur simple en cascade ; (b) Le classificateur multiple en cascade ; (c) Le classificateur des arbres

Actuellement, les classificateurs de base sont d'arbres de décision avec au moins 2 branches. Les caractéristiques Haar représentent l'entrée de ces classificateurs. Chaque classificateur particulier est spécifié par la forme et la position de la région d'intérêt.

III.3 Méthode de Viola et Jones

La méthode « Viola & Jones » [44,49] a été proposée au départ pour la détection de visages dans une image numérique ou séquence vidéo puis utilisée pour détecter d'autres objets comme les voitures,... La bibliothèque OpenCV présente une implémentation de cette méthode sous le nom « détecteur en cascades de haar ».

Cette méthode combine quatre contributions clés qui sont les caractéristiques pseudo-haar, l'approche d'image intégrale, la méthode d'apprentissage adaptative AdaBoost et l'algorithme en cascades de classifieurs. Dans la suite, Nous allons détailler ces étapes clées tout en précisant l'apport engendré de chacun d'entre elles sur la performance et l'efficacité de la méthode.

III.3.1 Caractéristiques pseudo-haar

Une caractéristique pseudo-haar est représentée par un rectangle défini par son sommet, sa hauteur, sa longueur et son poids. Le recourt au traitement d'images par ces caractéristiques est motivé par sa rapidité contre le traitement direct à travers le balayage de la totalité d'image pixel par pixel.

La figure III.3 ci-dessous présente des exemples de caractéristiques utilisées par Viola et Jones. Elles sont inspirées des descripteurs de haar qui ont été employées par Papageorgiou et *al* dans [53]. Les valeurs de ces caractéristiques sont calculées par la soustraction de la somme des pixels noirs de la somme des pixels blancs [54].

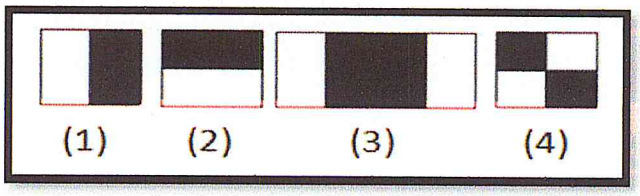


Figure III.3 : Exemples des caractéristiques pseudo-haar d'après [44,49].

III.3.2 Approche d'image intégrale

La méthode d'image intégrale est utilisée pour déterminer la présence ou l'absence des caractéristiques dans chaque position de l'image et à n'importe quelle taille. Le but de cette méthode à part la détection de caractéristiques est la réduction du temps de calcul de ces dernières. La valeur intégrale de chaque pixel est la somme de tous les pixels au-dessus de lui et de sa gauche.

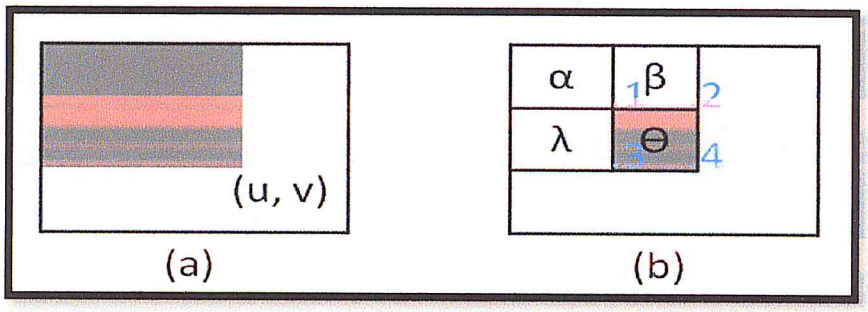


Figure III.4 *: image intégrale : (a) la valeur de l'image intégrale à la position (u, v), (b) calcul de la somme des valeurs de pixels dans le rectangle Θ d'après [44,49].*

Dans le cas de la figure III.4. (a), l'image intégrale est définie comme suit :

$$ii(u,v) = \sum_{\substack{u'<u \\ v'<v}} i(u',v').$$

Dans le cas de figure III.4. (b), où on souhaite avoir la valeur d'image intégrale pour un rectangle qui n'a pas un coin en haut à gauche de l'image (cas de rectangle Θ dans la figure III.4. (b)). Nous pouvons obtenir la valeur de Θ est égale par l'expression ci-dessous :

$$\theta = (\alpha + \beta + \lambda + \theta) - \big((\alpha + \beta) + (\alpha + \lambda)\big) + \alpha.$$

Autrement dit, la somme de niveaux de gris des pixels dans la région rectangulaire Θ est calculée rapidement à partir de quatre sommets de l'image intégrale selon l'équation ci-dessous :

$$\theta = ii(u_4, v_4) + ii(u_1, v_1) - \big(ii(u_3, v_3) + ii(u_2, v_2)\big).$$

De ce qui précède, la différence entre deux rectangles adjacents est obtenue à partir de six sommets à l'image intégrale $ii(u,v)$ et le calcul d'une caractéristique à trois rectangles nécessite huit sommets.

III.3.3 Algorithme AdaBoost

Paul viola et Michael Jones ont utilisé l'algorithme AdaBoost pour sélectionner les caractéristiques de haar à utiliser et pour fixer le niveau du seuil adéquat pour cette sélection. Abadoost combine plusieurs classifieurs « faible » issus des caractéristiques pseudo-haar pour former un classifieur « fort ». AdaBoost sélectionne un ensemble de classifieurs faibles où chacun « pousse » la réponse finale un degré vers la bonne direction. Il les combine et assigne un poids à chacun.

III.3.4 Algorithme en cascades de classifieurs

La quatrième contribution de la méthode « Viola & Jones » est la détection en cascades. Une cascade se compose de n filtres dont chacun est un classifieur « faible » composé d'une seule caractéristique pseudo-haar (Figure III.5). Au cours d'une détection, si un filtre échoue à passer une sous-région alors elle est immédiatement classée comme «Non visage » sinon la région est passée vers le filtre suivant. Les sous-régions de l'image qui traversent la totalité de cascade sont classés comme « visage » et tous les autres sont classées « Non Visage ». Les

poids qu'AdaBoost attribue aux filtres déterminent l'ordre des filtres dans la cascade commençant par le poids le plus lourd vers celui le plus faible pour éliminer les régions « Non visage » le plus tôt possible.

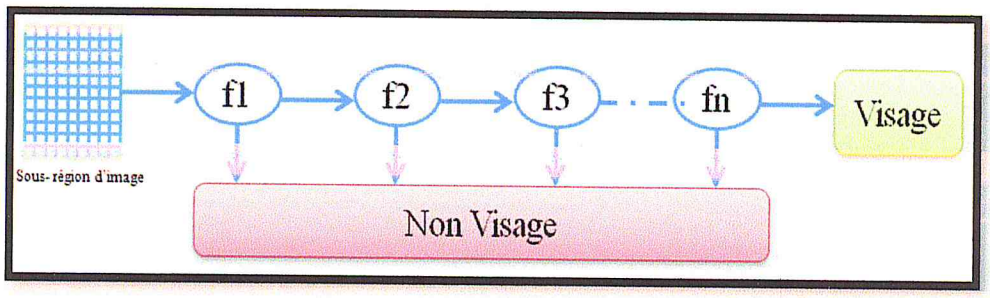


Figure III.5 : La chaine de classifieurs en cascade

Nous finirons notre description à propos la méthode « Viola & Jones » par l'énumération des avantages ajoutés par chacune des contributions citées :

- Les caractéristiques pseudo-haar permettent la détection des objets en plusieurs échelles (détection multi-échelles).
- L'image intégrale permet le calcul des caractéristiques en temps réel.
- L'algorithme AdaBoost sélectionne les caractéristiques les plus discriminantes pour la classification et forme un classifieur de bonne performance.
- La cascade minimise le temps de calcul et affine les frontières de classification.

III.4 Reconnaissance des visages sur le téléphone portable

PCA ou bien « Eigenface » [26, 27] est une approche bien connus pour l'extraction de caractéristiques et la réduction de a dimension. Elle été largement utilisés dans de nombreuses applications impliquant des données de grande dimension. Cependant, l'approche PCA n'utilise pas les infos des classes annoncées. Donc, il existe souvent des faux positifs.

III.6 La structure du système

En général, le système a deux éléments Figure III.7 : la détection et la reconnaissance de visages. Tout d'abord, une caméra d'un téléphone portable est utilisée pour capturer une image de la scène. Ensuite, la première partie permet de détecter tous les visages dans l'image, peu importe leur taille. Puis, tous les visages détectés sont normalisés à la même taille, par exemple 120*120 et convertir au niveau de gris.

Enfin, la deuxième partie du système compare le visage d'entrée avec tous les visages dans la base de données pour la reconnaissance. La réponse finale est la personne la plus proche trouvée.

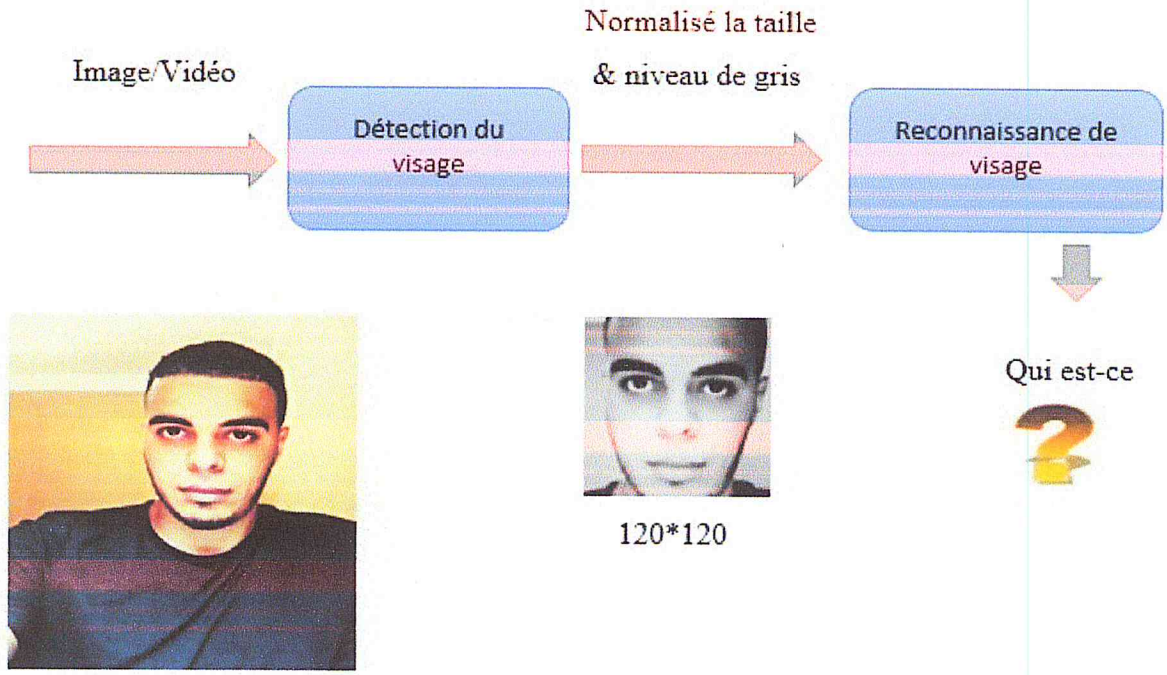


Figure III.6 : La structure générale du système

III.7 Vidéosurveillance intelligente :

L'analyse vidéo aussi appelée vidéosurveillance intelligente, est une technologie qui permet, au moyen de logiciels, d'identifier automatiquement, dans des séquences vidéo, des objets, des comportements ou des attitudes spécifiques. Elle transforme la vidéo en données qui seront transmises ou archivées pour permettre au système de vidéosurveillance d'agir en conséquence. Il pourra s'agir d'actionner une caméra mobile, dans le but d'obtenir des données plus précises de la scène ou tout simplement, d'envoyer une alerte au personnel de surveillance pour qu'il puisse prendre une décision sur l'intervention adéquate à apporter.

