

REPUBLICQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE
SCIENTIFIQUE

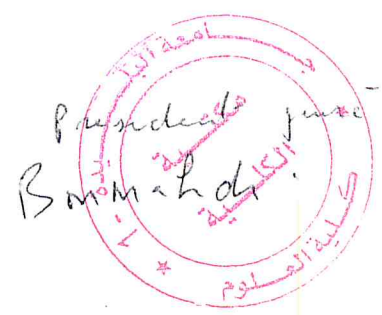
UNIVERSITE SAAD DAHLEB BLIDA
DEPARTEMENT D'INFORMATIQUE



PROJET DE FIN D'ETUDES
Présenté en vue de l'obtention du diplôme
MASTER EN INFORMATIQUE

SUJET :
**CONCEPTION D'UN SYSTEME
D'IDENTIFICATION BASE SUR
LA RECONNAISSANCE FACIALE**

Réalisé par : KHEROUFI Sabri
Encadré par : MANSOURI Khairedine
Supervisé par : AMINE CHERIF ZAHAR



Année Universitaire 2012-2013

MA-004-523-1

Remerciements

Je tiens tout d'abord à remercier DIEU, tout puissant, de m'avoir donné la force de réaliser ce projet tout au long de cette année.

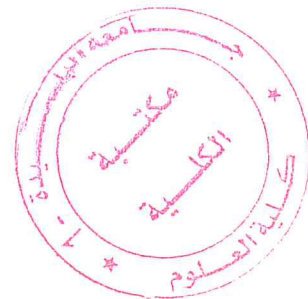
J'adresse mes plus vifs remerciements à mon promoteur Mr. Amine Cherif Zahar pour la confiance qu'il m'a accordé, pour ses précieux conseils, pour ses remarques pertinentes, ainsi que son encouragement sans lequel ce travail n'aurait jamais vu le jour.

Mes remerciements vont aussi à Mon Co promoteur Mr. Manssouri, Pour m'avoir donné les bases essentielles pour pouvoir réaliser ce projet, Pour son immense patience et surtout pour son assistance malgré ses nombreuses occupations.

Mes remerciements vont également à tous les enseignants de l'université Saad Dahleb Blida pour le savoir qu'ils nous ont permis d'acquérir et pour l'esprit d'analyse qu'ils nous ont permis de développer.

Je présente mes gratitudes au président et aux membres du jury qui me font l'honneur de juger mon travail.

Je remercie tous ceux, qui de près ou de loin, m'ont apporté leur contribution pour la réalisation de ce travail, en particulier



Dédicaces

Je dédie ce travail à :

Mes très chère parents, les premières personnes qui ont cru en moi, qui m'ont encouragés et soutenue le long de mon chemin.

Merci pour vos sacrifices, dévouements et surtout de m'avoir fait autant de confiance, de n'avoir jamais douté de mes capacités et de m'avoir inculqué les valeurs justes de la vie, avec autant de sagesse.

A mes très chers frères avec lesquelles j'ai partagé les plus beaux moments de ma vie et que sans eux je n'aurais jamais fait ce progrès.

A ma sœur et son époux qui m'ont soutenue et encourager pour avancer dans la vie, sans oublier ces adorables enfants.

A mes oncles et tantes qui m'ont poussé à continuer jusqu'au bout.

A tous mes cousins et cousines, mes chers amis et tout le reste de la famille, merci pour votre soutien.

Un spéciale dédicace à mon Papa, qui m'a toujours inspiré, il qui a donné un sens à ma vie sans le savoir, ta présence m'a beaucoup aidé, pas seulement pour la préparation de ce mémoire, mais plutôt dans mon existence.

Résumé

Les différents systèmes biométriques visent à établir l'identité d'une personne en mesurant une de ses caractéristiques physiques. Il peut y avoir plusieurs types de caractéristiques physiques, les unes plus fiables que d'autres, mais toutes doivent être infalsifiables et uniques pour pouvoir être représentatives d'un et un seul individu. D'autre part, ces caractéristiques sont loin d'être si parfaites et si précises due aux différentes contraintes qui les portent ou qui sont exigées par l'environnement où le système est mis en œuvre, ce qui pose un vrai problème de performance et de fiabilité.

Nous traitons dans notre étude quelques définitions de l'imagerie numérique et les différents prétraitements et normalisation de l'image, ensuite les différentes méthodes de détection de visage avec les travaux réalisés afin d'établir l'état de l'art.

Ensuite nous allons détailler l'approche qu'on a choisie qui est une approche qui se base sur la détection et l'appariement des attributs faciaux géométriques.

Enfin, on présentera les résultats obtenus à partir d'un test sur une base d'images pour faire un constat sur la performance de notre système.

Mots clés : système biométrique, caractéristiques physiques, imagerie numérique, prétraitement, normalisation, détection de visage, attributs faciaux géométriques, base d'images.

Abstract

The various biometric systems are designed to establish the identity of a person by measuring one of its physical characteristics. There are several types of physical characteristics, the ones are more reliable than other ones, but all must be unfalsifiable and unique to be representative of one and only one individual. On the other hand, these characteristics are far from perfect and if so accurate due to the various constraints that carry or required by the environment in which the system is implemented. This causes a serious problem of performance and reliability.

We deal in our study some definitions of digital imaging and various pretreatments and standardization of image, then the various face detection methods with the work carried out to establish the state of the art.

Then we will detail the approach we have chosen which is an approach that is based on the detection and matching of the facial geometric attributes.

Finally, the results obtained from a test on an image database will be presented to make a statement on the system performance.

Key-words: biometric systems, physical characteristics, digital imaging, pretreatment, standardization, face detection, facial geometrics attributes, image data base.

ملخص

إن مختلف الأنظمة البيومترية تم تصميمها لتحديد هوية الشخص من خلال قياس إحدى الخصائص الفيزيائية . فكما هو معلوم فإن لكل إنسان ملامح بيولوجية مميزة له . وهذه الخصائص هي أبعد ما تكون عن الكمال بسبب القيود المختلفة التي تفرضها البيئة التي يتم فيها تنفيذ النظام، مما يشكل مشكلة الأداء الحقيقي و الموثوقية.

وسوف نتطرق في دراستنا لبعض لتعاريف التصوير الرقمي ومختلف المعالجة المسبقة وتوحيد الصورة، ثم مختلف الأساليب المعتمدة لكشف الوجه.

ثم سنقوم بتفصيل النهج الذي اخترناه و الذي يقوم على الكشف ومطابقة سمات الوجه الهندسية وأخيراً، سيتم عرض النتائج التي تم الحصول عليها من اختبار في صورة ليدلي ببيان على أداء نظامنا.

الكلمات المفتاحية : الأنظمة البيومترية , الخصائص الفيزيائية , التصوير الرقمي , المعالجة المسبقة ,

توحيد , سمات الوجه الهندسية

Liste des Figures

Figure I.1	Architecture du mode d'apprentissage	07
Figure I.2	Architecture du mode authentification	07
Figure I.3	Architecture du mode identification	08
Figure I.4	Empreinte digitale	09
Figure I.5	Lecteur biométrique	10
Figure I.6	La géométrie de la main	10
Figure I.7	Une méthode de reconnaissance de visage	11
Figure I.8	La rétine d'œil humain	11
Figure I.9	L'iris d'œil	12
Figure I.10	Signal vocale	13
Figure I.11	Tablette graphique	14
Figure I.12	Dynamique de frappe sur clavier	14
Figure I.13	Technologies portant sur l'analyse biologique	15
Figure I.14	Comparaison de différentes modalités selon quatre critères principaux.	17
Figure I.15	Utilisation des systèmes biométriques dans le marché mondiale	18
Figure I.16	Les revenus biométriques entre 2009/2014 en US DOLLAR	18
Figure I.17	Domaines d'application de la biométrie	19
Figure II.1	Les paupières, œil ouvert	24
Figure II.2	Les lèvres	24
Figure II.3	Les cartilages du nez	25
Figure II.4	Anatomie du nez	25
Figure II.5	Harmonie faciale, rapports des trois étages de la face	26
Figure II.6	Techniques de mesure des principaux diamètres de la face	27
Figure II.7	Mensuration orbitopalpébrale	29
Figure II.8	Angle nasofrontale et angle nasolabiale	30
Figure II.9	Anatomie descriptive et mensuration du nez	30
Figure III.1	Image biométrique de la même personne	33
Figure III.2	Les étapes de la reconnaissance de visage	36
Figure III.3	Exemple de variation d'éclairage	39
Figure III.4	Exemple de variation de poses	39
Figure III.5	Exemple de variation d'expressions faciales	40
Figure III.6	Le principe des méthodes globales	43
Figure III.7	Détection de 12 points	45
Figure III.8	Courbe CMC	47
Figure III.9	Influence du seuil de décision sur les erreurs d'un système biométrique	48
Figure III.10	Représentation du taux d'erreurs	48
Figure III.11	La courbe ROC	49
Figure IV.1	Quand les visages ne sont pas vus dans leurs état naturel, la capacité du système visuel humain a les distingués est dégradée	51
Figure IV.2	Les 12 points détectés	52
Figure IV.3	Les 6 points détectés	53
Figure IV.4	Exemples d'images de la base XM2XTS	55
Figure IV.5	Extrait de la base couleur FERET	55
Figure IV.6	Extrait de la base AR, ensemble des vues collectés pour un individu ...	56
Figure IV.7	Image faciale extraite de la base CVL	56
Figure IV.8	Base de données ORL	57
Figure IV.9	Exemple de changement d'orientation du visage	57
Figure IV.10	Exemple de changement d'éclairage	58
Figure IV.11	Exemple de changement d'échelle	58

Liste des Figures

Figure IV.12	Exemple de changement des expressions faciales	58
Figure IV.13	Exemple de port de lunettes.....	58
Figure IV.14	Exemple de changement de coiffure et port barbe	59
Figure IV.15	Exemple d'individus de différents âges, races et sexes	59
Figure IV.16	Paires de la base LFW aligned	60
Figure IV.17	Exemple de visage dans la base FEI	60
Figure V.1	Architecture du système	63
Figure V.2	Diagramme de flow de données principale	63
Figure V.3	Diagramme de flow de données de prétraitement	64
Figure V.4	Diagramme de flow de données d'extraction des paramètres	70
Figure V.5	Diagramme de flow de données normalisation	71
Figure V.6	Diagramme de flow de données de décision	72
Figure VI.1	Déroulement d'une session de travail	77
Figure VI.2	Page d'authentification de l'administrateur	78
Figure VI.3	Fenêtre d'erreur	79
Figure VI.4	Fenêtre d'accueil	79
Figure VI.5	Opération d'identification d'un nouvel individu	80
Figure VI.6	Fenêtre ouvrir une image de visage	80
Figure VI.7	Lancer l'identification	81
Figure VI.8	Fenêtre d'état civile de l'individu	81
Figure VI.9	Nouvel individu	82
Figure VI.10	Fenêtre de traitement effectué sur le visage identifié	82
Figure VI.11	Graphe de reconnaissance et taux d'erreurs	83
Figure A.1	Représentation de « A » par groupe de pixels	93
Figure A.2	Variétés des formes d'un contour	96
Figure A.3	Exemple d'application de détecteur de cany	99
Figure A.4	Exemple d'application de l'approche Deriche	100

Liste des Tableaux

Tableau II.1	Répartition des valeurs indiciaires en fonction de la forme de visage.....	27
Tableau II.2	Répartition des valeurs indiciaires en fonction de la forme faciale et cépholique	28
Tableau II.3	Répartition des valeurs indiciaires en fonction de forme frontale et zygomatique.....	28
Tableau II.4	Répartition des valeurs indiciaires en fonction de la forme mandibulaire et zygomatique	28
Tableau II.5	Répartition des valeurs indiciaires en fonction de la forme du nez	29
Tableau II.6	Répartition des valeurs indiciaires en fonction de la forme de l'arête nasale	30
Tableau II.7	Répartition des valeurs indiciaires en fonction de la forme de la bouche et lèvres	30
Tableau III.1	Répartition des articles sur les techniques biométriques soumis et acceptés dans la revue IEEE PAMI	36
Tableau IV.1	Principales caractéristiques des bases de visages	61
Tableau V.1	Voisinage d'un pixel	66

Table des matières

Introduction générale	1
-----------------------------	---

CHAPITRE I : La biométrie

I.1. Introduction	4
I.2. Biométrie et les systèmes biométriques	4
I.2.1. Définition de la biométrie	4
I.2.2. Origine de la biométrie	5
I.2.3. Caractéristiques d'une modalité biométrique	5
I.2.4. Architecture d'un système biométrique	6
I.2.5. Mode de fonctionnement d'un système biométrique	7
I.2.5.1. Mode d'apprentissage (Enrôlement)	7
I.2.5.2. Mode de vérification	7
I.2.5.3. Mode Identification	8
I.3. Types de la biométrie	8
I.4. Présentation des systèmes biométriques	9
I.4.1. Les systèmes basés sur l'analyse morphologique ou physiologique	9
I.4.1.1. La reconnaissance des empreintes digitales	9
I.4.1.2. La reconnaissance de la main	9
I.4.1.3. La reconnaissance de la forme de visage	10
I.4.1.4. Rétine de l'œil	11
I.4.1.5. Iris de l'œil	12
I.4.1.6. Reconnaissance de la voix	12
I.4.2. Techniques dédiées à la biométrie comportementale	13
I.4.2.1. Signature dynamique	13
I.4.2.2. Rythme de frappe au clavier	14
I.4.3. Technologies portant sur l'analyse biologique	15
I.4.3.1. L'analyse de l'ADN	15
I.4.3.2. Les groupes sanguins	15
I.4.3.3. Les cheveux et les poiles	15
I.5. Evaluation de performances des systèmes biométriques	16
I.6. La part du marché par technologie	18
I.7. Les applications de la biométrie	19
I.7.1. Contrôle d'accès	19
I.7.2. Authentification des transactions	20
I.7.3. Répression	20
I.7.4. Personnalisation	21
I.8. Conclusion	21

CHAPITRE II : Généralités sur la reconnaissance des visages

II.1. Introduction	23
II.2. Le visage humain	23
II.2.1. Rappel anatomique (anatomie du visage humain)	23
II.2.2. Les régions du visage humain	23
II.2.2.1. La région orbitaire	23
II.2.2.2. La région labiale	24
II.2.2.3. La région nasale	25
II.2.3. Les différents étages de la face	25

Table des matières

II.3. L'anthropologie	26
II.3.1. Généralités sur les mesures anthropologiques et la notion d'indice	26
II.3.2. Mensuration	27
II.3.2.1. La face	27
II.3.2.2. Indices orbitaires et oculaire	29
II.3.2.3. Le nez	29
II.3.2.4. La bouche et les lèvres	30
II.4. Conclusion	31

CHAPITRE III : Systèmes de reconnaissance des visages

III.1. Introduction	33
III.2. La reconnaissance de visages	33
III.3. Motivation (pourquoi la reconnaissance de visages ?)	34
III.4. La place de la reconnaissance faciale parmi les autres techniques biométriques ...	35
III.5. Systèmes biométriques basé sur la reconnaissance de visages	36
III.5.1. Détection de visage	37
III.5.2. Extraction des caractéristiques du visage	37
III.5.3. La reconnaissance de visage (Identification)	38
III.6. Principales difficultés de la reconnaissance de visage	38
III.6.1. Changement d'illumination	38
III.6.2. Variation de pose	39
III.6.3. Expressions faciales	39
III.6.4. Présence ou absence des composants structurels	40
III.6.5. Occultation partielles	40
III.6.6. Les vrais jumeaux	40
III.7. Détection de visages	41
III.7.1. Approches basées sur les connaissances acquises	41
III.7.2. Approches basées sur le « Template-Matching »	41
III.7.3. Approches basées sur l'apparence	42
III.7.4. Approches basées sur des caractéristiques invariantes	42
III.8. Techniques de reconnaissances de visage	43
III.8.1. Approche holistique ou globale	43
III.8.1.1. Réseau de neurones	44
III.8.1.2. Eigen Face	44
III.8.1.3. Méthodes de Markov cachés(HMM)	44
III.8.1.4. Discret cosine transforme (DCT)	44
III.8.2. Approches locales	45
III.8.2.1. Méthodes géométriques	45
III.8.2.2. Méthodes basées sur les graphes	46
III.8.3. Approche hybride	46
III.9. Indicateur de performance d'un système biométrique	46
III.9.1. Système opérant en mode identification	46
III.9.2. Système opérant en mode authentification	47
III.10. Conclusion	49

Table des matières

CHAPITRE IV : Approche adoptée

IV.1. Introduction	51
IV.2. Système de reconnaissance de visage	52
IV.3. Algorithme des K-PPV	53
IV.4. Les bases de données du visage existantes	54
IV.4.1. La base XM2VTS	54
IV.4.2. La base FERET	55
IV.4.3. La base AR	56
IV.4.4. La base CVL	56
IV.4.5. La base de données ORL	57
IV.4.6. Base Labeled Faces in the Wild(LFW)	59
IV.4.7. La base FEI	60
IV.5. Conclusion	61

CHAPITRE V: Conception

V.1. Introduction	63
V.2. Architecture générale du système proposé	63
V.2.1. Module d'acquisition	64
V.2.2. Module de prétraitement	64
V.2.2.1. Passage aux niveaux des gris	64
V.2.2.2. Lissage	65
V.2.2.3. Seuillage	66
V.2.2.4. Nettoyage	67
V.2.2.5. Squelettisation	68
V.2.3. Module d'extraction des paramètres	70
V.2.4. Module de normalisation	71
V.2.5. Module de décision	72
V.3. Conclusion	74

CHAPITRE VI : Implémentation

VI.1. Introduction	76
VI.2. Outils d'implémentation	76
VI.2.1. Le langage de développement	76
VI.2.2. Pourquoi choisir DELPHI ?	76
VI.2.3. Matériel utilisé	76
VI.3. Déroulement d'une session de travail	77
VI.4. Description des IHM de notre système	77
VI.5. Conclusion	83
Conclusion générale et perspective	85
Bibliographie	87

Table des matières

ANNEXE :

A.1. Généralités sur les traitements d'images	93
A.1.1. Image analogique	93
A.1.2. La numérisation	93
A.2.3. Pixel « Picture Element »	93
A.1.4. Image numérique	94
A.1.4.1. Caractéristiques d'une image numérique	94
A.1.5. Luminance	94
A.1.6. Bruit	95
A.1.7. Filtrage numérique	95
A.1.7.1. Filtre passe-bas (Lissage)	95
A.1.7.2. Filtre passe-haut (Accentuation)	95
A.1.7.3. Filtre passe-bande (différentiation)	95
A.1.7.4. Filtre directionnel	96
A.1.8. Détection de couleur	96
A.1.8.1. Approche contours	96
A.1.8.2. Approche gradient	97
A.1.8.3. Approche Laplacien	97
A.1.8.4. Approche de Canny	98
A.1.8.5. Approche Deriche	99
A.1.9. Les méthodes de détection de contours	100
A.1.9.1. Squelettisation	100
A.1.9.2. Propriétés des squelettes	100

Introduction générale

Dans son environnement quotidien, un individu a besoin de s'identifier dans une multitude de contextes : pour entrer dans son immeuble ou accéder à son lieu de travail, pour retirer de l'argent à un distributeur ou payer en magasin ainsi que pour demander un service social ou autre.

Depuis quelques décennies, les méthodes usuelles d'identification étaient basées sur ce que l'on possède (carte d'identité, carte à puce, badge magnétique) ou sur ce que l'on sait (mot de passe, code PIN).

Afin de développer les moyens de reconnaissance, la recherche connaît depuis quelques années un renouveau spectaculaire et manifeste un intérêt majeur aux données "biométriques", c'est-à-dire aux caractéristiques propres à chaque personne : les traits de son visage, sa voix, ses empreintes digitales, la forme de sa main, sa signature et même son ADN. Ainsi, les techniques basées sur la biométrie interviennent dans les phénomènes de mode, principalement véhiculées par les films au cinéma et à la télévision. Cependant, plus récemment, l'augmentation de la fraude de l'identité a créé un besoin croissant de la technologie biométrique dans un de certain nombre d'applications nécessitant un haut degré de sécurité : accès à des sites sensibles, surveillance d'aéroport.

A la différence de ces modalités biométriques, la reconnaissance faciale ne nécessite pas théoriquement la coopération des participants. Elle apparaît donc comme une alternative très intéressante, à condition cependant qu'un taux de reconnaissance suffisant soit garanti. Ce caractère non invasif a été la raison majeure de l'intérêt grandissant de la reconnaissance faciale, de la part d'organisations de recherche publiques et privées.

Comme tout autre sujet de reconnaissance de formes, les problèmes liés à la reconnaissance de visages peuvent être caractérisés par les deux difficultés suivantes :

La première difficulté est d'abord liée aux variations intrinsèques du visage produites par exemple par les changements d'expressions faciales, l'évolution de la physionomie du visage et les transformations du visage voulues ou subies.

Cette variabilité englobe également des variations environnementales provoquées par exemple par les changements de conditions d'éclairage, l'orientation du visage de la personne ou l'occlusion d'un visage par des accessoires ou par d'autres objets.

La seconde difficulté caractérise la similarité entre des classes d'individus différents. Ici, les apparences faciales de deux personnes différentes peuvent être similaires par exemple en

Introduction générale

raison des liens familiaux (jumeaux, jumelles, père/fils, mère/fille, etc.) ou plus généralement de l'appartenance à une même race.

Dans ce mémoire, nous nous intéressons plus spécifiquement à la tâche d'identification par reconnaissance faciale. Nous cherchons à concevoir un système efficace basée sur une base de données minimale (adoptant un minimum de positions faciales).

La conception de notre application s'appuie sur les DFD, l'implémentation du logiciel étant faite grâce à l'environnement DELPHI. Nous ne visons aucune des applications citées ci-dessus en particulier. Néanmoins, le développement d'un tel outil nous ouvre les domaines de la vidéo surveillance et de l'aide à la décision dans le contexte de la sécurité.

Notre mémoire se compose de six chapitres :

- Le premier chapitre traite des généralités de la biométrie et des systèmes biométriques.
- Le second chapitre présente généralités sur la reconnaissance des visages humains.
- Le chapitre trois traite les systèmes de reconnaissance de visages humains.
- Le quatrième chapitre résume l'approche que nous avons adoptée dans notre travail.
- Le cinquième chapitre est consacré à la conception de notre application.
- Nous développons l'implémentation de notre travail dans le sixième chapitre.

CHAPITRE I

La biométrie

I.1. Introduction :

La protection des données est toujours une priorité pour toutes les entités économiques ou administratives surtout dans les domaines sensibles tels que la sécurité militaire et les recherches nucléaires, de peur qu'elles soient accessibles par des personnes malveillantes.

Actuellement, sécuriser un système d'information devient de plus en plus une tâche délicate, surtout après l'implication des nouvelles technologies dans la plupart des échanges client-entreprise comme la vente en ligne, les transactions bancaires, le contrôle d'accès, etc. En effet, chaque nouvelle technologie a des failles de sécurité qui doivent être prises en compte par l'entreprise, soit pour les annuler ou les minimiser, et cela nécessite l'achat de nouveaux matériaux, l'embauche de nouveau personnel et parfois même le changement de tout le système d'information. A cet effet, l'entreprise doit connaître les ressources à protéger et les droits des utilisateurs du système afin de mettre en place un système de sécurité efficient.

Deux méthodes classiques ont été utilisées par les entreprises pour prouver l'identité d'un utilisateur. La première se repose sur la vérification de l'identité à l'aide d'un mot de passe, tandis que la deuxième se base sur l'utilisation d'une carte à puce ou un badge. Cependant, ces méthodes d'authentification sont facilement falsifiables car il est facile de voler un badge ou d'oublier un mot de passe. La biométrie quant à elle, entre comme une alternative aux méthodes précédentes, elle offre un niveau de sécurité plus élevé en se basant sur des caractéristiques physiques, biologiques ou comportementales de l'individu qui peuvent le différencier des autres. Certains systèmes biométriques utilisent une seule caractéristique, d'autres combinent plusieurs afin de diminuer les taux d'erreurs.

Dans ce premier chapitre, nous allons présenter des notions générales sur la biométrie, les modalités biométriques, le fonctionnement d'un système biométrique et la part du marché par technologie. [HR, 2013]

I.2. Biométrie et le Système biométrique :

I.2.1. Définition de la biométrie :

La biométrie consiste à identifier une personne à partir d'une ou de plusieurs de ses caractéristiques physiologiques (empreintes digitales, visage, iris, contour de la main, etc.), ou comportementales (signature, démarche, etc.). Etymologiquement, la biométrie humaine est synonyme d'anthropologie physique [GO, 1961]. Une autre définition de la biométrie est

Chapitre I : La biométrie

donnée par Roethenbaugh [GR, 1998] : « 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 ». Son but est d'assurer la protection des clients contre la fraude ou le vol grâce à ses caractéristiques qui ne peuvent être perdues ou volées comme c'est le cas pour un mot de passe.

I.2.2. Origine de la biométrie

L'intérêt porté à la biométrie remonte au VI^{ème} siècle, où l'empreinte du pouce laissée sur une poterie d'argile permettait de sceller des accords commerciaux entre les babyloniens [MA, 2009]. De même, elle était utilisée pour différencier les jeunes enfants des marchands en Chine [FM]. En effet, la distinction entre les empreintes des personnes a poussé l'anatomiste Marcello Malpighi (1628–1694) à étudier plus en détails les empreintes avec un microscope et le physiologiste tchèque Jan Evangelista Purkyně (1787–1869) à les catégoriser selon certains critères [FM].

L'intuition que l'homme a eu, que certaines caractéristiques physiques peuvent l'identifier ne s'est pas arrêtée à la trace du doigt (empreinte digitale). Toutefois, à la fin du XIX^{ème} siècle (fin 1890), le policier parisien Alphonse Bertillon (1853-1914) a cherché à mettre le corps en équation, en mesurant plusieurs paramètres [AB, 1983] afin d'identifier les criminels. Dans ses travaux, il a affirmé qu'en prenant quatorze mensurations (taille, pieds, mains, nez, oreilles,...etc.) sur n'importe quel individu, il n'y a qu'une seule chance sur deux cent quatre-vingt-six millions pour qu'on retrouve les mêmes mesures chez une autre personne. Ainsi, Bertillon inventa l'anthropométrie judiciaire, adoptée rapidement dans toute l'Europe, puis aux États-Unis.

Depuis, différents moyens physiques et comportementaux permettant la reconnaissance de l'individu ont été utilisés. Parmi ces moyens, communément appelés "modalités biométriques", on trouve : le visage, l'empreinte digitale, l'iris, la forme de la main, l'analyse de la démarche...etc. Récemment, d'autres modalités ont été introduites comme l'analyse des veines de la main, le réseau veineux de la rétine, l'empreinte de l'oreille et l'ADN.

