République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de le Recherche Scientifique
Université Mouloud Mammeri Tizi-Ouzou
Faculté de Génie Electrique et d'Informatique
Département d'Informatique

MEMOIRE DE FIN D'ETUDES

En vu d'obtention du diplôme de master en informatique

THEME

Conception et réalisation d'un système automatique de reconnaissance faciale

Proposé et dirigé par :

Mr Samir Redaoui

Réalisé par :

M^{elle}AldjiaMessaili

M^{elle}LydiaSi Hadj Mohand

PROMOTION 2011/2012

Résumé

Depuis plusieurs années, des efforts importants sont fournis dans le domaine de la recherche en biométrie. Ce phénomène s'explique en partie par la présence d'un contexte international où les besoins en sécurité (internet, e-Learning, criminologie, transactions bancaire) sont de plus en plus importants et où les enjeux économiques sont colossaux.

La biométrie est définie comme la reconnaissance des personnes à base de leurs caractéristiques physiologiques ou comportementales. Dans les caractéristiques physiques, on trouve le visage.

Actuellement ils existent de nombreuses méthodes de reconnaissance faciale qui permettent de reconnaître et d'identifier une personne dans une image. On peut diviser ces méthodes en deux catégories, les méthodes géométrique et les méthodes globales, la performance de ces méthodes dépend de la précision (nombre de paramètres) avec laquelle les informations utiles du visage sont extraites (comme certains partie du visage les yeux, le nez, la bouche, …).

Nous présentons dans ce travail une technique de reconnaissance de visages basée sur ACP (l'Analyse en Composante Principales), qu'est l'un des algorithmes les plus utilisé en reconnaissance de visages.

L'évaluation du système se fera sur la base de données standard, ORL conçue spécialement par un labo de recherche.

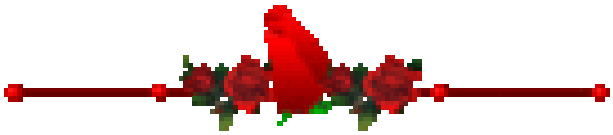
Remerciements

Nos vifs remerciements accompagnés de toute notre gratitude vont tout d'abord à notre promoteur Mr S.Redaoui pour son suivi et son engagement lors d'élaboration de ce projet.

Nous le remercions pour ses orientations et suggestions efficaces et pour ses conseils judicieux.

Nous remercions vivement les membres du jury qui nous ont fait l'honneur d'accepter d'évaluer notre travail.

Finalement, nos remerciements vont à toute personne ayant contribue de près ou de loin à l'aboutissement de ce modeste travail.



Dédicaces

Je dédie ce modeste travail :

- A ceux qui m'ont tout donné sans rien attendre en retour mis à part ma réussite, à ceux qui m'ont appris à aller au bout de mes ambitions, à ceux qui ont toujours cru en moi : à mes très chers parents.

-A la mémoire de mes grands parents.

-A ma grand-mère.

-A mes adorables chères soeurs : Djamila et son époux Hamid, Fatiha, Khelidja et son époux Malek

.

-A mes adorables chères frères : Mouhand et sa femme Saadia, Mhena et sa femme Samia, Amrane, Mounir.

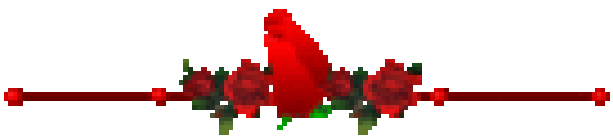
- A mes très chers neveux : Amer, Sadi.

-A mes très chères nièce : Dania, Tinhinane

-A tout mes amis(es).

-A ma chère collègue Lydia.

Aldjia



Dédicaces

Je dédie ce modeste travail :

- A ceux qui m'ont tout donné sans rien attendre en retour mis à part ma réussite, à ceux qui m'ont appris à aller au bout de mes ambitions, à ceux qui ont toujours cru en moi : à mes très chers parents.

-A la mémoire de mes grands-pères.

-A mes grands-mères.

-A mes adorables chères sœurs : Fouzia et son époux Hamid, Samira et son époux Idir, Nassima, sabrina,lylia.

-A tous mes cousins et cousines.

-A mes oncles et tantes.

- A mon très cher neveux : Mohand Salah.

-A mes nièces : Imen et Salma.

-A tout mes amis(es).

-A ma chère collègue Aldjia.

Lydia

Sommaire

Introduction générale 1

Chapitre I : Introduction à la biométrie

Introduction 3

I.1 Définition 3

I.2 Intérêt de la biométrie 3

I.3 Comparaison entre l'authentification biométrique et l'authentification par les moyens classiques. 5

I.4 Le marché de la biométrie 5

I.5 Applications des systèmes biométriques 6

I.6 Les caractéristiques communes des systèmes biométriques 7

I.7 Architecture d'un système biométrique 7

I.8 Type de la biométrie 9

I.9 Panorama des différentes biométries 10

I.9.1 La reconnaissance de l'iris 10

I.9.2 La rétine 11

I.9.3 L'ADN 12

I.9.4 La voix 13

I.9.5 Les empreintes digitales 14

I.9.6 La géométrie de la main 15

I.9.7 La dynamique de frappe sur un clavier 16

I.9.8 La signature 17

I.9.9 Le visage 18

I.9.10 Les réseaux veineux 19

I.10 La performance des systèmes biométriques 20

I.11 Comparaison des techniques biométriques 23

I.11 La multimodalité 25

Conclusion 26

Chapitre II : état de l'art de la reconnaissance du visage

II.1 Introduction 28

II.2 Pourquoi choisir le visage 28

II.3 La reconnaissance automatique du visage 29

II.4 Principales difficultés de la reconnaissance du visage 30

II.4.1 Changement d'illumination 30

II.4.2 Variation de poses 31

II.4.3 Expressions faciales 31

II.4.4 Présence ou absence des composants structurels 32

II.4.5 Occultations partielles 32

II.5 Les méthode d'extraction des caractéristiques du visage 32

II.5.1 Les méthodes locales 32

II.5.1.1 Elastic Bunch Graph Matching(EBGM) 33

II.5.1.2La méthode de Markov caché(HMM) 34

II.5.2 Les méthodes globales ou holistiques 35

II.5.2.1 Analyse en Composante Principale (ACP) 36

II.5.2.2 Analyse Linéaire Discriminante (LDA) 36

II.5.2.3 Réseau de Neurones Artificiels (RNA) 37

II.5.2.4 Les Séparateurs à Vaste Marge (SVM) 38

II.5.3 Les méthodes hybride 38

II.6 L'Analyse en Composante Principale (ACP) 39

Introduction 39

II.6.1 Principe mathématique de l'ACP 40
II.6.2 Quelques propriétés de l'ACP 41
II.6.3 ACP dans la reconnaissance du visage 42
II.7 Algorithme de l'ACP 42
II.7.1 Processus d'apprentissage 43
II.7.2 Processus de reconnaissance 46
II.8 conclusion 48

Chapitre III : conception

III.1 Introduction 49
III.2 Langage de modélisation 49
III.2.1 Définition de l'UML 49
III.2.2 Les différents types de diagramme UML 50
III.2.3 Les acteurs d'un système 51
III.3 Quelques diagrammes de notre système 51
III.3.1 Le diagramme de cas d'utilisation 51
III.3.2 Les diagrammes de séquence 54
III.3.3 Les diagrammes d'activité 62
III.3.4 Le diagramme de classes 64
III.4 Conclusion 67

Chapitre IV : Réalisation

IV.I Introduction 68
IV.2 Langage de programmation 68
IV.3 Les outils de développement 69
IV.3 .1 L'environnement de développement (Microsoft Visual Studio) 69
IV.3 .2 La bibliothèque Qt 70