Les systèmes de vidéosurveillance intelligente utilisent des algorithmes mathématiques pour détecter des objets ou en mouvements dans l'image et filtrer les mouvements non pertinents. Ils créent une base de données consignant les attributs de tous les objets détectés et leurs propriétés de mouvements. La prise de décision par le système ou la recherche d'événements d'intérêt dans des séquences archivées se fait à partir de règles (par ex.: si une personne traverse une limite, envoyer une alerte ….) [56]

III.8 Systèmes de vidéosurveillance avec caméras IP

Une caméra IP ou caméra réseau, peut être représentée comme la jonction en une seule unité d'une caméra et d'un ordinateur. Elle capture et envoie des images en temps réel à travers un réseau IP, permettant aux utilisateurs autorisés de visualiser localement ou à distance, stocker et gérer la vidéo à travers une infrastructure de réseau IP.

Une caméra IP est équipée d'un serveur web, serveur FTP (File Transfer Protocol) [57], client FTP, client e-mail et un gestionnaire d'alarme. Elle opère comme un serveur indépendant et possède sa propre adresse IP. De ce fait, elle peut être connectée au réseau partout où il y a une connexion. En plus de la vidéo, une caméra IP peut aussi supporter d'autres fonctionnalités tel que l'audio, et l'activation d'alarmes via des entrées et sorties numériques [57].

III.9 Architecture des systèmes de vidéosurveillance intelligente

Il y a deux catégories d'architectures pour mettre en place un système de vidéosurveillance intelligente : centralisé et distribué. Dans les architectures centralisées, la vidéo et d'autres informations sont collectées par les caméras, puis elles sont acheminées vers un serveur centralisé pour l'analyse. Dans les architectures distribuées, les caméras réseau ou les encodeurs vidéo, ou d'autres composants du réseau (par exemple, commutateurs) sont « intelligents » et sont capables de traiter la vidéo et d'extraire les informations pertinentes. En concevant intelligemment un système de vidéosurveillance intelligente et en distribuant la charge, les coûts globaux d'un système peuvent être sensiblement abaissés et l'exécution peut être améliorée [57].

III.9.1 Architecture centralisée

Dans les architectures centralisées, toute la vidéo obtenue par les caméras est acheminée au serveur pour un traitement centralisé. Les infrastructures basées sur des caméras analogiques

emploient la plupart du temps des DVR (Digital Video Recorder) comme serveur, tandis que dans un système utilisant des caméras réseau, des PC-serveurs sont utilisés pour le traitement automatique [57].

- Architecture centralisée à base de DVR

Dans les systèmes CCTV (Closed Circut Tele Vision) traditionnels de télévision, la vidéo obtenue par les caméras analogiques est introduite dans un DVR équipé des fonctionnalités de vidéo intelligente. Les DVRs ont des encodeurs qui convertissent la vidéo du format analogique au numérique, puis ils exécutent l'analyse intelligente (par exemple, le comptage des gens ou l'identification des visages). Ils compressent également la vidéo, l'enregistrent, et distribuent les alarmes et la sortie vidéo aux opérateurs autorisés [57].

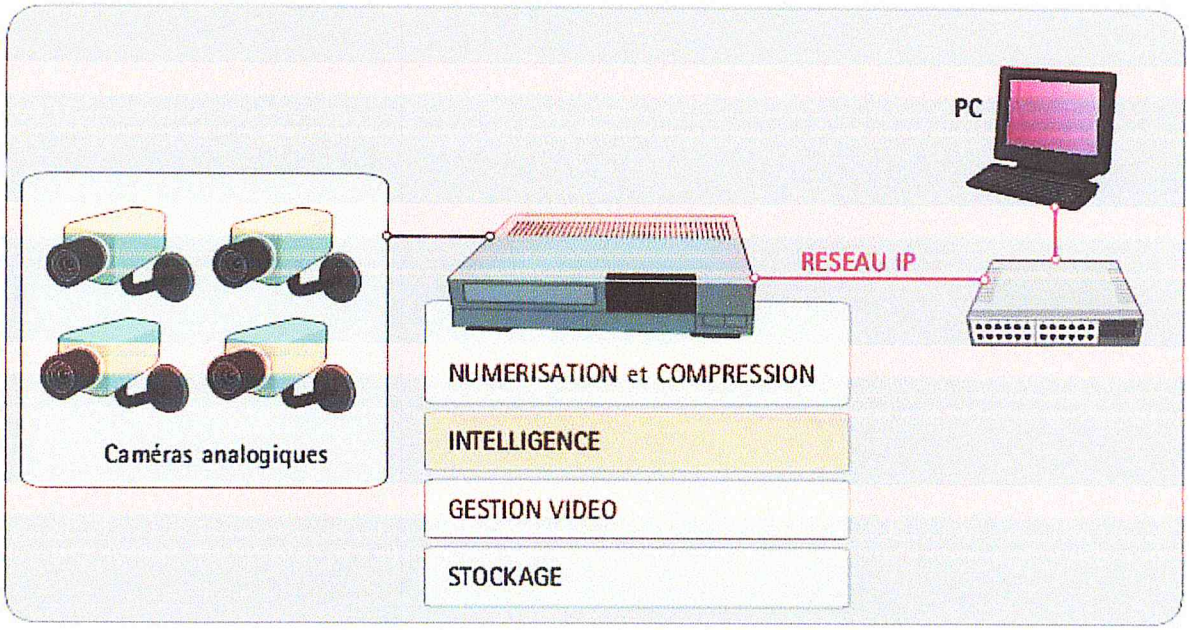


Figure III.7 : système centralisé à base de DVR [57].
(Les fonctionnalités d'intelligence se situent dans le DVR).

- Architecture centralisée à base d'un PC-server

Pour surmonter les insuffisances des DVRs, de nouvelles architectures centralisées ont été conçues, elles utilisent un PC serveur pour le traitement de la vidéo. La vidéo provenant des caméras réseau est directement acheminée au serveur, tandis que la vidéo provenant des caméras analogiques doit être numérisée d'abord par un encodeur vidéo, puis acheminée vers le serveur [57].

Cette architecture est plus flexible et extensible que celle à base de DVR parce que la numérisation et la compression ne se font plus par le système de gestion de la vidéo, mais plutôt par les caméras réseaux ou les encodeurs vidéo dans le cas des caméras analogiques, ceci permet d'alléger les tâches de système de gestion de la vidéo. Malgré cela, les serveurs doivent être équipés d'une grande puissance, car les tâches de traitement de la vidéo sont complexes ce qui a pour conséquence la limitation de nombres de caméras traitées par un serveur [57].

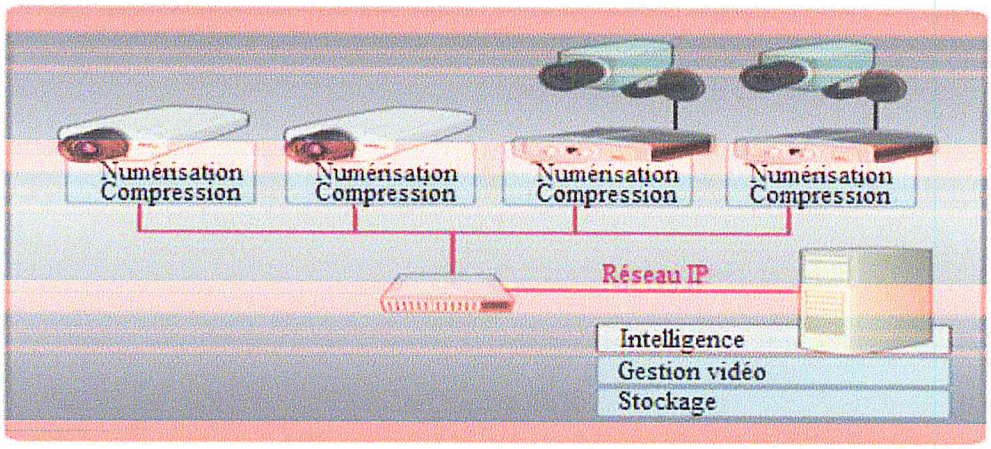


Figure III.8 : système centralisé à base d"un PC serveur [57].
(Les fonctionnalités d"intelligence sont dans le serveur).

III.9.2 Architecture distribuée

Les architectures distribuées sont conçues pour surmonter les limitations des systèmes centralisés qui surchargent le point central du système, tel qu'un PC serveur ou un DVR. En distribuant le traitement à différents éléments dans un réseau, la consommation de la bande passante peut être réduite, mais aussi, les calculs nécessaires à l'analyse vidéo pourront être effectués sur des caméras intelligentes dotées de processeurs, les encodeurs ou dans les commutateurs réseau. De plus, ces architectures sont souples, puisque l'ajout de caméras n'est pas forcément limité par la puissance de calcul de l'enregistreur numérique ou du serveur [57].

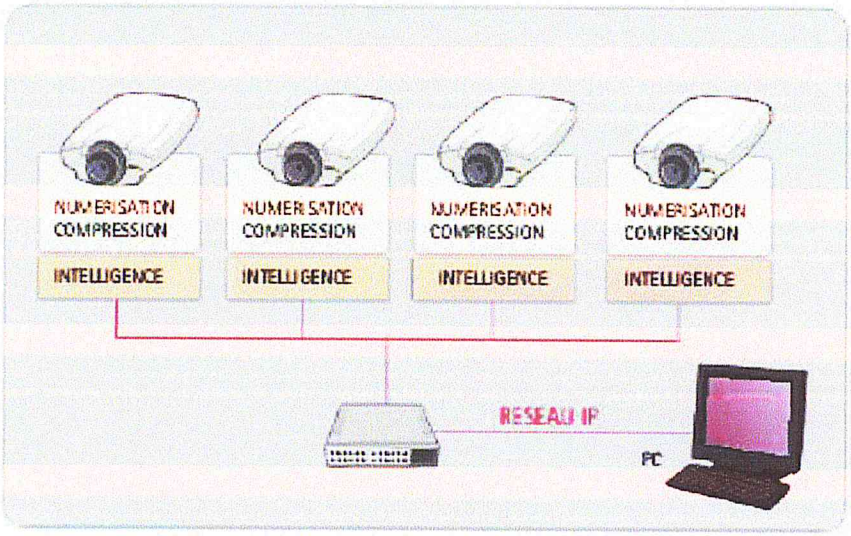


Figure III.9 : système distribué, caméras IP [57].