I.2.3. Caractéristiques d'une modalité biométrique :

L'authentification par la biométrie est plus forte que celle utilisant les moyens classiques d'identification tels que les cartes, clés ou mots de passe car elle constitue un lien fort et permanent entre une personne physique et son identité. [BB, 2011]

Chapitre I : La biométrie

Les propriétés principales d'une modalité biométrique sont :

- **L'universalité** : signifie que toute la population doit posséder cette modalité (caractéristique physique ou comportementale). [BB, 2011]
- **L'unicité** : signifie que deux personnes différentes doivent avoir des représentations de leur biométrie différentes. [BB, 2011]
- **La stabilité** : est une stabilité dans le temps et une stabilité pour chaque personne. Une biométrie, pour servir de moyen d'authentification, doit être relativement stable dans le temps et surtout doit être stable pour une personne quelles que soient les circonstances de l'acquisition (conditions extérieures, conditions émotionnelles de la personne ...). [BB, 2011]
- **L'acceptabilité** : et la facilité d'usage se rapportent aux contraintes liées à l'acquisition et l'utilisation d'une modalité biométrique. [BB, 2011]
- **La non-reproductibilité** : concerne la facilité ou non à falsifier une modalité biométrique. [BB, 2011]

I.2.4. Architecture d'un système biométrique :

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

- **Le module de capture**: est responsable de l'acquisition des données biométriques d'un individu (cela peut être un appareil photo, un lecteur d'empreintes digitales, une caméra de sécurité, etc.). [MN, 2009]
- **Le module d'extraction de caractéristiques** : prend en entrée les données biométriques acquises par le module de capture et extrait seulement l'information pertinente afin de former une nouvelle représentation des données. Idéalement, cette nouvelle représentation est censée être unique pour chaque personne et relativement invariante aux variations intra-classe. [MN, 2009]
- **Le module de correspondance** : compare l'ensemble des caractéristiques extraites avec le modèle enregistré dans la base de données du système et détermine le degré de similitude (ou de divergence) entre les deux. [MN, 2009]
- **Le module de décision** : vérifie l'identité affirmée par un utilisateur ou détermine l'identité d'une personne basée sur le degré de similitude entre les caractéristiques extraites et le(s) modèle(s) stocké(s). [MN, 2009]

Chapitre I : La biométrie

I.2.5. Mode de fonctionnement d'un système biométrique :

Un système biométrique peut s'exécuter en trois modes :

I.2.5.1. Mode d'apprentissage (Enrôlement):

Est la première phase de tout système biométrique. Il s'agit de l'étape pendant laquelle un utilisateur est enregistré dans le système pour la première fois où une ou plusieurs modalités biométriques sont capturées et enregistrées dans une base de données. Cet enregistrement peut s'accompagner par l'ajout d'information biographique. [MN, 2009]
Les différents modules de ce mode sont représentés dans la figure suivante:

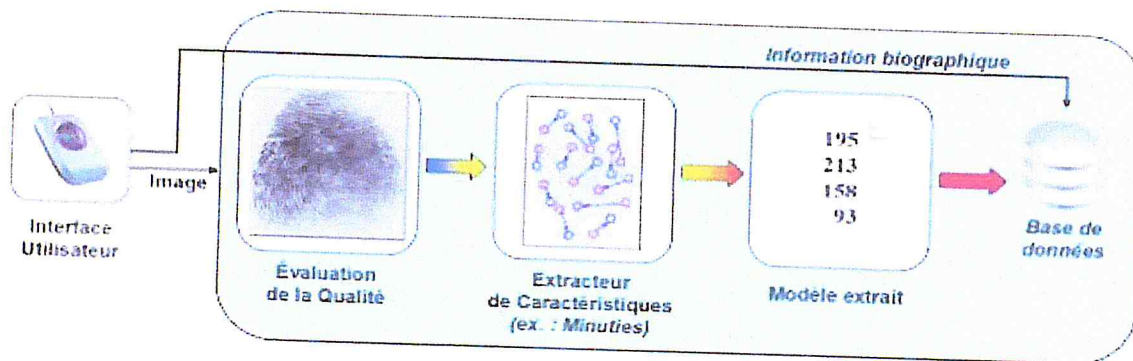


Figure I.1. Architecture du mode apprentissage. [MN, 2009]

I.2.5.2. Mode de vérification :

Il s'agit de vérifier l'identité d'une personne qui a un numéro d'identification (ID). Ce procédé consiste à vérifier l'échantillon biométrique de la personne avec le modèle qui correspond à son identifiant. Elle répond à la question "l'individu est-il bien celui qu'il prétend être?". [MN, 2009]

Les différents modules de ce mode sont représentés dans la figure suivante:

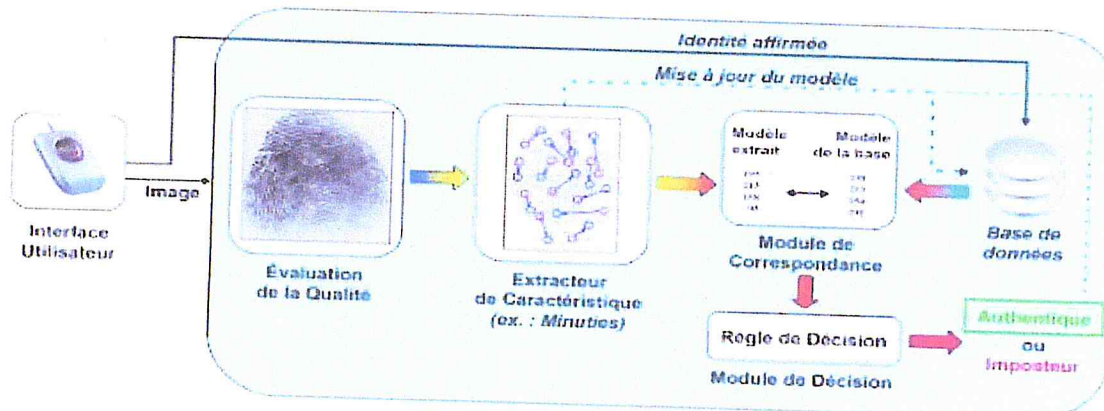


Figure I.2 Architecture du mode authentification. [MN, 2009]

Chapitre I : La biométrie

I.2.5.3. Mode identification :

Pour les systèmes d'identification, la comparaison est faite avec toutes les références stockées dans la base de données et la décision est la réponse à la question, "est-ce que cette personne est dans la base de données, et si oui qui est-elle?". [MN, 2009]

Les différents modules de ce mode sont représentés dans la figure suivante:

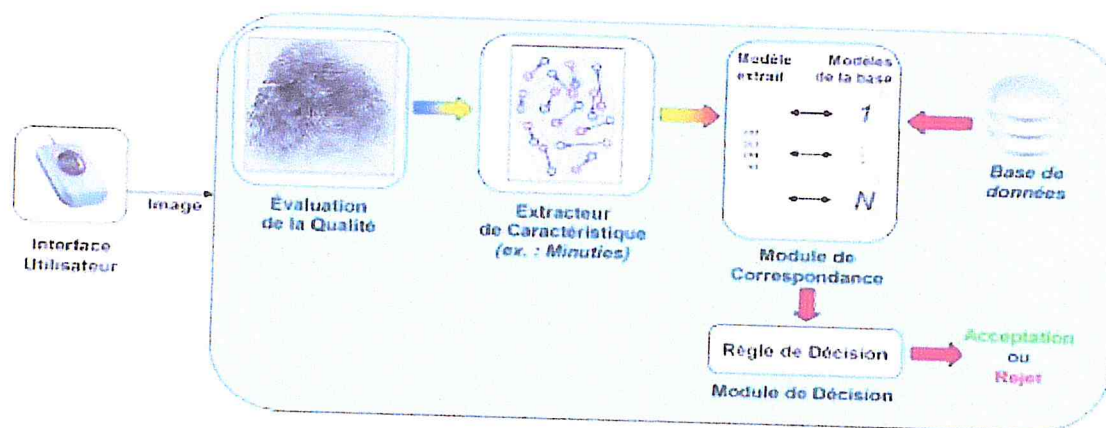


Figure I.3 Architecture du mode identification [MN, 2009]

I.3. Types de la biométrie :

Les systèmes biométriques sont généralement classés par l'industrie dans deux grandes catégories : La biométrie morphologique ou physiologique et la biométrie comportementale, à l'instar de la Commission Nationale de l'Informatique et de Libertés (CNIL) de France [NZ, 2009]:

- **La biométrie morphologique :** basée sur l'identification de traits physiques. cette catégorie regroupe : les empreintes digitales, la forme de la main, les traits du visage, la rétine et l'iris de l'œil. [NZ, 2009]
- **La biométrie comportementale :** basée sur l'analyse de certains comportements d'une personne comme : le tracé de sa signature, le séquentiel de sa voix, sa démarche ou sa façon de taper sur un clavier. [NZ, 2009]
- **La biométrie biologique :** La biométrie biologique décrit les individus selon leurs caractéristiques biologiques. L'ADN est la biométrie biologique la plus utilisée, elle permet d'identifier une personne à partir d'échantillons organiques divers : salive, cheveu, sang... Elle est surtout utilisée dans le domaine policier et judiciaire mais aussi dans le domaine civil: accidents, catastrophes... [BB, 2011]

I.4. Présentation des systèmes biométriques :

I.4.1 Les systèmes basés sur l'analyse morphologique ou Physiologique :

I.4.1.1. La reconnaissance des empreintes digitales :

La reconnaissance des empreintes digitales (Figure I.4) 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 [SA, 2010].



Figure I.4 Empreinte digitale [SA, 2010]

Avantage:

- La Taille du capteur est petite ce qui facilite son intégration.
- Les capteurs sont moins coûteux.
- Un bon compromis entre le TFR et le TFA.
- Le taux de ressemblance des empreintes peut atteindre 1/64 milliards [LF, 2005].
- 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.4.1.2. La reconnaissance de la main :

Cette technique consiste à déterminer les caractéristiques de la main d'un individu : forme, largeur, longueur, courbure des doigts, etc. L'utilisateur doit poser la paume de sa main sur une plaque qui possède des guides afin de l'aider à positionner ses doigts. Cette

Chapitre I : La biométrie

technologie prend deux photos, une du dessus de la main, l'autre du côté de la main en utilisant un miroir à angle (Figure I.5 & Figure I.6). Son principal avantage est qu'elle ne laisse pas de trace (contrairement aux empreintes digitales). Cependant, cette modalité n'est pas stable dans le temps (la forme de la main change avec l'âge). [SI]



Figure I.5 Lecteur biométrique [SI]

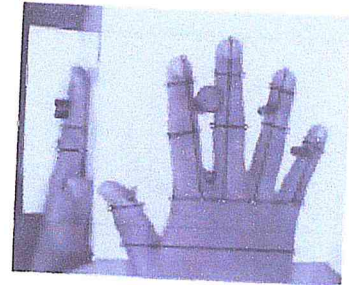


Figure I.6 la géométrie de la main [SI]

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

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 .

I.4.1.3. La reconnaissance de la forme de 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 [ZX, 2006] a montré beaucoup d'avantages au niveau de la vitesse et de l'efficacité de la reconnaissance.

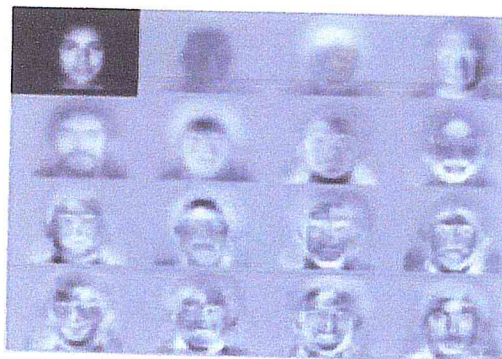


Figure I.7 Une méthode de reconnaissance du visage. [ZX, 2006]

Avantage:

- 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.

I.4.1.4. Rétine de l'œil :

La rétine est l'organe sensible de la vision, situé sur la surface interne du globe oculaire elle se compose d'un nombre énorme de photorécepteurs alimentés par des vaisseaux sanguins (Figure I.8), la configuration de ces vaisseaux représente l'un des caractères biométriques.

Elle a été proposée en 1930 mais le premier lecteur est apparu en 1984 par la compagnie Eye Dentity [SA, 2010].

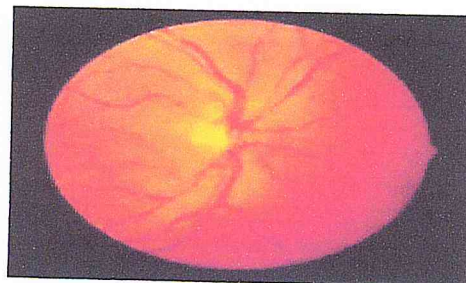


Figure I.8 La rétine d'œil humain. [SA, 2010]

Chapitre I : La biométrie

Avantages:

- Donne de bonnes performances à cause de la stabilité du schéma sanguin.
- Il est presque impossible de la falsifier (destruction des vaisseaux sanguins 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

I.4.1.5. Iris de l'œil :

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.9) de deux individus sont distinctifs [SA, 2010], et c'est en 1993 que le premier système basé sur l'identification par l'iris a été mis en œuvre par Defence Nuclear Agency. [DJ, 2008]

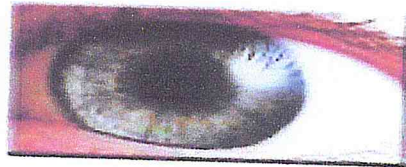


Figure I.9 L'iris d'œil [DJ, 2008]

Avantage:

- 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'œil gauche de l'œil droit.

Inconvénients :

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

I.4.1.6 Reconnaissance de la voix :

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.

Chapitre I : La biométrie

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. [TK, 2007]



Figure I.10 Signal vocal. [TK, 2007]

Avantage :

- Technique facile à implémenter.
- C'est la seule 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

I.4.2. Technologies dédiées à la biométrie Comportementale :

I.4.2.1. Signature dynamique :

Dès 1929, Osborne établit que l'écriture dépend de plusieurs facteurs caractéristiques. Pour imiter une signature, il faut donc non seulement imiter la forme de l'écriture mais aussi tenir compte de ces facteurs liés notamment à la vitesse, aux conditions environnantes et à la dextérité musculaire [FV, 2007].

La signature caractérise le signataire soit par sa forme soit par sa dynamique. Il existe deux types de signatures hors-ligne et en ligne. La première est produite sur un papier tandis que la deuxième sur un dispositif dédié. L'utilisateur fournit d'abord un ensemble de signatures de référence et en phase d'authentification, la signature est comparée aux références de la personne proclamée. Cette technologie examine un ensemble de dynamiques comme la vitesse, la direction et la pression de l'écriture, le temps pendant lequel le stylo est en contact avec le papier, le temps pris pour faire la signature et les positions où le stylo est relevé et abaissé sur le papier [LH, 2009].



Figure I.11 Tablette graphique. [LH, 2009]

Avantage :

- Bien acceptée comme moyen d'identification.
- Couramment utilisée pour les transactions

Inconvénients :

- Non utilisable pour des contrôles d'accès en extérieur.
- Sensible à l'état émotionnel de l'individu.
- Besoin d'une tablette graphique.

I.4.2.2. Rythme de frappe au clavier :

L'utilisation de matériels informatiques a également suscité un intérêt pour la biométrie. Par exemple, les travaux de Monroe et Rubin [EM, 2008] 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.



Figure I.12 Dynamique de frappe sur le clavier. [LH, 2009]

Avantage :

- Non intrusif (geste naturel pour un individu).

Inconvénients :

- Dépend de l'état physique de la personne.

Chapitre I : La biométrie

I.4.3. Technologies portant sur l'analyse biologique :

Selon [BM], l'utilisation de ces marqueurs biologiques a plus d'intérêt pour l'authentification d'une personne que pour son identification.

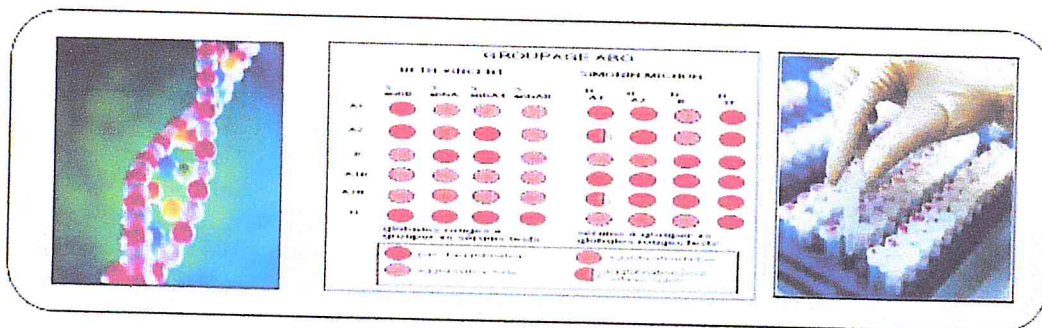


Figure I.13 Technologies portant sur l'analyse biologique. [BM]

I.4.3.1. L'analyse de l'ADN :

L'analyse des empreintes génétiques (ADN) est utilisée pour identifier une personne à partir d'un morceau de peau, d'un cheveu ou d'une goutte de sang. Auparavant, elle a été considérée comme un outil criminalistique. Toutefois, les échantillons d'ADN trouvés sur les lieux des crimes étaient trop infimes pour être analysés. Pour cela, des appareils d'amplification en chaîne par polymérase (Polymerase Chain Reaction, PCR) étaient utilisées afin de recopier et amplifier l'échantillon biométrique, procurant ainsi aux criminalistes des brins d'ADN répliqués et exploitables. [BM]

I.4.3.2. Les groupes sanguins :

En 1900, le pathologiste américain, Karl Landsteiner, a découvert pour la première fois en 1900 l'existence de groupes sanguins chez l'être humain. Il a mis en évidence le système ABO, dont le premier test de reconnaissance a été développé à partir de 1915. Landsteiner a découvert également les groupes P et MN ainsi que le facteur rhésus et fut lauréat du prix Nobel en 1930. Ses travaux ont été par la suite utilisés à des fins judiciaires. [BM]

I.4.3.3. Les cheveux et les poils :

Rudolf Virchow, médecin et anthropologue allemand, a étudié pour la première fois en 1869 des poils humains. Puis en 1910, V. Balthazard, professeur de médecine à la Sorbonne, et M. Lambert ont publié la première étude approfondie. [BM]

Chapitre I : La biométrie

Cette modalité permet d'identifier certaines caractéristiques propres à chaque individu, et d'apporter des éléments d'identification intéressants.

Remarque : actuellement d'autres techniques de reconnaissance biométrique sont en cours de développement [PJ, 2006], comme : la biométrie basée sur la géométrie de l'oreille, les odeurs, les pores de la peau et les tests d'ADN.

I.5. Evaluation des performances des Systèmes biométriques :

Chaque caractéristique (ou modalité) biométrique a ses forces et ses faiblesses, et le choix dépend de l'application visée. On ne s'attend à ce qu'aucune modalité biométrique ne réponde efficacement aux exigences de toutes les applications. En d'autres termes, aucun système biométrique n'est "optimal". Faire correspondre un système biométrique spécifique à une application dépend du mode opérationnel de l'application et des caractéristiques biométriques choisies. Plusieurs études ont été menées afin d'évaluer les performances des systèmes biométriques. La société américaine – The International Biometric Group – a par exemple effectué une étude basée sur quatre critères d'évaluation [DV, 2005]:

Intrusivité : ce critère permet de classifier les systèmes biométriques en fonction de l'existence d'un contact direct entre le capteur utilisé et l'individu à reconnaître. La reconnaissance faciale est une technique « non intrusive », car il n'existe aucun contact entre le capteur (la caméra) et le sujet, elle est bien acceptée par les utilisateurs à l'inverse d'autres techniques « intrusives » comme l'iris où un contact direct est nécessaire entre le capteur et l'œil. [DV, 2005]

Fiabilité : dépend de la qualité de l'environnement (éclairage par exemple) dans lequel l'utilisateur se trouve. Ce critère influe sur la reconnaissance de l'utilisateur par le système. Nous verrons ce point en détail dans la section suivante. [DV, 2005]

Coût : doit être modéré. À cet égard nous pouvons dire que la reconnaissance faciale ne nécessite pas une technologie coûteuse. En effet, la plupart des systèmes fonctionnent en utilisant un appareil à photo numérique de qualité standard. [DV, 2005]

Effort : requis par l'utilisateur lors de la saisie de mesures biométriques, et qui doit être réduit le plus possible. La reconnaissance faciale est la technique biométrique la plus facile à utiliser car non contraignante. [DV, 2005]

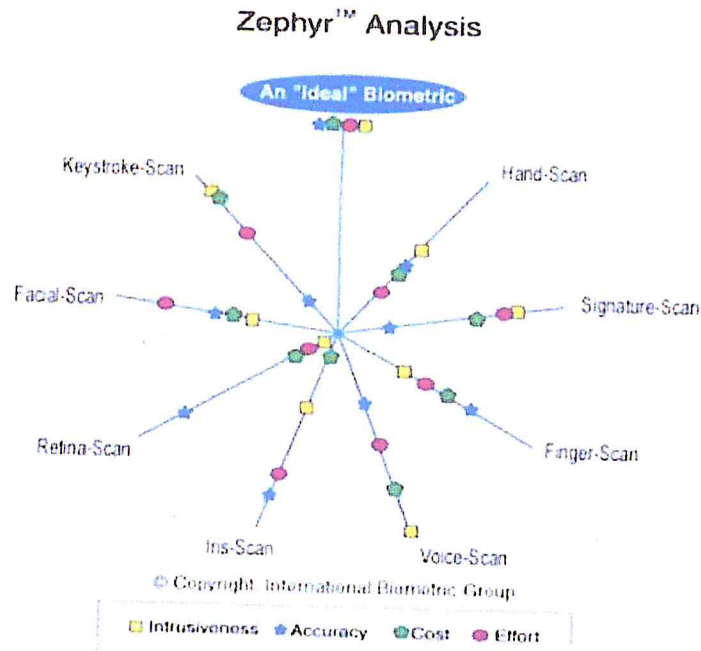


Figure I.14 Comparaison de différentes modalités selon quatre critères Principaux : l'intrusivité, le pouvoir discriminant, le coût et l'effort. [MN, 2009]

Légende :

- **Effort** : effort requis pour l'utilisateur lors de la mesure.
- **Intrusion** : décrit dans quelle mesure l'utilisateur perçoit le test comme intrusif.
- **Coût** : coût de la technologie (lecteurs, capteurs, etc...)
- **Précision** : efficacité de la méthode (capacité à identifier quelqu'un).

Les résultats de cette étude et comme on le voit sur la Figure.1.2, peuvent être présenté comme suit:

- Des techniques les moins « intrusives » aux plus « intrusives » : la voix, la frappe sur le clavier, la signature, la main, la face (visage), l'empreinte digitale, l'iris et enfin la rétine. [SA, 2008]
- Des techniques les plus fiables aux moins fiables : l'iris, la rétine, l'empreinte digitale, la face, la main, la voix, et enfin à un niveau équivalent, la frappe sur le clavier et la signature. [SA, 2008]
- Des techniques les moins chères aux plus chères : la frappe sur le clavier, la voix, la signature, l'empreinte digitale, la face, la main, la rétine et enfin l'iris. [SA, 2008]

Chapitre I : La biométrie

- Des techniques les plus faciles d'utilisation aux plus difficiles : la face, la signature, l'iris, la frappe sur le clavier, la voix, l'empreinte digitale, la main et enfin la rétine. [SA, 2008]

I.6. La part du marché par technologie :

Les empreintes digitales continuent à être la principale technologie en termes de part de marché, près de 50 % du chiffre d'affaire total (hors applications judiciaires). Plus de la moitié de ce taux est consacré aux systèmes AFIS (Automatic Fingerprint Identification System). Le succès de ces systèmes est dû essentiellement à leur précision et leur coût relativement bas. La reconnaissance du visage est placée en deuxième position avec 11,4% du marché (hors applications judiciaires). La figure suivante (Figure I.15 & Figure I.16) montre la part du marché de chaque modalité biométrique. [BM]

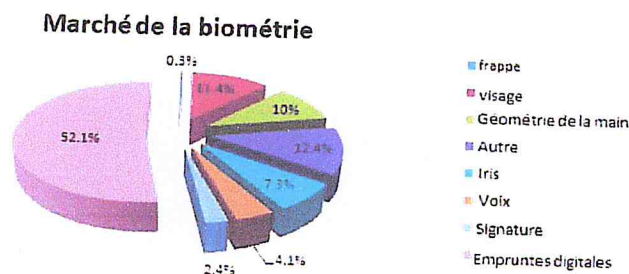


Figure I.15 Utilisation des systèmes biométriques dans le marché mondial. [MB, 2007]

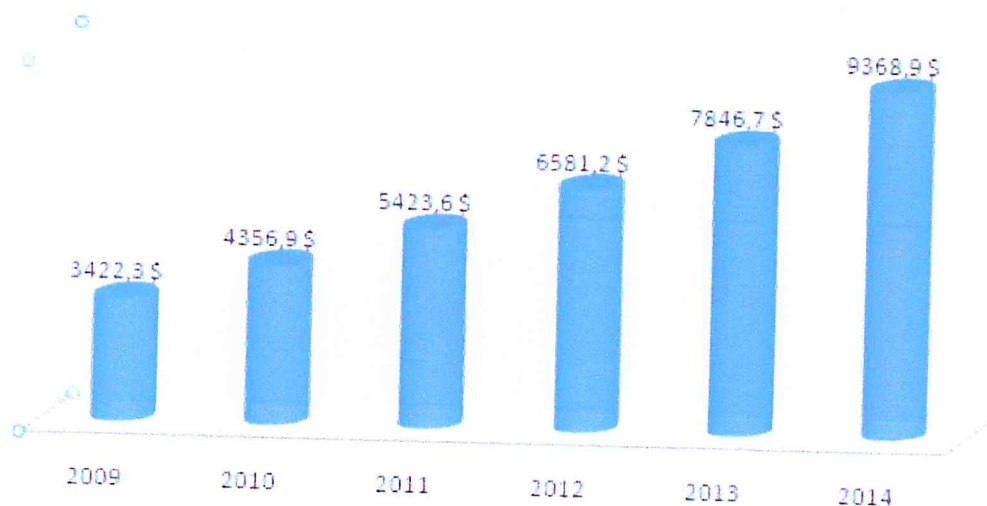


Figure I.16 Les revenus biométriques entre 2009/2014 en M US\$. [OM, 2009]

Ce graphe représente l'évolution industrielle biométrique dans les six précédentes années, on remarque que le bénéfice est multiplié par trois en l'espace de six ans, cela

Chapitre I : La biométrie

constitue un enjeu financier important qui suscite l'intérêt des entreprises aux technologies de pointe.

I.7. Les applications de la biométrie :

La biométrie marie les dernières technologies avec les découvertes biologiques afin d'assurer sécurité et confort. Cela a augmenté et diversifié ses champs d'applications pour des accès virtuels ou physiques [DV, 2005] (Figure I.17). Les principales applications des systèmes biométriques sont regroupées en trois classes différentes:

- **Applications commerciales:** telles que l'accès aux réseaux informatiques, la sécurité des données électroniques, le commerce électronique, l'accès à Internet, la carte de crédit, les transactions financières et la gestion des registres médicaux. [DV, 2005]
- **Applications gouvernementales:** comme la carte d'identification nationale, le permis de conduire, la sécurité sociale, contrôle du passeport, ...etc. [DV, 2005]
- **Applications juridiques:** telles que l'identification de cadavre, la recherche criminelle, l'identification de terroristes, des enfants disparus, ...etc. [DV, 2005]



Figure I.17 Domaines d'application de la biométrie [DV, 2005]

Donc on peut distinguer quatre grands types d'applications de la biométrie : le contrôle d'accès, l'authentification des transactions électroniques, les personnalisations....