IV.4 Description des interfaces 71

IV.4.1 Page accueil 71

IV.4.2 Fenêtre Utilisateur/administrateur..... 72

IV.4.2.1 Fenêtre d'authentification par mot de passe..... 72

IV.4.3 Espace Administrateur 73

IV.4.3.1 Fenêtre Ajouter Utilisateur 74

IV.4.3.2 Fenêtre Supprimer Utilisateur 75

IV.4.3.3 Fenêtre Modifier Utilisateur 76

IV.4.3.4 Fenêtre consulter base de données 77

IV.4.3.5 Fenêtre créer la base de données..... 78

IV.4.3.6 Fenêtre changer le mot de passe 79

IV.4.3.7 Fenêtre changer le niveau de sécurité 80

IV.4.4 Espace Utilisateur 81

IV.4.4. 1 Fenêtre D'identification 82

IV.4.4.2 Fenêtre d'authentification 83

IV.5 Evaluation du système 84

IV.5.1 La base ORL 84

IV.5.2 La courbe roc de notre système..... 89

IV.6 Conclusion 92

Conclusion générale 93

Annexe

Table des figures

Figure I.1: Un graphe présente l'évolution des revenus de l'industrie biométrique 2007-2015 6
Figure I.2: Architecture d'un système biométrique 8
Figure I.3 : photo pour l'iris de l'œil. 11
Figure I.4 : Capteur d'images de l'iris. 11
Figure I.5 : photo pour la rétine de l'œil. 12
Figure I.6 : Structure de la molécule d'ADN 12
Figure I.7 : capture de la voix 12
Figure I.8: la reconnaissance vocale avec texte prompte 12
Figure I.9 : la forme d'une empreinte digitale 14
Figure I.10 : différents types de minuties 15
Figure I.11 : Exemple de capteur d'empreinte digitale 15
Figure I.12 : Scanner biométrique 16
Figure I.13 : géométrie de la main 16
Figure I.14 : dynamique de frappe au clavier 17
Figure I.15 : Illustrations des supports d'acquisition de signatures 18
Figure I.16 : appareil de reconnaissance du visage 19
Figure I.17 : appareil pour la reconnaissance des réseaux veineux de la main 19
Figure I.18 : appareil pour la reconnaissance des réseaux veineux du doigt 19
Figure I.19 : Courbe présente la variation de taux de FAR et FRR en fonction du seuil de décision 22
Figure I.20 : Les biométries les plus utilisées en fonction du Coût et la Précision 23
Figure I.21 : Les différents systèmes multimodaux 26
Figure II.1 Fonctionnement d'un système de reconnaissance automatique des visages 29
Figure II.2 Exemple de variation d'éclairage 31

Figure II.3 Exemple de variation de poses 31

Figure II.4 Exemple de variation d'expressions..... 32

Figure II.5 Distances entre points caractéristiques..... 33

Figure II.6 Localisation des points caractéristiques 34

Figure II.7 Création du treillis 34

Figure II.8 Face Bunch Graph..... 34

Figure II.9 Les 5 états du HMM de haut en bas d'une image du visage..... 35

Figure II.10 Exemple d'eigenface 36

Figure II.11 La projection PCA et LDA d'un ensemble de données 37

Figure II.12 Exemple de projection suivant la PCA 39

Figure II.13 Processus de reconnaissance par PCA 47

Figure III.1 : Diagramme des cas d'utilisations 53

Figure III.2 : Diagramme de séquence pour le ces d'utilisation accéder à l'espace administrateur..... 54

Figure III.3 : Diagramme de séquence pour le cas utilisation ajouter utilisateur..... 55

Figure III.4 : Diagramme de séquence pour le cas utilisation supprimer utilisateur 56

Figure III.5 : Diagramme de séquence pour le cas utilisation consulterBDD..... 57

Figure III.6 : Diagramme de séquence pour le cas utilisation configurer seuil 58

Figure III.7 : Diagramme de séquence pour le cas utilisation apprentissage..... 59

Figure III.8 : Diagramme de séquence pour le cas utilisation authentification..... 60

Figure III.9 : Diagramme de séquence pour le cas utilisation identification 61

Figure III.10 : Diagramme d'activité pour le cas de suppression 62

Figure III.11 : Diagramme d'activité pour le cas d'authentification 63

Figure III.12 : Diagramme d'activité pour le cas d'identification 63

Figure III .13: Diagramme de classe du système 66

Figure IV.1 : Vue général de l'interface de l'environnement Microsoft Visual Studio..... 69

Figure IV.2 : Logo de la bibliothèque QT..... 70

Figure IV.3 : Page d'accueil 71

Figure IV.4 : Fenêtre espace Utilisateur/administrateur 72

Figure IV .5 : Fenêtre d'authentification 72

Figure IV.6 : Message d'erreur 72

Figure IV.7 : Espace Administrateur 73

Figure IV.8 : Fenêtre Ajout Utilisateur 74

Figure IV.9 : Fenêtre Supprimer Utilisateur 75

Figure IV.10 : Fenêtre Modifier Utilisateur. 76

Figure IV.11 : Fenêtre Consulter Base de Données. 77

Figure IV.12 : Fenêtre créer base de données 78

Figure IV.13 : Changer mot de passe 79

Figure IV.14 : Changer le niveau de sécurité du système 80

Figure IV.15 : Espace Utilisateur 81

Figure IV.16 : Fenêtre D'identification 82

Figure IV.17 : Fenêtre d'authentification. 83

Figure IV.18 : Extrait de la base ORL. Pour chacune des 40 personnes enregistrées, on dispose de 10 vues avec des changements de pose, d'expression et d'éclairage 84

Figure IV.19 : Résultat du teste avec la même image que celle de la base de données 85

Figure IV.20 : Résultat du teste d'une image avec une pause différente 85

Figure IV.21 : Résultat du teste d'une image avec une autre pause 86

Figure IV.22 : Résultat du teste d'une image d'une personne portant des lunettes avec un seuil de 2245 87

Figure IV.23 :Résultat du teste d'une image d'une personne portant des lunettes avec un seuil de 1185 87

Figure IV.24 : Résultat du teste d'une image d'une personne avec une expression faciale différente 88

Figure IV.25 : Résultat du teste d'une image d'une personne dans un environnement avec un éclairage différent 89

Figure IV.26 : Graphe représente la variation des taux de FRR et FAR en fonction du seuil. 90

Figure IV.27 : La courbe roc de notre système 91

Table des tableaux

Tableau .I.1. : Comparaison entre l'authentification biométrique et l'authentification par les moyens classiques. 5

Tableau I.2 : Avantages et inconvénients des techniques biométriques. 24

Tableau I.3 : Tableau récapitulatif des principales techniques. 24

Tableau VI.1 : les taux d'erreur FAR et FRR de notre système. 90

Introduction générale

La croissance internationale des communications, des déplacements d'individus, transactions financières et des accès aux services, …, implique de s'assurer de l'identité des individus. Il y'a donc un intérêt grandissant pour les systèmes d'identification et d'authentification. Leur dénominateur commun, est le besoin d'un moyen simple, pratique et fiable pour vérifier l'identité d'une personne sans l'assistance d'une autre personne.

Trois façons générique existent pour vérifier/identifier un individu : ce que l'on sait (exemple : mot de passe), ce que l'on possède (exemple : badge), ce que l'on est ou ce que l'on sait faire (empreinte digitale, dynamique de frappe au clavier, visage, …) il s'agit de la biométrie.

L'authentification biométrique présente de nombreux avantages, puisqu'elle permet de s'affranchir des intermédiaires que constituent les clefs, cartes et autres codes personnels susceptibles d'être oubliés, perdus ou volés. Elle supprime le risque qui peut être occasionné par le prêt d'une clef ou la communication d'un mot de passe à un tiers.

La biométrie permet l'authentification d'individus à partir de leurs caractéristiques physiologiques ou comportementales. Ces caractéristiques doivent être :

– universelles : présentes chez tous les individus ;
– uniques : spécifiques à chaque individu pour permettre de le différencier par rapport aux autres ;
– permanentes : pour permettre une authentification au cours du temps ;
– mesurables : pour permettre l'enregistrement et les comparaisons futures.

Il existe plusieurs caractéristiques physiques et comportementales uniques pour un individu, ce qui explique la diversité des systèmes appliquant la biométrie, citons : L'empreinte digitale, La dynamique des signatures, l'iris, la rétine, la reconnaissance vocale et celle du visage. L'intérêt des applications utilisant la biométrie se résume en deux classes : faciliter le mode de vie, éviter la fraude.

La reconnaissance faciale fait partie des techniques biométriques. On remarque que dans la vie quotidienne chacun de nous identifie tout au long de la journée différents visages. Ainsi lorsque nous rencontrons une personne, notre cerveau va chercher dans notre mémoire et vérifier si cette personne est répertoriée ou non.

Plusieurs méthodes ont été développées pour la reconnaissance de visage 2D (méthodes locales, globales et hybrides).
Dans le cadre de notre travail de fin d'étude, nous nous intéressons à la vérification de l'identité des personnes en utilisant le visage, en se basant sur la technique d'Analyse en Composantes Principales ou ACP qui est une technique 2D.