III.10 Communication dans les systèmes distribués

Pour assurer l'échange entre les différentes machines qui composent un système distribué, il est nécessaire d'utiliser un modèle de communication. Parmi les différents modèles existants, il y'a les services des couches TCP ou UDP qui sont basiques, d'autres de haut niveau comme l'appel d'une procédure à distance ou l'invocation d'une méthode à distance.

III.10.1 Protocoles TCP et UDP

Pour assurer la communication entre les entités d'un système distribué, des protocoles au niveau transport tel que TCP et UDP sont employés. Ces derniers sont implémentés dans des logiciels et du matériel chargés sur chaque entité.

- Protocole UDP (User Datagram Protocol)

UDP propose un mode de transport allégé (en mode non connecté) qui permet de s'affranchir de l'ensemble des lourds mécanismes mis en oeuvre par TCP [59]. En effet, UDP se charge de transporter des datagrammes et les informations qu'ils contiennent, de la source à leur destination sans contrôler ni le flux ni la congestion [58].

- Protocole TCP (Transmission Control Protocol)

TCP est un protocole de niveau transport en mode connecté dit « fiable ». Il garantit, en effet, la délivrance des données en séquence, en contrôle la validité. Il permet aussi d'organiser

un contrôle du flux de bout en bout et met en oeuvre un mécanisme de détection et de gestion de la congestion [59].

III.10.2 Les sockets

Les sockets sont le mécanisme de communication le plus fondamental et le plus adopté par la quasi-totalité des systèmes distribués du fait qu'elles sont supportées par la plupart des systèmes d'exploitation et langages de programmation. Elles ont été introduites en 1982 dans les distributions BSD (Berkley System Distribution) d'Unix dans le but, au même titre que les tubes ou la mémoire partagée, de fournir un mécanisme de communications interprocessus. L'intérêt des sockets, par rapport aux autres mécanismes d'IPC (Inter-Process Communication), vient notamment du fait qu'elles permettent à des processus de communiquer entre eux à travers un réseau [60].

Un socket permet à un processus (le client) d'envoyer un message à un autre processus (le serveur), celui-ci peut alors effectuer toute sorte de tâches et éventuellement retourner un résultat au processus client.

III.11 Sécurité des réseaux

Une communication sécurisée se déroule selon trois étapes distinctes :

- **Authentification** : Cette étape doit permettre à l'utilisateur ou au périphérique de s'identifier sur le réseau ou l'hôte distant. Pour ce faire, certaines données d'identité sont communiquées au réseau ou au système, comme par exemple un code d'utilisateur et un mot de passe, un certificat X509 (SSL), et le recours à la norme 802.1x.

- **Autorisation :** cette étape consiste à autoriser et à accepter l'authentification, c'est-à-dire à vérifier si la machine est bien celle qu'elle prétend être. On vérifie à cet effet l'identité donnée par rapport aux informations contenues dans la base de données ou dans une liste d'identités réputées correctes et approuvées. Au terme de l'autorisation, la machine est totalement connectée et opérationnelle dans le système.

- **Confidentialité :** cette étape c'est la dernière consiste à appliquer le degré de confidentialité souhaité. Pour ce faire, la communication est cryptée afin que les

données ne puissent être utilisées ou lues par personne d'autre. Selon le type de déploiement et de chiffrement utilisé, il peut arriver que le recours au cryptage nuise assez fortement aux performances. La confidentialité peut être assurée de plusieurs façons. [61]

III.12 Définition du modèle client/serveur

Le modèle client-serveur s'articule autour d'un réseau auquel sont connectés deux types d'ordinateurs le serveur et le client. Le client et le serveur communiquent via des protocoles. Les applications et les données sont réparties entre le client et le serveur de manière à réduire les coûts. Le client-serveur représente un dialogue entre deux processus informatiques par l'intermédiaire d'un échange de messages. Le processus client sous-traite au processus serveur des services à réaliser. Les processus sont généralement exécutés sur des machines, des OS et des réseaux hétérogènes [55].

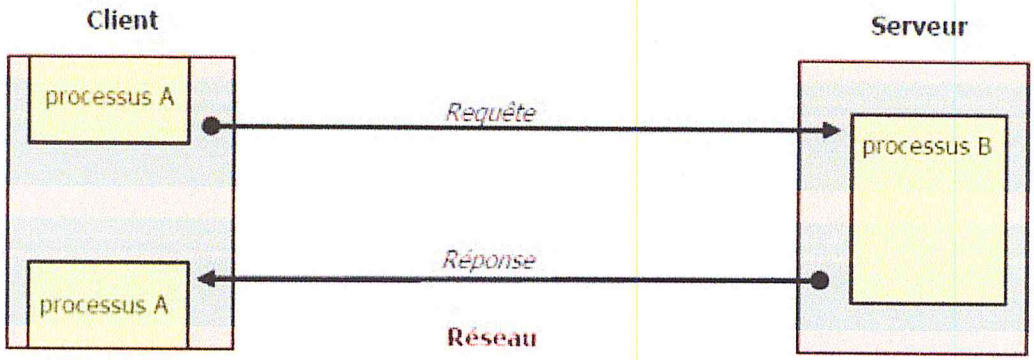


Figure III.10: Le modèle client/serveur

III.12.1 Caractéristiques des systèmes client-serveur

Les éléments qui caractérisent une architecture client-serveur sont [55] :

- **Service**

Le modèle client-serveur est une relation entre des processus qui tournent sur des machines séparées. Le serveur est un fournisseur de services. Le client est un consommateur de services.

- **Partage de ressources**

Un serveur traite plusieurs clients et contrôle leurs accès aux ressources

- **Protocole asymétrique**

Conséquence du partage de ressources, le protocole de communication est asymétrique le client déclenche le dialogue ; le serveur attend les requêtes des clients.

- **Transparence de la localisation**

L'architecture client-serveur doit masquer au client la localisation du serveur (que le service soit sur la même machine ou accessible par le réseau). Transparence par rapport aux systèmes d'exploitation et aux plates-formes matérielles. Idéalement, le logiciel client serveur doit être indépendant de ces deux éléments

- **Message**

Les messages sont les moyens d'échanges entre client et serveur.

- **Encapsulation des services**

Un client demande un service. Le serveur décide de la façon de le rendre une mise à niveau du logiciel serveur doit être sans conséquence pour le client tant que l'interface message est identique.

- **Evolution**

Une architecture client-serveur doit pouvoir évoluer horizontalement (évolution du nombre de clients) et verticalement (évolution du nombre et des caractéristiques des serveurs).

III.12.2 La répartition des tâches

Dans l'architecture client/serveur, une application est constituée de trois parties [55] :

- L'interface utilisateur
- La logique des traitements
- La gestion des données

Le client n'exécute que l'interface utilisateur (souvent un interfaces graphique) Ainsi que la logique des traitements (formuler la requête), laissant au serveur de bases de données la gestion complète des manipulations de données

La liaison entre le client et le serveur correspond à tout un ensemble complexe de logiciels appelé middleware qui se charge de toutes les communications entre les processus.

III.12.3 Les différents modèles de client/serveur

En fait, les différences sont essentiellement liées aux services qui sont assurés par le serveur [55]. On distingue couramment :

- Le client -serveur de donnée

Dans ce cas, le serveur assure des taches de gestion, stockage et de traitement de donnée .c'est le cas le plus connu de client- serveur est utilisé par tous les grands SGBD :

La base de données avec tous ses outils (maintenance, sauvegarde….) est installée sur un poste serveur.
Sur les clients, un logiciel d'accès est installé permettant d'accéder à la base de données du serveur
Tous les traitements sur les données sont effectués sur le serveur qui renvoie les informations demandées par le client.

- Le client -serveur de présentation

Dans ce cas la présentation des pages affichées par le client est intégralement prise en charge par le serveur. Cette organisation présente l'inconvénient de générer un fort trafic réseaux.

- Le client –serveur de traitement

Dans ce cas, le serveur effectue des traitements a la demande du client .Il peut S'agir de traitement particulier sur des données, de vérification de formulaire de saisie, de traitements d'alarmes Ces traitements peuvent être réalisés par des programmes installés sur des serveurs mais également intégrés dans des bases de données, dans ce cas, la partie donnée et traitement sont intégrés.

III.12.4 Présentation de l'architecture de système

- Présentation de l'architecture à 2 niveaux

L'architecture à deux niveaux (aussi appelée *architecture 2-tier*, *tier* signifiant *rangée* en anglais) caractérise les systèmes clients/serveurs pour lesquels le client demande une ressource

et le serveur la lui fournit directement, en utilisant ses propres ressources. Cela signifie que le serveur ne fait pas appel à une autre application afin de fournir une partie du service.

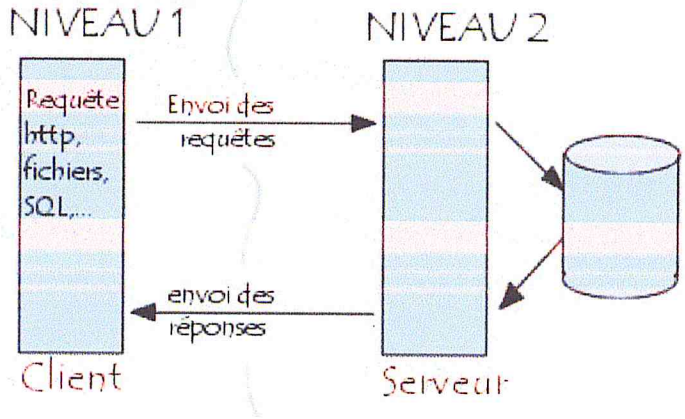


Figure III.11 : Architecture a 2 niveaux

- **Présentation de l'architecture à 3 niveaux**

Dans l'architecture à 3 niveaux (appelée *architecture 3-tier*), il existe un niveau intermédiaire, c'est-à-dire que l'on a généralement une architecture partagée entre :

1. Un client, c'est-à-dire l'ordinateur demandeur de ressources, équipée d'une interface utilisateur (généralement un navigateur web) chargée de la présentation ;
2. Le serveur d'application (appelé également middleware), chargé de fournir la ressource mais faisant appel à un autre serveur
3. Le serveur de données, fournissant au serveur d'application les données dont il a besoin.