I.7.1. Contrôle d'accès :

Le contrôle d'accès peut être lui-même subtilisé en deux sous catégories : le contrôle d'accès physique et le contrôle d'accès virtuel, on parle de contrôle d'accès physique lorsqu'un utilisateur cherche à accéder à un lieu sécurisé, on parle de contrôle d'accès virtuel dans le cas où un utilisateur cherche à accéder à une ressource ou à un service via un réseau informatique. [LH, 2009]

Chapitre I : La biométrie

- **Contrôle d'accès physique** : longtemps, l'accès à un lieu sécurisé (bâtiments ou salle par exemple) s'est fait à l'aide de clefs ou de badges, grâce à la biométrie, la même opération peut être effectuée automatiquement de nos jours, l'une des utilisations les plus célèbres de la biométrie de la main pour le contrôle d'accès dans plusieurs grands aéroports.
- **Contrôle d'accès virtuel** : Le contrôle d'accès virtuel permet par exemple l'accès aux réseaux d'ordinateurs ou l'accès sécurisé aux sites web, le marché du contrôle d'accès virtuel est dominé par les systèmes basés sur une connaissance, typiquement un mot de passe. Avec la chute des prix des systèmes d'acquisition, les applications biométriques devraient connaître une popularité croissante : un exemple d'application est l'intégration par appel dans un système d'exploitation d'un module de reconnaissance du locuteur de manière à protéger les fichiers d'un utilisateur.

I.7.2. Authentification des transactions :

L'authentification des transactions représente un marché gigantesque puisque cela englobe aussi bien le retrait d'argent des guichets des banques, les paiements par cartes bancaires les transferts des fonds, les paiements effectués à distance par téléphone ou sur internet ...etc.

Mastercard estime ainsi que les utilisations frauduleuses de carte de crédit pourraient être réduites de 80 % en utilisant des cartes à puce qui incorporeraient la reconnaissance des empreintes digitales. Les 20% restant seraient principalement dus au paiement à distance. Pour lesquelles il existerait toujours un risque. Pour les transactions à distance, des solutions sont déjà déployées en particulier pour les transactions par téléphone. Ainsi, la technologie de reconnaissance du locuteur de Nuance (Nuance Verifier TM) est utilisée par les clients du Home Shopping Network, une entreprise de téléshopping. [LH, 2009]

I.7.3. Répression :

Une des applications les plus immédiates de la biométrie pour la répression est la criminologie. La reconnaissance d'empreintes digitales en est l'exemple le plus connu. Elle fut acceptée dès le début du XXe siècle comme moyen d'identifier formellement un individu et son utilisation s'est rapidement répandue. [LH, 2009]

Chapitre I : La biométrie

I.7.4. Personnalisation :

Les technologies biométriques peuvent être aussi utilisées afin de personnaliser les appareils que nous utilisons tous les jours. Cette application de la biométrie apporte un plus grand confort d'utilisation. Afin de personnaliser les réglages de sa voiture, Siemens propose par exemple d'utiliser la reconnaissance des empreintes. [LH, 2009]

I.8. Conclusion :

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

Le marché de la biométrie est en plein expansion et plusieurs entreprises sont en train d'investir dans ce domaine. Cela permet de prédire que la biométrie aura un avenir prometteur.

CHAPITRE II

Généralités sur la reconnaissance des visages

Chapitre II: Généralités sur la reconnaissance de visages

II.1. Introduction :

La reconnaissance de visages humains est l'un des domaines de recherche les plus ciblés en informatique. La réalisation de notre logiciel de reconnaissance nécessite une compréhension approfondie de l'anatomie du visage de l'être humain ainsi que les concepts et notions fondamentales sur les traitements d'images.

II.2. Le Visage humain :

Le visage humain constitue la composante essentielle de la technologie de reconnaissance faciale. Il est essentiel alors d'avoir une connaissance profonde de sa morphologie et de son anatomie et de la tendance générale de la croissance et du vieillissement crano-faciale pour en tirer les points les plus discriminants et les plus stables.

Le visage humain a toujours suscité l'intérêt. Plusieurs disciplines s'y sont intéressées et cela à des fins différentes. Parmi ces disciplines on citera : l'art du portrait, l'anthropologie, l'anatomie, la médecine légale, la chirurgie, l'orthodontie et l'informatique où la reconnaissance du visage humain a fait l'objet de plusieurs recherches [AA, 2005].

II.2.1. Rappel anatomique (L'apport de l'anatomie dans l'étude du visage):

L'anthropologue travaillant dans le domaine de reconnaissance faciale doit avoir une parfaite connaissance de l'anatomie crano-faciale, alors il faut connaître les caractéristiques et les différentes structures du visage humain. En fonction de la mobilité, ce dernier comporte les parties suivantes : [AA, 2005]

- **Parties invariantes d'un moment à l'autre :** ses os, ses cartilages et leurs tissus cellulo-graisseux.
- **Parties variante :** ses muscles et ses ligaments qui changent.

L'anatomie nous aide à déceler la part de l'une ou l'autre de ces parties sur les traits visibles faciaux, ce qui est essentiel pour les recherches concernant les techniques de reconnaissance et reconstitution faciale.

II.2.2. les régions du visage humain :

II.2.2.1. La région orbitaire :

D'après les recherches, les paupières sont deux voiles musculo-membraneux, mobiles, qui recouvrent et protègent la partie antérieure du globe de l'œil. On distingue classiquement la paupière supérieure et celle inférieure.

Chapitre II: Généralités sur la reconnaissance de visages

Les limites des paupières répondent au rebord de l'orbite, au-delà duquel les paupières se continuent avec les ligaments des régions voisines. Ces limites ne sont apparentes que du côté médial et sont représentées:

- en haut, par le bord inférieur du sourcil.
- en bas, par le sillon palpébro-génien qui sépare la paupière inférieure de la joue.

Les paupières supérieure et inférieure sont séparées l'une de l'autre par la fente palpébrale.

Les extrémités des paupières forment les commissures palpébrales également appelées canthus (Figure II.1) [AA, 2005].

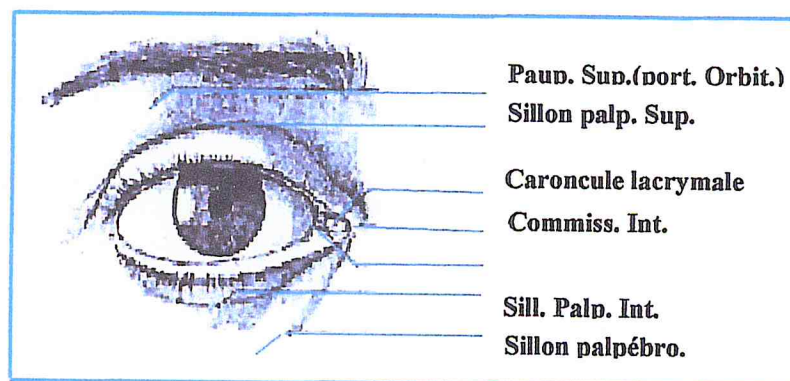


Figure II.1. Les paupières, œil ouvert. [AA, 2005]

II. 2.2.2. La région labiale :

Les lèvres sont deux replis musculo-membraneux, mobiles, qui forment la paroi antérieure de la cavité buccale et circonscrivent l'orifice buccal.

D'après une recherche citée par Rossel, on distingue une lèvre supérieure et une lèvre inférieure séparées par une fente orale et réunies latéralement au niveau des commissures labiales. Elles comprennent une partie muqueuse rouge et une partie cutanée. La ligne les séparant porte le nom de limbe [AA, 2005].

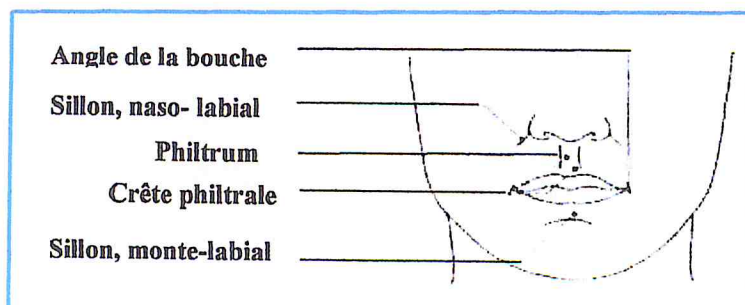


Figure II.2. Les lèvres. [AA, 2005]

II.2.2.3. La région nasale :

D'après une recherche (1996), le nez a la forme d'une pyramide implantée au milieu de la face. Il possède un squelette ostéo-cartilagineux recouvert par des muscles et des téguments. Il délimite la partie initiale de la cavité nasale ou vestibule.

Les différentes structures composant le nez [AA, 2005]:

- La racine du nez est la concavité transversale qui existe toujours plus ou moins accentuée, en haut du nez, entre les yeux, sous la base du front.
- La partie supérieure du nez est dure et osseuse; elle possède un squelette propre formé par les deux os nasaux.
- Les ailes du nez sont deux parties latérales limitées inférieurement par les deux ouvertures des narines et, contre la joue, par un sillon plus ou moins arrondi et plus ou moins profond, le sillon naso-labial.
- L'extrémité du nez est le point de réflexion du lobule.
- Le dos du nez est la ligne de profil du nez depuis sa racine jusqu'à sa pointe.
- Le bord inférieur ou base du nez s'étend de l'extrémité au point d'attache de la racine avec le nez (F).

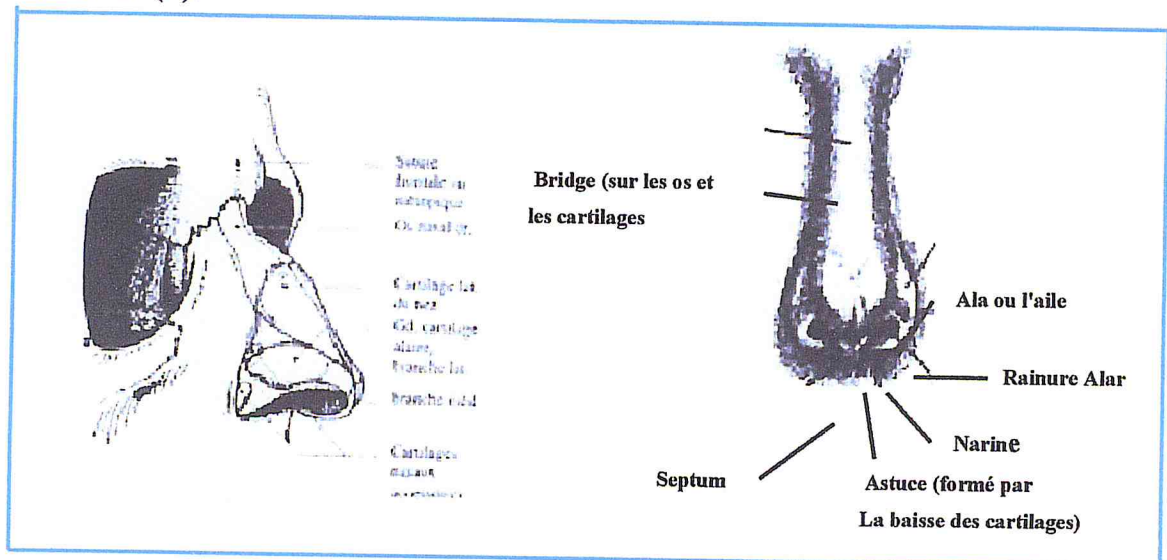


Figure II.3. Les cartilages du nez. [AA, 2005]. Figure II.4. Anatomie du nez. [AA, 2005]

II.2.3. Les différents étages de la face :

En théorie, le visage comporte trois étages: [AA, 2005]

- l'étage frontal,
- l'étage nasal, depuis la ligne des sourcils jusqu'au plan sous-nasal,
- l'étage buccal, depuis le plan sous-nasal jusqu'à la pointe du menton.

Chapitre II: Généralités sur la reconnaissance de visages

L'étage buccal peut être découpé en trois sous étages: [AA, 2005]

- l'étage sous-nasal jusqu'à la ligne bi commissurale,
- l'étage partant de la ligne bi commissurale jusqu'au sillon labio-mentonnier,
- l'étage allant du sillon labio-mentonnier jusqu'au menton.

Habituellement, on a une proportion d'un tiers par étage.

Il existe aussi un parallélisme des lignes faciales entre les lignes bipupillaire, biophriaque (ligne des sourcils), bicommissurale et bigoniaque.

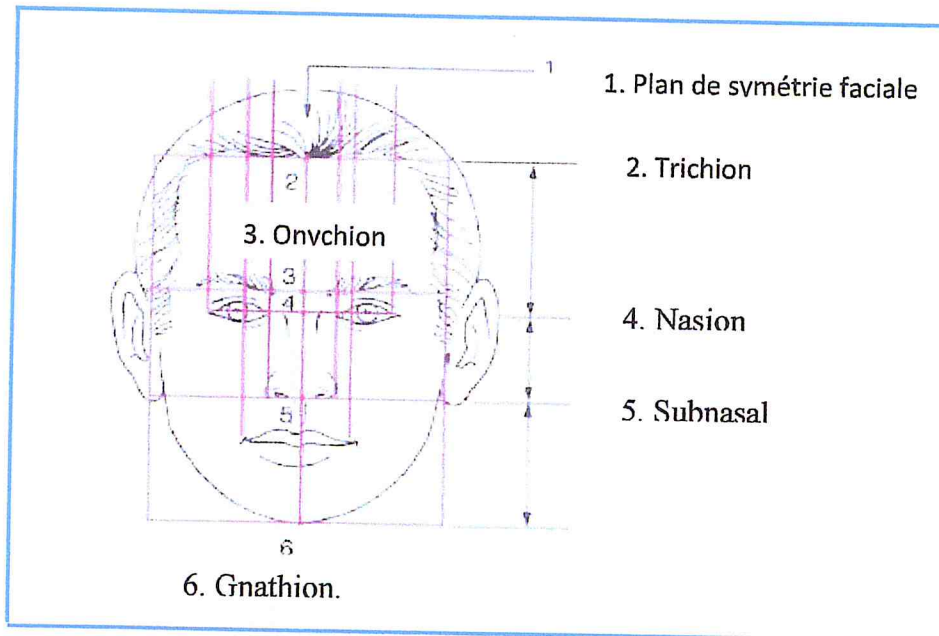


Figure II.5. Harmonie faciale, rapports des trois étages de la tête. [AA, 2005]

II.3. L'anthropologie :

L'anthropologie anatomique s'intéresse à l'étude de l'origine de l'Homme, à son évolution et à la distribution de ses caractéristiques morphologiques et cela pour repartir aisément le genre humain en groupes différents. [AA, 2005]

II.3.1. Généralités sur les mesures anthropologiques et la notion d'indices :

Les mensurations sont effectuées par références à des points (réels ou virtuels, selon le cas) en utilisant un instrument, le compas à pointes mousses par exemple, et en faisant attention à ne pas déprimer la peau. Deux dimensions d'un même organe (par exemple longueur et largeur de la tête) sont confrontées en faisant le rapport de 100 fois la mesure, la plus faible à la plus forte. Le quotient obtenu est qualifié d'indice et sa valeur est donnée sans unité.

Les valeurs indiciaires et angulaires ont l'avantage sur les mesures, qu'elles permettent de travailler sans tenir compte de l'échelle, lors du travail sur des documents ce qui est le cas en techniques de reconnaissance faciale [AA, 2005].

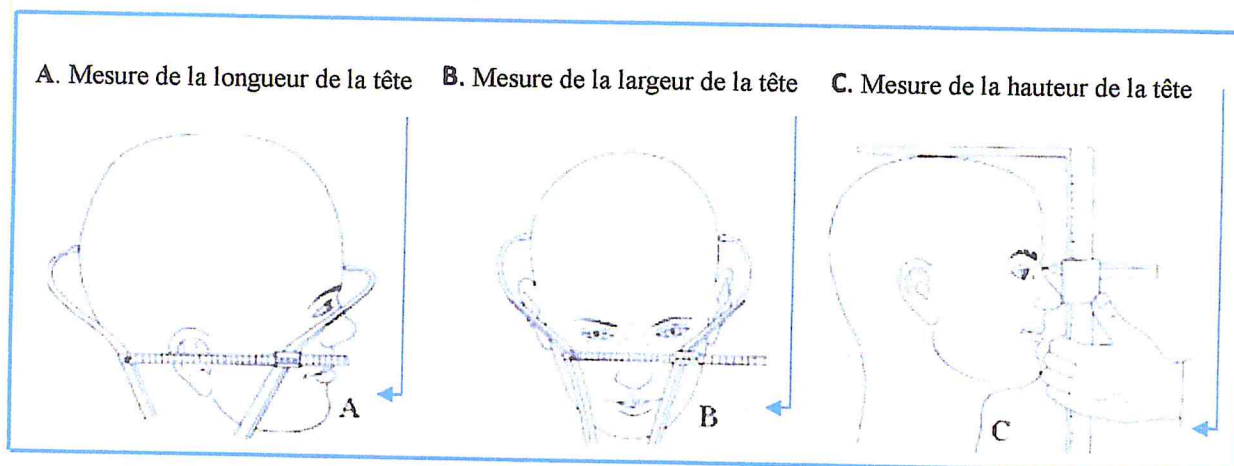


Figure II.6. Techniques de mesure des principaux diamètres de la tête. [AA, 2005]

II.3.2. Mensuration:

Nous nous contenterons ici d'une présentation rapide des mensurations et indices les plus classiquement utilisés [AA, 2005].

II.3.2.1. La face :

Hauteur de la face (ou Hauteur Morphologique) : C'est la distance du bord inférieur du menton (*gnathion*) au point nasal (*nasion*), lors de prise de mesure la position mandibulaire doit être au repos sans intercuspidation, avec un petites espace libre molaire. [AA, 2005]

La hauteur de la face est en corrélation avec la longueur de la tête et la hauteur du nez.

Largeur Bizygomatique de la face : C'est la distance horizontale maximum entre les deux arcades zygomatiques. Elle présente une corrélation directe avec la hauteur de la face, les largeurs de la tête et du nez.

Les valeurs se classent de la façon suivante : [AA, 2005]

Faces très larges (hypereuryprosopes)	jusqu'à 78,9
Faces larges (euryprosopes)	De 79,0 à 83,9
Faces moyennes (mésoprosopes)	De 84,0 à 87,9
Faces étroites (leptoprosopes)	De 88,0 à 92,0
Faces très étroites (hyperleptoprosopes)	A partir de 93,0

Tableau II.1. Répartition des valeurs indiciaires en fonction de la forme du visage.

Chapitre II: Généralités sur la reconnaissance de visages

L'indice est donc d'autant plus élevé que la face est plus étroite.

Chez l'enfant la face est relativement courte ; elle s'allonge au cours de la croissance, en même temps que le crâne. Il objective la largeur de la face relativement à celle de la tête.

Normalement ces deux largeurs croissent de pair, mais dans certains cas l'une l'emporte sur l'autre (forte brachycéphalie par exemple, ou au contraire largeur marquée de la face). Les valeurs se divisent en trois classes : [AA, 2005]

Faces étroites (micropsides)	Jusqu'à 89,9
Faces moyennes (mésopsides)	De 90,0 à 92,9
Faces larges (macropsides)	A partir de 93,0

Tableau II.2. Répartition des valeurs indiciaires en fonction de la forme faciale et céphalique

Cet indice traduit l'étroitesse ou l'élargissement relatif du front par rapport à la largeur de la face. On peut diviser ses valeurs en trois classes : [AA, 2005]

Front étroit	Jusqu'à 75,9
Front moyen	De 76,0 à 77,9
Front large	A partir de 78,0

Tableau II.3. Répartition des valeurs indiciaires en fonction de la forme frontale et zygomatique

Largeur Bigoniaque : C'est la largeur maximum entre les deux angles de la mâchoire, sans déprimer la peau. Ces angles (ou *gonions*) sont difficiles à situer exactement, car il y a souvent un arrondi à ce niveau. D'autre part les sujets obèses peuvent avoir une hypertrophie graisseuse parotidienne, juste en arrière du gonion.

Il traduit à la fois l'aspect carré de la mâchoire et l'étroitesse du visage, car les deux éléments de l'indice peuvent varier. Les valeurs peuvent se classer ainsi : [AA, 2005]

Mâchoires étroites	Jusqu'à 75,9
Mâchoires moyennes	De 76,0 à 77,9
Mâchoires larges	A partir de 78,0

Tableau II.4. Répartition des valeurs indiciaires en fonction de la forme mandibulaire et zygomatique.

II.3.2.2. Indices orbitaires et oculaires :

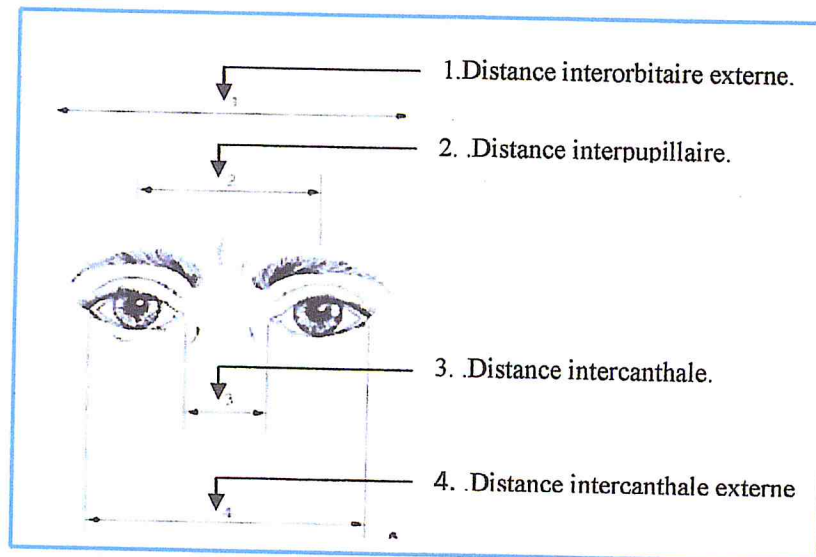


Figure II.7. Mensurations orbitopalpebrales. [AA, 2005]

II.3.2.3. Le Nez :

La largeur du nez est l'écartement maximum entre les ailes du nez. Elle présente une certaine corrélation avec la largeur de la face, mais n'en présente pas avec la hauteur du nez : cela donne un intérêt particulier à l'indice nasal. [AA, 2005]

La hauteur du nez est la distance entre le point nasal (ou nasion) et le point sousnasal. Ses valeurs se classent de la manière suivante : [AA, 2005]

Nez extrêmement étroits (ultraleptorhiniens)	Jusqu'à 39,9
Nez très étroits (hyperleptorhiniens)	De 40,0 à 54,9
Nez étroits (Leptorhiniens)	De 55,0 à 69,9
Nez moyens (mésorhiniens)	De 70,0 à 84,9
Nez larges (platyrhiniens)	De 85,0 à 99,9
Nez très larges (hyperplatyrhiniens)	De 100 à 114,9
Nez extrêmement larges (ultraplatyrhiniens)	à partir de 115,0

Tableau II.5. Répartition des valeurs indiciaires en fonction de la forme du nez.

Ce tableau indique la divergence ou la convergence de l'os nasal. Cet indice peut être mesuré sur un crâne sec ou sur l'être vivant.

Les valeurs se classent de la façon suivante : [AA, 2005]

Arête nasale convergente	De 10 à 30
Arête nasale parallèle	De 30 à 45
Arête nasale divergente	De 45 à 75

Tableau II.6. Répartition des valeurs indiciaires en fonction de la forme de l'arête nasale.

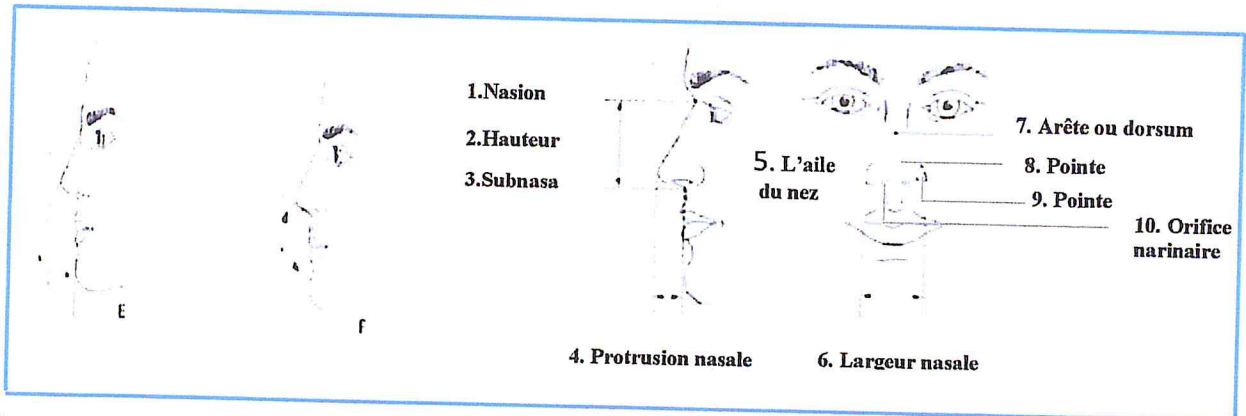


Figure II. 8. Angle nasofrontal et Angle nasolabial. Figure II.9. Anatomie descriptive et mensurations du nez.

E. Angle nasofrontal, sa largeur moyenne est comprise entre 25° et 40°

F. Angle nasolabial, sa valeur moyenne est de 90° . [AA, 2005]

II.3.2.4. La bouche et les lèvres :

Dimensions des lèvres : La hauteur des lèvres se mesure, la bouche normalement fermée, de la tangente aux deux courbes de la muqueuse labiale supérieure au point le plus inférieur de la muqueuse labiale inférieure. On mesure ainsi la partie éversée de la muqueuse : la musculature faciale ne doit donc pas être contractée. [AA, 2005]

La largeur de la bouche : est la distance d'une commissure à l'autre, là où la muqueuse rejoint la peau, la bouche étant normalement fermée, sans être pincée. La largeur de la bouche est en corrélation avec la largeur de la face, beaucoup plus qu'avec la hauteur des lèvres. Les valeurs absolues de ces dimensions sont tout aussi intéressantes que leur indice.

Ses valeurs peuvent s'interpréter ainsi : [AA, 2005]

Lèvres fines	Jusqu'à 34,9
Lèvres moyennes	De 35,0 à 44,9
Lèvres épaisses	A partir de 45,0

Tableau II.7. Répartition des valeurs indiciaires en fonction de la forme de la bouche et lèvres.

II.4. Conclusion :

Dans ce chapitre nous avons présenté les principaux concepts de l'anatomie du visage qui représentent essentiellement les bases de toutes les approches de reconnaissance de visages et qui nous seront utiles pour l'approche que nous allons adopter.

CHAPITRE III

Systemes de reconnaissance des visages

III.1. introduction :

La prochaine frontière de l'informatique vise à construire des machines qui se comportent autant que possible comme des humains. Bien qu'il soit très facile pour un humain de reconnaître que les dix images de la (Figure III.1), concernant la même personne, s'assurer qu'un ordinateur en soit capable est encore un défi scientifique de taille. Si un jour, nous serions capables de créer un tel logiciel informatique, alors on pourra avoir des applications immédiates à la reconnaissance :

- Des visages de criminels ou de terroristes.
- Des employés autorisés dans un laboratoire de haute sécurité.
- De textes et formules.
- Ou même des objets à partir de photos aériennes.