Ce présent document s'articule autour de quatre chapitres principaux : Dans le premier chapitre nous donnerons des notions générales sur la biométrie et les différentes techniques biométriques existantes. Dans le deuxième chapitre, nous présenterons la biométrie faciale et ses multiples approches et nous finiront ce chapitre par la présentation de notre approche de reconnaissance. Le troisième chapitre portera sur la conception de notre système. En fin, le dernier chapitre sera alors celui de Réalisation, dans ce chapitre, on décrira les outils de développement matériels et logiciels. Ensuite on présentera les principales interfaces de notre application.

I.1 Introduction :

De nos jours, on parle de plus en plus de l'insécurité dans divers secteurs ainsi que des moyens informatiques à mettre en œuvre pour contrer cette tendance : le contrôle d'accès aux ordinateurs, l'e-commerce, les opérations bancaires basées sur l'identification du demandeur, etc. Cette insécurité est due à l'usage des méthodes classiques d'identification qui posent de gros problèmes de fiabilité comme: le mot de passe qui peut être oublie ou décrypté via des logiciels spécifiques. Afin de répondre à ces besoins liés à la sécurité, la biométrie se présente comme une technologie potentiellement puissante.

I.2 Définition de la biométrie:

La biométrie est « toutes caractéristiques physique ou traits personnels automatiquement mesurables, robustes et distinctives qui peuvent être utilisées pour identifier un individu ou pour vérifier une identité prétendue d'un individu » **[1]**.

Une définition alternative :
La biométrie est la science qui vérifie l'identité des individus à travers des mesures physiologiques ou des traits comportementaux. Il peut y avoir plusieurs types de caractéristiques physiques, les unes plus fiables que les autres, mais toutes doivent être universelles (exister chez tous les individus), uniques (permettre de différencier un individu par rapport a un autre), permanentes (autoriser l'évolution dans le temps), mesurables (autoriser une comparaison future) et enfin on peut les collecter (enregistrer les caractéristiques d'un individu avec l'accord de celui-ci) **[2]**.

I.3 Intérêt de la biométrie :

Dans son environnement quotidien, un individu a besoin de s'identifier dans une multitude de contextes : pour accéder à son lieu de travail, pour retirer de l'argent d'un distributeur ou payer ses achats, pour demander un service social… Autant de codes et de mots de passe à mémoriser et à protéger.

Traditionnellement, Il existe deux manières d'identifier une personne :

1. Méthodes basées sur une connaissance (knowledge-based). Cette connaissance correspond, par exemple, à un mot de passe pour ouvrir une session ou un code SIM pour un téléphone portable.

2. Méthodes basées sur une possession (token-based). Il peut s'agir d'une pièce d'identité, d'un badge, d'une clé …

Plus généralement, les techniques d'authentification basées sur ce que l'on possède et sur ce que l'on sait présentent de nombreux inconvénients. Les objets permettant l'authentification sont souvent perdus ou volés et les mots permettant de s'identifier sont facilement oubliés. De plus, ce type de données est souvent partagé par plusieurs personnes. Par ailleurs, d'un point de vue sécurité, l'utilisation d'un mot de passe valide sur un réseau n'assure pas que la personne qui s'est connectée est bien celle qu'elle prétend être. On sait seulement qu'elle possédait la bonne clé d'accès. L'identité et la protection des données privées ne peuvent pas être garanties et l'utilisation frauduleuse d'un de ces mécanismes ne peut pas être prouvée. Ces limitations des systèmes classiques d'authentification entraînent une perte de confiance et une augmentation des possibilités de fraude. La biométrie apporte une solution à ces différents problèmes. D'une part, le partage des données permettant l'authentification devient impossible. D'autre part, la confiance dans l'authentification est accrue puisque la personne doit être physiquement présente.

La biométrie exploite les caractéristiques d'une personne qu'elles soient innées comme les empreintes digitales ou acquises comme la signature. Ces caractéristiques sont attachées à chaque individu et ne souffrent donc pas des faiblesses des méthodes basées sur une connaissance ou une possession. En effet les caractéristiques biométriques ne peuvent être oubliées ou perdues. De plus, elles sont très difficiles à deviner, à voler, ou à dupliquer **[3]**.

L'intérêt des applications utilisant la biométrie se résume en deux classes : faciliter le mode de vie, éviter la fraude.

I.4 Comparaison entre l'authentification biométrique et l'authentification par les moyens classiques.

Authentification biométrique	Authentification par mot de passe / clé
- basée sur des mesures physiologiques ou des traits comportementaux. - authentifie l'utilisateur. - le caractère est attache à l'utilisateur de façon permanente. - L'échantillon biométrique peut varier dans le temps, il est incertain. - utilise une comparaison probabiliste.	- basée sur quelques choses que l'utilisateur "possède" ou "sait". - authentifie la clé. - il peut être emprunté, perdu ou volé. - l'identificateur ne vari pas, il est sur. - nécessite une comparaison exacte pour l'authentification.

Tableau .I.1. : Comparaison entre l'authentification biométrique et l'authentification par les moyens classiques.

I.5 Le marché de la biométrie :

La biométrie commence à remplacer le mot de passe à l'ouverture d'un logiciel ou d'un poste informatique et surtout, se démocratise dans le contrôle d'accès aux locaux. La biométrie aujourd'hui est en plein essor, et pour cela le marché de la biométrie a connu une véritable explosion. On note un accroissement des sites équipés par cette technologie, qui a pour but d'assurer à la fois le contrôle, la gestion et la sécurité au sein de différents établissements. On s'attend à ce que le chiffre d'affaires de l'industrie biométrique incluant les applications judiciaires et celles du secteur public, se développe rapidement. Une grande partie de la croissance sera attribuée au contrôle d'accès aux systèmes d'information (ordinateur / réseau) et au commerce électronique, bien que les applications du secteur public continuent à être une partie essentielle de l'industrie.

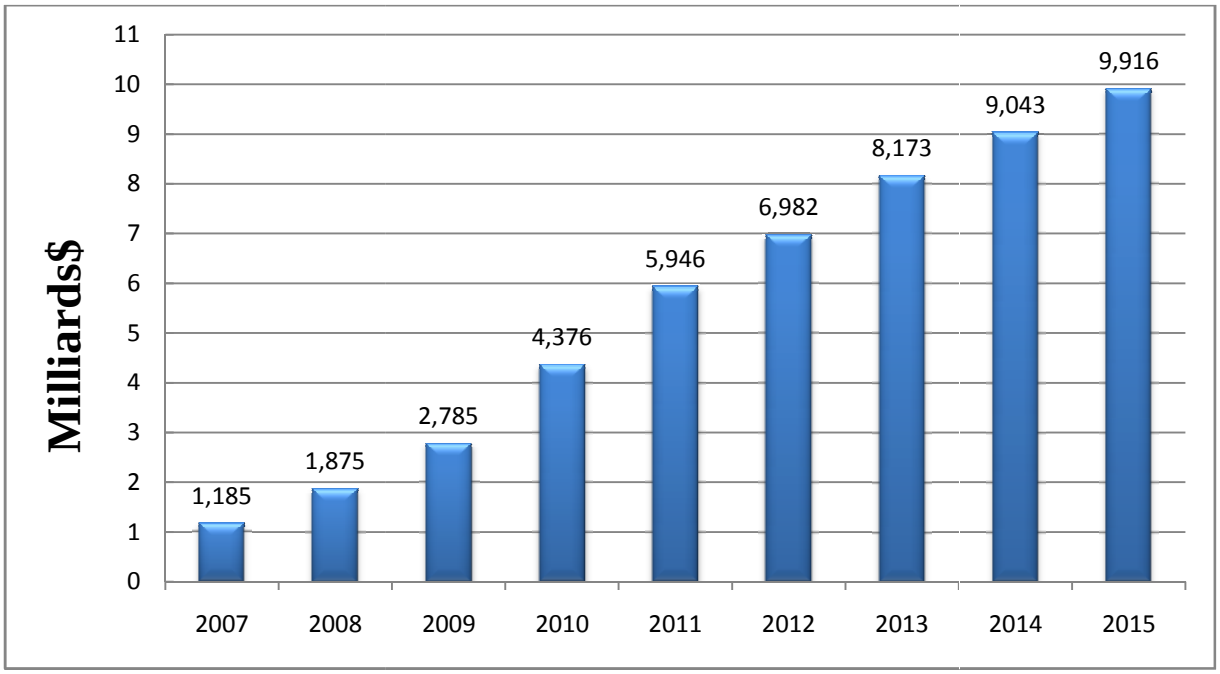


Figure I.1 : **Un graphe présente l'évolution des revenus de l'industrie biométrique 2007-2015[1]**

I.6 Applications des systèmes biométriques :

Les systèmes biométriques sont appliqués dans plusieurs domaines et ses applications sont divisées en trois groupes principaux **[4]**:

- **Les applications commerciales** : on trouve deux types
  - Contrôles d'accès: c'est l'accès physique à un lieu sécurisé ou bien un accès virtuel à une ressource ou un service.
  - Authentification des transactions : telle que le paiement par carte bancaire, par téléphone ou sur internet.
- **Les applications gouvernementales** : telles que la carte nationale d'identification, permis du conducteur, la sécurité sociale, le contrôle de passeport, etc …
- **Les applications juridiques** : telles que l'identification de cadavre, la recherche de criminels, l'identification de terroriste, les enfants disparus, etc....