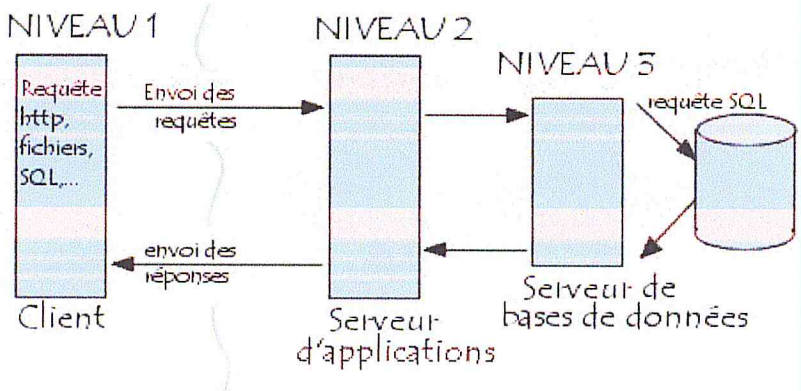


Figure III.12 : Architecture a 3 niveaux

III.13 Conception et Modalisation

III.13.1 Langage de modélisation

Nous allons décrire le côté conceptuel de notre plateforme en utilisant la notation UML (Unified Modeling Language), qui est un langage qui fournit des outils permettant de modéliser le système à concevoir [62].

III.13.2 Diagramme de cas d'utilisation

Dans ce cas d'utilisation, l'utilisateur fournir son nom d'utilisateur et le mot de passe pour pouvoir accéder au système si les informations sont incorrectes un message d'erreur doit apparaitre.

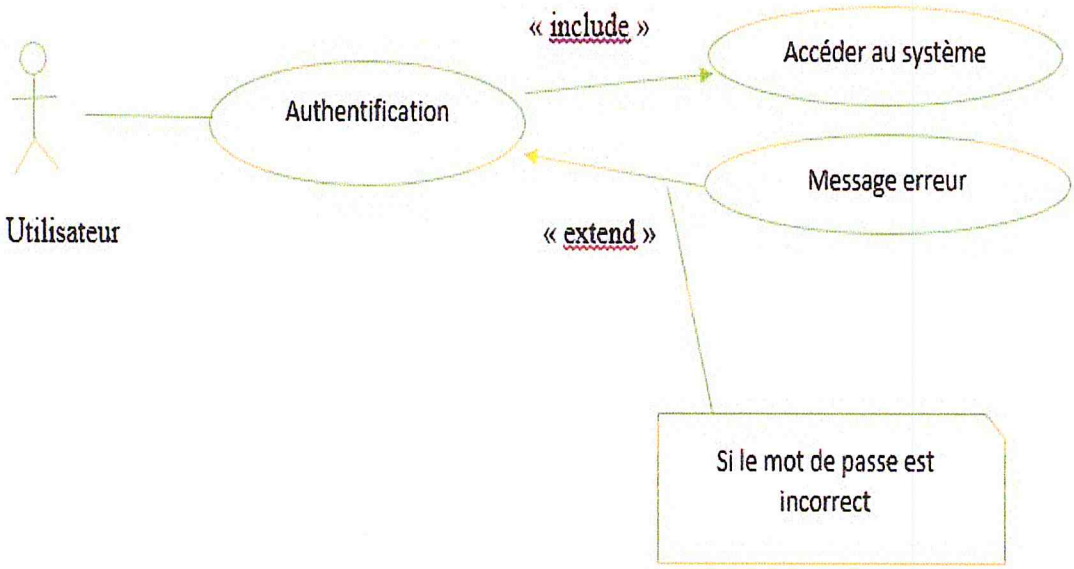


Figure III.13 : Diagramme de cas d'utilisation « Authentification »

Dans ce cas d'utilisation, l'administrateur peut accéder au système en ajoutant ou en supprimant des visages ainsi de reconnaitre des personnes.

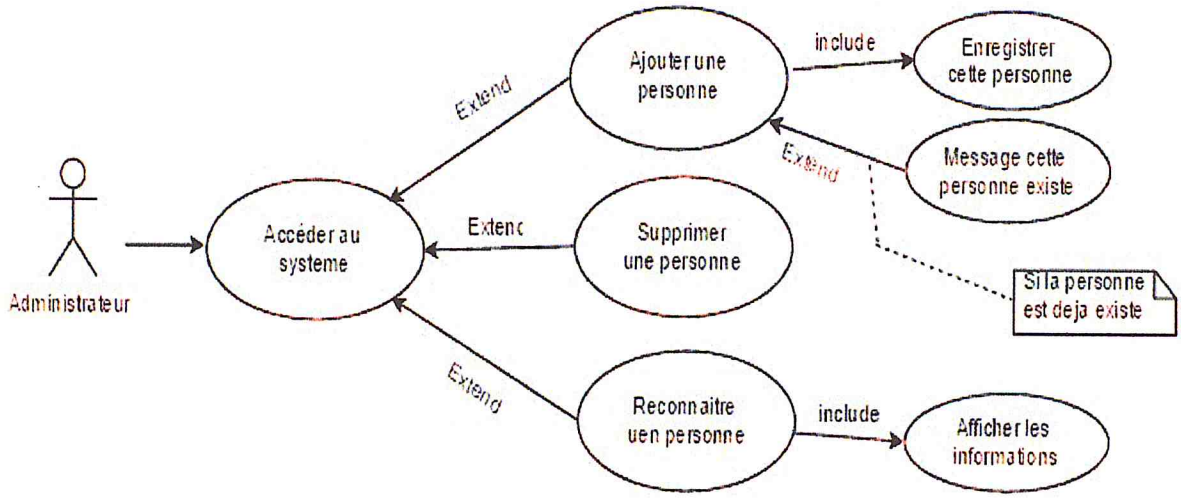


Figure III.14 : Diagramme de cas d'utilisation « administrateur »

Dans ce cas d'utilisation, l'utilisateur a une seule fonctionnalité avec laquelle il peut faire la reconnaissance des personnes.

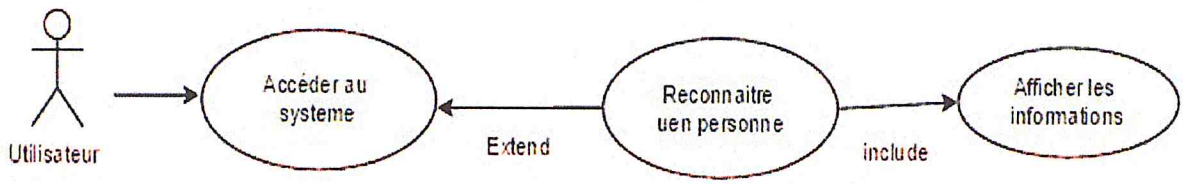


Figure III.15 : Diagramme de cas d'utilisation

III.13.3 Description du diagramme de cas d'utilisation

Cas d'utilisation	Description
Accéder au système	Accéder au système si l'opération est réussie
Message erreur	Afficher le message d'erreur si l'opération est fausse
Détection et Ajouter	Détection et l'ajoute de la nouvelle personne
Enregistrer une personne	Ajouter les informations et les images d'une personne

Reconnaitre une personne	Identification de visage détecté
Afficher les informations	Affichage les informations de la personne détecté
Message cette personne existe	Afficher un message si la personne est existe déjà dans la base de données
Supprimer une personne	La suppression d'une personne qui est dans la base de données

Tableau III.1 : Description du diagramme de cas d'utilisation

III.13.4 Diagramme de séquence

Dans ce diagramme de séquence, l'utilisateur doit fournir le mot de passe pour accéder au système :

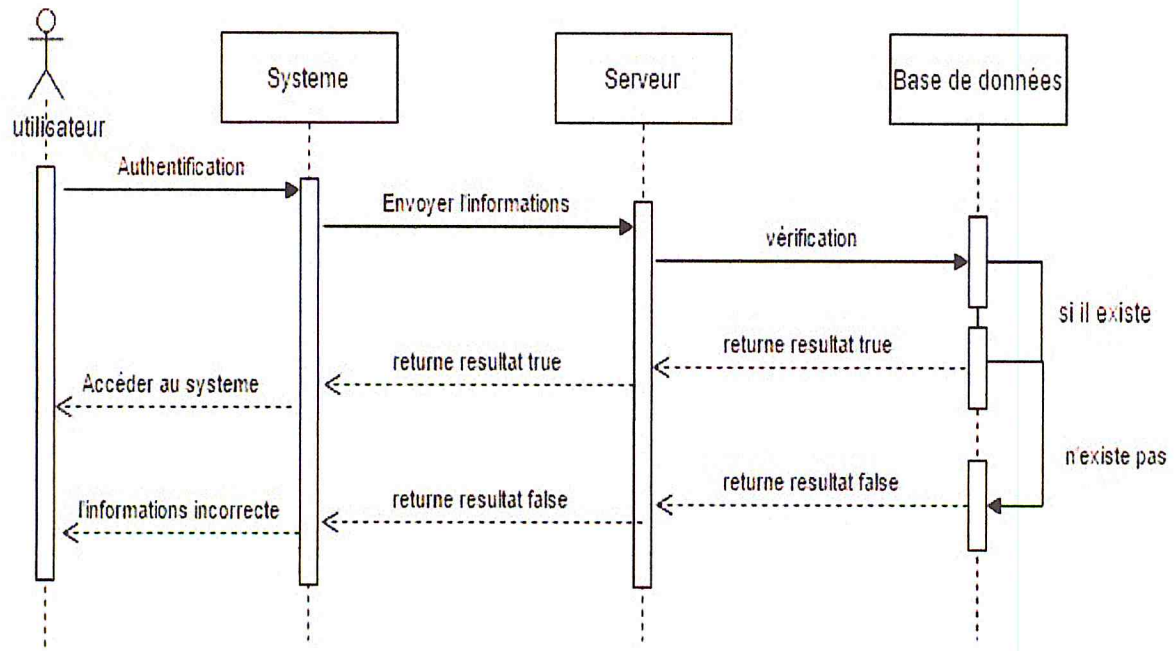


Figure III.16 : Diagramme de séquence « Authentification »

Dans ce diagramme de séquence, l'administrateur après avoir fournir le mot de passe il accède au système, il ajoute une nouvelle personne avec ces images capturés à l'aide d'une caméra, Et le système vérifiera si la personne est existe déjà dans la base de données, si oui donc un message dire qu'il est déjà dans la base sinon il enregistre cette personne.