Dans le spectre de la biométrie, la reconnaissance de visages revêt un caractère particulier du fait du grand nombre de travaux qui lui sont consacrés et un sujet dont l'intérêt n'est plus à démontrer : biométrie, vidéo-surveillance, Interface Homme Machine avancées ou encore indexation d'images/vidéos.



Figure III.1. Image biométrique de la même personne.

III.2. La reconnaissance de visages humains:

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

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

Les systèmes de reconnaissance du visage reposent sur des algorithmes d'analyse de l'image, pouvant identifier les personnes qui y sont associées. Ces programmes créent une image du visage, en mesurant ses caractéristiques. Ils en produisent ensuite un fichier

individuel, dénommé "Template ou signature". Les Template sont alors comparées avec toutes les images existantes au niveau de la base de données, en ressortant un score de similitude.

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

Par ailleurs, on peut classifier les systèmes de reconnaissance du visage en deux grandes catégories selon la source de capture de l'image : reconnaissance du visage dans une séquence vidéo ou bien à partir d'images fixes. Dans ce dernier cas, on peut aussi différencier les systèmes basés sur des images 3D [XK, 2004] de ceux utilisant des images 2D.

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

III.3. Motivation : (pourquoi la reconnaissance de visages ?)

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

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

En plus, cette technique est très efficace pour les situations non standards, c'est les cas où on ne peut avoir la coopération de l'individu à identifier, par exemple lors d'une arrestation des criminels. Certes que la reconnaissance des visages n'est pas la plus fiable comparée aux autres techniques de biométrie, mais elle peut être ainsi si on utilise des approches plus efficaces en plus du bon choix des caractéristiques d'identification représentant le visage en question. [BS, 2014]

III.4. La place de la reconnaissance faciale parmi les autres techniques biométriques :

Les empreintes digitales sont les caractéristiques biométriques les plus communément utilisées pour la reconnaissance de criminels. Le premier système automatique d'authentification utilisant les empreintes digitales a été commercialisé au début des années soixante. D'autres parts, plusieurs études ont démontré que l'iris est la caractéristique la plus fiable car la texture de l'iris reste stable au cours de la vie (c.f. section 1.3). Toutefois, ces méthodes présentent l'inconvénient majeur d'être intrusives, ce qui limite énormément leurs domaines d'applications. De plus, une méthode comme l'identification de l'iris reste contraignante pour les utilisateurs qui n'apprécient pas de placer leur œil devant un appareil. A l'inverse, des systèmes d'identification basés sur l'analyse des images de visage ne présentent aucune contrainte pour les utilisateurs. La reconnaissance faciale est une modalité qui peut être implémentée de manière indépendante des autres modalités biométriques, elle est souvent utilisée dans des applications de surveillance. La reconnaissance faciale offre plusieurs avantages : le système de capture (c.à.d. les caméras) est facile à installer, il est accepté dans les lieux publics ce qui permet d'avoir des bases de données de plus en plus grandes et ainsi d'améliorer les performances de la reconnaissance. [SA, 2008]

Depuis quelques années, la reconnaissance faciale suscite un intérêt croissant auprès de la communauté scientifique, qui s'est notamment manifesté à travers l'organisation de conférences internationales spécialisées telle que « The International Conference on Audio and Video-based Biometric Person Authentication (AVBPA) » depuis 1997, et « the International Conference on Automatic Face and Gesture Recognition (AFGR) » depuis 1995. Par ailleurs, les États-Unis ont mené depuis 1993 une série de tests de reconnaissance faciale dont les résultats sont accessibles au public. Ces tests sont désignés sous les noms de FERET [PHJ, 1998] ; [SPH, 1998], XM2VTS [KJJ, 1999], FRVT 2000 [DMP, 2001] et FRVT 2002 [PPR, 2003].

Dans [SJD, 2007] les auteurs présentent une analyse statistique des publications sur les techniques biométriques soumises et publiées dans un numéro spécial de la revue IEEE

Transaction on PAMI (Tableau III.1). Nous constatons que la reconnaissance faciale arrive largement en tête avec un pourcentage de 33% du nombre total de publications. Ceci démontre bien l'intérêt scientifique pour cette technique.

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

Tableau III. 1. Répartition des articles sur les techniques biométriques soumis et acceptés dans la revue IEEE PAMI. [SA, 2008]

III.5. Systèmes biométriques basés sur la reconnaissance de visage :

La reconnaissance automatique de visage s'effectue en trois étapes principales :

1. Détection de visages.
2. Extraction et normalisation des caractéristiques du visage.
3. Identification et/ou vérification.

Les techniques de traitement utilisées dans chaque étape sont très critiques pour les applications biométriques et doivent par conséquent, être optimisées pour améliorer les performances du système global. [SA, 2008]

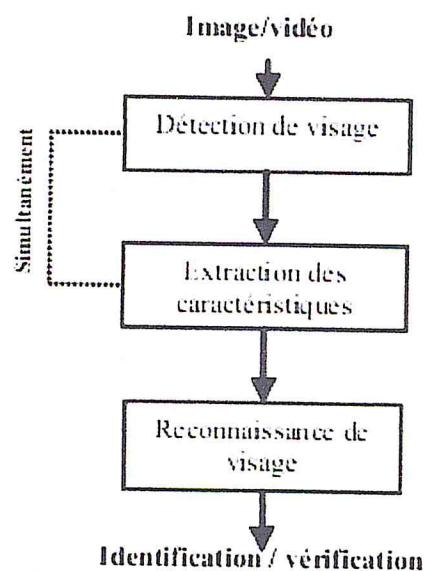


Figure III.2. Les étapes de la reconnaissance de visages. [SA, 2008]

Dans ce qui suit nous allons détailler chaque étape du système de reconnaissance faciale, et nous présenterons les principales difficultés rencontrées.

III.5.1. Détection de visage :

Dans la littérature scientifique, le problème de localisation de visages est aussi désigné par la terminologie "détection de visages". Plusieurs travaux de recherches ont été effectués dans ce domaine. Ils ont donné lieu au développement d'une multitude de techniques allant de la simple détection du visage, à la localisation précise de ses régions caractéristiques tels que les yeux, le nez, les narines, les sourcils, la bouche, les lèvres, les oreilles, etc.

Cependant, les solutions proposées jusqu'à maintenant sont loin d'être satisfaisantes car elles fonctionnent uniquement dans des environnements contrôlés, et par conséquent elles ne gèrent pas la variabilité des conditions d'acquisition de la vie quotidienne tels que la barbe la moustache, la pose et des facteurs tels que l'éclairage et les caractéristiques de l'appareil photographique affectent l'aspect d'un visage dans l'image acquise [SA, 2008].

III.5.2. Extraction de caractéristiques du visage :

L'extraction des caractéristiques telles que les yeux, le nez, la bouche est une étape prétraitement nécessaire à la reconnaissance faciale. On peut distinguer deux pratiques différentes :

. **L'extraction de régions entières du visage** : elle est souvent implémentée avec une approche globale de reconnaissance de visage.

. **L'extraction des points particuliers des différentes régions caractéristiques du visage** : tels que les coins des yeux, de la bouche et du nez. Elle est utilisée avec une méthode locale de reconnaissance et aussi pour l'estimation de la pose du visage.

Par ailleurs, plusieurs études ont été menées afin de déterminer les caractéristiques qui semblent pertinentes pour la perception, la mémorisation et la reconnaissance d'un visage humain. Dans [VB, 1988] ; [JGH, 1981] par exemple, les caractéristiques pertinentes rapportées sont : les cheveux, le contour du visage, les yeux et la bouche. Cette étude a également démontré le rôle important que joue le nez dans la reconnaissance faciale à partir des images de profil. En effet, dans ce cas de figure, il est évident que la forme distinctive du nez est plus intéressante que les yeux ou la bouche [VB, 1988]. Dans [JGH, 1981], les auteurs ont particulièrement établi que la partie supérieure du visage est plus utile pour la reconnaissance faciale que la partie inférieure [JGH, 1981]

III.5.3. La reconnaissance de visage (Identification) :

Le module 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 [SA, 2008].

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

Pour le cerveau humain, le processus de la reconnaissance de visages est une tâche visuelle de haut niveau. Bien que les êtres humains puissent détecter et identifier des visages dans une scène sans beaucoup de peine, construire un système automatique qui accomplit de telles tâches représente un sérieux défi. Ce défi est d'autant plus grand lorsque les conditions d'acquisition des images sont très variables. Il existe deux types de variations associées aux images de visages : inter et intra-sujet. La variation inter est limitée à cause de la ressemblance physique entre les individus. Par contre la variation intra-sujets est plus vaste. Elle peut être attribuée à plusieurs facteurs que nous analysons ci-dessous [SA, 2008]:

III.6.1. Changement d'illumination :

L'apparence d'un visage dans une image varie énormément en fonction de l'illumination de la scène lors de la prise de vue (Figure III.3). Les variations d'éclairage rendent la tâche de reconnaissance de visage très difficile. En effet, le changement d'apparence d'un

visage dû à l'illumination, se révèle parfois plus critique que la différence physique entre les individus, et peut entraîner une mauvaise classification des images d'entrée. Ceci a été expérimentalement observé dans Adini et al [YY, 1997] où les auteurs ont utilisé une base de données de 25 individus. L'identification de visage dans un environnement non contrôlé reste donc un domaine de recherche ouvert. Les évaluations FRVT [DMP, 2001] ont révélé que le problème de variation d'illumination constitue un défi majeur pour la reconnaissance faciale



Figure III.3. Exemple de variation d'éclairage. [SA, 2008]

III.6.2. Variation de pose :

Le taux de reconnaissance de visage baisse considérablement quand des variations de pose sont présentes dans les images. Cette difficulté a été démontrée par des tests d'évaluation élaborés sur les bases FERET et FRVT [DMP, 2001] ; [PPR, 2003]. La variation de pose est considérée comme un problème majeur pour les systèmes de reconnaissance faciale. Quand le visage est de profil dans le plan image (orientation $< 30^\circ$), il peut être normalisé en détectant au moins deux traits faciaux (passant par les yeux). Cependant, lorsque la rotation est supérieure à 30° , la normalisation géométrique n'est plus possible (Figure III.4)



Figure III.4. Exemples de variation de poses. [SA, 2008]

III.6.3. Expressions faciales :

Un autre facteur qui affecte l'apparence du visage est l'expression faciale (Figure III.5).

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

additionnelle significative qui peut être utilisée pour résoudre ce problème [RJJ, 2001]. L'approche géométrique que nous avons proposée nous semble bien adoptée pour résoudre ce problème, car nous avons appliqué tous les calculs sur la partie supérieure du visage qui reste invariante lors du changement des expressions du visage.



Figure III.5. Exemples de variation d'expressions faciales. [SA, 2008]

III.6.4. Présence ou absence des composants structurels :

La présence des composants structurels telle que la barbe, la moustache, ou bien les lunettes peut modifier énormément les caractéristiques faciales telles que la forme, la couleur, ou la taille du visage. De plus, ces composants peuvent cacher les caractéristiques faciales de base causant ainsi une défaillance du système de reconnaissance. [BS, 2014]

III.6.5. Occultations partielles :

Le visage peut être partiellement masqué par des objets dans la scène, ou par le port d'accessoire tels que lunettes, écharpe... Dans le contexte de la biométrie, les systèmes proposés doivent être non intrusifs c'est-à-dire qu'on ne doit pas compter sur une coopération active du sujet. Par conséquent, il est important de savoir reconnaître des visages partiellement occultés. Gross et al [RJJ, 2001] ont étudié l'impact du port de lunettes de soleil, et du cache-nez occultant la partie inférieure du visage sur la reconnaissance faciale. Ils ont utilisé la base de données AR [AR, 1998]. Leurs résultats expérimentaux semblent indiquer que, dans ces conditions, les performances des algorithmes de reconnaissance restent faibles

III.6.6. Les vrais jumeaux :

Qui ont le même indicatif d'ADN, peuvent tromper les personnes qui ne les connaissent pas (les personnes familières avec les jumeaux ont reçu une grande quantité d'information sur ces derniers et sont donc beaucoup plus qualifiées à distinguer les jumeaux.).

Il est peu probable que la vérification automatique de visage, ne pourra jamais détecter les différences très subtiles qui existent entre les jumeaux. [BS, 2014]

III.7. Détection de visages :

La détection de visages est la première étape dans le processus de reconnaissance faciale.

Son efficacité a une influence directe sur les performances du système de reconnaissance de visages. Il existe plusieurs méthodes pour la détection de visages, certaines utilisent la couleur de la peau, la forme de la tête, l'apparence faciale, alors que d'autres combinent plusieurs de ces caractéristiques. [Yan, 2002]

Les méthodes de détection de visages peuvent être subdivisées en quatre catégories:

III.7.1. Approches basées sur les connaissances acquises :

Cette méthodologie s'intéresse aux parties caractéristiques du visage comme le nez, la bouche et les yeux. Elle est basée sur la définition de règles strictes à partir des rapports entre les caractéristiques faciales. Ces méthodes sont conçues principalement pour la localisation de visage. Tout d'abord, les caractéristiques du visage sont localisées à l'aide de la méthode de projection proposée par *Kanade* [TK, 1973] pour détecter les contours d'un visage, 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 [Yan, 1994] quant à eux ont étudié leurs évolutions 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. [Yan, 2002]

III.7.2. Approches basées sur le « Template-matching » :

Les Template 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.

Yuille et al. [Yui, 1992] 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. [Yan, 2002]

III.7.3. 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 [Tur, 1991], elle consiste à projeter l'image dans un espace et à calculer la distance euclidienne entre l'image et sa projection. [Yan, 2002]

III.7.4. Approches basées sur des caractéristiques invariantes :

Ces approches sont utilisées principalement pour la localisation des visages. 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.

Yow et Cipolla [Yow, 1997] ont développé une méthode basée sur l'extraction de points d'intérêts (les maximaux locaux de la dérivée seconde d'un filtre gaussien). Ces points sont ensuite utilisés pour réaliser une détection de contours qui sont à leur tour groupés en régions. Le regroupement des contours est basé sur un critère de proximité et un critère de similarité en orientation et en épaisseur. A partir de chaque région, l'algorithme définit alors un vecteur pour lequel il calcule la moyenne et la matrice de covariance par rapport aux différents vecteurs des modèles. [Yan, 2002]

III.8. Techniques de reconnaissance de visage :

Les approches de la reconnaissance de visage peuvent être subdivisées en trois catégories :

Les approches holistiques ou globales, les approches locales et les approches hybrides [FEB].

III.8.1. Approche holistique ou globale :

Les méthodes globales sont basées sur des techniques d'analyse statistique bien connues. Il n'est pas nécessaire de repérer certains points caractéristiques du visage (comme les centres des yeux, le centre de la bouche, etc.) à part pour normaliser les images. Dans ces méthodes, les images de visage (qui peuvent être vues comme des matrices de valeurs de pixels) sont traitées de manière globale et sont généralement transformées en vecteurs, plus faciles à manipuler. [SPR, 2006]

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

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

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

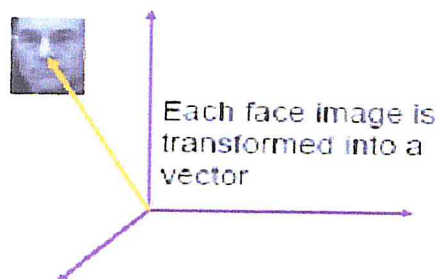


Figure III.6. le principe des méthodes globales

Parmi les méthodes les plus importantes réunies au sein de cette approche on trouve :

III.8.1.1. Réseau de neurones :

Un réseau de neurones est un assemblage d'un grand nombre d'unités de traitement hautement reliées, travaillant ensemble pour exécuter une tâche de classification donnée. Pour effectuer cette classification, différents types de réseaux de neurones peuvent être utilisés.

En général, on leur transmet les pixels de l'image à classifier dans la couche d'entrée et après les traitements, le réseau va décider que l'image traitée est un visage ou non [LK, 2010].

III.8.1.2. Eigen Face :

L'utilisation de méthodes statistiques appliquées à la modélisation et à la reconnaissance de visage est largement répandue. En 1911, c'est l'introduction du concept d'Eigen Faces à des fins de reconnaissance basée sur une analyse en composantes principales (ACP).

Les Eigen Objects visent d'analyser certaines parties bien précises du visage, La personne peut par exemple être reconnue uniquement grâce à ses yeux [LK, 2010].

III .8.1.3. Méthodes de Markov Cachés(HMM) :

Les méthodes de Markov cachés(HMM) ont été introduites dans les années 70(1966), par Baum. Ils ont connus un succès dans la reconnaissance vocale ou ils sont utilisés comme modèle de référence, puis ils se sont imposés dans d'autres domaines tels que la modélisation de référence des formes, l'analyse de la séquence biologique comme : la recherche de motifs et de séquences dans les gènes.

Les méthodes de Markov Cachés HMMs sont massivement utilisées en reconnaissance de formes, en intelligence artificielle ou encore peuvent être appliquées à la reconnaissance de visages. [LK, 2010].

III.8.1.4. Discret Cosine Transform (DCT) :

L'utilisation de la transformée de cosine discrète (Discrete Cosine Transformou DTC) à des fins de reconnaissance de visage est assez récente. Relativement similaire aux Eigen Faces dans sa mise en œuvre, elle est par contre beaucoup plus rapide tant en phase d'apprentissage qu'en phase de reconnaissance. [LK, 2010].

III.8.2. Approches locales :

Les méthodes locales, basées sur des modèles, utilisent des connaissances a priori que l'on possède sur la morphologie du visage et s'appuient en général sur des points caractéristiques de celui-ci. Kanade présenta un des premiers algorithmes de ce type [TK, 1973] en détectant certains points ou traits caractéristiques d'un visage puis en les comparant avec des paramètres extraits d'autres visages. Ces méthodes constituent une autre approche pour prendre en compte la non-linéarité en construisant un espace de caractéristiques local et en utilisant des filtres d'images appropriés, de manière à ce que les distributions des visages soient moins affectées par divers changements.

Toutes ces méthodes ont l'avantage de pouvoir modéliser plus facilement les variations de pose, d'éclairage et d'expression par rapport aux méthodes globales. Toutefois, elles sont plus lourdes à utiliser puisqu'il faut souvent placer manuellement un assez grand nombre de points sur le visage alors que les méthodes globales ne nécessitent de connaître que la position des yeux afin de normaliser les images, ce qui peut être fait automatiquement et de manière assez fiable par un algorithme de détection. [SPR, 2006]

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

Parmi les méthodes les plus importantes réunies au sein de cette approche on trouve :

III.8.2.1. Méthodes géométriques :

Elle est basée sur l'extraction de la position relative des éléments qui constituent le visage (tel que le nez, la bouche et les yeux) pour former un modèle géométrique.

Pour ce faire, il faut extraire les 12 points suivants : (A B C D E F G H I J) qui seront utilisés dans le calcul d'un vecteur caractéristique $V [AD BC SG SH SM]$ qui représente l'individu. C'est cette méthode que nous avons choisie dans notre application [MB, 2007].

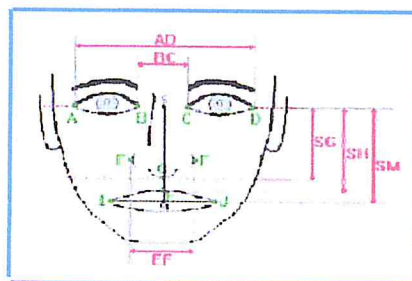


Figure III.7. Détection de 12 points. [MB, 2007]

III.8.2.2. Méthode basées sur les graphes :

Plutôt que d'utiliser des méthodes purement géométriques, certains chercheurs ont choisi de représenter les caractéristiques locales du visage sous forme de graphes. Ils ont proposé une méthode de détection des caractéristiques locales du visage, basée sur la décomposition en ondelettes de Gabor. La reconnaissance de visage est alors formulée comme un problème de mise en correspondance de graphes. [MB, 2007]

III.8.3. Approches hybrides :

Les méthodes hybrides permettent d'associer les avantages des méthodes globales et locales en combinant la détection de caractéristiques géométriques (ou structurales) avec l'extraction de caractéristiques d'apparence locales. Elles permettent d'augmenter la stabilité de la performance de reconnaissance lors de changements de pose, d'éclairément et d'expressions faciales. [SPR, 2006]

III.9. Indicateurs de performance d'un système biométrique :

Les indicateurs de performance d'un système biométrique sont différents selon que le système opère en mode identification ou authentification. [BF, 2004]

III.9.1. Système opérant en mode identification : La mesure de performance dans ce cas peut se faire par le calcul du pourcentage des personnes bien reconnues, appelé le Taux d'Identification (TID), qui est défini par la formule suivante [MN, 2009]

$$TID = \frac{\text{nombre de tests ayant conduit à une identification correcte}}{\text{nombre total de tests}}$$

Ou en utilisant la courbe CMC (Cumulative Match Characteristics) (Figure III.8), qui indique le taux d'identification (TID) en fonction d'une variable qu'on appelle le rang ; on dit qu'un système reconnaît au rang 1 lorsqu'il choisit la plus proche image comme résultat de la reconnaissance. On dit qu'un système reconnaît au rang 2, lorsqu'il choisit, parmi deux images, celle qui correspond le mieux à l'image d'entrée...etc. On peut donc dire que plus le rang augmente, plus le taux de reconnaissance correspondant est lié à un niveau de sécurité faible. [BF, 2004]

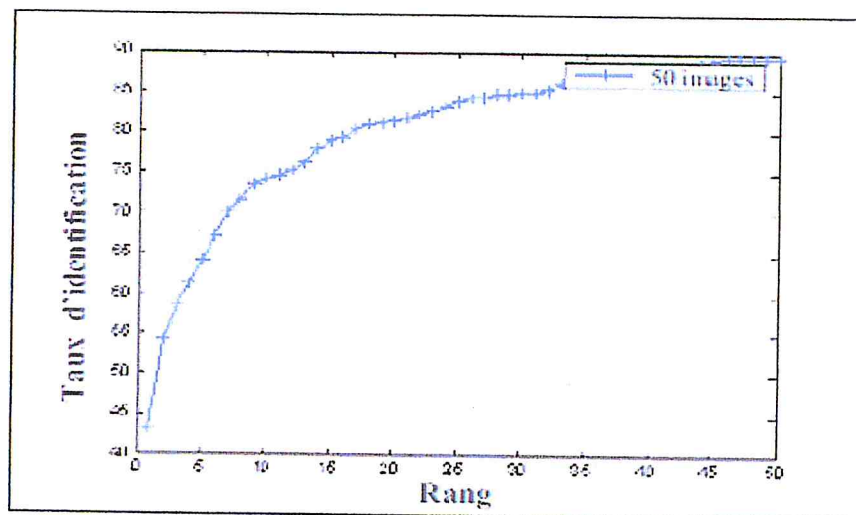


Figure III.8. Courbe CMC [BF, 2004]

III.9.2. Système opérant en mode authentification :

La mesure de performance d'un système biométrique en mode authentification se fait à l'aide d'un ensemble d'indicateurs obtenus en phase de test comme: le taux des Fausses Acceptations (False acceptance rate, FAR), le taux des Faux Rejets (FRR) et le taux d'égalité d'erreur (EER). [BF, 2004]

- Le taux de fausse acceptation (« False Accept Rate », FAR) : [BF, 2004] C'est le pourcentage de personnes censées ne pas être reconnues mais qui sont tout de même acceptées par le système. Ce pourcentage est donné par la formule suivante:

$$TFA = \frac{\text{nombre de fausses acceptations}}{\text{nombre de personnes testées}}$$

- Le taux de faux rejets ("False Reject Rate", FRR) : [BF, 2004] C'est le pourcentage de personnes censées être reconnues mais qui sont tout de même rejetées par le système. Il est donné par la formule suivante:

$$TFR = \frac{\text{nombre de faux rejets}}{\text{nombre de personnes testées}}$$

La relation entre TFR et le TFA est illustrée dans la figure (Figure III.10).

La figure suivante montre l'influence du seuil de décision sur les erreurs du système biométrique : [BF, 2004]

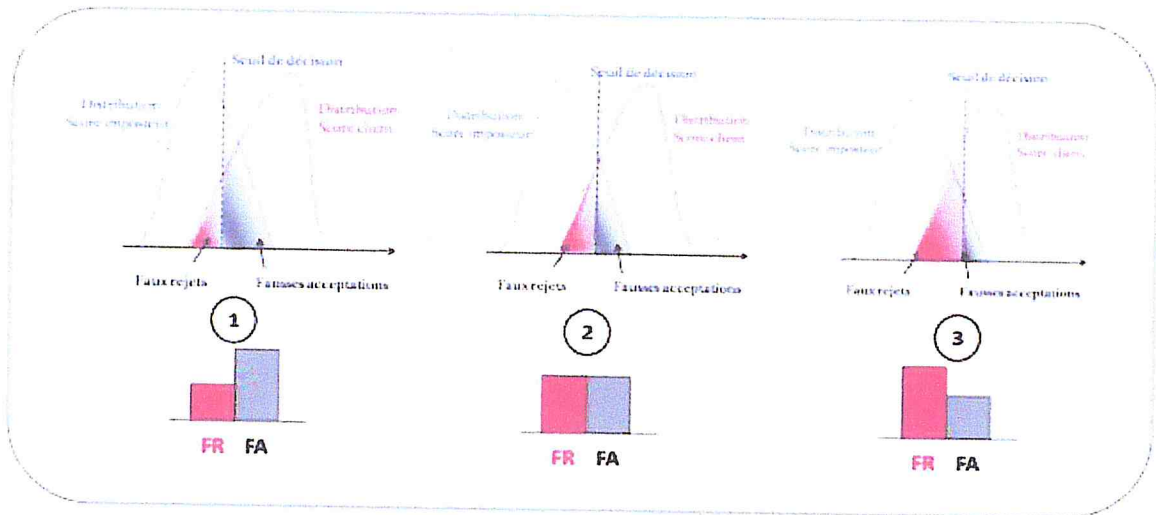


Figure III.9. Influence du seuil de décision sur les erreurs d'un système biométrique

- 1- Seuil de décision choisi dans le but de réduire le nombre de faux rejets
 - 2- Seuil de décision choisi pour obtenir autant de faux rejets que de fausses acceptations
 - 3- Seuil de décision choisi dans le but de réduire le nombre de faux rejets
- Taux d'égale erreur (Equal Error Rate, EER) : [BF, 2004] Comme illustré dans la figure ci-dessus (Figure III.9), ce taux correspond au point où le taux de fausses acceptations est égal au taux de faux rejets ($TFA = TFR$), ce qui représente le meilleur compromis entre ces deux types de taux présentés précédemment.

Il constitue une mesure de performance courante.