I.7 Les caractéristiques communes des systèmes biométriques :

On peut citer trois caractéristiques principales communes aux systèmes biométriques **[5]** :

- **L'unicité** : pour l'identification d'une personne au sein d'une population on utilise un critère unique. En effet la biométrie utilise l'iris, le doigt, le visage, la rétine, etc… qui présentent des caractéristiques uniques au sein d'une large population.
- **Caractère publique d'une donnée biométrique** : le code personnel est secret et il doit rester pour que le système de contrôle fonctionne. Mais le critère biométrique ne l'est pas et n'importe qui peut le capturer et l'imiter. Le système biométrique doit se rendre compte et éliminer les artefacts construits pour le tromper.
- **Mesure d'un système biométrique** : le système biométrique n'utilise pas toute la totalité de la donnée capturée. Il en extrait certaine caractéristiques, ce qui réduit la quantité de l'information à traiter. Puis effectue un calcule et obtient un résultat à partir des données recueillies.

I.8 Architecture d'un système biométrique :

Quel que soit le système biométrique mis en place, celui-ci comporte toujours deux modules principaux : module d'apprentissage et le module de reconnaissance (figure I.2). Il existe un troisièmes module facultatif qui est le module d'adaptation.

Pendant l'apprentissage, le système va acquérir une ou plusieurs mesures biométriques qui serviront à construire un modèle de l'individu. Ce modèle de référence servira de point de comparaison lors de la reconnaissance. Le modèle pourra être réévalué après chaque utilisation grâce au module d'adaptation**.**

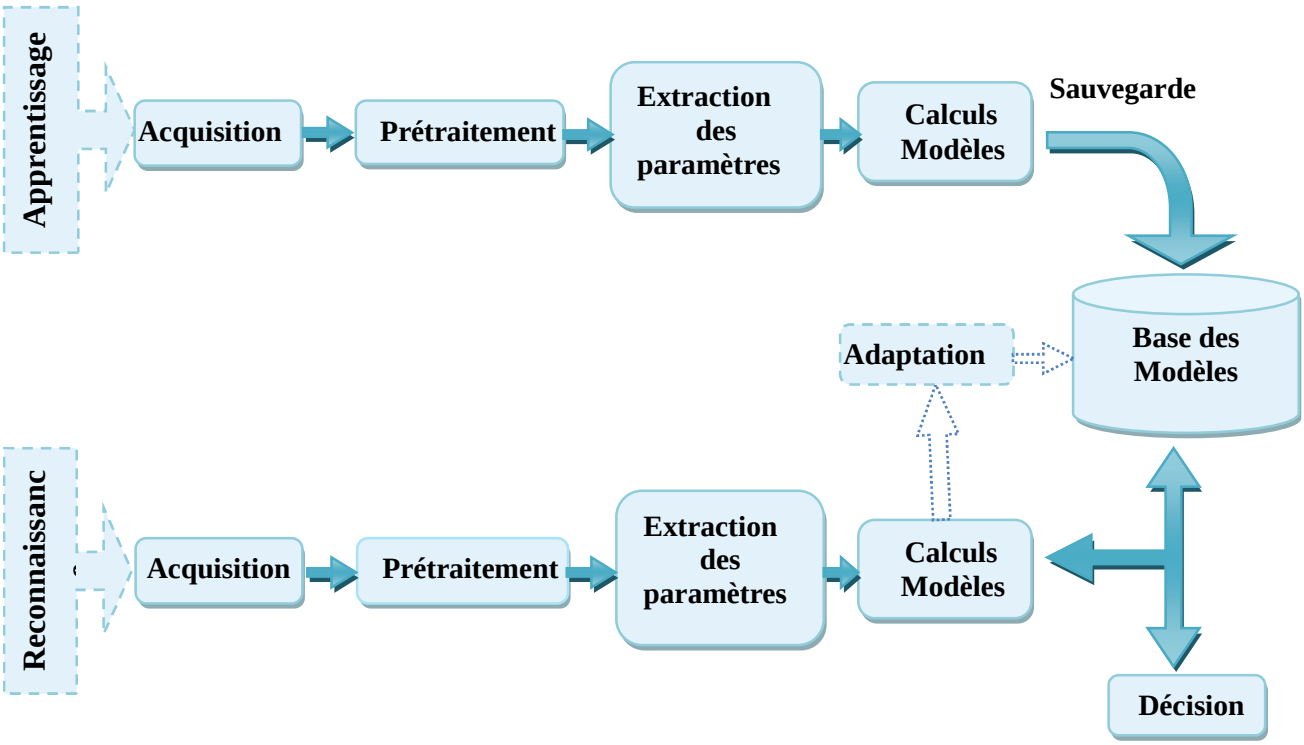


Figure I.2: Architecture d'un système biométrique [6].

a. Module d'apprentissage :

Pendant l'apprentissage le système va acquérir une ou plusieurs mesures biométriques grâce à un capteur. On parle d'acquisition ou de *capture*. En général, cette capture n'est pas directement stockée, elle subit un prétraitement. En effet, le signal contient de l'information inutile à la reconnaissance et seuls les paramètres pertinents sont extraits. Ces paramètres construisent un modèle de l'individu. Le modèle est une représentation compacte du signal qui permet de faciliter la phase de reconnaissance. Le modèle peut être stocke dans une base de données ou sur une carte à puce.

b. Module de reconnaissance :

Au cours de la phase de reconnaissance, la caractéristique biométrique est capturée et prétraitée et les Paramètres pertinents sont extraits comme dans la phase d'apprentissage. La suite de la reconnaissance sera effectuée différemment suivant le mode opératoire du système:

En mode identification, le système doit deviner l'identité de la personne. Il va comparer le signal capturé avec tous les modèles contenus dans la base de données. Puis, il va tirer le modèle le plus proche du signal pour répondre à la question du type : «*Qui suis-je?*». C'est une tâche très difficile car la base de données peut contenir des milliers d'individus. On perd beaucoup de temps pour calculer toutes les comparaisons possibles.

En mode vérification ou authentification, le système va comparer le signal capturé avec un seul des modèles de la base de données avec pour but de répondre à la question : « *Suis-je bien la personne que je prétends être?* »**[7]**. Donc L'utilisateur propose une identité au système et le système doit vérifier que l'identité de l'individu est bien celle proposée.

c. Le module d'adaptation :

Pendant la phase d'apprentissage, le système biométrique ne capture souvent que quelques instances d'un même attribut afin de limiter la gêne pour l'utilisateur. Il est donc difficile de construire un modèle assez général capable de décrire toutes les variations possibles de cet attribut (comme les conditions d'acquisition différentes) ; ce qui explique l'utilité de ce module. L'adaptation est quasi indispensable pour les caractéristiques non permanentes comme la voix **[8].**

I.9 Types de la biométrie :

L'extension de la biométrie au domaine de la reconnaissance des personnes consiste à déterminer l'identité d'un individu grâce à des mesures quantitatives. Ces mesures peuvent avoir pour objet les caractéristiques morphologiques ou les caractéristiques comportementales de cette personne **[9],** comme elles peuvent avoir les deux à la fois (caractéristiques mixtes).

La biométrie morphologique :

La biométrie morphologique décrit les individus par des mesures de leurs caractéristiques biologiques ou physiologiques. Ces mesures sont moins sujettes à l'influence du stress que la biométrie comportementale. Elles sont également plus difficiles à falsifier.
Les biométries morphologiques les plus courantes mesurent les empreintes digitales, le réseau veineux de la rétine, l'iris, l'empreinte de la main ou certaines caractéristiques du visage. *La*

biologie permet, quant à elle, de caractériser un individu par son ADN à travers une analyse de sa salive, de son sang, son odeur, l'urine, …etc.
La biométrie morphologique est, à l'heure actuelle, un des moyens les plus fiables pour reconnaître un individu, car elle mesure des caractéristiques qui sont indissociables de cet individu.