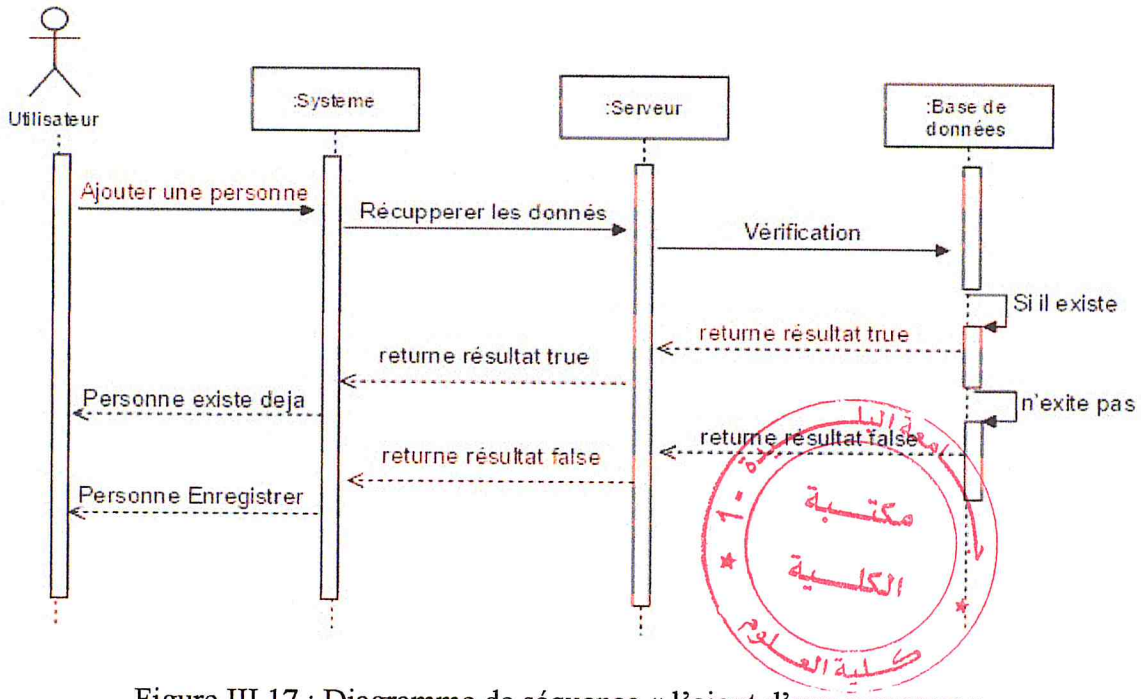


Figure III.17 : Diagramme de séquence « l'ajout d'une personne »

Dans ce diagramme de séquence, la reconnaissance est fait par la comparaison l'image de l'individu avec toute les images dans la base de données, si il y a une similarité le system va return une résultat true et affiche ID de cette personne sinon la résultat est false et le système affiche un message « personne inconnu »

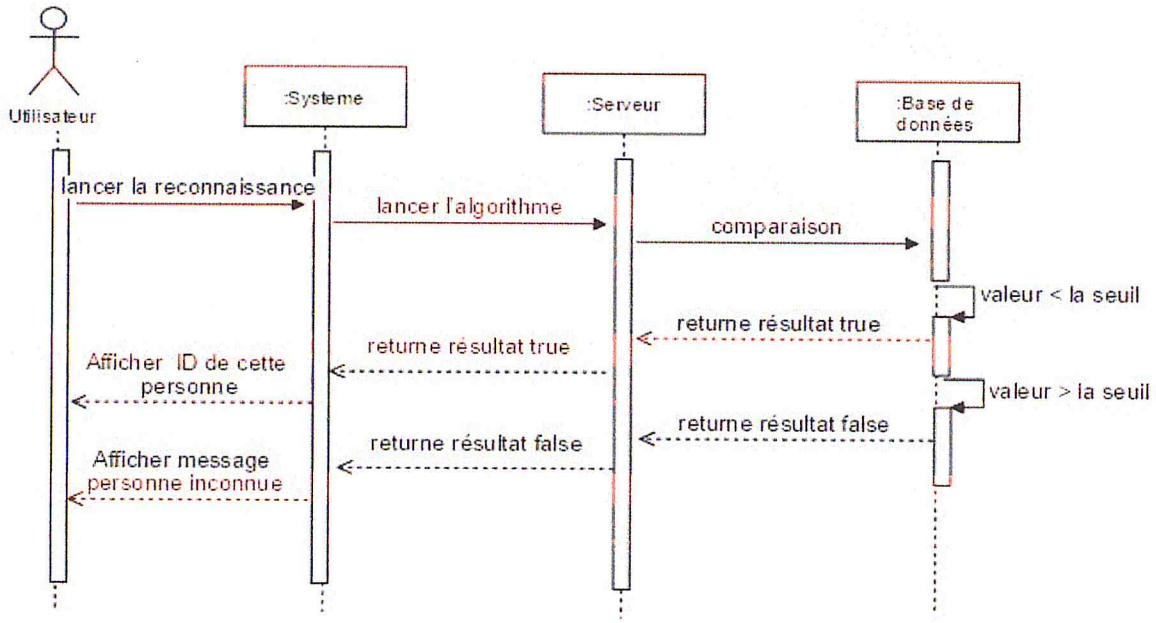


Figure III.18 : Diagramme de séquence « Reconnaissance »

III.13.5 Diagramme de classes

Le diagramme de classes représente la structure statique d'un système, il montre les différentes classes et les relations qui existent entre elles Figure III.18.

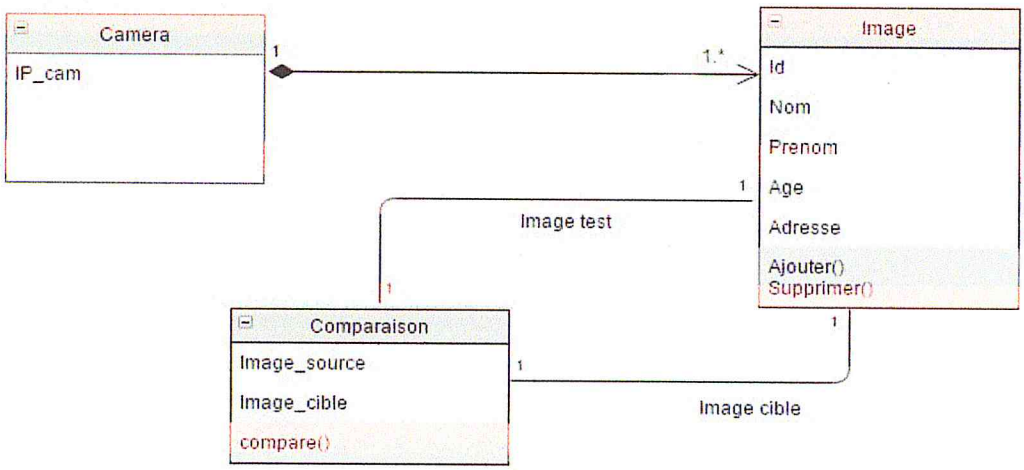


Figure III.19 : Diagramme de classes

III.13.6 Description des classes

Nom de classe	Identifient	Attribut	Type
Camera	IP_cam	IP_cam	varchar

Nom de classe	Identifient	Attribut	Type
Image	id	id	integer
		Nom	varchar
		Prenom	varchar
		Age	integer
		Adresse	varchar

Nom de classe	Identifient	Attribut	Type
Comparaison		Image_source	binary
		Image_cible	binary

Tableau III.2 : Description de diagramme de classe

III.14 Conclusion

Dans ce chapitre nous avons présenté deux parties :

La première partie nous avons détaillé la méthode de Viola et Jones [44,49] pour la détection de visage et Eigenface (PCA) pour la reconnaissance de visage. Ensuite nous avons parlé sur l'architecteur et les fonctions de notre système vidéosurveillance intelligente.

Dans la deuxième partie nous avons modélisé le fonctionnement du système. Ceci est fait à travers différents diagrammes permettant de bien spécifier la composition et le comportement de l'application.

Dans le chapitre suivant nous allons implémenter de ce que nous avons proposé dans ce chapitre.

CHAPITRE IV
IMPLEMENTATION

IV.1 Introduction

La dernière étape du processus de développement concerne l'implémentation de l'application en fonction des technologies choisies. Nous allons tout d'abord, présenter l'environnement matériel et logiciel utilisés pour développer notre projet et à la fin nous allons présenter aussi les interfaces de l'application.

IV.2 L'application sur le téléphone portable

Puisque nous voulons réutiliser les fonctions disponibles de la détection de visages et l'algorithme Eigenface avec la librairie OpenCV, et nous devons utiliser le SDK pour développer sur Android. SDK est une plate-forme de programmation qui permet au code Java qui s'exécute dans une machine virtuelle Java (JVM) d'appeler les bibliothèques écrites dans d'autres langages.

Le programme comporte deux étapes. D'abord, lorsqu'il est exécuté, la vidéo de la caméra est affichée. La détection des visages peut être faite. Le résultat retourné est l'image du visage détecte, envoie au serveur et enregistrer dans la base de données. Ensuite, on peut commencer l'étape de reconnaissance en appuyant sur le bouton « Reconnaissance » dans le menu du programme. Une ligne de texte annonce la personne reconnue.

IV.3 Environnement du travail

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

IV.3.1 Environnement matériel

Afin de mener à bien ce projet, il a été mis à notre disposition un ensemble de matériels

- **Un Ordinateur**

Un ordinateur Dell avec les caractéristiques suivantes :

– Processeur : Intel® Core(TM) i3 CPU M 380 @ 2.53Ghz

– RAM : 4.00 Go de RAM

– Disque Dur : 320 Go

– OS : Microsoft Windows 8

- **Téléphone Mobile**

Nous avons choisi le téléphone Lenovo A319 avec le système d'exploitation Android pour réaliser le programme de détection et reconnaissance de visages. Sa spécification est la suivante

Processeur : MTK 1.3GHz.
Système d'exploitation : Android™ 4.4 KitKat
Mémoire : ROM: 1 GB / RAM: 512 MB
Affichage Ecran : 10,16 cm (4.0 ') WVGA (800x480) TN
Camera : 5 MP auto-focus w/LED flash

IV.3.2 Environnement logiciel

- **Langage de Programmation (JAVA) :**

Est un langage orienté objet de type sécurisé et élégant qui permet aux développeurs de générer diverses applications sécurisées et fiables. Vous pouvez utiliser le langage Java pour créer entre autres des applications clientes Windows, des applications Mobiles, des composants distribués, des applications client-serveur et des applications de base de données. Nous avons choisi d'utiliser JAVA comme langage de programmation puisqu'il présente un intérêt majeur de portabilité. Pour développer notre système, nous avons exploité :
La version Luna Service Release 2 (4.4.2). Et JDK (8.6.0)

- **SGBD (SQL Server) :**

SQL Server est un système de gestion de base de données développé et commercialisé par la société Microsoft. Il est considéré parmi les leaders mondiaux des SGBD. Pour notre travail nous avons adopté la version SQL Server 2008 afin de profiter de sa simplicité et sa facilité d'utilisation avec le langage de programmation choisi JAVA.

- **La Bibliothèque OpenCV :**

OpenCV (Open source Computer Vision library), est une bibliothèque de traitement d'images et de vision par ordinateur, disponible sur le site web [41], OpenCV a été conçu pour l'efficacité de calcul et les applications en temps réel. Ainsi, la bibliothèque est écrite en C

le domaine de vision par ordinateur qui aide les utilisateurs à construire des applications assez sophistiqués rapidement.