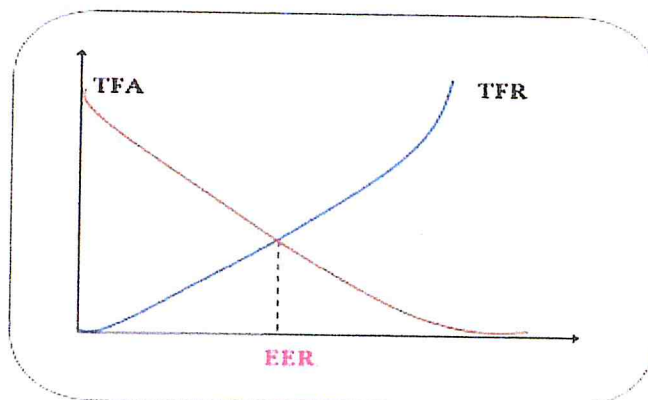


Figure III.10 Représentation du Taux d'erreur

- La courbe ROC (“Receiver Operating Characteristic”) [BF, 2004]

Cette courbe permet de tracer le taux de faux rejets (TFR) en fonction du taux de fausses acceptations (TFA).

Plus cette courbe tend à épouser la forme du repère, plus le système est performant, c’est-à-dire possédant un taux d’erreurs plus petit.

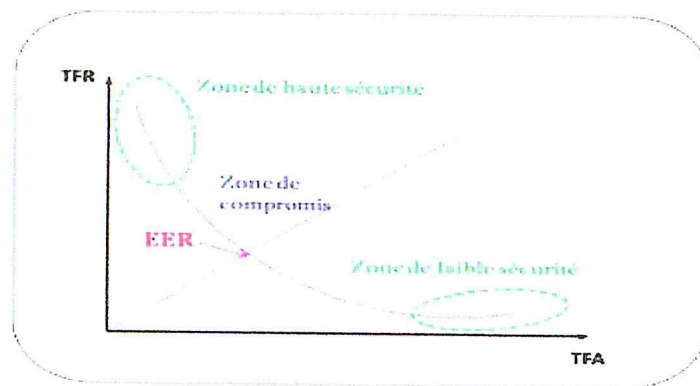


Figure III.11 - La courbe ROC. [BF, 2004]

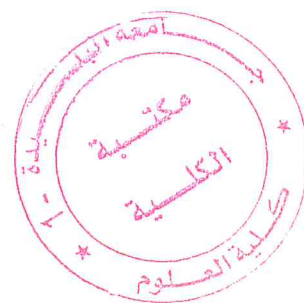
III.10. Conclusion :

Nous avons présenté dans ce chapitre un certain nombre de généralités concernant la reconnaissance des visages avec un survol sur la panoplie des méthodes existantes qui sont classifiées en trois approches : locales, globales et hybrides.

Les méthodes globales ont l’inconvénient de nécessiter un grand nombre de calculs, ce qui équivaut à dire qu’elles ne sont pas favorisées dans les systèmes de reconnaissance. Par contre les méthodes locales ont l’avantage de prendre en compte la particularité du visage en tant que forme naturelle à reconnaître. De ce fait ; nous avons adopté la méthode géométrique dans notre approche de l’identification de visage humain. Le chapitre suivant présentera en détail cette démarche.

CHAPITRE IV

Approche adoptée



IV.1. Introduction :

De nombreuses méthodes de reconnaissance de visages ont été proposées au cours des trente dernières années. La reconnaissance faciale automatique est un challenge tel qu'il a suscité de nombreuses recherches dans des disciplines différentes : psychologie, neurologie, mathématiques, physique et informatique (reconnaissance des formes, réseaux de neurones, vision par ordinateur). C'est la raison pour laquelle la littérature sur la reconnaissance de visages est vaste et diversifiée.

Les neurologistes étudient depuis longtemps le mécanisme par lequel le cerveau reconnaît les visages, et beaucoup croient que le cerveau perçoit les visages d'une manière spécifique et très différente des autres objets visuels. Par exemple, les études ont constaté qu'une rotation d'image faciale de 180 dégrade la reconnaissance beaucoup plus qu'une même rotation pour des objets quelconques (Figure IV.1). Dans un travail innovant [MMG, 1997], Moscovitch et al. ont démontré que le cerveau des hommes traite les visages et les objets dans des aires séparées à savoir que les visages sont traités dans une aire spéciale.

Cette approche a fait office de référence pendant la dernière décennie jusqu'au travail récent de Jiang et al. [XTV, 2006] qui montre que le traitement des visages et des objets ne reposent finalement pas sur des mécanismes différents.

Les systèmes de reconnaissance de visages sont très souvent classés à partir des conclusions d'études psychologiques sur la façon dont les hommes utilisent les caractéristiques faciales pour reconnaître les autres.

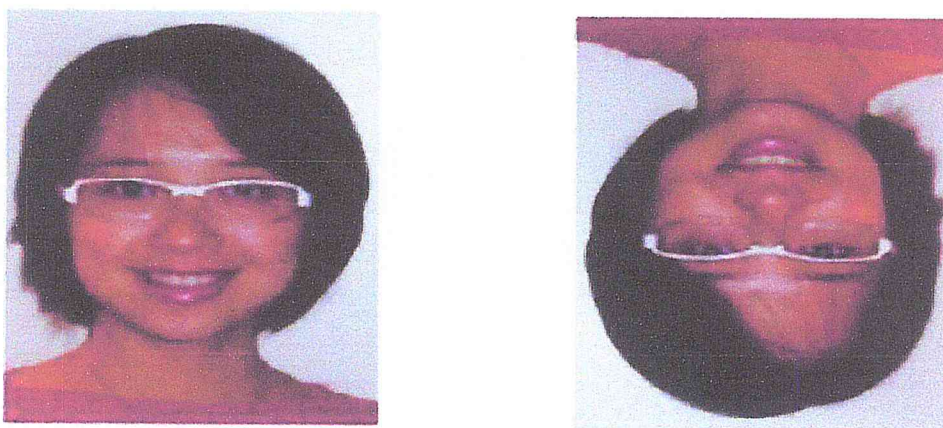


Figure IV.1. Quand les visages ne sont pas vus dans leur état naturel, la capacité du système visuel humain à les distinguer est dégradée. [KB, 2013]

IV.2. Système de reconnaissance de visages:

Nous présentons dans cette partie, la méthode utilisée pour effectuer la reconnaissance de visages.

Rappelons pour commencer l'objectif à atteindre, On possède une image contenant un visage dont on veut identifier. Les points caractéristiques (à extraire) sont définis par un modèle géométrique. Où on a 6 points bien choisis qui sont suffisants pour identifier un visage, mais pour des bases de données plus larges le nombre de points caractéristiques doit être plus grand, parce que on risque de trouvé des ressemblances entre individus qui aurons peut-être les mêmes emplacements des points caractéristiques qui implique les mêmes distances entre ces points, c'est pour cela qu'on doit élargir le nombre de points caractéristiques pour minimiser le taux de ressemblances. Le choix des points caractéristiques est basé sur le fait que la région des yeux, celle du nez et celle de la bouche soient importantes pour l'identification, les points qu'on utilise couvrent l'ensemble des trois régions, ils sont au nombre de 12 (Figure IV.2) : Nous avons réutilisé 6 points, et rajoute 6 points tel qu'illustré par la (Figure IV.3) :

- Les quatre coins des yeux : A, B, C, et D.
- Le point E centre de gravité de A, B, C et D (milieu de la tête).
- Le point F à la base du nez.

Les coordonnées des 6 points seront utilisées dans le calcul d'un vecteur caractéristique qui représente l'individu, les composantes du vecteur caractéristiques sont des distances normalisées entre les 6 points extraits.

Les informations choisies pour modéliser le visage doivent être discriminantes, compactes. Nous avons sélectionné 5 distances possibles entre les points:

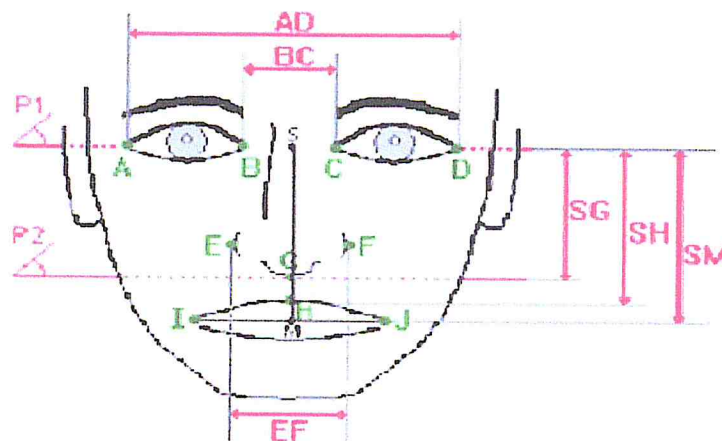


Figure IV.2. Les 12 point détecté [MC, 2002]

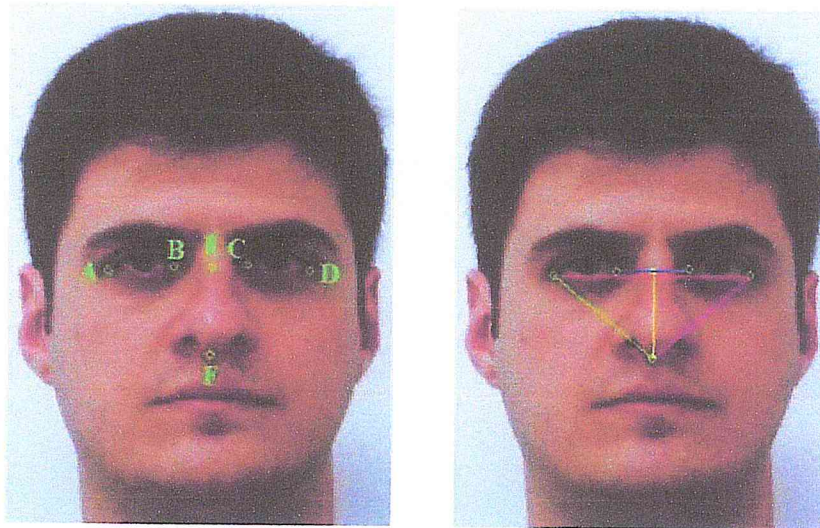


Figure IV.3. Les 6 points détectés.

- Région des yeux : Généralement l'œil gauche a la même taille que l'œil droit et donc les points A et B sont symétriques aux points C et D par rapport à E, pour éviter la redondance d'information ($AB = CD$ et $AC = BD$) nous n'avons utilisé que les 2 distances AD et BC pour coder la région des yeux.
- Région du nez : La hauteur du nez est représentée par la distance EF, et la distance AF, et la distance DF.
- Ainsi, dans sa totalité, le vecteur caractéristique est : $V [AD \ BC \ EF \ AF \ DF]$

Avec ce système on attribue une identité à un individu ou on le déclare inconnu. La méthode de reconnaissance adoptée est celle des k plus proches voisins (KPPV).

La distance utilisée est la distance euclidienne Avec la méthode des K-PPV, il faut calculer la distance entre le vecteur caractéristique de la personne à identifier et chaque vecteur W_i de la base.

IV.3. Algorithme des k-ppv :

L'algorithme des k-plus-proches-voisins (K-PPV) est l'un des algorithmes les plus simples d'apprentissage automatique supervisé. On supposant qu'une base d'apprentissage correctement étiquetée soit à disposition, cette méthode permet d'obtenir de très bons résultats de classification. [LR, 2007]

IV.4. les bases des données du visage existantes :

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

Les bases les plus anciennes (ORL et YALE) ont été le plus utilisées et permettent de comparer plus facilement de nouvelles méthodes à celles de l'état de l'art. Les plus récentes (Color FERET, FRGC, CVL, AR et IV2) contiennent plus de personnes et sont donc utiles pour des évaluations à plus grande échelle. D'autres bases de visages sont disponibles et destinées à des évaluations adaptées à certaines variabilités du visage telles que les bases UMIST, BANCA, PF01, Yale et PIE. Ces trois dernières bases par exemple (PF01, Yale et PIE) disposent d'un nombre important de poses différentes mais renferment seulement quelques dizaines de personnes acquises lors d'une seule session.

Notre choix s'est arrêté sur les bases XM2VTS, Color FERET, AR, CVL en plus de la base ORL pour développer notre corpus de travail. Nous détaillons principalement ces bases d'images ci-dessous. Une liste plus complète et plus détaillée est disponible dans. [FRH]

IV.4.1. La base XM2VTS :

La base XM2VTS [KJJ, 1999] (The Extended M2VTS Database) est une base de données multimodale qui renferme des images faciales 2D et 3D, ainsi que des séquences vidéo avec des enregistrements de la voix. La base de données a été acquise dans le cadre du projet M2VTS (Multi Modal Verification for Teleservices and Security applications) à l'Université de Surrey (Royaume-Uni). La base de données contient 295 personnes enregistrées en 4 sessions durant une période de 4 mois. La base de données de visage 2D contient des prises de vue faciales et de profil. Deux prises de vue faciales ont été enregistrées, à chaque session, ce qui fait un total de 8 images pour chaque personne. La (Figure IV.4) illustre un exemple d'images d'une personne. Les images en colonnes représentent les sessions auxquelles elles appartiennent.



Figure IV.4. Exemples d'images de la base XM2VTS. [KJJ, 1999]

IV.4.2. La base FERET :

La base de données FERET a été collectée dans le cadre du programme Facial Recognition Technology [PHR, 2000], [DCF] mené par le National Institute of Standards and Technology (NIST) Américain. Il s'agit de la plus grande base disponible pour les chercheurs qui a été acquise avec des poses différentes et durant 15 sessions entre 1993 et 1996. Les images, initialement collectées depuis un appareil photographique de 35mm ont ensuite été digitalisées. Une première version de cette base de données a été réalisée en 2001 et contient 14051 images faciales en niveaux de gris avec une résolution de 256 x 384 pixels.

La version la plus récente, réalisée en 2003, renferme des images numériques couleurs de plus grande qualité avec une résolution de 512 x 768 pixels et une compression sans perte de données à la différence des premières images en niveaux de gris. En plus, de multiples erreurs de noms d'images, d'identifiants, et dates de capture, qui figurent sur la première base à niveau de gris ont été corrigées. Cette dernière base contient 11338 images représentant 994 personnes différentes. Pour chaque individu, on dispose d'une vue faciale régulière fa et une vue faciale alternative fb prise un peu après fa. D'autres poses ont été acquises pour la majorité de ces individus allant du profil gauche au profil droit avec des rotations de 15, 22, 45, 67 et 90° en profondeur de la tête. Pour quelques personnes de la base, on dispose d'autres vues duplicate collectées dans des conditions similaires à fa et fb mais dans des sessions ultérieures. Aucune contrainte n'est imposée sur la date de la prise de vue de l'image duplicate I. par contre, la vue duplicate II a été collectée au moins 540 jours après la première prise de vue.



Figure IV.5. Extrait de la base Color FERET : Les images sont transformées en niveau de gris. [DCF]

IV.4.3. La base AR :

La base AR [AR, 1998] a été constituée en 1998 au sein du laboratoire Computer Vision Center (CVC) à Barcelone, en Espagne. 116 personnes (63 hommes et 53 femmes) sont enregistrées. Les images sont en couleur de taille 768 x 576 pixels. 13 vues de chaque sujet ont été collectées. Pour la majorité de ces personnes, 13 autres vues ont été acquises lors d'une deuxième session à deux semaines d'intervalle.

Un extrait des images collectées lors de la première session est donné en (figure IV.6), Ces vues renferment des changements d'expression faciale, d'éclairage, ainsi que des occultations partielles des yeux (lunettes de soleil) et de la partie basse du visage (cache-col).

Lors de la seconde session, les 13 vues sont collectées dans les mêmes conditions que pour la première.

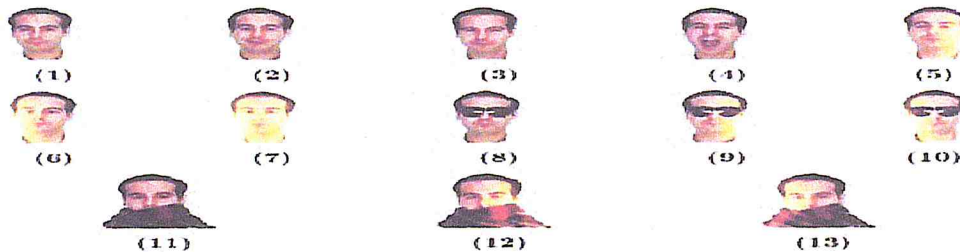


Figure IV.6. Extrait de la base AR. Ensembles des vues collectées pour un individu de la base [AR, 1998]

IV.4.4. La base CVL :

Cette base de données de visage a été créée au Computer Vision Laboratory (CVL) à l'université de Ljubljana (Slovénie) [CVL]. 114 personnes y sont enregistrées. Les images sont en couleur de taille 640 x 480 pixels. 7 vues de chaque sujet ont été collectées. Ces vues renferment différentes poses et expressions prises dans des conditions de luminosité uniformes. Parmi ces images, trois seulement sont de face. La (figure IV.7) illustre un exemple d'images de face de la base CVL



Figure IV.7. Images faciales extraites de la base CVL. [CVL]

IV.4.5. La Base de données ORL :

Conçu par AT&T laboratoires de l'université de Cambridge en Angleterre, la base de données ORL (Olivetti Research Laboratory) est une base de données de référence pour les systèmes de reconnaissances automatique des visages. En effet tous les systèmes de reconnaissances de visages trouvés dans la littérature ont été testés par rapport à l'ORL, cette popularité est due aux nombre de contraintes imposés par cette base car la plus part des changements possibles et prévisibles du visage ont été pris en compte, comme par exemple : le changement de coiffure, la barbe, les lunettes, les changements dans les expressions faciales, etc. Ainsi que les conditions d'acquisition telles que : le changement d'illumination et le changement d'échelle dû à la distance entre le dispositif d'acquisition et l'individu.

La base de données ORL est constituée de 40 individus, chaque individu possède 10 poses, donc la base contient 400 images. Les poses ont été prises sur des intervalles de temps différents pouvant aller jusqu'à trois mois. L'extraction des visages à partir des images a été faite manuellement. Nous présenterons dans ce qui suit les figures montrant les spécificités de la base de données de référence ORL. [KB, 2013]

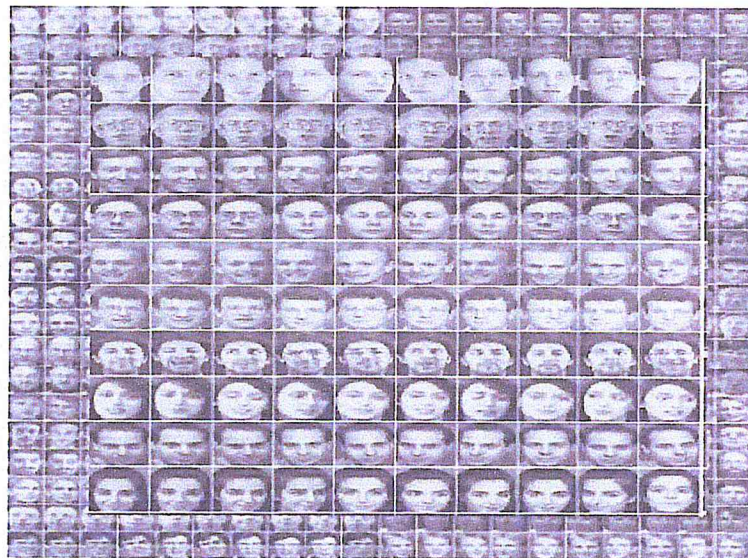


Figure IV.8. Base de données ORL [KB, 2013]

Voici un exemple où l'acquisition se fait sous différentes orientations du visage et sous différents éclairages:



Figure IV.9. Exemple de changements d'orientations du visage [KB, 2013]

Voici un exemple où l'acquisition se fait sous différents éclairages :



Figure IV.10. Exemple de changements d'éclairage [KB, 2013]

Cet exemple montre les changements d'échelle dus à la distance entre le dispositif d'acquisition et l'individu :



Figure IV.11. Exemple de changements d'échelle [KB, 2013]

La base de données ORL prend aussi en considération les expressions faciales, telles que les grimaces. En voici un exemple :



Figure IV.12. Exemple de changements des expressions faciales [KB, 2013]

La Base ORL prend en compte le fait qu'un individu peut porter ou ne pas porter des lunettes. Cet exemple en est l'illustration :



Figure IV.13. Exemple de port de lunettes [KB, 2013]

Un individu peut aussi porter une barbe ou changer de coiffure, la base ORL prend en considération ces particularités :

La base ORL comprend aussi des individus de différents âges, sexe et couleurs de peaux :



Figure IV.14. Exemple de changements de coiffure et de port de barbe [KB, 2013]



Figure IV.15. Exemple d'individus de différents âges races et sexes [KB, 2013]

IV.4.6. Base Labeled Faces in the Wild (LFW):

Très récemment, une nouvelle base de visages intéressante nommée Labeled Faces in the Wild⁶ a été présentée. Cette base de données qui contient 13233 images de 5749 personnes est considérée naturelle car les images ont été collectées directement sur le site d'information Yahoo ! News en utilisant un détecteur automatique de visage. Cette base est plus difficile pour les chercheurs car aucune contrainte sur les paramètres de prise de vue n'a été imposée (la base contient donc des variations importantes de pose, d'âge, d'expression, des images de mauvaise qualité, etc.). Dans le protocole d'évaluation associé à cette base, la question de la reconnaissance de visages devient une tâche de comparaison de l'identité de deux images dans une paire : étant donnée une paire d'images faciales, il s'agit de déterminer si elles sont issues de la même personne ou pas. Grâce aux étiquettes associées aux images originales, une paire

d'images de la base LFW est soit classée dans la catégorie Same, si les deux images proviennent d'une même personne, soit classée dans la catégorie Diff, si les deux images proviennent de deux personnes différentes. La (figure IV.16) montre quelques exemples de paires d'images de cette base. Cette base est disponible sous trois versions : original qui contient les images détectées sans alignement, funneled qui contient les images alignées automatiquement par l'algorithme de Huang et al. [GVL, 2007], aligned qui contient les images alignées automatiquement par l'algorithme de Wolf et al. [LT, 2009].



Figure IV.16. Paires de la base LFW aligned

IV.4.7. La base FEI :

Base de données Brésilienne de Visage, elle contient un ensemble d'images de visage prises entre juin 2005 et mars 2006 au laboratoire d'intelligence artificielle de FEI où Brésil. Il y a 14 images pour chacun de 200 individus, un total de 2800 images, Le nombre de sujets masculins et femelles sont exactement identique et égalent à 100. Tous les visages sont principalement représentés par les étudiants et le personnel à FEI, entre 19 et 40 ans, et les images sont colorées et prises sur blanc homogènes un fond en position frontale droite avec la rotation de profil de jusqu' à environ 180 degrés, chaque image est de taille 640x480 pixels. La (Figure IV.17) montre quelques exemples des variations d'image de la base de données de visage de FEI. [FEB]



Figure IV.17. Exemple de visage enregistré dans la base FEI. [FEB]

Base de données	Nombre de personnes	Pose	Illumination	Facial expression	Données 3D
AR	116	1	4	4	Non
BANCA	208	1	++	1	Non
CAS-PEAL	66-1040	1	9-15	6	Non
CMU Hyper	54	1	4	1	Non
CMU PIE	68	3	43	3	Non
Equinox IR	91	1	3	3	Non
FEI	100	4	2	2	Non
FERET	1199	9-20	2	2	Non
Havard RL	10	1	77-84	1	Non
KFDB	1000	7	16	5	Non
MIT	15	3	3	1	Non
MPI	200	3	3	1	Oui
NDHID	300	1	3	2	Oui
NIST MID	1573	2	1	--	Non
ORL	10	1	--	--	Non
UMIST	20	-	1	--	Non
U.Texas	284	--	1	--	Non
U.Oulu	215	1	16	1	Non
XM2VTS	295	--	1	--	Oui
Yale	15	1	3	6	Non
Yale B	10	9	64	1	Non

Tableau IV.1. Principales caractéristiques des bases de visages. [SA, 2008]

IV.5. Conclusion :

Dans ce chapitre, nous avons présenté quelques Base de données d'images faites par des labos de recherches, nous avons expliqué aussi l'approche géométrique (symétrique) afin de réaliser un système de détection et de reconnaissance faciale efficace qui utilise une base de données des images standardisée (FEI) et dont la conception détaillée sera présenté dans le chapitre suivant.

CHAPITRE V

Conception

V.1. Introduction :

Après avoir passé en revue quelques généralités sur la biométrie puis énuméré un certain nombre de techniques et d'approches tant globales que locales sur la reconnaissance de visages humains, ainsi l'approche que nous avons proposé. Ce chapitre traite de notre conception que nous avons faite tout en exploitant les outils et les méthodes de conception informatiques adéquats à notre type d'application. Pour cela, nous avons utilisé le diagramme de flots de données comme modèle de conception.

V.2. Architecture générale du système proposé :

Généralement, un système biométrique s'appuie sur les étapes suivantes :

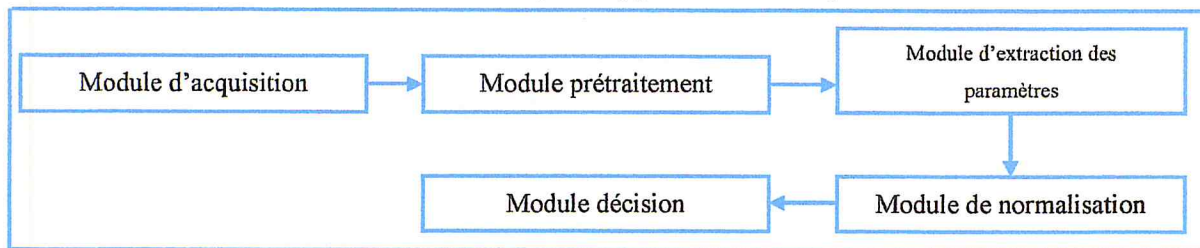


Figure V.1. Architecture du système.

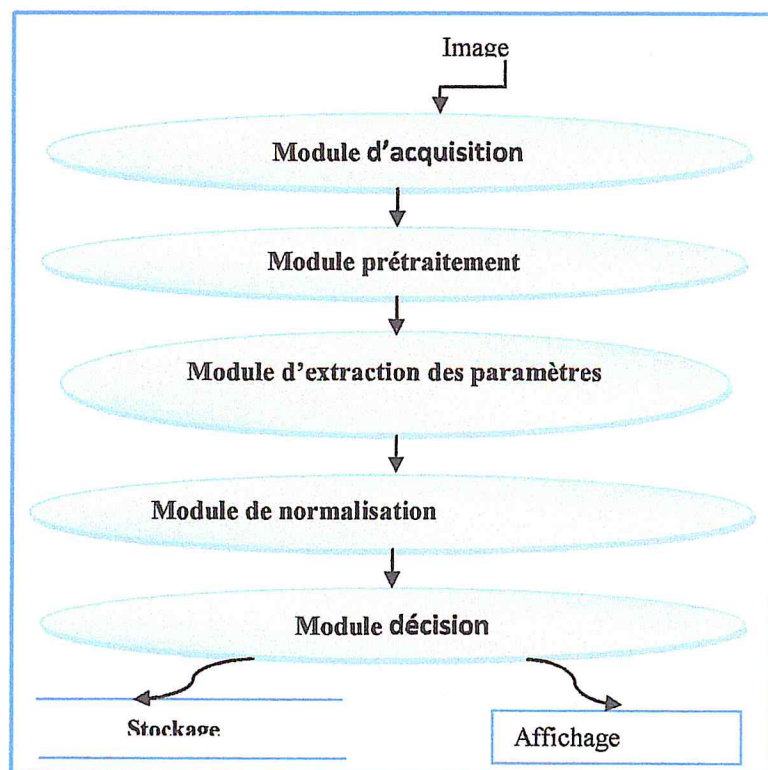


Figure V.2. Diagramme de flow de données principale.