La biométrie comportementale :

La biométrie comportementale mesure et caractérise des éléments qui sont propres aux comportements d'un individu. De nombreux comportements peuvent être observés et analysés afin de caractériser une personne : le tracé de sa signature (inclinaison et vitesse de déplacement du stylo, la pression exercée), sa démarche et sa façon de taper sur un clavier (vitesse de frappe).

Les biométries mixtes :

Certaines modalités se situent à la croisée des biométries morphologiques et comportementales par exemple : la voix **[9]**, L'analyse des battements du cœur par l'intermédiaire des signaux d'un électrocardiogramme **[10]**, l'analyse de l'activité électrique du cerveau mesurée par Électro-encéphalographie **[11]**.

I.10 Panorama des différentes biométries:

I.10.1 La reconnaissance de l'iris :

L'iris est le muscle présentant la partie colorée de l'œil, situé entre la pupille et le blanc de l'œil. Les motifs de l'iris se forment aux cours des deux premières années. Ils sont stable (ne change pas) durant la vie d'un individu et indépendants du code génétique. Ce qui permet une différentiation entre les iris des personnes et même entre les vrais jumeaux et les yeux d'une même personne.

Ces systèmes sont plus performants et très fiables, car il est difficile de tromper le système du fait que l'iris ne peut être modifié par intervention chirurgicale et l'iris artificiel est facile à détecter. Pour cela ils peuvent être utilisés dans des applications nécessitant une haute sécurité avec un excellant niveau de performance comme : bases nucléaires, bases spatiales (NASA).
D'après les fabricants ces systèmes n'ont commis jusqu'à présent aucun fau rejet, et malgré ça ils restent non acceptables par le grand public.

Figure I.3 : photo pour l'iris de l'œil.

Ces systèmes fonctionnent tout en capturant une image de l'iris avec un appareil à l'aide d'une lumière infrarouge, et en extrant les caractéristiques de l'iris qui sont comparés à un ou plusieurs gabarits.

L'iris possède environ 200 point pouvant être utilisés comme comparaison, notamment des cercles, des sillons et des tâches.

Figure I.4 : Capteur d'images de l'iris

I.10.2 La rétine :

La rétine comporte plusieurs vaisseaux sanguins qui sont unique et stables dans le temps. Ils ne peuvent être affectés que par certaines maladies. Pour ces raisons, la reconnaissance de la rétine est actuellement considérée comme une des méthodes biométriques les plus sûres, et est utilisée dans des applications de sécurité très élevée comme les applications militaires ou nucléaires. Cette technique est très ancienne par rapport à celle de l'iris, en effet les premières études remontent aux années 30.

Les caractéristiques de la rétine sont liées à la distribution géométrique des vaisseaux sanguins. Le système illumine le fond d'œil avec un rayon lumineux pour extraire 192 point de repère. L'œil doit être situé très près de la tête de lecture et l'utilisateur doit fixer son regard sur un point déterminé pendant plusieurs secondes, les personnes hésitent en général à approcher un organe aussi sensible que l'œil près de l'appareil de mesure ce qui explique pourquoi cette méthode est mal acceptée par le grand public. En plus quelques risques pour la

santé ont été révélés et limitent l'utilisation de cette technologie dans des locaux de haute sensibilité.

Figure I.5 : photo pour la rétine de l'œil.

I.10.3 L'ADN :

L'ADN ou Acide DésoxyriboNucléique est une molécule contenant l'information "génétique héréditaire". L'analyse de l'ADN ne nécessite pas forcément une prise de sang, puisqu'elle peut être réalisée à partir d'un cheveu, d'un échantillon de salive, de cellule de la peau.

Pour une reconnaissance ADN, le modèle sera constitué d'une liste de certaines caractéristiques génétiques de la personne.

L'ADN est spécifique à chaque individu, il est la méthode la plus fiable pour identifier une personne (99.99% de fiabilité), mais actuellement pas adaptée à la reconnaissance en temps réel, car elle nécessite des délais de plusieurs semaines pour avoir le résultat d'analyses.

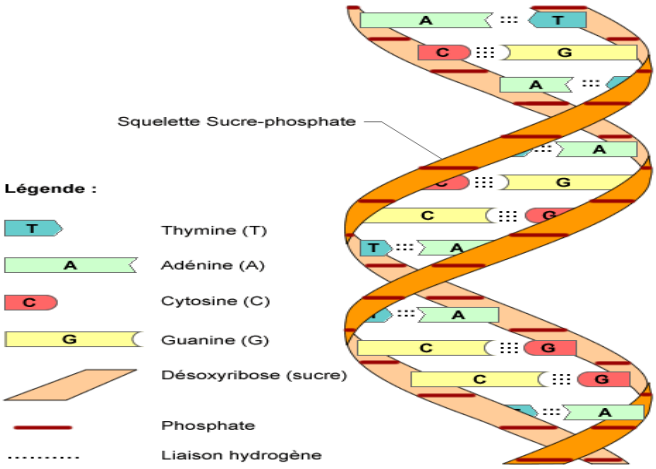


Figure I.6 : Structure de la molécule d'ADN

I.10.4 La voix :

La reconnaissance vocale consiste à déterminer les caractéristiques de la voix d'un individu qui sont constituées par une combinaison des facteurs comportementaux (vitesse, rythme, etc…) et physiologiques (tonalité, âge, sexe, fréquence, accent, harmonique, etc…).

Cette technologie ne nécessite pas un contacte avec le lecteur du système, pour cela elle est très acceptée et utilisée dans plusieurs secteurs comme les centres d'appel, les opérations bancaires, l'accès à des comptes, sur PC domestiques, pour l'accès à un réseau ou encore pour des applications judiciaires.

Il existe plusieurs modalités de reconnaissance du locuteur :

- Avec texte fixe : la voix du locuteur est combinée avec un texte (mot ou bien une phrase) qui sera aussi utilisé au moment du teste.
- Avec texte prompte : pendant la reconnaissance, le système prompte une ou plusieurs phrases que le locuteur doit répéter.
- Indépendant du texte : le locuteur parle librement sans texte exigé à répéter.

Pour le fonctionnement de ces systèmes, une table de références de voix est construite à partir des caractéristiques extraites de la voix du locuteur qui lit une série de phrases ou de mots à plusieurs reprises. Ces caractéristiques, forment une empreinte unique, sont ensuite traitées par un algorithme et conservées pour comparaison ultérieure.

Figure I.7 : capture de la voix

Figure I.8: la reconnaissance vocale avec texte prompte

I.10.5 Les empreintes digitales :

La reconnaissance d'empreinte digitale représente la méthode la plus ancienne d'identification biométrique. Le premier système automatique d'authentification utilisant les empreintes digitales a été commercialisé au début des années soixante. De nos jours les empreintes digitales sont toujours largement utilisées et reconnues comme méthodes d'identification fiable et mature. Elles sont communément utilisées pour la reconnaissance de criminels. Cependant les empreintes digitales sont une mesure biométrique assez mal acceptée par les utilisateurs à cause de l'association qui est souvent faite avec la criminologie. Les empreintes digitales sont uniques pour chaque personne la probabilité de trouver deux empreintes digitales similaires est de 1 sur 10 puissances 24. Les jumeaux, par exemple, venant de la même cellule, auront des empreintes très proches **[12]** mais pas semblables.

Une empreinte digitale est constitué d'un ensemble de lignes localement parallèles forment un motif unique pour chaque individu (figure I.9), on distingue les crêtes (ou striés, ce sont les lignes en contacte avec une surface au touché) et les vallées (ce sont les creux entre deux stries).

Figure I.9 : la forme d'une empreinte digitale

Chaque empreinte possède un ensemble de points singuliers globaux (les centres et les deltas) et locaux (les minuties), les centres correspondent à des lieux de convergences des crêtes tandis que les deltas correspondent a des lieux de divergences.

La reconnaissance se fait à partir des propriétés locales (minuties). Les deux types de minuties qui sont principalement utilisés pour la reconnaissance digitale sont la terminaison et la bifurcation. Les minuties et leurs caractéristiques (position, orientation) sont extraites de l'image afin de former le modèle de l'empreinte, ce modèle va être comparé avec l'ensemble des modèles des minuties sauvegardés des utilisateurs.