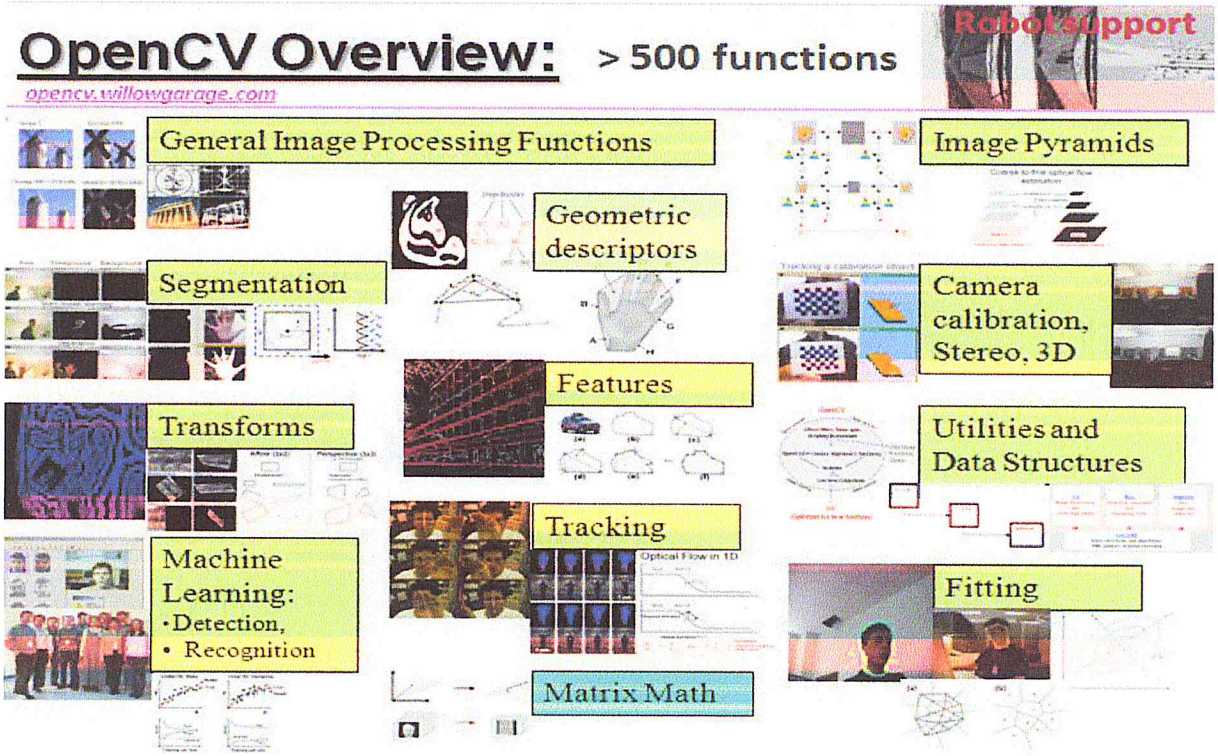


Figure IV.1 : Une vue générale de librairie OpenCV [42]

La bibliothèque OpenCV contient plus de 500 fonctions qui couvrent de nombreux domaines de la vision ordinateur y compris l'imagerie médicale, la sécurité, l'interface utilisateur, étalonnage de la caméra, la vision stéréoscopique, et la robotique. Elle propose la plupart des opérations classiques en traitement bas niveau des images :

- lecture et affichage d'une image ou d'une vidéo (fichier ou caméra), écriture sur le disque
- filtrage, lissage
- calcul de l'histogramme des niveaux de gris ou d'histogrammes couleurs
- binarisation, segmentation en composantes connexes
- morphologie mathématique

La bibliothèque OpenCV se compose des 4 composantes principales, dont 4 (CXCORE, CV, Machine Learning (MML), highGUI) [43].

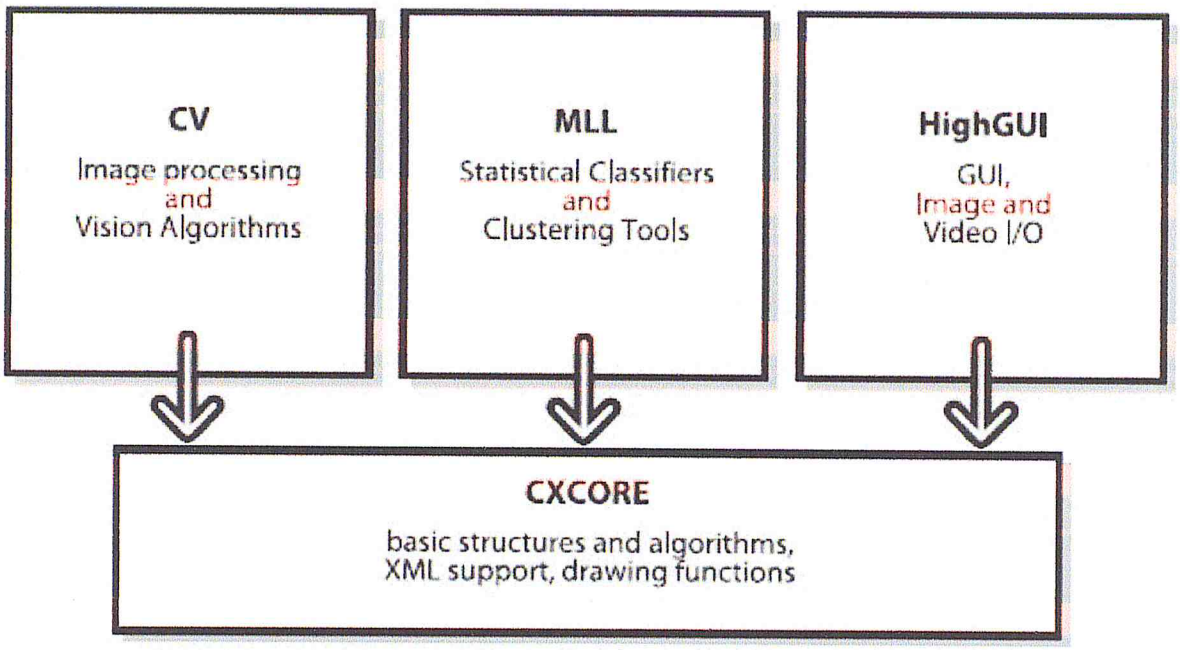


Figure IV.2: La structure de la librairie OpenCV [43]

CXCORE : Contient les structures de données, les calculs matriciels, la transformation des données, la persistance des objets, la gestion de mémoire, la gestion des erreurs, et le chargement dynamique de code, ainsi que la structure de données du dessin, du texte et des mathématiques.

CV : Contient le traitement d'image, de la reconnaissance des formes, l'analyse de la structure d'image, du mouvement et suivi, et la calibration de la caméra.

ML : Contient le regroupement, la classification et les fonctions d'analyse de données.

HighGUI : Contient une interface graphique d'utilisateur et le stockage des 'images ou de la vidéo.

En outre, il existe encore un composant important qui n'apparait pas dans la Figure IV.2. Il est le composant CvAux qui la reconnaissance de visage en utilisant un modèle caché de Markov (HMM Ŕ Hidden Markov Model) et les algorithmes expérimentaux de segmentation. CvAux couvre :

- objets Eigen, une technique de reconnaissance de calcul efficace qui est, par essence, une procédure modèle correspondant
- 1D et 2D modèles cachées de Markov, une technique statistique de reconnaissance résolue par programmation dynamique.

- Les descripteurs de texture
- Le suivi des yeux et de la bouche
- Le suivi 3D
- Trouver les squelettes des objets dans une scène
- Vidéo surveillance

Nous allons travailler avec cette bibliothèque, car elle possède un algorithme de détection de visage et la reconnaissance qui nous intéresse.

IV.4 Interfaces graphique de l'application

Dans ce qui suit, nous allons présenter les principales fonctionnalités de notre application. Notre plateforme interagit avec deux types d'acteur, à savoir : l'administrateur, l'utilisateur simple. Chacun des acteurs à un droit de certain fonction lui permettant de communiquer et d'interagir avec la plateforme.

- **Administrateur** : a le droit de tout, ajouter et supprimer des personnes ainsi la reconnaissance des visages, il peut aussi voir les visages qui sont dans la base de données.
- **Utilisateur** : à un seul droit est d'accéder à l'interface de la reconnaissance de visages

Afin de montrer les différentes interactions, nous allons présenter chacune des interfaces.

- **Interface Login**

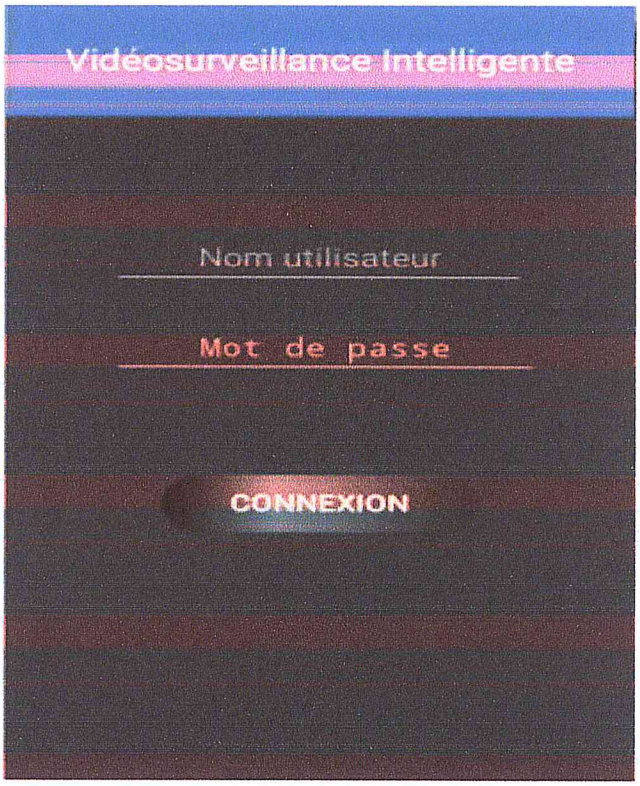


Figure IV.3 : Interface Login

Cette interface s'affiche au lancement de chacune des applications (administrateur, utilisateur) et pour accéder à l'interface principale du système, elle exige à l'utilisateur de renseigner les informations nécessaires afin de lui permettre de se connecter à la plateforme. Les informations sont le nom d'utilisateur et le mot de passe si la vérification est réussie le système ouvre l'interface principale. Sinon un message d'erreur qui indiquera la vérification a échoué.