Dans ce qui suit, nous allons détailler ces différents modules :

V.2.1. Module d'acquisition :

Ce module consiste d'un chargement d'image à partir d'une base d'images, et extraction dans une image acquise.

V.2.2. Module de Prétraitement :

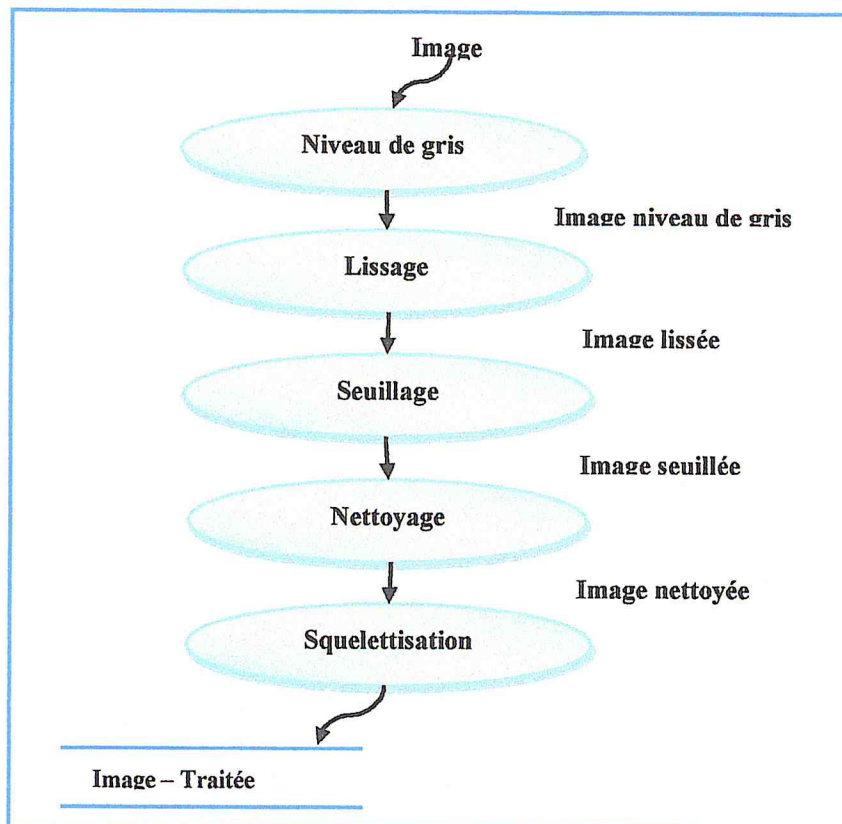


Figure V.3. Diagramme de flow de données de prétraitement.

L'image acquise dans l'étape précédente ne peut pas être exploitée dans son état brut à cause du bruit (effet de luminance et du background) qui influe négativement sur les performances du système ce qui nécessite des prétraitements bien définis en utilisant cinq types de filtres.

V.2.2.1. Passage aux niveaux de gris :

Comme tout autre système, le notre utilise la transformation en niveaux de gris qui est donnée par la formule générale suivante :

$$\text{Gris } [i, j] = (\text{R } [i, j] + \text{G } [i, j] + \text{B } [i, j])/3.$$

Cette transformation qui converti une image couleur en niveau de gris pourrait être le calcul de la moyenne des 3 composantes RGB et l'utilisation de cette valeur moyenne pour chacune des composantes.

REMARQUE : Nous avons préféré le passage aux niveaux de gris dans notre cas parce que notre approche ne se base pas sur la couleur, et par conséquent la taille de l'image sera réduite parce qu'on codifie une seul couleur des RGB.

Algorithme Niveaudegris ()

Données : I : image

Début

Pour i = 1 **jusqu'à** Largeur image **faire**

Pour j = 1 **jusqu'à** Hauteur image **faire**

$Img_NVG [i, j] := (I [i, j, R] + I [i, j, G] + I [i, j, B]) / 3;$

FinPour

FinPour

Fin.

V.2.2.2. Lissage :

Le lissage est une opération fondamentale en traitement d'images, elle vise à atténuer ou supprimer les petits détails dans une image. Le masque utilisé c'est un masque 5×5 :

$$H = \begin{bmatrix} 1 & 4 & 6 & 4 & 1 \\ 4 & 16 & 24 & 16 & 4 \\ 6 & 24 & 36 & 24 & 6 \\ 4 & 16 & 24 & 16 & 4 \\ 1 & 4 & 6 & 4 & 1 \end{bmatrix}$$

Algorithme Lissage

Données : I : Img_NVG.

Début

Pour i = 1 jusqu'à Largeur image faire

Pour j = 1 jusqu'à Hauteur image faire

R=0 ;

Pour L = -2 jusqu'à 2 faire

Pour K = -2 jusqu'à 2 faire

$R = R + \text{Img_NVG}[I + K, j + L] * h[K+3, L+3];$

FinPour

FinPour

$\text{Img_Liss}[i, j] = R/256;$

FinPour

FinPour

Fin.

V.2.2.3. Seuillage :

L'opération de seuillage consiste à mettre à zéro (0) tous les pixels ayant un niveau de gris inférieur à une certaine valeur (Seuil) et à la valeur « un » (1) si le pixel ayant un niveau de gris supérieur ou égal à ce seuil.

Le seuil est donné par la formule suivante :

$\text{Seuil} = I[i-1, j-1] + I[i-1, j] + I[i-1, j+1] + I[i, j-1] + I[i, j+1] + I[i+1, j-1] + I[i+1, j] + I[i+1, j+1].$

$[i-1, j-1]$	$[i-1, j]$	$[i-1, j+1]$
$[i, j-1]$	$[i, j]$	$[i, j+1]$
$[i+1, j-1]$	$[i+1, j]$	$[i+1, j+1]$

Tableau V.1. Voisinage d'un pixel $[i, j]$.

Algorithme Seuillage

Données : I : Img_Liss;

Début

Pour i = 1 jusqu'à Largeur image faire

Pour j = 1 jusqu'à Hauteur image faire

Seuil = I [i-1, j-1] + I [i-1, j] + I [i-1, j+1] + I [i, j-1] + I [i, j+1] + I [i+1, j-1] + I [i+1, j] + I [i+1, j+1].

Si Img_Liss < Seuil / 8 alors

Img_SLG [i, j] := 0

Sinon

Img_SLG [i, j] := 1;

FinSi

FinPour

FinPour

Fin.

V.2.2.4. Nettoyage:

L'opération nettoyage sert à éliminer les points noirs isolés qui n'appartiennent pas aux zones prédéfinies.

Algorithme Nettoyage

Donnée : I : image_seuil

Debut

Pour it=1 jusqu'à Nb_iteration faire

Pour i=1 jusqu'à Longueurimage faire

Pour j=1 jusqu'à Hauteurimage faire

Si I[i,j]=0 alors

$r = \sum_{i=8}^i \text{voisin} / 255$


```
    Si r>4 alors
         $\theta[i,j]= 255$ 
    Sinon
         $\theta[i,j]= 0$ 
    Fin si
Sinon
     $\theta[i,j]= 255$ 
Fin si
Fin pour
Fin pour
I=  $\theta$ 
Pour i=1 jusqu'à Langueurimage faire
    Pour j=1 jusqu'à Hauteurimage faire
        Si  $\theta[i,j]= 255$  alors
             $r = \sum_{i=8}^i \text{voisin}/255$ 
            Si r<3 alors
                I [i,j]=0
            Sinon
                I [i,j]=255
            Fin si
        Sinon I[i,j]=0
    Fin si
Fin pour
Fin pour
Image_net = m
```

V.2.2.5. Squelettisation :

L'objectif de la squelettisation est de représenter une image binaire avec un ensemble minimum de pixels. Le squelette doit rendre compte des propriétés géométriques de la forme et conserver les relations de connexité.

Algorithme Squelettisation

Données : I : image_Nett

Debut

Pour it=1 jusqu'à itération faire

Pour i=1 jusqu'à Largeurimage faire

Pour j=1 jusqu'à Hauteurimage faire

Si I[i,j]=0 alors

r=0

Si I[i-1,j-1]=0 alors

r=r+1

Si I[i-1,j]=0 alors

r=r+2

Si I[i-1,j+1]=0 alors

r=r+4

Si I[i-1,j+1]=0 alors

r=r+8

Si I[i-1,j+1]=0 alors

r=r+16

Si I[i-1,j+1]=0 alors

r=r+32

Si I[i-1,j+1]=0 alors

r=r+64

Si I[i,j-1]=0 alors

r=r+128;

Si (r=3) or (r=6) or (r=12) or (r=24) or (r=48) or (r=96) or (r=192) or (r=129)

alors

$\theta[i,j] = 255$

Sinon

$\theta[i,j] = 0$

Fin si

Sinon

$\theta[i,j] = 255$

Fin si

Fin pour

Fin pour

Fin pour

Image_sqtl = θ

V.2.3. Module d'extraction des paramètres :

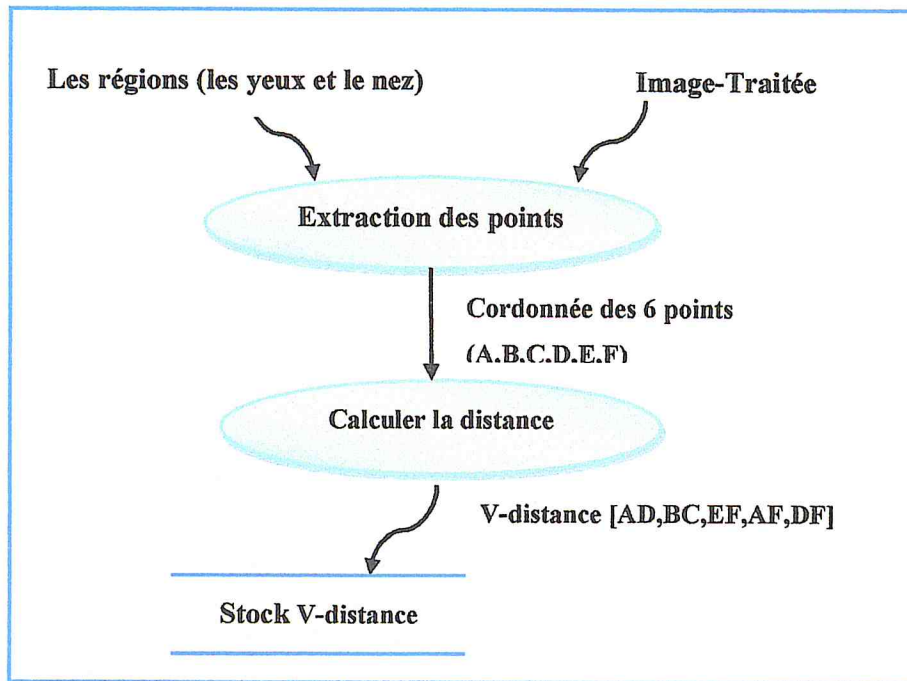


Figure V.4. Diagramme de flow de données d'extraction des paramètres

Algorithme extraction des points

Données : Image-sqlt , NB de point, region des yeux , region du nez .

Debut

Pour k=1 jusqu'à NB de pont faire

Pour i=1 jusqu'à Largeur Image faire

Pour j=1 jusqu'à Hauteur Image faire

Si $I(i,j) \in \text{region}$ alors

Ipoint= i

Jpoint=j

Fin si

Fin pour

Fin pour

Fin pour

$AD = \text{SQRT}((iA - iD)^2 + (jA - jD)^2)$

$BC = \text{SQRT}((iB - iC)^2 + (jB - jC)^2)$

$EF = \text{SQRT}((iE - iF)^2 + (jE - jF)^2)$

$AF = \text{SQRT}((iA - iF)^2 + (jA - jF)^2)$

$DF = \text{SQRT}((iD - iF)^2 + (jD - jF)^2)$

Fin

V.2.4. Module de normalisation :

Pour que les étapes de comparaison qui suivent le processus d'identification soient efficaces et pertinentes, il est nécessaire que les données soient normalisées. Il s'agit là d'une étape classique d'un processus de classification. La normalisation permet d'assurer l'homogénéité des données.

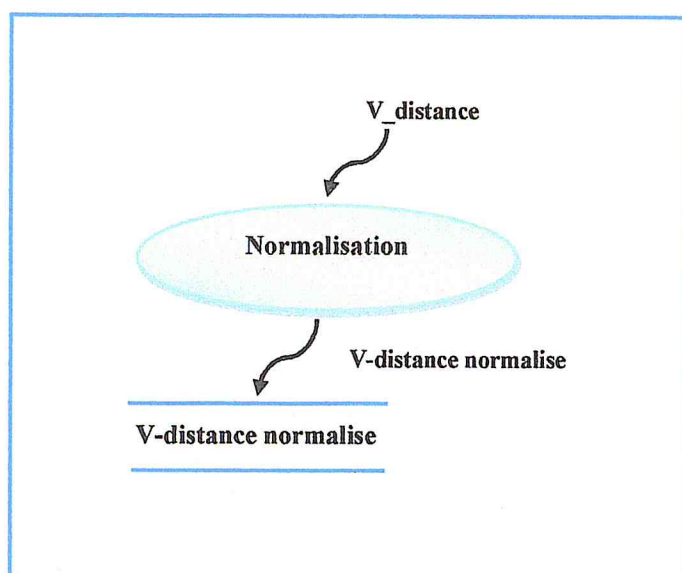


Figure V.5. Diagramme de flow de données de normalisation.

Algorithme Calcul des distances

Données : coordonnées des 6 points A B C D E F.

Debut

Somme = $\text{SQRT}((AD)^2 + (BC)^2 + (EF)^2 + (AF)^2 + (DF)^2)$.

AD_Norm = AD / Somme.

BC_Norm = BC / Somme.

EF_Norm = EF / Somme.

AF_Norm = AF / Somme.

DF_Norm = DF / Somme.

V = [AD, BC, EF, AF, DF].

Fin

V.2.5. Module décision :

Pour prendre une décision finale (visage connu ou non connu), nous avons utilisé l'algorithme des K plus proches voisin (Kppv). La distance utilisée est celle de la somme des valeurs absolues appelée aussi distance de Minkowski de degré 1 ou distance City-Block car elle nécessite moins de calculs.

Avec la méthode des Kppv, nous calculons la distance entre le vecteur caractéristique de la personne à identifier et chaque vecteur des personnes dans la base de données

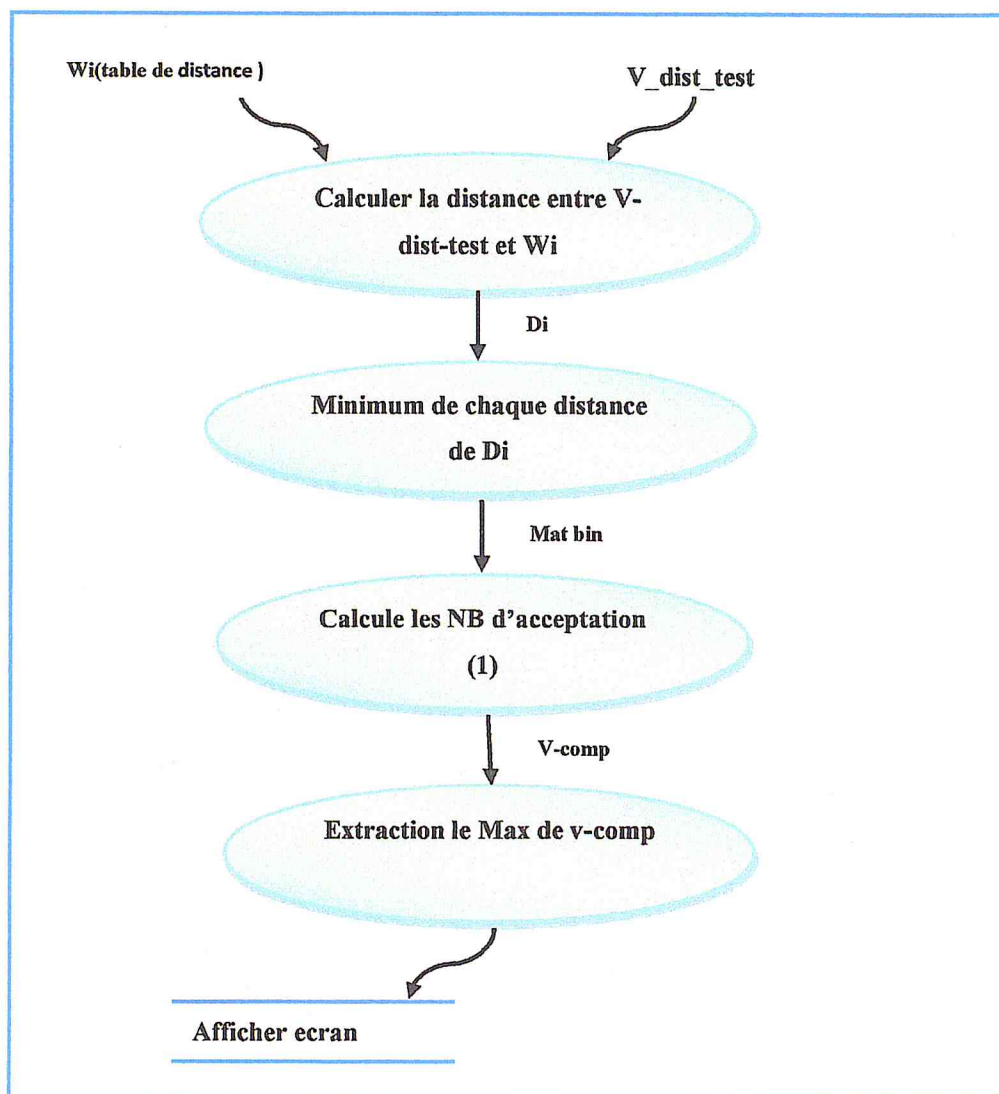


Figure V.6. Diagramme de flow de données de décision.

Algorithme decision

Debut : Vect-Test : vecteur // vecteur caractéristique de l'individu test

E= {Wi} // Vecteur des candidates à identification

N = entier // NB de personne dans la base.

Variable : D : tableau des distances.

Sortie : le visage le plus proche

Debut

Pour i=1 jusqu'à N **faire**

 Calcule les distances Di entre Vect-Test et Wi

Fin pour

Pour i=1 jusqu'à 5 **faire**

Pour j=1 jusqu'à N **faire**

 K=1

Tantque (k<= N-1) **faire**

Si D [i, j] > D [i, k] **alors**

 Mat Bin [i, j] = 0

 K=N.

Else

 Mat Bin [i,j]=1.

Fin si

 K=k+1

Fin tanque.

Fin pour

Fin pour

Pour i=1 jusqu'à 5 **faire**

Pour j=1 jusqu'à N **faire**

Si Mat Bin [i,j] =1 **alors**

 V_Comp[j] = V_comp[j]+1.

Fin pour

Fin pour

X=0

Extraction du Maximum de V_Comp

X=X+1

Si X=1 **alors**

 Individu connu

Si non

 Trouver la plus petit distance qui correspondant à l'individu le plus proche parmi les X distance.

Fin si

Fin

V.3. Conclusion :

Nous avons abordé dans ce chapitre le passage par une étape de conception afin de bien définir, détailler et situer le problème à résoudre ce qui va engendrer un logiciel efficace et fiable dont le détail d'implémentation est présenté dans le chapitre suivant.

CHAPITRE VI

Implémentation

VI.1. Introduction :

Dans ce chapitre nous présentons les outils utilisés pour mettre en œuvre notre système de reconnaissance faciale tout en exploitant la conception décrite dans le chapitre précédent et les interfaces de notre application.

VI.2. Outils d'implémentation :

Notre application se base sur la solution Borland en ce qui concerne l'environnement de développement intégré (EDI) DELPHI7 à cause de sa richesse en composants et sa souplesse ainsi que la facilité de la tâche de programmation.

VI.2.1. Le langage de développement :

Delphi désigne à la fois un environnement de développement intégré et un langage de programmation orienté objet.

En 2001, Borland édita une version l'Unix de DELPHI appelé Kylix, qui ne connut pas le succès attendu par l'éditeur.

Comme il s'agit d'un outil RAD (Rapid Application Developpent), DELPHI est très simple à prendre en main et il est tout à fait aisé de crée toutes sortes d'applications.

Actuellement, DELPHI reste l'un des outils les plus utilisés avec la possibilité de produire des programmes Win32 ou .NET à partir du même langage et de la même bibliothèque de composants.

VI.2.2. Pour quoi choisir DELPHI ? :

- Amélioration de l'interface utilisateur.
- Intégration totale à l'environnement Windows.
- Réutilisation et communication avec d'autre programmes Windows.
- Programmer proprement par événement et par exception.
- Il possède un éditeur de texte très riche en fonctionnalités telles que : la coloration syntaxique, l'indentation.

VI.2.3. Matériel utilisé :

Un Micro-ordinateur :

- Processeur : Intel ® Core™ 2 Duo CPU.
- Mémoire RAM : 4Go
- Carte graphique : 32 bits

VI.3. Déroulement d'une session de travail :

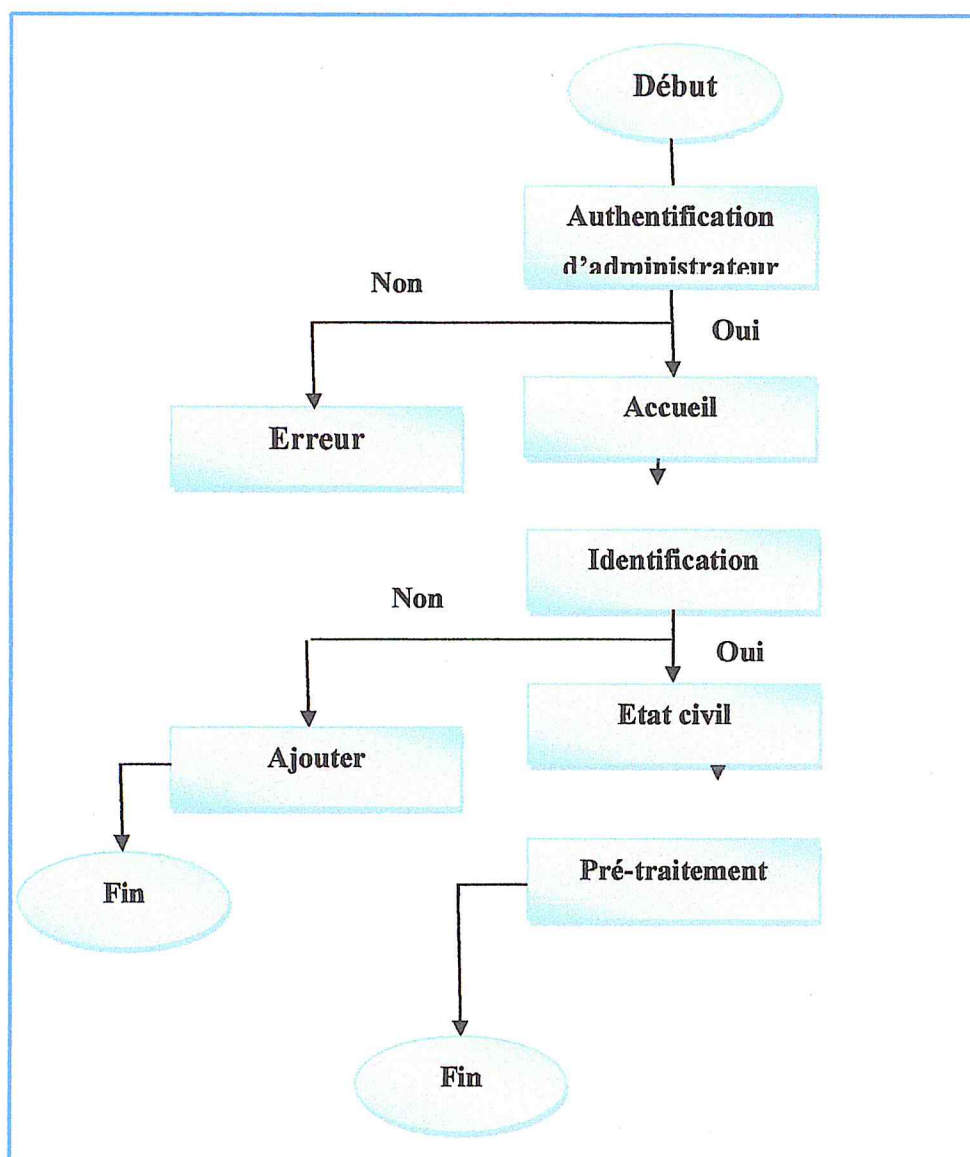


Figure VI.1. Déroulement d'une session de travail.

VI.4. Description des IHM de notre système :

Après avoir lancé l'application, une fenêtre d'accueil s'affichera (Figure VI.2), à partir de cette fenêtre l'utilisateur doit s'authentifier afin de lancer le système de reconnaissance.

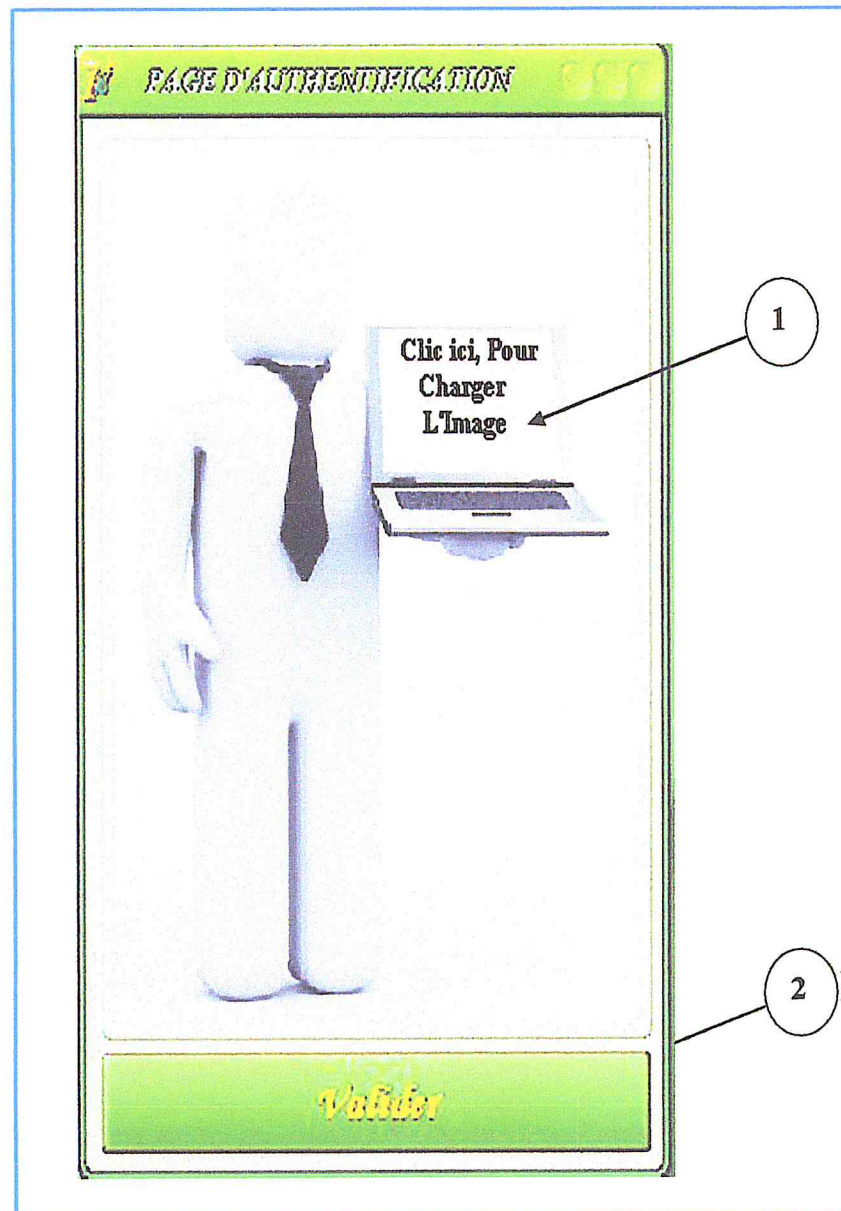


Figure VI.2. Page d'authentification de l'administrateur.