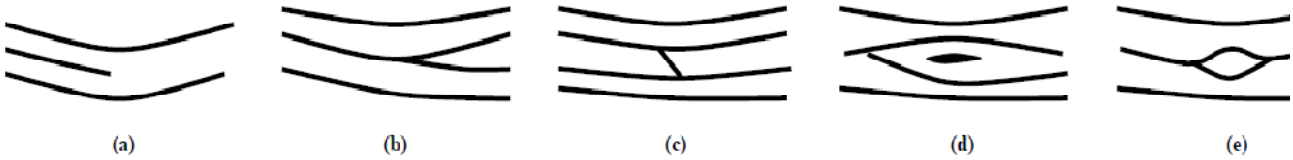


Figure I.10 : différents types de minuties : a. terminaison, b. bifurcation, c. pont, d. île, e. lac

Il existe divers capteurs pour l'acquisition de l'empreinte digitale par exemples: le capteur optique **(a)**, Capteur capacitif **(b),** capteur de pression **(c)**, capteur de champ-électrique**.**

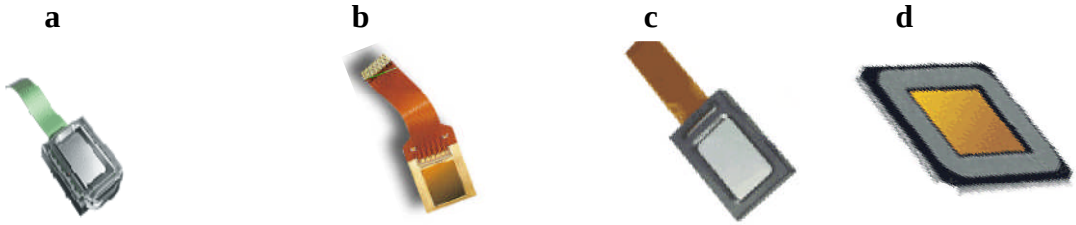


Figure I.11 : Exemple de capteurs d'empreinte digitale

L'identification par empreinte digitale souffre de certains problèmes qui affectent la performance du système par exemple la manière dont l'utilisateur pose son doigt sur le scanner (parfois, seule une partie de l'empreinte est visible), de son orientation, de son humidité (*i.e.* sueur) ainsi que de la pression que l'utilisateur exerce sur le scanner et qui résulte en une déformation non uniforme de l'empreinte. La présence de blessures temporaires ou permanentes sur les empreintes affecte aussi la performance du système.

I.10.6 La géométrie de la main :

Les systèmes de reconnaissance biométrique de la géométrie de la main sont sur le marché depuis les années 1980 et sont utilisées dans certains endroits par tout dans le monde **[13]**. Cette méthode consiste à déterminer les caractéristiques de la main d'un individu : sa forme, sa longueur, sa largeur, son épaisseur, sa surface, la courbure des doigts, les articulations et les lignes de la main etc.

Les systèmes de reconnaissance de la géométrie de la main sont simples d'usage. L'utilisateur doit poser la paume de sa main sur une plaque qui possède des guides afin de l'aider à

positionner ses doigts. Un appareil photo placé au dessus de la main prend une image de celle-ci et des miroirs disposés a certains angles permettent la prise d'une image latérale, on crée ainsi un modèle de vérification qui est comparé au modèle créé lors de l'apprentissage.

Figure I.12 : Scanner biométrique

Figure I.13 : géométrie de la main

Les systèmes de reconnaissances de la géométrie de la main sont très répandus parce qu'ils sont faciles à utiliser, largement acceptés par le public et relativement peut couteux.
En raison de la taille du système de capture, ce type de technologie est limité à certaines applications. L'inconvénient, c'est que ces systèmes ne peuvent servir qu'à la vérification et non a l'identification. Le taux d'erreurs dans la reconnaissance est assez élevé, en particulier pour des jumeaux ou d'autres membres de la même famille en raison d'une forte ressemblance. De plus la forme de la main évolue avec l'âge.

I.10.7 La dynamique de frappe sur un clavier :

La dynamique de frappe est l'étude de caractéristiques biométriques extraites à partir d'une analyse de la manière dont un utilisateur utilise un périphérique à touches (clavier d'ordinateur, téléphone portable…) afin de différencier des individus.

L'analyse de la dynamique de frappe est apparue bien avant les ordinateurs et les claviers. En effet, dès l'époque du télégraphe, les opérateurs étaient capables de se reconnaître simplement grâce au rythme avec lequel ils envoyaient les impulsions en Morse **[14].** Les premiers travaux qui ont démontré qu'il a été possible de différencier les individus à partir de leur façon de taper aux claviers sont apparus aux années 1980.

Un système basé sur la dynamique de frappe au clavier est un dispositif logiciel qui calcule le temps ou un doigt effectue une pression sur une touche et le temps ou un doigt est dans les airs (entre les frappes). Cette mesure est capturée environ mille fois par seconde. La séquence

de frappe est prédéterminée sous la forme d'un mot de passe. Initialement l'utilisateur doit composer son mot de passe à quelques reprises afin que soit constitué un gabarit de référencé.

Figure I.14 : dynamique de frappe au clavier

Il est probable que suivant la configuration des touches, et suivant le style de clavier le profil de dynamique de frappe évolue lors d'un changement de clavier entraînant ainsi une difficulté supplémentaire.
Cette méthode présente l'avantage de permettre une identification continue de l'utilisateur et de détecter un changement d'utilisateur en temps réel et de façon transparente.

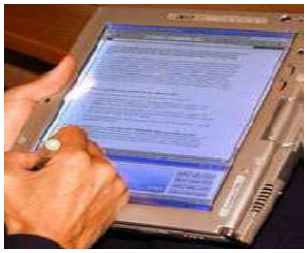
I.10.8 La signature :

La signature est depuis plusieurs siècles le moyen le plus répandu pour manifester sa propre volonté. Signer un document pour s'identifier est un geste naturel pour tout le monde. Dans la vie de tous les jours, nous signons régulièrement des documents. Chaque personne possède une signature qui lui est propre et qui peut donc servir à l'identifier. La reconnaissance de la signature est une des techniques biométriques comportementales.

Il existe deux modes de reconnaissance : le mode statique et le mode dynamique. Le mode statique n'utilise que de l'information géométrique de la signature. Le mode dynamique utilise à la fois l'information géométrique et dynamique, c'est-à-dire les mesures de vitesse, d'accélération, etc. Le mode dynamique est plus riche en information que le mode statique et donc plus discriminant.

Dans le système d'identification par la signature, l'utilisateur doit signer avec un stylo lecteur sur une tablette graphique (ou équivalent voir la **figure I.15**). Ce dispositif va mesurer plusieurs caractéristiques lors de la signature, tel que la vitesse, l'ordre des frappes, la pression et les accélérations, le temps total, etc.






PDA **ANOTO** **Tablet PC** **Tablette Graphique**

Figure I.15 : Illustrations des supports d'acquisition de signatures

La signature à l'avantage par rapport aux autres mesures biométriques d'être couramment utilisée pour les transactions. Pour cette raison, la considération de la signature comme moyen d'identification est en général bien acceptée. Le problème de la reconnaissance par signature provient de la très grande variabilité qui existe entre deux occurrences de la signature d'un même individu.

I.10.9 Le visage :

De nos jours la méthode de reconnaissance de visage est la plus populaire et acceptable parce que on peut l'utiliser à distance sans la collaboration avec l'objet. Ces systèmes utilisent des appareils photo ou des cameras comme moyens de capture d'images. La personne à identifier doit se positionner devant l'appareil ou bien en mouvement à une certaine distance, donc la prise de photo d'une personne peut être volontairement ou involontairement. Pour cela cette technique est utilisée dans les applications de contrôle des frontières, la sécurité des établissements, les zones urbaines et l'identification des conducteurs.

Les caractéristiques sur lesquels se base le système pour l'identification d'une personne sont : la forme du visage, l'écartement des yeux, la position des oreilles, les coins de la bouche et sa taille, etc... Ces systèmes doivent prendre en considération les changements d'une personne (barbe, moustaches, lunette, maquillage, etc…).

La difficulté de cette technique varie selon que l'environnement soit contrôlé ou non. Dans un environnement contrôlé les paramètres tels que l'arrière plan, la direction et l'intensité des sources lumineuses, l'angle de la prise de vue, la distance de la caméra par rapport à la personne sont pris en considération par le système. Dans un environnement non-contrôlé, une série de pré-traitements sont souvent nécessaires avant de faire la reconnaissance proprement

parlé. Il faut tout d'abord détecter la présence ou l'absence de visage dans l'image (face detection). Le visage doit ensuite être segmenté (face segmentation). Enfin, si nous travaillons sur un flux vidéo, le système doit suivre le visage d'une image à l'autre (face tracking).