- **l'interface principale**

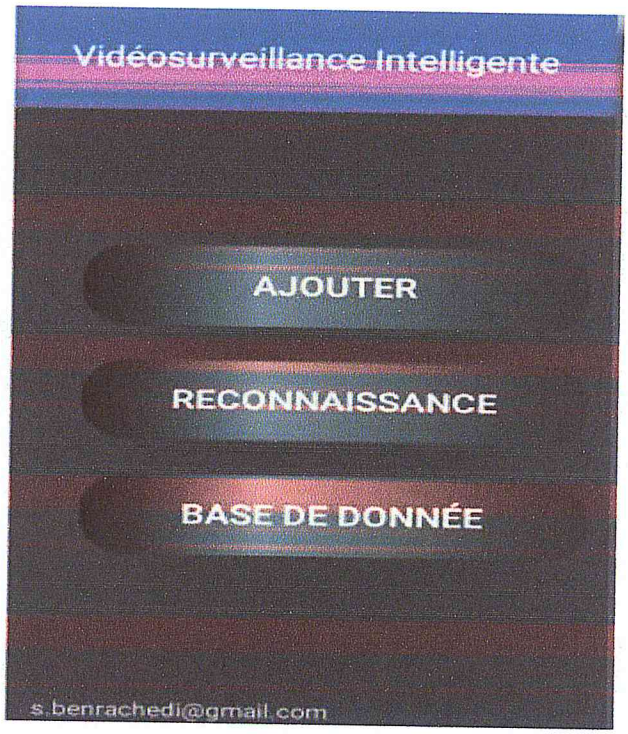


Figure IV.4: Interface Principale

Cette interface présente le menu principal elle se compose de trois boutons :

- **Ajouter** : pour accéder l'interface de la détection et l'ajout d'une nouvelle personne
- **Reconnaissance** : pour accéder à l'interface de la reconnaissance d'un individu
- **Base de données** : pour accéder à l'interface qui contient tous les visages de notre base

- **IV.4.3 l'interface détection et ajoute**

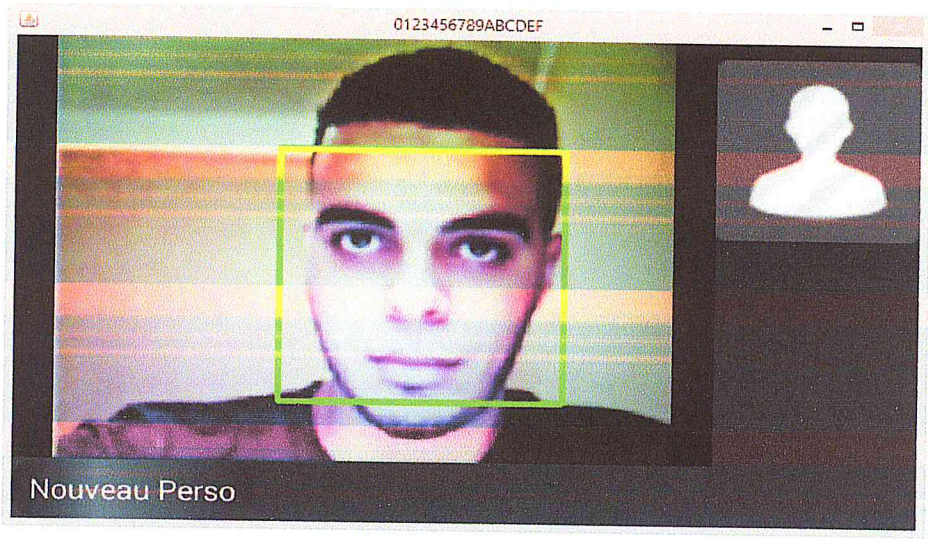


Figure IV.5 : Interface de détection

Dans (Figure IV.5) On cliquant sur le bouton « Nouveau Person » une nouvelle fenêtre (Figure IV.6) doit apparaitre pour remplir les informations ainsi que les images capturée concernant la personne détectée pour qu'on fin de compte ces informations seront sauvegarder en base de donnée.

Pour une seul personne nous allons besoin d'une plusieurs images pour l'utiliser dans l'étape de la reconnaissance de visage, et à chaque fois qu'on cliquant sur ajouter l'l'image va aperçu a droit en haut dans l'ImageView. Ensuite l'image doit être convertir au niveau de gris et redimensionné la taille en 120*120.

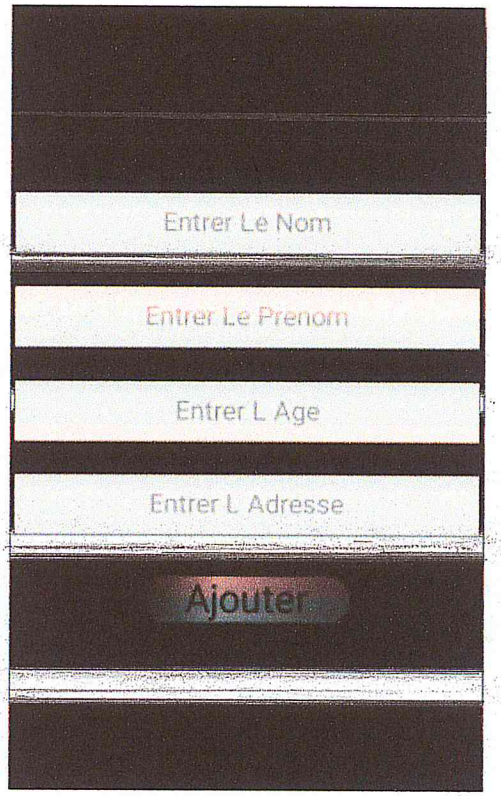


Figure IV.6: Interface de formulaire

- **l'interface de Reconnaissance**

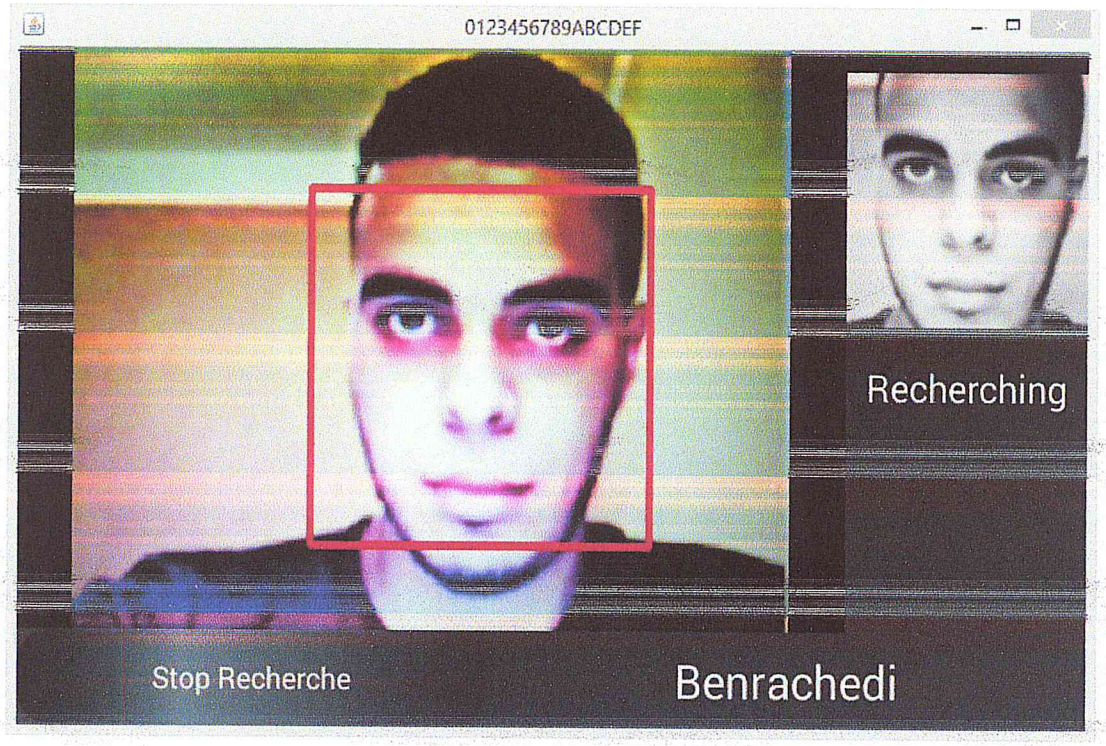


Figure IV.7: l'interface de Reconnaissance

On cliquant sur le bouton « Start Recherche » (Figure IV.7) le système se lance à la recherche d'une personne correspondante au profil de la personne qui est présente à la camera. S'il y a une similarité des caractéristiques le système doit indiquer un carreau rouge sur le visage avec un complément d'informations sur cette personne. Par contre si le résultat est négatif le système indiquera un carreau vert.

- **l'interface de La Base de données**

Figure IV.8 : l'interface de La Base de données

Cette interface (Figure IV.8) nous permet de visualiser tous les visages existants dans la base de données.

Pour supprimer une personne on doit cliquer sur son image, une fenêtre s'ouvrira qui apparaitra ses images avec un bouton « supprime »

IV.5 Résultats des expériences

Parce que nous avons utilisé deux algorithmes la détection (Viola et Jone) avec les caractéristiques haar et la reconnaissance (Eigenface PCA) sur un téléphone mobile, nous allons présenter les résultats obtenus lors du test :

Ces approches ont certains points forts. Tout d'abord, ils sont les techniques avec la plus grande précision, en moyenne 90% pour la détection et 80%-90% pour la reconnaissance, dépendant de la base de données. Ensuite, ils ont une très bonne vitesse d'exécution, 0,1 seconde pour détecter un visage et 2 seconde pour la reconnaissance d'un visage en utilisant une base de données de 25 images. L'algorithme de la reconnaissance dépend beaucoup de la

base d'image pour l'apprentissage. Si la base d'images est trop grande, la recherche du visage plus proche prendra trop longtemps. Si la base d'images n'est pas très riche du point de vue des conditions différentes de la scène, comme celles d'éclairage ou résolution, cet algorithme ne donne pas de bons résultats.

Dans le tableau suivant on présente les résultats de taux d'exécution pour les étapes de détection et reconnaissance pour l'application sur le téléphone portable.

	Taux d'exécution
La Détection	Entre 90% et 95%
La Reconnaissance	environ 80%

Tableau IV.1 : Résultat de taux d'exécution sur et sur le téléphone portable pour la détection et la reconnaissance

IV.6 Conclusion

Dans ce chapitre, nous avons présenté notre application, en commençant par décrire l'environnement de développement ainsi que les outils logiciels et matériels utilisés pour la réalisation de l'application. Et nous avons aussi défini les déférentes interfaces et les fonctions présenter par le système.

CONCLUSION GENERALE

Conclusion Générale

Le but final a été de construire une application vidéosurveillance intelligente sur une téléphone mobile on appliquant des techniques de la détection et la reconnaissance de visages, à partir d'un camera de mobile on détecte un visage puis compare ce visage détecte avec la base de données des visages si la comparaison est positif, caméra faite une alerte ainsi affiché les informations de ce visage et envoyé son id au serveur,

Pour la détection nous avons utilisé l'algorithme de Viola et Jones [44,49] avec les caractéristiques Haar de la librairie OpenCV, et Pour la reconnaissance nous avons appliqué l'algorithme Eigenface (PCA) [26, 27]. Ces approches ont certains points forts. Tout d'abord, ils sont les techniques avec la plus grande précision, en moyenne 90% pour la détection et 80%-90% pour la reconnaissance, dépendant combien de visage dans la base de données.