L'administrateur doit charger sa propre image qui représente le mot de passe et terminer cette opération par la validation de l'image en cliquant sur le bouton « valider ». Deux cas sont possibles :

- Soit l'authentification est incorrecte dans ce cas un message d'erreur s'affichera (Figure VI.3),
- Soit l'authentification est correcte alors une fenêtre « ACCUEIL ADMINISTRATEUR » s'affichera à l'écran. (Figure VI.4).



Figure VI.3. Fenêtre d'erreur.

A partir de la fenêtre d'accueil d'administrateur, l'administrateur aura la possibilité de visionner un visage, d'ajouter, de supprimer, et même de consulter les détails d'un individu enregistré.

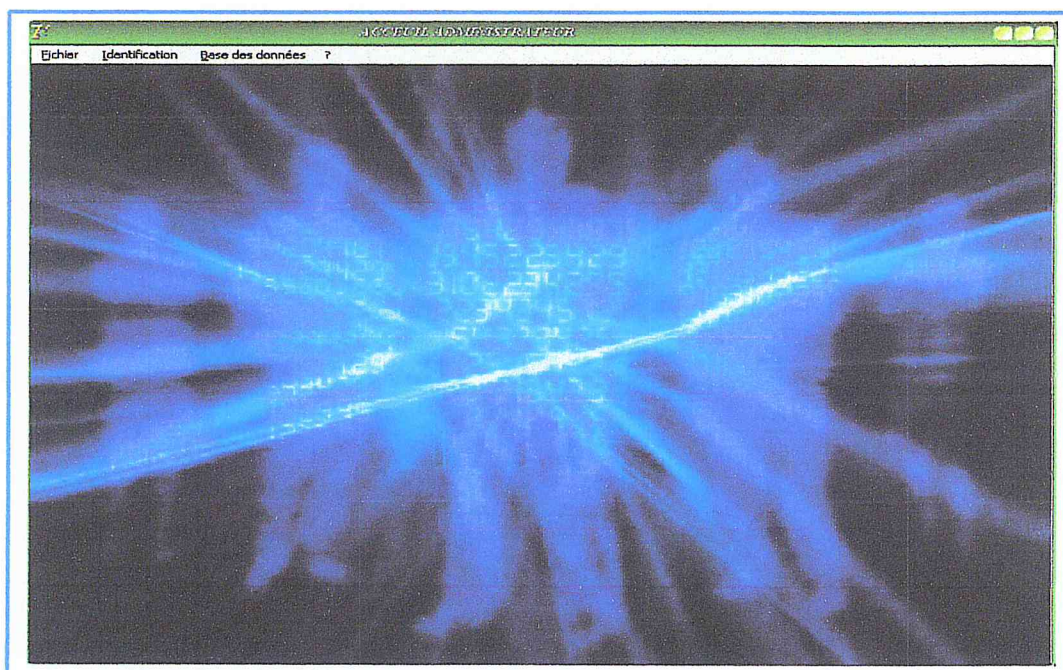


Figure VI.4. Fenêtre d'accueil d'administrateur.

La procédure à suivre pour identifier un individu se résume au chargement du fichier contenant le visage (4) puis faire cliquer sur le bouton « IDENTIFICATION » ce qui actionnera l'exécution du programme d'identification (5).

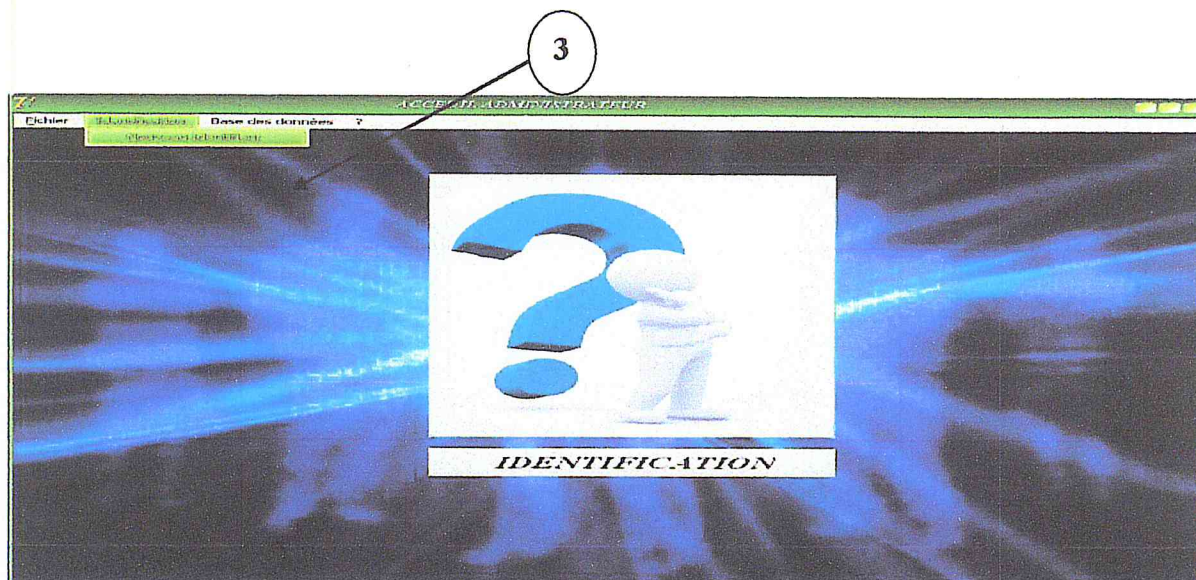


Figure VI.5. Opération d'identification d'un nouvel individu.

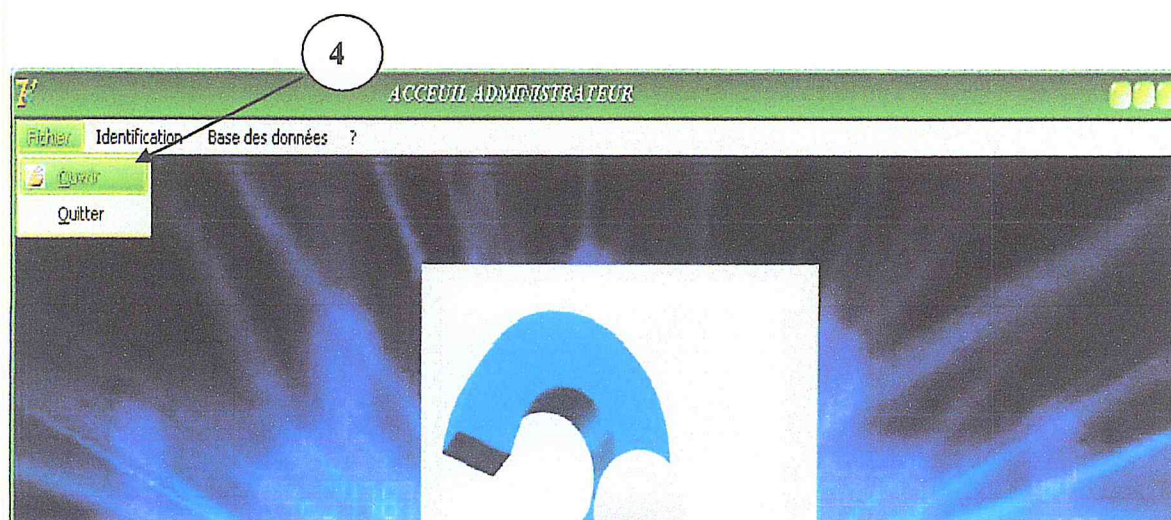


Figure VI.6. Fenêtre Ouvrir une image du visage.

Pour identifier un visage la procédure à suivre est de choisir et charger un visage (Figure VI.6) afin de lancer l'identification (Figure VI.7).

Deux cas sont possibles :

1. Soit le visage est reconnu alors une fenêtre « Etat Civil » s'affichera (Figure VI.8).
2. Soit le visage est inconnu alors une fenêtre « Ajouter » s'affichera (Figure VI.9).

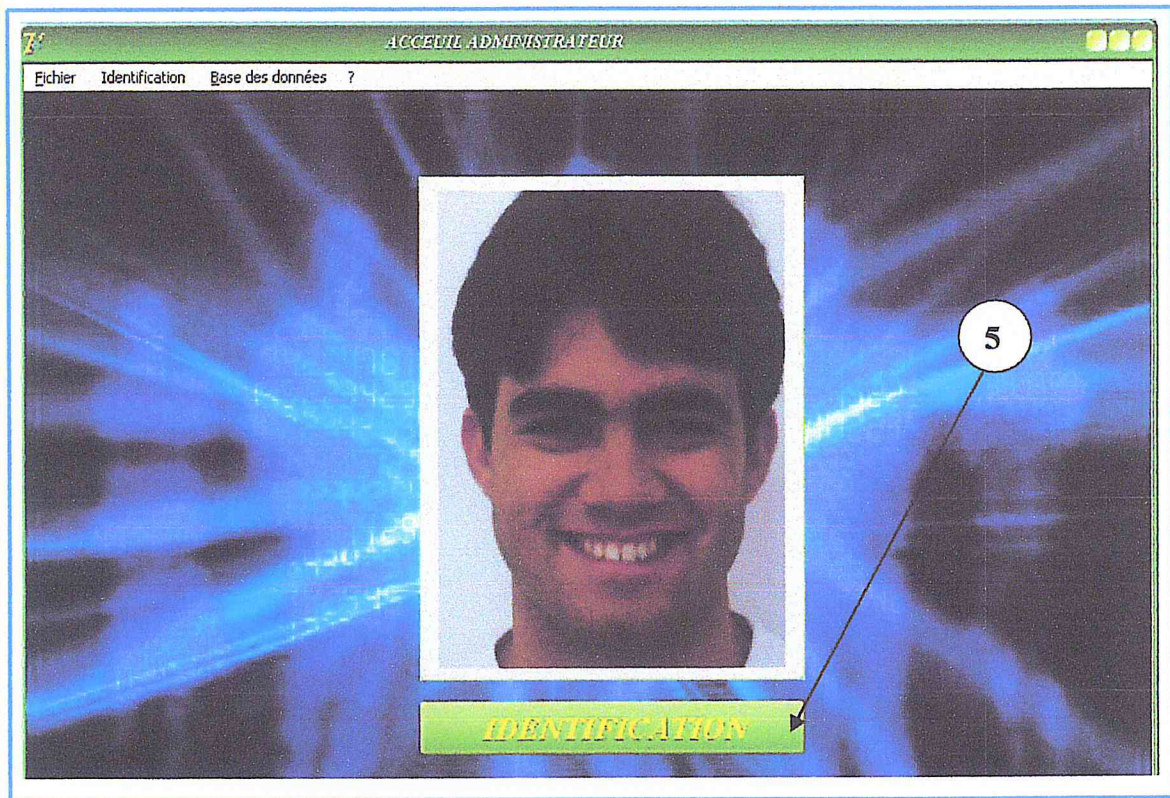


Figure VI.7. Lancer l'identification

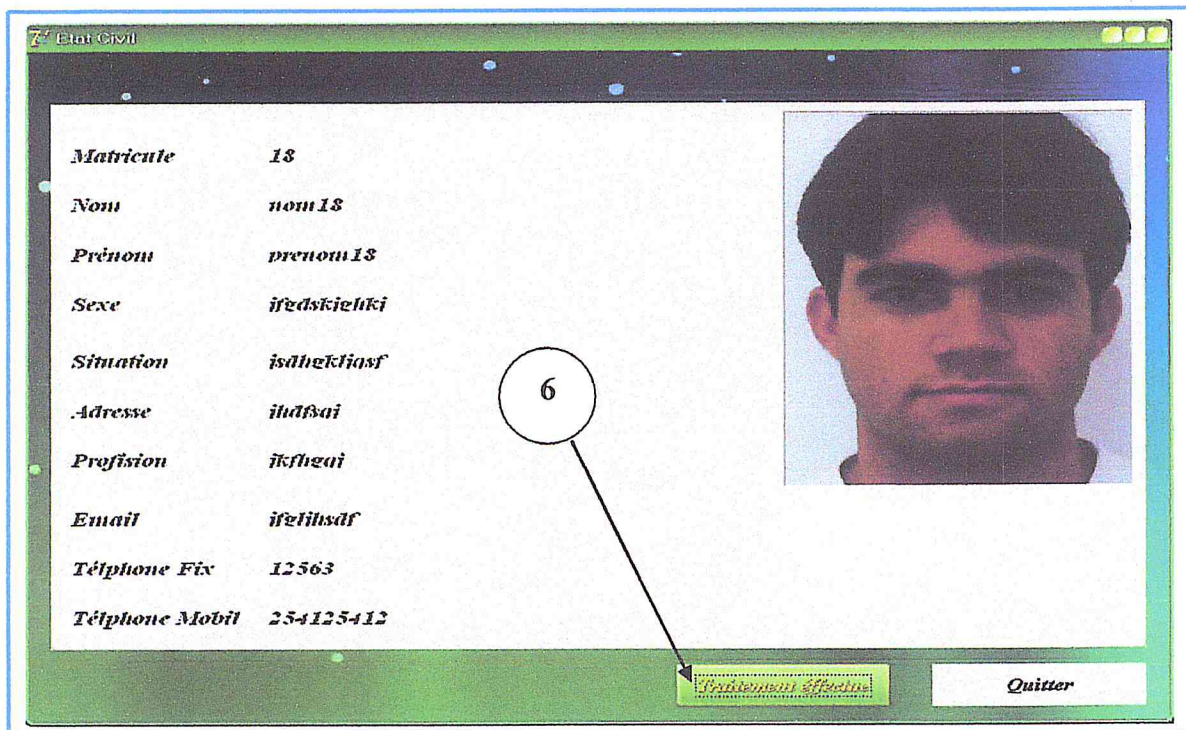


Figure VI.8. Fenêtre d'état civil de l'individu

The screenshot shows a window titled "Nouvel individu" with a form for entering personal information. The fields are: Matricule, Nom, Prénom, Sexe, Situation, Adresse, Profession, Email, Téléphone Fix, and Téléphone Mobil. To the right is a photo of a man. Below the photo are fields for Code (containing '7'), Dist_EF, Dist_AF, Dist_BC, and Dist_DF. At the bottom are buttons for "Enregistrer" and "Annuler".

Figure VI.9. Nouvel individu

La figure suivante représente l'enchaînement des étapes constituant le prétraitement appliqué sur l'image chargée précédemment.

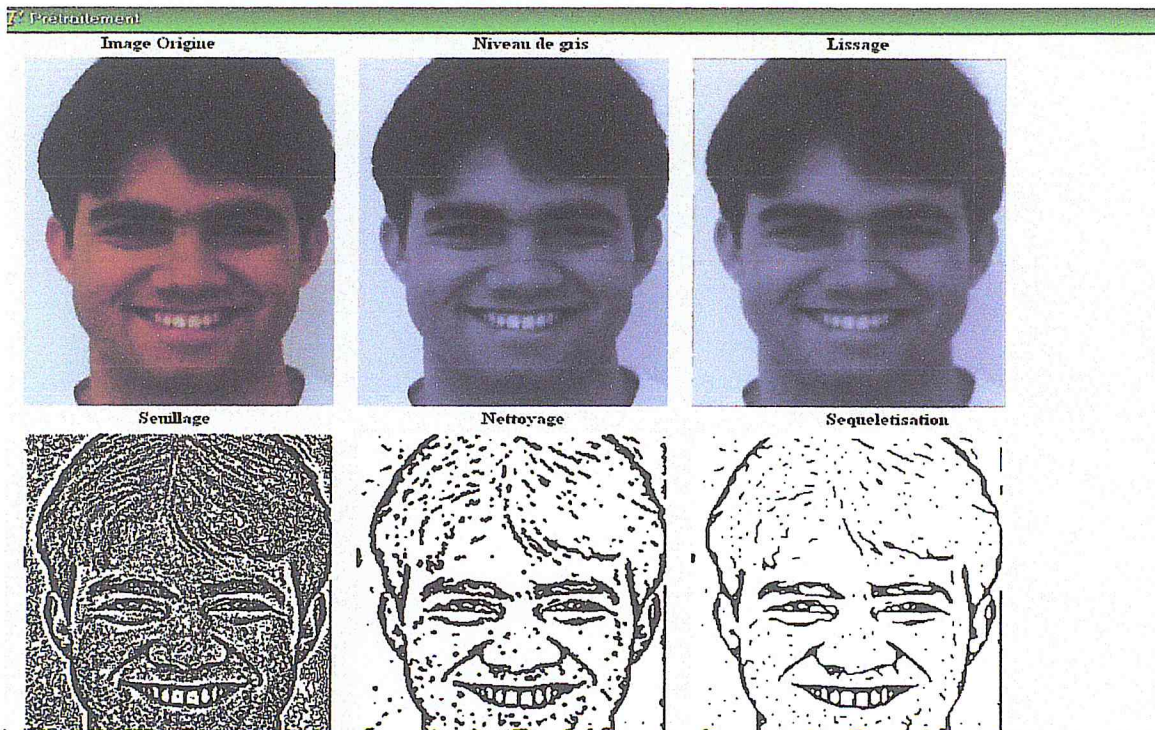


Figure VI.10. Fenêtre du traitement effectuée sur le visage identifié.

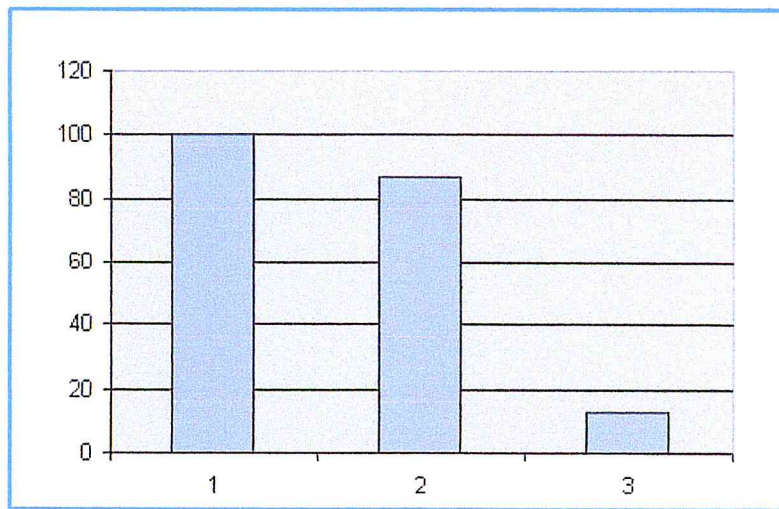


Figure VI.11. Graphe de reconnaissance et taux d'erreurs.

1. la base 2. Taux d'acceptation = 87% 3. Taux d'erreur = 13%

- 1 Charger l'image du visage.
- 2 Valider ou non l'entre à l'accueil d'administrateur.
- 3 Nouveau identifié
- 4 Chargement l'image du visage
- 5 Lancer l'identification.
- 6 Les traitements effectués sur le visage
- 7 Valider l'enregistrement d'un nouvel individu.

VI 5. Conclusion :

Dans ce chapitre, en exploitant les différents diagrammes vus dans l'étape de conception, on a abouti à réaliser une application d'identification de personnes à travers la reconnaissance de visages tout en visualisant quelques captures d'écran des interfaces réalisées tout au long du processus de développement.

CONCLUSION
GÉNÉRALE
ET
PERSPECTIVE

Conclusion générale

Notre but était de concevoir un système d'identification qui soit facile et peu coûteux dans l'implémentation et qui utilise une modalité biométrique particulière (le visage humain). Le visage est l'une des formes les plus domestiques et qui est très bien acceptée par les utilisateurs. Car elle est non invasive. La tâche est simple ; l'image du visage est captée par une caméra. Le sujet peut se présenter devant celle-ci et selon la technique utilisée, le système extrait les caractéristiques du visage pour faire la comparaison avec des données préexistantes dans la base de données du système.

La mise en œuvre de notre application a nécessité de mener une démarche méthodologique allant de la collecte d'informations sur le sujet à la détermination des points nécessaires à la formalisation et à la spécification du cahier de charges de notre application prenant en considération le temps imparti ainsi que les ressources pour sa mise en œuvre. La cinquième étape de notre travail a consisté à concevoir notre travail. Enfin, vient l'étape d'implémentation du logiciel, à son test et à sa validation.

Tout ceci nous a permis de concrétiser un ensemble de connaissances, jusque là théoriques et à consolider un ensemble d'acquis lors de notre scolarité universitaire.

Le travail est loin d'être terminé et nous souhaitons qu'il soit poursuivi dans le futur en insistant sur les points suivants :

- Identification des personnes dans un environnement non contrôlé.
- Système de reconnaissance faciale en 3D.
- Œil bionique.

BIBLIOGRAPHIE

BIBLIOGRAPHIE

- [LH, 2009] LALLALI SALIHA, HAMACHE LILA : Conception et réalisation d'une authentification par Finger Hashing sur carte à puce (ESI, oued-smar Alger, 2008 / 2009).
- [SA, 2008] SOUHILA GUERFI ABABSA : authentification d'individus par reconnaissance de caractéristiques biométriques liées aux visages 2D / 3D (Université Evry Val d'Essonne, 3 octobre 2008).
- [NZ, 2009] NASSIM HAMITOUCHE, ZAKARIA SALMI : Système d'identification biométrique de personne par reconnaissance de l'iris (ESI, oued-smar Alger, 2008/ 2009).
- [FV, 2007] FRANÇOIS VO CONG TRI : Application de la biométrie dans la sécurité informatique (Examen probatoire du cycle ingénieur C.N.A.M en informatique, 6 Juillet 2007).
- [TCA] Techniques de contrôle d'accès par biométrie (Commission techniques de sécurité physique- Club de la sécurité des systèmes d'information Français).
- [MB, 2007] MELLAL TOUFIK, BENAKLI KAMEL: Système de reconnaissance de visage basé sur les GMM (INI, oued-smar Alger, 2006/ 2007).
- [AA, 2005] ALKHATIB MOHAMED ABAN : le rôle de l'anthropologie dans les techniques émergentes de reconnaissance faciale (Université clande bernard-Lyon 1, 15 Septembre 2005).
- [LK, 2010] LAIEB MOUNA, KHALFAOUI SOUMAYA : Détection et reconnaissance de visage dans un système de vidéosurveillance (Université 20 Août 1955, skikda, département d'informatique.), 2009/2010.
- [FEB] <http://fei.edu.br/~cet/facedatabase.html>
- [SS, 2008] SLIME Samir, Environnement de segmentation d'image à base d'une approche biométrique (ESI, oued-smar Alger, 2007/2008).
- [MN, 2009] MORIZET Nicolas. Reconnaissance Biométrique par Fusion Multimodale du Visage et de l'Iris. École Doctorale d'Informatique Télécommunications et Électronique de Paris, 18 Mars 2009.
- [GO, 1961] G .Olivier. « Morphologie et types humains »; Vigot Frères, 1961, 171 pages.
- [GR, 1998] G. Roethenbaugh « An Introduction to Biometrics and General History »; Biometrics Explained, Section 1; 1998.
- [PJ, 2006] Pascal JOYEUX. La biométrie et ses différentes techniques. Centre de Lyon – Rhône-Alpes. 28 November 2006.
- [FM] Frédéric MASSICOTTE. La biométrie, sa fiabilité et ses impacts sur la pratique de la Démocratie Libérale. Université du QUÉBEC À MONTRÉAL.

BIBLIOGRAPHIE

- [BB, 2011] BALOUL Mossâb, BOULEKNAFET Zinelabidine. Intégration des mesures de qualité dans les systèmes d'authentification biométriques application pour la vérification du locuteur et du visage. Ecole Nationale d'Informatique, 2011.
- [SA, 2010] min projet Saliha Artabaz « biométrie multimodale » école doctorale Institut
- [LF, 2005] Liméry Lionel, Fao Frédéric, Guiraud Ludovic « reconnaissance des empreintes digitale serrure biométrique »2005.
- [SI] Securiteinfo.com « Le Grand Livre de Securiteinfo.com » ; tous droits réservés (c) 2002-2004; site web: <http://www.securiteinfo.com>.
- [ZX, 2006] Zhifeng Li ET Xiaou Tang « EIGENFACE RECOGNITION USING DIFFERENT TRAININGDATA SIZES » 2006.
- [DJ,2008] Daugman John « Iris Recognition Handbook of Biometrics S.1 Spring » 2008.
- [TK, 2007] Toufik AMELLAL, Kamel BENAKLI, « Système de reconnaissance de visage basé sur les GMM ». Institut National de formation en Informatique (I.N.I), Alger, 2007
- [EM, 2008] ELHADDAD MOHAMED et BENAMAR MOHAMED « 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.
- [BM] Biometrie-online.Net [en ligne]. <http://www.biometrie-online.net/>
- [DV, 2005] DANG Hoang vu, Biométrie pour l'identification. Institut de la Francophonie pour l'Informatique, Juillet 2005, 31p.
- [TK, 1973] T. Kanade. 'Picture Processing System by Computer Complex and Recognition of Human Faces'. In: Doctoral dissertation, Kyoto University, November 1973
- [SPR, 2006] S. Arca, P. Campadelli, and R. Lanzarotti. "A Face Recognition System Based On Automatically Determined Facial Fiducial Points". Pattern Recognition, Vol. 39, No. 3, pp. 432-443, 2006.
- [YYS, 1997] Y. Adini, Y. Moses, S. Ullman, Face recognition: The problem of compensating for changes in illumination direction. IEEE Trans. Patt. Anal. Mach. Intel. 19, 721-732, 1997.
- [DMP, 2001] D. Blackburn, M. Bone, P. J Phillips. "Face recognition vendor test 2000". Tech. rep. <http://www.frvt.org>, 2001
- [PPR, 2003] P. J. Phillips, P. J.Grother, R. J.Micheals, D. M. Blackbrun, E. Tabassi, and J. M. Bone. Face recognition vendor test 2002: Evaluation report. NISTIR 6965. Available online at <http://www.frvt.org>, 2003.