Figure I.16 : appareil de reconnaissance du visage

I.10.10 Les réseaux veineux :

Ce système a été inventé par l'ingénieur britannique Joe Rice en 1984**[15].** La biométrie des réseaux veineux repose sur la reconnaissance de l'entrelacement des vaisseaux sanguins du doigt ou de la main qui sont unique pour chaque personne. Cette technologie est qualifiée de « sans trace » du fait qu'il n'y a pas de contacte directe du lecteur avec la peau du doigt ou de la main. Ce qui signifie que l'empreinte n'est pas laissée sur le lecteur comme l'empreinte digitale, elle est donc difficile à obtenir pour un imposteur. Et comme les vaisseaux sanguins sont cachés sous la peau, donc il est impossible de capturer et de copier cette biométrie à l'insu de l'individu.

Ces systèmes fonctionnent tout en illuminant la main ou le doigt avec une lumière infrarouge, le réseau veineux apparaît en noir. Il est enregistré sous forme de "carte d'identité" dans une base de données, et pourra ensuite servir de comparaison lors de l'authentification.

Figure I.17 : appareil pour la reconnaissance des réseaux veineux de la main

Figure I.18 : appareil pour la reconnaissance des réseaux veineux du doigt

I.11 La performance des systèmes biométriques :

Les systèmes biométriques sont utilisés dans plusieurs applications et pour envisager leurs déploiements dans la vie courante, il est nécessaire de les évaluer afin d'estimer leurs performances en utilisation réelle.

L'évaluation de performance des systèmes biométriques est classifiée en trois types différenciés par le niveau de spécificité d'une application **[16]** :

- **L'évaluation technologique :** ne teste que la partie algorithmique du système (extraction des caractéristiques, comparaison et décision).
- **L'évaluation scénario :** teste un système biométrique plus complet comportant aussi le capteur, l'environnement et la population spécifique à l'application testée.
- **L'évaluation opérationnelle :** teste le système biométrique global en condition réelle d'utilisation.

Les critères d'évaluations de la performance :

La performance des systèmes biométrique se mesure selon plusieurs aspects qui sont plus ou mois important à tester selon l'application **[17][18]:**

- Condition de teste et les capteurs utilisés.
- Le protocole d'acquisition.
- La disposition de la personne.
- Le nombre d'utilisateurs.
- Le nombre d'échantillon par utilisateur.
- Le profil démographique des utilisateurs.
- L'habitude des utilisateurs.
- Les laps de temps séparant l'acquisition.
- La facilité d'usage pour l'utilisateur.
- La sécurité.
- Le cout.
- La fiabilité du système.
- Les nécessités de maintenance.
- Le tau d'erreurs de reconnaissance.

Selon le droit d'utilisation des systèmes biométrique on distingue deux types d'utilisateurs:

- **Les clients** : sont autorisés à utiliser le système ou à pénétrer dans la zone protégée.
- **Les imposteurs** : n'ont aucune autorisation, mais ils essaient d'utiliser le système.

Un système biométrique pendant la phase de décision fait une des quatre décisions suivantes **[19]:**

- Le client est accepté.
- Le client est rejeté : on parle ici de faux rejet (FRR False Rejection Rate).
- L'imposteur est accepté : on parle de fausse acceptation (FAR False Acceptation Rate)
- L'imposteur est rejeté.

La mesure de taux d'erreur :

Les deux mesures FAR et FRR permettent de calculer l'exactitude d'un système biométrique pendant l'authentification. Dans tout système biométrique la signature capturée lors de l'authentification n'est jamais identique à celle qui se trouve dans la base de données du système, alors il en résulte un facteur de ressemblance qui varie entre 0 et 100%. Et la comparaison est faite par rapport à un seuil fixé à l'avance. Si ce seuil est plus petit le système acceptera plus de client donc le taux de FRR diminuera, mais il acceptera aussi les imposteurs d'où l'augmentation du taux de FAR. Et inversement, Si le seuil de décision est plus grand le système rejette plus d'imposteurs donc le taux de FAR diminuera, mais il rejette aussi les clients d'où l'augmentation du taux de FRR. Donc il est impossible de diminuer le FAR et le FRR simultanément.

Pour qu'un système soit plus performent il faut que les taux de FAR et FRR soient égaux à zéro. Comme se n'est jamais le cas, on a considéré la valeur d'égalité de FAR et FRR le point ou le système soit plus performent, et plus cette valeur est petite plus le système est plus performent. De plus puisque la sécurité est le but principal de tout système, il est préférable que le FAR soit le plus petit possible pour que le système soit plus performent.

Le FAR et le FRR se calculent à l'aide des formules suivantes :

$$\textbf{FAR} = \frac{\quad}{\quad}$$

$$\textbf{FRR} = \frac{\quad}{\quad}$$

Un autre taux d'erreur peut être mesuré, c'est le taux d'erreur totale TER qui est le pourcentage d'erreur totale que commet le système par rapport à toutes les comparaisons effectuées.

$$\textbf{TER} = \frac{\quad}{\quad}$$

On fait varier le seuil de décision tout en calculant les taux de FAR et FRR on obtient la courbe suivante :

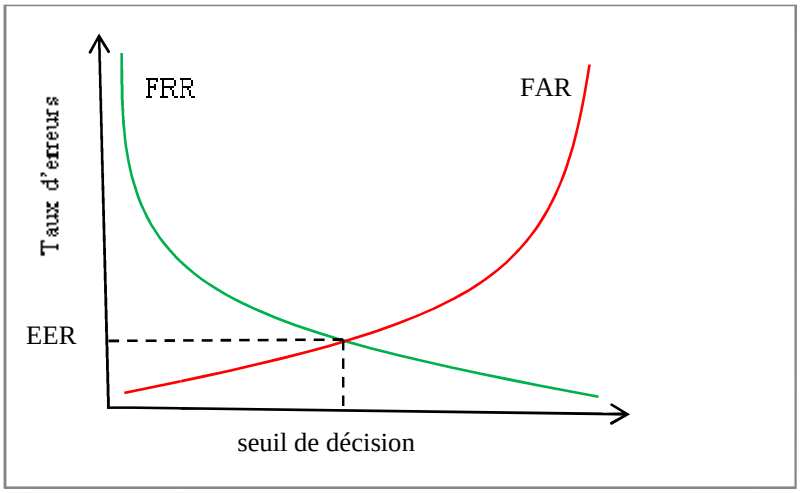


Figure I.19 : Courbe présente la variation de taux de FAR et FRR en fonction du seuil de décision [17]

L'authentification est un problème de décision peut être formulé de la manière suivante :

Soient les hypothèses suivantes :

H_0 « la capture C provient d'un imposteur ».

H_1 « la capture C provient d'un client ».

on considère que la capture C provient d'un client si on a $\mathbf{P(H_1/C) > P(H_0/C)}$.

En appliquant la loi de Byes :

$$\frac{\mathbf{P(C/H1)P(H1)}}{\boldsymbol{P(C)}} > \frac{\mathbf{P(C/H0)P(H0)}}{\boldsymbol{P(C)}}$$

On obtient

$$\frac{\mathbf{P(C/H1)}}{\mathbf{P(C/H0)}} > \frac{\mathbf{P(H0)}}{\boldsymbol{P(H1)}}$$

Sachant que $P(H_0)$ et $P(H_1)$ représentent respectivement les probabilités qu'un imposteur ou un client accède au système et qui sont des valeurs difficiles à estimer.

I.12 Comparaison des techniques biométriques :

Il existe plusieurs techniques biométriques et elles sont utilisées dans diverses applications. Chaque technique biométrique a ses forces et faiblesses, et le choix dépend de l'application. Aucune technique biométrique ne répond efficacement aux exigences de toutes les applications. En d'autres termes, aucune technique biométrique n'est optimale.

L'applicabilité d'une technique biométrique spécifique dépend fortement des conditions du domaine d'application. Par exemple, il est bien connu que la technique basé sur l'empreinte digitale est plus précises que la technique basé sur la voix. Cependant, dans une application de transaction bancaire à distance, la technique basée sur la voix peut être préférée puisqu'elle peut être intégrée dans le système de téléphone existant **[20].**

La figure I.20 montre une comparaison des techniques biométriques en fonction de cout et de la précision.