Dans un premier temps, nous avons vu les différents types et caractéristiques des systèmes biométrie existants dans différents domaines. Par la suite, nous avons étude une bibliographique dans laquelle nous avons dressé un état de l'art sur les différents techniques de la détections et la reconnaissance de visages, ensuite nous avons abordé sur l'architecture distribuée adoptée à notre système et les technologies utilisées, plus spécifiquement les sockets, constituant d'ailleurs le moyen de communication utilisé au sein de notre plateforme.

Par la suite, nous avons présenté une conception détaillée de notre système conformément à l'architecture distribuée et en s'appuyant sur le paradigme client / serveur, nous avons présenté ses différentes fonctionnalités que nous avons expérimentées à travers des tests réels dans le dernier chapitre qui concerne la réalisation.

Bibliographie

[01] R. M. Bolle, J. H. Connell, S. Pankanti, N. K. Ratha, and A. W. Senior. « The Relation between the ROC Curve and the CMC». In : Proceedings of the Fourth IEEE Workshop on Automatic Identification Advanced Technologies, pp. 15- 20, 2005.

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

[03] Saliha Artabaz « biométrie multimodale ».Ecole doctorale. Institut National de formation en Informatique (I.N.I)», Min projet, Alger, 2009/2010.

[04] J. Daugman « Iris Recognation » Handbook of Biométrics S.1 Spring. 2008.

[05] T. Amellal, K. Benakli, « Système de reconnaissance de visage basé sur les GMM ». Institut National de formation en Informatique (I.N.I), Alger, 2007.

[06] Zhifeng Li et Xiaoou Tang « EIGENFACE RECOGNITION USING DIFFERENT TRAININGDATA SIZES », Département of Information Engineering The Chinese University of Hong Kong Shatin, N.T., Hong Kong, 2006.

[07] Liméry Lionel , Fao Frédéric , Guiraud Ludovic, reconnaissance des empreintes digitale serrure biométrique, 2005.

[08] M. Elhaddad, M. et M. Banamar « Conception et réalisation d'une plateforme biométrique multimodale basée sur la fusion en Scores » Institut National de formation en Informatique (I.N.I), Alger, 2008.

[09] N. Morizet «Reconnaissance Biométrique par Fusion Multimodale du Visage et de l'Iris », Télécom ParisTech, Mars 2009

[10] http://www.biometrie-online.net/

[11] R. Beveridge and M. Kirby. « "Biometrics and Face Recognition". Colloquium, p. 25,» 2005.

[12] M. Hsuan Yang, D.J. Kriegman et N. Ahuja. Detecting faces in images : A survey. Dans IEEE Transactions on Pattern Analysis and Machine Intelligence, volume 24(1), pages 34–58, 2002.

[13] M. Turk and A. Pentland. "Eigenfaces for recognition". Journal of Cognitive Neuroscience, Vol. 3, No. 1, pp. 71–86, 1991.

[14] H. A. Rowley, S. Baluja, et T. Kanade, "Neural Network based Face Detection", IEEE Trans, Pattern Anal. Mach, Intell, 23-38, January 1998

[15] C. Kotropoulos and I. Pitas. « Rule-Based Face Detection in Frontal Views ». Proc. Int'l Conf. Acoustics, Speech and Signal Processing, vol. 4, pp. 2537-2540, 1997.

[16] T. Kanade. « Picture Processing by Computer Complex and Recognition of Human Faces », PhD thesis, Kyoto Univ., 1973.

[17] J. Yang, D. Zhang, A.F. Frangi, J. Yang, « Two-dimensional PCA: a new approach to appearance-based face representation and recognition », IEEE Trans. Pattern Anal. Mach. Intell. 131–137,2004.

[18] P. Sinha, "Processing and Recognizing 3D Forms," PhD thesis, Massachusetts Inst. of Technology, 1995.

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

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

[21] L. C. De Silva, K. Aizawa, and M. Hatori, Detection and tracking of facial features by using a facial feature model and deformable circular template, IEICE Trans. Inform. Systems E78–D(9), 1195–1207, 1995.

[22] A.J. O'Toole, H. Abdi, Low-dimensional representation of faces in higher dimensions of the face space, Opt. Soc. Am. 10 (3), 405–411,1993.

[23] A.K. Jain, B. Chandrasekaran. Dimensionality and sample size considerations in pattern recognition practice, in: P.R. Krishnaiah, L.N. Kanal (Eds.), Handbook of Statistics, vol. 2, pp. 835–855, 1982.

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

[25] S.J. Raudys, A.K. Jain, Small sample size effects in statistical pattern recognition: recommendations for practitioners, IEEE Trans. Pattern Anal. Mach. Intell. 13 (3) 252–264, 1991.

[26] L. Sirovich, M. Kirby, Low-dimensional procedure for the characterization of human faces, J. Opt. Soc. Am. A 4 (3) (1987) 519–524.

[27] M. Turk and A. Pentland. "Eigenfaces for Recognition," J. Cognitive Neuroscience, vol. 3, no. 1, pp. 71-86, 1991.

[28] A. Martinez, A.C. Kak. PCA versus LDA. IEEE Trans. Pattern Anal. Mach. Intell. 23 (2) 228–233, 2001.

[29] W. Zhao, R. Chellappa, P.J. Phillips, Subspace linear discriminant analysis for face recognition, Technical Report CAR-TR-914, Center for Automation Research, University of Maryland, 1999.

[30] S. Haykin, "Neural Networks_ A comprehensive Foundation", Livre, Macmilan College Publishing Company, 1994.

[31] Z. Zhang, M. Lyons, M. Schuster et S. Akamatsu, "Comparison between Geometry-Based and Gabor Wavelets-Based Facial Expression Recognition Using Multi-Layer Perceptron", IEEE International Conference on Automatic Face and Gesture Recognition, pages 454–459, Avril 1998.

[32] S. Lawrence, C.L. Giles, A. Tsoi, A. Back. Face recognition: a convolutional neural-network approach, IEEE Trans. Neural Networks 8 (1) 98–113, 1997.

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

[34] L. Wiskott, R. Fellous, N. Kruger, C. von Malsburg. Face recognition by elastic bunch graph matching, IEEE Trans. Pattern Anal. Mach. Intell. 775–779, July 1997.

[35] B.S. Manjunath, R. Chellappa, C.V.D. Malsburg, A feature based approach to face recognition, in: Proceedings, IEEE Conference on Computer Vision and Pattern Recognition, vol. 1, pp. 373–378, 1992.

[36] M.D. Kelly. Visual identification of people by computer, Technical Report AI-130, July 1970, Stanford AI Project, Stanford, CA, 1970.

[37] T.S. Lee, Image representation using 2-d Gabor wavelets, IEEE Trans. Pattern Anal. Mach. Intell. 18 (10) 959–971, 1996.

[38] X. Tana, C. Songcan. Face recognition from a single image per person : Asurvey. Pattern Recognition, 2006.

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

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

[41] http://SourceForge.net/projects/opencvlibrary

[42] htttp://opencv.willowgarage.com

[43] https://learningopencv.wordpress.com/2010/05/23/opencv-structure-and-content-overview/

[44] P Viola, MJ Jones, Robust Real-Time Face Detection, International Journal of Computer Vision, 2004 Ŕ Springer.

[45] H. Schneiderman and T. Kanade."A Statistical Method for 3D Object Detection Applied to Faces and Cars". PhD thesis, RI, 2000.

[46] H. Schneiderman and T. Kanade, "A Statistical Method for 3D Object Detection Applied to Faces and Cars" Proc. IEEE Conf. Computer Vision and Pattern Recognition, vol. I, pp. 746-751, 2000.

[47] S.Z. Li, Z.Q. Zhang. FloatBoost Learning and Statistical Face Detection, PAMI(26), No. 9, pp. 1112-1123, 2004.

[48] G. Bradski, A. Kaehler and V. Pisarevsky, "Learning-Based Computer Vision with OpenCV." Intel Technology Journal, May 2005.

[49] P. Viola, M. Jones. Rapid object detection using a boosted cascade of simple features. In Proceedings, IEEE Conference on Computer Vision and Pattern Recognition, 2001.

[50] R. Lienhart, J. Maydt, An Extended Set of Haar-like Features for Rapid Object, Detection. IEEE ICIP 2002, Vol. 1, pp. 900-903, Sep. 2002.

[51] H.A. Rowley, S. Baluja, T. Kanade, Neural Network-Based Face Detection; Computer Vision and Pattern Recognition, Proceedings CVPR '96, IEEE Computer Society Conference, 1996.

[52] D. Roth, M. Yang, N. Ahuja, A Snowbased Face Detector, In Neural Information Processing 12, 2000.

[53] C. Papageorgiou, M. Oren et T. Poggio, "*A General Framework for Object detection*", International Conference on Computer Vision, pages 555-562, Janvier

1998.

[54] P. A. Negri, "Détection et Reconnaissance d'objets structurés : Application aux Transports Intelligents", Thèse, Université Pierre et Marie Curie - Paris VI, France, Septembre 2008.

[55] BELKHOUCHE Souheyla, « Etude et Administration des Systèmes de Supervision dans un Réseau Local », Université Abou Bakr Belkaid– Tlemcen, décembre 2011.

[56] V. Gouaillier, "Intelligent Video Surveillance: Promises and Challenges", Technological and Commercial Intelligent Report, CRIM, Apr 2009.

[57] Fredrik NILSSON, "Intelligent network video: Understanding modern video surveillance systems", CRC Press, 2009.

[58] J. P OSTEL, "User Datagram Protocol"", RFC 768 (Standard), août 1980.

[59] J. POSTEL, "Transmission Control Protocol"", RFC 793 (Standard), septembre 1981. Updated by RFC 3168.

[60] Samir TORKI, "Entités autonomes en environnements virtuels distribués"", Thèse en vue de l'"obtention du doctorat, Toulouse III-Paul Sabatier, 5 décembre 2008.

[61] Guide technique de la vidéo sur IP. [En ligne] www.axis.com , http://www.concept-telecom.fr/doc/techguide.pdf

[62] Y. Layouni, « Méthodologie d'aide à la conception de structures intégrées mixtes » , 2008.

[63] http://www.journaldunet.com/ebusiness/internet-mobile/ventes-smartphone-monde.shtml

[64] X. Tan, S.C. Chen, Z.-H. Zhou, F. Zhang, Recognizing partially occluded, expression variant faces from single training image per person with SOM and soft kNN ensemble, IEEE Trans. Neural Networks 16 (4) 875–886, 2005

[65] N.P. Costen, T.F. Cootes, C.J. Taylor. Compensating for ensemble specific effects when building facial models, Image Vision Comput. 20 673–682, 2002.