BIBLIOGRAPHIE

- [RJJ, 2001] R. Gross, J. Shi, J. Cohn. Quo Vadis FaceRecognition?. Third Workshop on Empirical Evaluation Methods in Computer Vision, December,2001.
- [BS, 2014] BETTAHAR Abdessettar ET SABER Fathi. 'Extraction des caractéristiques pour l'analyse biométrique d'un visage'. UNIVERSITE KASDI MERBAH OUARGLA, 2014.
- [PHJ, 1998] P. J. Phillips, H. Wechsler, J. Huang, and P. Rauss. The FERET database and evaluation procedure for face-recognition algorithms. *Image Vis. Comput.* 16, 295–306, 1998
- [SPH, 1998] S. A. Rizvi, P. J. Phillips, H.A. Moon. Verification protocol and statistical performance analysis for face recognition algorithms. In *Proceedings, IEEE Conference on Computer Vision and Pattern Recognition.* 833–838, 1998
- [KJJ, 1999] K. Messer, J. Matas, J. Kittler, J. Luetin, and G. Maitre. XM2VTSDB: The Extended M2VTS Database. In *Proceedings, International Conference on Audio- and Video-Based Person Authentication.* 72–77, 1999
- [SJD, 2007] S. Prabhakar, J. Kittler, D. Maltoni, L. O’Gorman, and T. Tan. Introduction to the Special Issue on Biometrics: Progress and Directions, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 29, n°4/4/ 2007
- [VB, 1988] V. Bruce. *Recognizing faces.* Lawrence Erlbaum Associates, London, U.K, 1988.
- [JGH, 1981] J.W. Shepherd, G.M. Davies, H.D. Ellis, *Studies of cue saliency*, in: G.M. Davies, H.D. Ellis, J.W. Shepherd (Eds.), *Perceiving and Remembering faces*, Academic Press, London, UK, 1981
- [OM, 2009] OUAFEK Redouane ,MEGHALSI Mohamed Reda. 'La détection des visages dans une image'. Ecole nationale Supérieure en Informatique (E.S.I) Oued-Semar, Alger, 2009
- [MA, 2009] MELLAKH Anouar. Reconnaissance des visages en conditions dégradées. l'Institut National de Télécommunications : l'université d'Evry-Val d'Essonne. 7 Avril 2009, 169p.
- [AB, 1983] ALPHONSE Bertillon. *Ethnographie moderne et les races sauvages.* 1883
- [HR, 2013] HACEB Rafik. Développement d'un système de reconnaissance du visage 3D. Ecole nationale Supérieure en Informatique (E.S.I) Oued-Semar, Alger. 2013.
- [Yan, 1994] G. Yang and T. S. Huang. "Human Face Detection in Complex Background," *Pattern Recognition*, vol. 27, no. 1, pp. 53-63, 1994.

BIBLIOGRAPHIE

- [Yan,2002] Ming-Hsuan Yang, David J. Kriegman et Narendra Ahuja. Detecting faces in images: A survey. Dans IEEE Transactions on Pattern Analysis and Machine Intelligence, volume 24(1), pages 34–58, 2002
- [Yui, 1992] 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.
- [Tur, 1991] M. Turk and A. Pentland. "Eigenfaces for Recognition," J. Cognitive Neuroscience, vol. 3, no. 1, pp. 71-86, 1991.
- [Yow, 1997] K.C. Yow and R. Cipolla, "Feature-Based Human Face Detection," Image and Vision Computing, vol. 15, no. 9, pp. 713-735, 1997
- [XK, 2004] X.G. Lu, D. Colbry, and A.K. Jain. Three-dimensional model based face recognition. In International Conference on Pattern Recognition, pages 362–366, Cambridge, UK, 2004
- [BF, 2004] BELLILI Manel, FARSI Meriem. Application de la DCT modifiée et GMM Orthogonale pour la Vérification du visage. . Ecole nationale Supérieure en Informatique (E.S.I) Oued-Semar, Alger. 2012.
- [MMG, 1997] M. Behrman, M. Moscovitch, G. Winocur. Facing the issue : New research shows that the brain process faces and objects in separate brain systems. Journal of Cognitive Neuroscience, 1997
- [XTV, 2006] X.Jiang, E. Rosen, T. Zeffiro, J. Vanmeter, V. Blanz, and M. Riesenhuber. Evaluation of a shape-based model of human face discrimination using fmri and behavioral techniqueq. Neuron, 50(1) : 159-72, April 2006.
- [KB, 2013] Kheffif Bouchra. Mise au point d'une application de reconnaissance faciale, Université Abou Bakr Belkaid –Tlemcen. 2013.
- [MC, 2002] Mohamed Tayeb Laskri, Djallel Chefrou. Who_Is : système d'identification des visages humains, Université Badji Mokhtar Annaba. 2002.
- [LR, 2007] L. Ralaivola. Projet informatique, 06 février 2007.
- [FRH] Face Recognition Home Page. <<http://www.face-rec.org/databases/>>.
- [PHR, 2000] P. J. Philips, H. Moon, S. A. Rizvi, P. J. Rauss, The FERET evaluation methodology for face-recognition algorithms, IEEE Trans. on Pattern Analysis and Machine Intelligence, vol.22, no.10, pp.1090-1100, 2000
- [DCF] Le site web de la base de données Color FERET, <http://www.nist.gov/humanid/colorferet>
- [AR, 1998] A.M. Martinez, R. Benavente, The AR face database, Technical Report 24, Computer Vision Center, Espagne, 1998

BIBLIOGRAPHIE

- [CVL] CVL Face Database, <http://www.lrv.fri.uni-lj.si/facedb.html>
- [GVL, 2007] G. B. Huang, V. Jain, and E. Learned-Miller. Unsupervised joint alignment of complex images. In ICCV, pages 1-8, 2007
- [LT, 2009] L. Wolf, T. Hassner, and Y. Taigman. Similarity scores based on background samples. In ACCV, 2009

ANNEXE

A.1. Généralité sur les traitements d'image :

La grande montée en puissance des ordinateurs, l'amélioration et la miniaturisation des systèmes d'acquisition d'images et la chute du coût des matériels électroniques ont récemment permis un formidable essor de l'utilisation de l'image numérique.

Une image est la représentation d'une scène acquise à l'aide de systèmes de production d'images (appareils photographique, caméra, radiographies, scanner, sonar,...). Sa forme peut être analogique (ex: négatif, photographie, vidéo..) ou numérique (images numérisées suivant divers formats (images compressées ou non...) ou obtenues par des capteurs fournissant des images numérisées) et dans ce cas un traitement par ordinateur est possible.

A.1.1. Image analogique:

Avec la parole, l'image constitue l'un des moyens les plus importants qu'utilise l'homme pour communiquer avec autrui. C'est un moyen de communication universel dont la richesse du contenu permet aux êtres humains de tout âge et de toute culture de se comprendre [SS, 2008].

A.1.2. La numérisation:

La numérisation d'une image analogique est la conversion de celle-ci de son état analogique (distribution continue d'intensités lumineuses), en une image numérique représentée par une matrice bidimensionnelle de valeurs numériques où :

- Cordonnées cartésiennes d'un point de l'image.
- niveau de gris en ce point.

A.1.3. Pixel «Picture Element»:

Une image numérique est constituée d'un ensemble de points appelés *pixels* (pixel est une abréviation de (*PICTure ELe ment*) Le pixel représente ainsi le plus petit élément constitutif d'une image numérique.

L'ensemble de ces pixels est contenu dans un tableau à deux dimensions constituant l'image [LH, 2009]. La lettre A, par exemple, peut être affichée comme un groupe de pixels dans la figure ci-dessous:

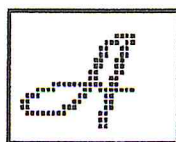


Figure A.1. Représentation de "A" par un groupe de pixels.

A.1.4. Image numérique:

Contrairement aux images obtenues à l'aide d'un appareil photo analogique, ou dessinées sur du papier, les images manipulées par un ordinateur sont numériques (représentées par une série de bits). L'image numérique est l'image dont la surface est divisée en éléments de tailles fixes appelés cellules ou pixels, ayant chacun comme caractéristique un niveau de gris ou de couleurs prélevé à l'emplacement correspondant dans l'image réelle, ou calculé à partir d'une description interne de la scène à représenter [SS, 2008].

A.1.4.1. Caractéristique d'une image numérique :

a) Niveau de gris:

Le niveau de gris est la valeur de l'intensité lumineuse en un point. La couleur du pixel peut prendre des valeurs allant du noir au blanc en passant par un nombre fini de niveaux intermédiaires. Le nombre de niveaux de gris dépend du nombre de bits utilisés pour décrire la " couleur " de chaque pixel de l'image. Plus ce nombre est important, plus les niveaux possibles sont nombreux.

b)Image en couleurs :

Même s'il est parfois utile de pouvoir représenter des images en noir et blanc, les applications multimédias utilisent le plus souvent des images en couleurs. La représentation des couleurs s'effectue de la même manière que les images monochromes (noir et blanc) avec cependant quelques particularités. En effet, il faut tout d'abord choisir un modèle de représentation. On peut représenter les couleurs à l'aide de leurs composantes primaires. Les systèmes émettant de la lumière (écrans d'ordinateurs,...) sont basés sur le principe de la synthèse additive : les couleurs sont composées d'un mélange de rouge, vert et bleu (modèle R.V.B.).

c)Histogramme :

Un histogramme est un graphique statistique permettant de représenter la distribution des intensités des pixels d'une image, c'est-à-dire le nombre de pixels pour chaque intensité lumineuse. Par convention un histogramme représente le niveau d'intensité en abscisse en allant du plus foncé (à gauche) au plus clair (à droite).

A.1.5. Luminance:

C'est le degré de luminosité des points de l'image. Elle est définie aussi comme étant le quotient de l'intensité lumineuse d'une surface par l'aire apparente de cette surface, pour un

observateur lointain, le mot luminance est substitué au mot brillance, qui correspond à l'éclat d'un objet.

La moyenne ou luminance (brillance) d'une image numérique en niveau de gris est définie comme la moyenne des pixels de l'image.

A.1.6. Bruit:

Un bruit (parasite) dans une image est considéré comme un phénomène de brusque variation de l'intensité d'un pixel par rapport à ses voisins, il provient de l'éclairage des dispositifs optiques et électroniques du capteur.

A.1.7. Filtrage numérique :

Pour améliorer la qualité visuelle de l'image, on doit éliminer les effets des bruits (parasites) en lui faisant subir un traitement appelé filtrage.

Le filtrage consiste à modifier la distribution fréquentielle des composantes d'un signal selon des spécifications données.

Le système linéaire utilisé est appelé filtre numérique, parmi ces systèmes, nous distinguons :

A.1.7.1. Filtre passe-bas (lissage) :

Ce filtre n'affecte pas les composantes de basse fréquence dans les données d'une image, mais doit atténuer les composantes de haute fréquence. L'opération de lissage est souvent utilisée pour atténuer le bruit et les irrégularités de l'image. Elle peut être répétée plusieurs fois, ce qui crée un effet de flou. En pratique, il faut choisir un compromis entre l'atténuation du bruit et la conservation des détails et contours significatifs.

A.1.7.2. Filtre passe-haut (Accentuation) :

Le renforcement des contours et leur extraction s'obtiennent dans le domaine fréquentiel par l'application d'un filtre passe-haut.

Le filtre digital passe-haut a les caractéristiques inverses du filtre passe-bas. Ce filtre n'affecte pas les composantes de haute fréquence d'un signal, mais doit atténuer les composantes de basse fréquence.

A.1.7.3. Filtre Passe-bande (Différentiation) :

Cette opération est une dérivée du filtre passe-bas. Elle consiste à éliminer la redondance d'information entre l'image originale et l'image obtenue par filtrage passe-bas. Seule la différence entre l'image source et l'image traitée est conservée.

A.1.7.4. Filtre directionnel :

Dans certains cas, on cherche à faire apparaître des détails de l'image dans une direction bien déterminée. Pour cela, on utilise des filtres qui opèrent suivant des directions (horizontales, verticales et diagonales).

A.1.8. Détection de contours :

Un contour c'est une frontière entre deux objets dans une image discontinuité de l'image (variation brusque d'intensité).

La détection de contours est une technique de réduction d'information dans les images, qui consiste à transformer l'image en un ensemble de courbes, pas forcément fermées, formant les frontières significatives de l'image.

Si les structures extraites sont simples à manipuler (courbes fines, régulières, stables...), elles peuvent être utiles pour la mise en correspondance d'images (robotique, indexation,...).

A.1.8.1. approche contours :

Cette approche consiste à rechercher des régions en déterminant d'abord les points frontières entre deux homogènes de caractéristiques différentes, puis en regroupant les points situés à l'intérieur des contours fermés. Ces points frontières ou points de contours présentent une discontinuité importante de luminance par rapport à leurs voisins. Ces discontinuités peuvent être extraites par des filtrages soit de type gradient ou de type laplacien.

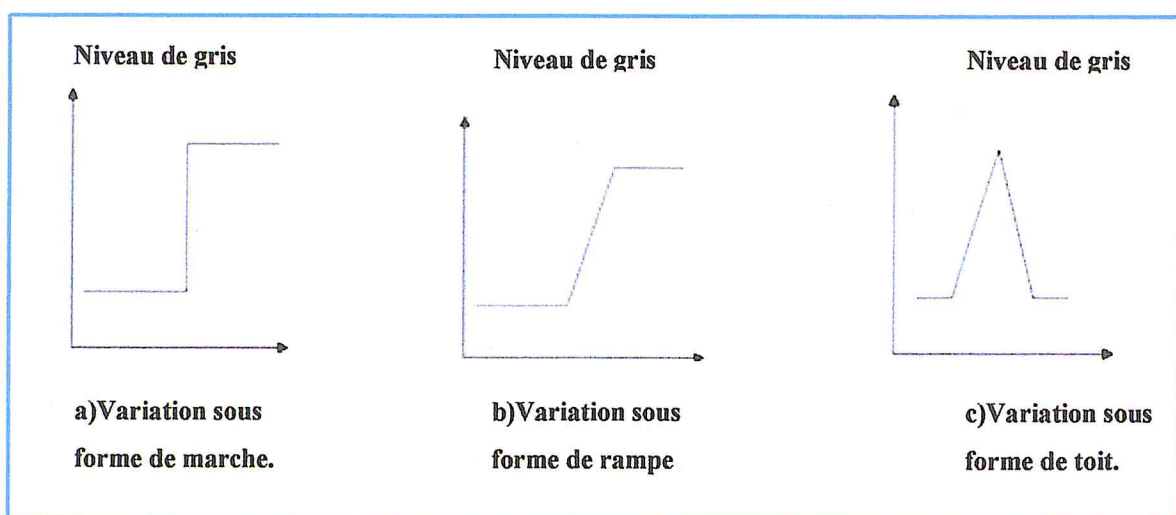


Figure A.2. Variétés des formes d'un contour.

A.1.8.2. Approche gradient :

Cette approche repose sur la recherche d'un extremum de la dérivée première, ou du passage par zéro de la dérivée seconde du gradient.

Soit la fonction image $I(x, y)$, le gradient de I en un point (x, y) est un vecteur bidimensionnel

$$\bar{G} \text{ qui s'écrit : } |\bar{G}| = \sqrt{\left(\frac{\partial I(x,y)}{\partial x}\right)^2 + \left(\frac{\partial I(x,y)}{\partial y}\right)^2} .$$

$$G_x(x, y) = \frac{\partial I(x,y)}{\partial x} = I(x,y) * h1(x,y).$$

$$G_y(x, y) = \frac{\partial I(x,y)}{\partial y} = I(x,y) * h2(x,y).$$

$H1(x, y), H2(x, y)$: masques de convolution.

L'extraction des points contours s'effectue en sélectionnant des points d'amplitude de gradient élevée, en se donnant un seuil S fixé a priori. Autrement dit l'amplitude du gradient est forte si $G > S$.

Il existe plusieurs masques de convolution, nous pouvons citer :

- Opérateur de ROBERTS.
- Opérateur de SOBEL.
- Opérateur de PREWITT.

A.1.8.3. Approche Laplacien :

Cette approche permet l'extraction des contours en calculant le laplacien et en déterminant ensuite les passages par zéro de celui-ci. En développant les dérivées partielles

$\frac{\partial I(x,y)}{\partial x}$ et $\frac{\partial I(x,y)}{\partial y}$ d'une image $I(x, y)$ au deuxième ordre, on peut trouver les expressions

approchées de $\frac{\partial^2 I(x,y)}{\partial x^2}$ et $\frac{\partial^2 I(x,y)}{\partial y^2}$. On définit le laplacien L par :

$$L = \frac{\partial^2 I(x,y)}{\partial x^2} + \frac{\partial^2 I(x,y)}{\partial y^2}$$

La valeur du laplacien est déterminée en chaque point $L = \frac{\partial^2 I(x,y)}{\partial x^2} + \frac{\partial^2 I(x,y)}{\partial y^2}$ (x, y) de l'image $I(x, y)$.

Le calcul du laplacien est approximé en convolant l'image avec des masques 3×3 ou 4×4 . il existe plusieurs masques laplacien :

$$h1 = \begin{bmatrix} 0 & -1 & 0 \\ -1 & 4 & -1 \\ 0 & -1 & 0 \end{bmatrix} \quad h2 = \begin{bmatrix} 1 & -2 & 1 \\ -2 & 4 & -2 \\ 1 & -2 & 1 \end{bmatrix} \quad h3 = \begin{bmatrix} -1 & 0 & -1 \\ 0 & 4 & 0 \\ -1 & 0 & -1 \end{bmatrix}$$

Ces deux méthodes (Approche gradient et Laplacien) semblent donc inefficaces, si l'amplitude du gradient aux points de contours varie fortement selon les parties de l'image. Il n'existe pas de seuil S permettant la sélection des points contour au bruit sans sélectionner ceux dus au bruit. Le laplacien amplifie le bruit présent dans l'image car il s'agit d'une méthode dérivative.

Nous allons présenter maintenant deux approches qui ont permis une meilleure compréhension d'une condition de bonne détection de contours, ce qui a conduit ainsi à des détecteurs de très bonne qualité. On les a vus émerger ces dernières années.

A.1.8.4. Approche de canny :

Canny a proposé un filtre déterminé analytiquement à partir de trois critères :

- 1- garantir une bonne détection : c'est-à-dire une réponse forte même à de faibles contours.
- 2- Garantir une bonne localisation: minimisation des distances entre les contours détectés et les contours réels,
- 3- Réponse unique : l'opérateur doit donner une réponse unique au même type de contours.

Canny a développé une forme mathématique pour les critères concernant la performance du détecteur. L'opérateur théorique est complexe à mettre en œuvre, il a été approché au vue de sa forme par l'opérateur dérivée première d'une Gaussienne.

La solution retenue par canny peut être mise en œuvre de la manière suivante :

- 1- Lisser l'image avec un filtre Gaussien.
- 2- Calculer le Gradient en chaque point de l'image.
- 3- Extraire les maximaux locaux, qui consiste à comparer la norme du Gradient d'un point $M(x, y)$ a celle de ses deux voisins $M1$ et $M2$ situés sur la droite passant par M dans la direction du Gradient.
- 4- Seuiller par hystérésis les maximaux locaux.

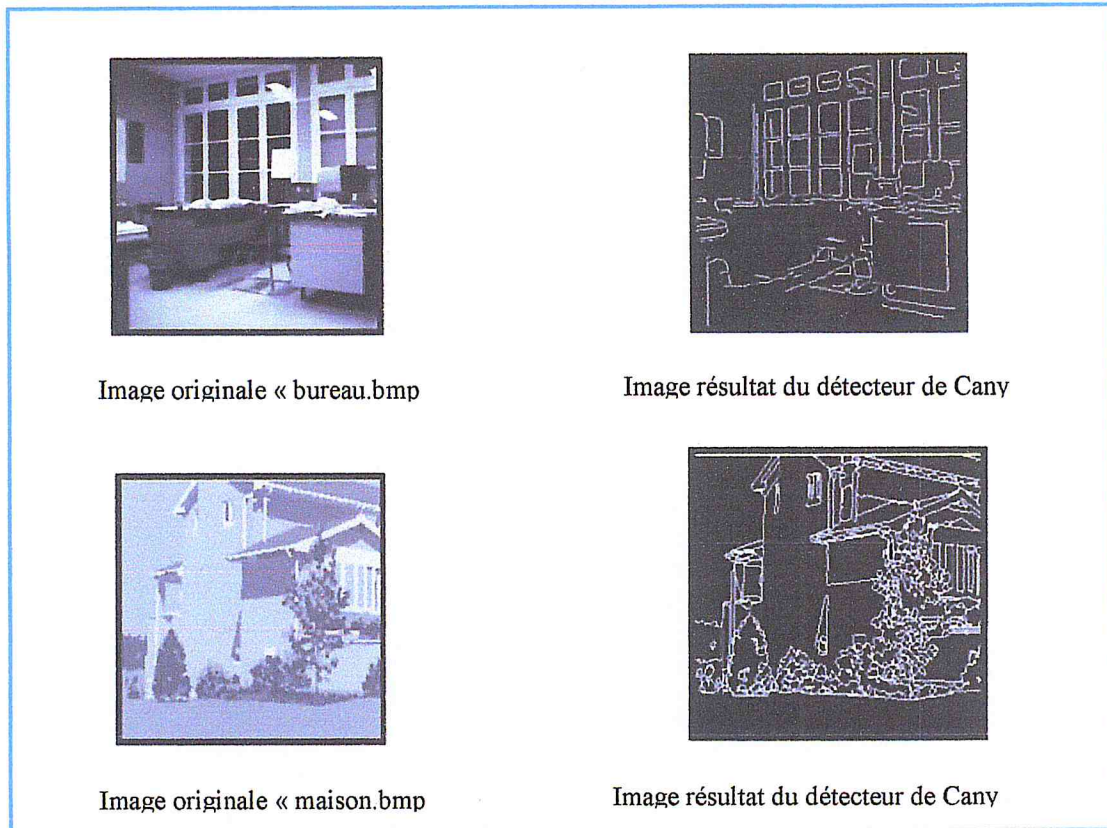


Figure. A.3. Exemple d'application de détecteur de cany

A.1.8.5. Approche de Deriche :

Au filtre de Canny, on préfère souvent le détecteur de Deriche, qui répond exactement aux mêmes critères de qualité que celui de Canny, mais qui possède une réponse impulsionnelle finie. Il a pu donc être synthétisé de façon récursive particulièrement efficace. Le filtre de Deriche a une expression générale de la forme :

$$f(x) = -ce^{-ax} \sin(wx) \quad a, w \text{ et } c \text{ sont des réels positifs}$$

La méthode de Deriche peut être donnée comme suit :

- 1- Calcul de l'image Gradient selon X.
- 2- Calcul de l'image Gradient selon Y.
- 3- Calcul de l'image des normes du gradient et de leurs directions.
- 4- Extraction des maxima locaux.
- 5- Seuillage par hystérésis.

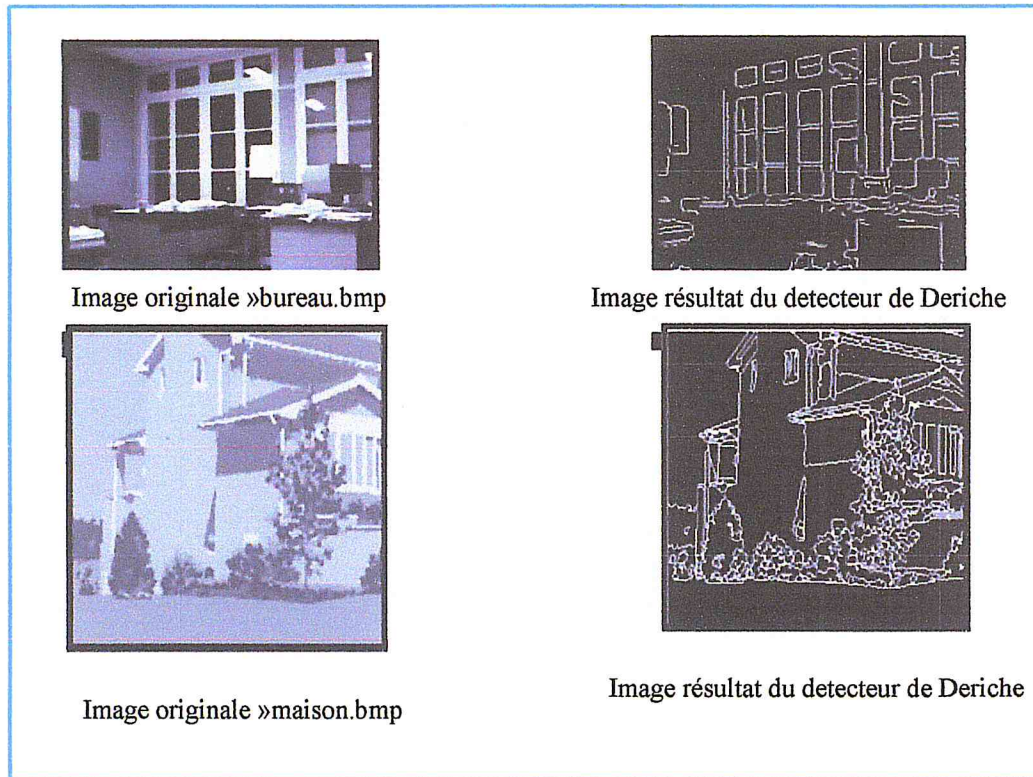
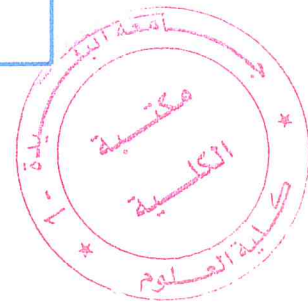


Figure. A.4. Exemple d'application de l'Approche de Deriche



A.1.9. Les méthodes de détection de contours :

A.1.9.1. Squelettisation :

La **squelettisation** est une classe d'algorithmes utilisée en analyse de formes. Elle consiste à réduire une forme en un ensemble de courbes, appelées **squelettes**, centrées dans la forme d'origine. La squelettisation est un outil d'analyse de forme non-scalaire, qui conserve les propriétés topologiques de la forme d'origine ainsi que les propriétés géométriques, selon la méthode employée.

A.1.9.2. Propriétés des squelettes :

Les squelettes possèdent différentes propriétés intéressantes:

- les squelettes sont théoriquement invariants par transformation linéaire (translation, rotation et changement d'échelle).
- la squelettisation est une transformation homotopique: elle préserve les propriétés topologiques de la forme.

D'autres propriétés sont spécifiques aux squelettes pondérés:

- tous les squelettes pondérés sont uniques,

- dans le cas des squelettes pondérés, la squelettisation est une transformation réversible, dans le sens où il est possible de reconstruire la forme d'origine à partir du squelette pondéré,
- un squelette pondéré fournit une description hiérarchique de la forme: les points squelette éloignés du contour décrivent l'aspect global de la forme et les points squelette proches du contour décrivent des particularités apparaissant dans le contour.

Une autre propriété des squelettes en général est considérée comme un défaut: la squelettisation est une transformation semi-continue. En effet, la moindre perturbation dans le contour ou au sein de la forme peut produire la création d'une branche importante dans le squelette.