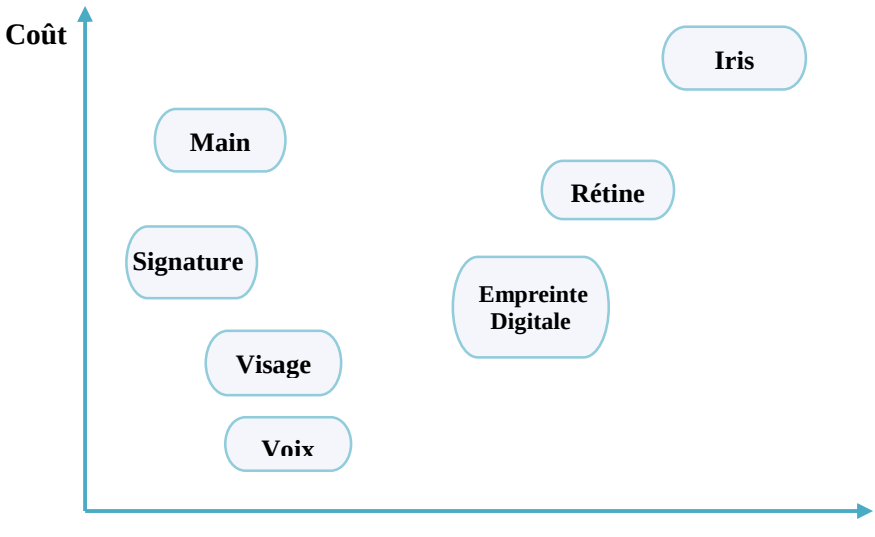


Figure I.20 : Les biométries les plus utilisées en fonction du Coût et la Précision [21]

Les avantages et les inconvénients des techniques biométriques les plus utilisées sont donnés par le tableau suivant :

Technique	Avantages	Inconvénients
Empreintes digitales	Coût Ergonomie moyenne Facilité de mise en place Taille de capteur	Qualité optimale des appareils de mesure Acceptabilité moyenne Possibilité d'attaque(rémanence de l'empreinte,…)
Forme de la main	Très bonne ergonomie Bonne acceptabilité	Système encombrant et couteux Perturbation possible par des blessures et l'authentification des membres d'une même famille
Visage	Coût Peut encombrant Bonne acceptabilité	Jumeau Psychologie, Déguisement Vulnérable aux attaques
Rétine	Fiabilité, Pérennité	Coût Acceptabilité faible Installation difficile
Iris	Fiabilité	Acceptabilité très faible Contrainte d'éclairage
Voix	Facile	Vulnérable aux attaques
Signature	Ergonomie	Dépendant de l'état émotionnel de la personne Fiabilité
Frape au clavier	Ergonomie	Dépendant de l'état physique de la personne

Tableau I.2 : Avantages et inconvénients des techniques biométriques [22]

Méthodes	Utilisation %	Nombre de points mesurables	fiabilité
Empreintes digitales	50	(80)	Assez bonne
Reconnaissances faciales	15	Selon la photo	Variable
Reconnaissance de la main	10	(90)	Bonne
Iris	6	(224)	Proche de 99%
Signature	< 5	Selon la signature	Variable
Voix	Peu utilisée	Dépend des bruits de fond	Peut fiable
Rétine	Rare	400	Excellente

Tableau I.3 : Tableau récapitulatif des principales techniques [23]

D'après la figure I.20 et le tableau I.2 et le tableau I.3 on remarque que les systèmes biométriques basées sur les empreintes digitales sont les plus utilisés dans le monde, et cela grâce a leur grande précision et un coût réduit, néanmoins ils souffrent de possibilités d'attaque et d'une acceptabilité moyenne de la part de la population. Ce qui démontre bien qu'aucun système biométrique quel qu'il soit n'a encore réussi à atteindre la perfection recherché. Pour ces raisons la recherche est encore très active dans ce domaine.

I.13 La multimodalité :

La multimodalité est l'utilisation de plusieurs systèmes biométriques. En effet, l'utilisation de plusieurs systèmes a pour but premier d'améliorer les performances de reconnaissance. En augmentant la quantité d'informations discriminante de chaque personne, on souhaite augmenter le pouvoir de reconnaissance du système. De plus, le fait d'utiliser plusieurs modalités biométriques réduit le risque d'impossibilité d'enregistrement ainsi que la robustesse aux fraudes **[18].**

Les différentes multimodalités possibles

On peut différencier 5 types de systèmes multimodaux selon les systèmes qu'ils combinent (Figure I.21) **[18]**:

- ***multi-capteurs*** lorsqu'ils associent plusieurs capteurs pour acquérir la même modalité, par exemple un capteur optique et un capteur capacitif pour l'acquisition de l'empreinte digitale.
- ***multi-instances*** lorsqu'ils associent plusieurs instances de la même biométrie, par exemple l'acquisition de plusieurs images de visage avec des changements de pose, d'expression ou d'illumination.
- ***multi-algorithmes*** lorsque plusieurs algorithmes traitent la même image acquise, cette multiplicité des algorithmes peut intervenir dans le module d'extraction en considérant plusieurs ensembles de caractéristiques et/ou dans le module de comparaison en utilisant plusieurs algorithmes de comparaison.
- ***multi-échantillons*** lorsqu'ils associent plusieurs échantillons différents de la même modalité, par exemple deux empreintes digitales de doigts différents ou les deux iris. Dans ce cas les données sont traitées par le même algorithme mais nécessitent des

références différentes à l'enregistrement contrairement aux systèmes multi-instances qui ne nécessitent qu'une seule référence.

- ***multi-biométries*** lorsque l'on considère plusieurs biométries différentes, par exemple visage et empreinte digitale.

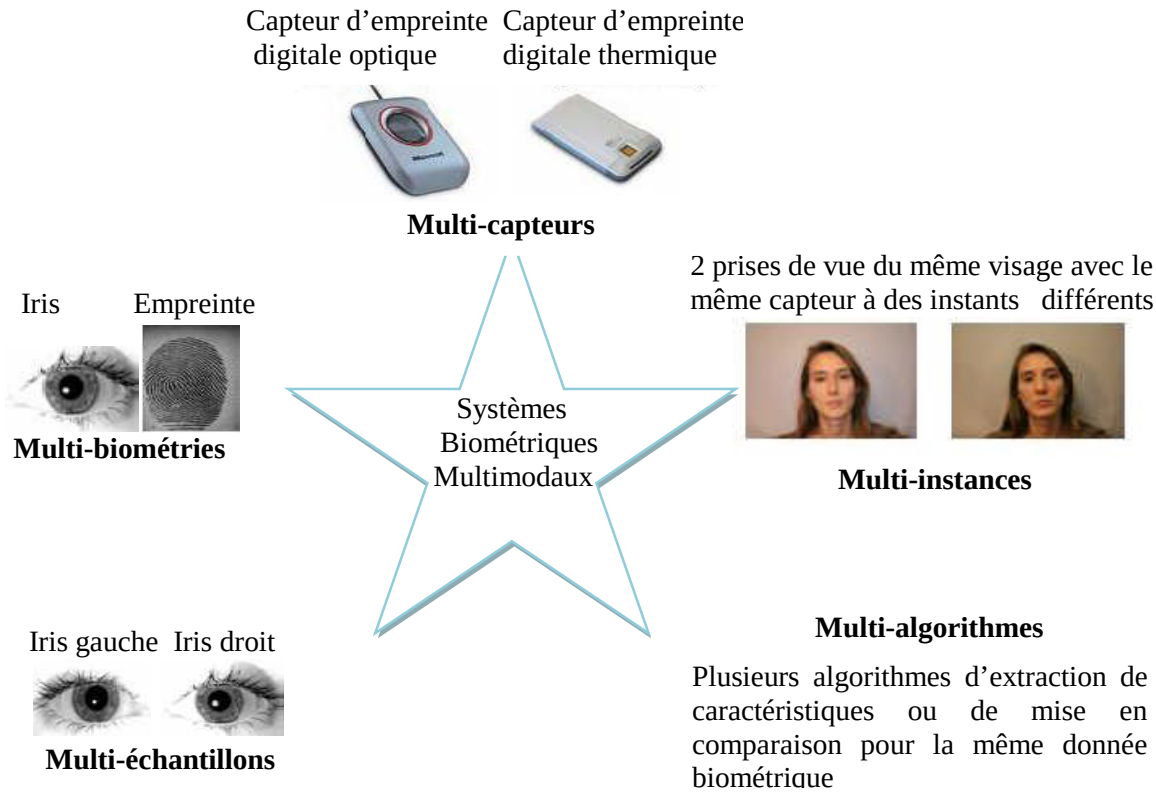


Figure I.21 : Les différents systèmes multimodaux

I.14 Conclusion :

Dans ce chapitre nous avons étudié le concept de la biométrie, tout en abordant la définition, les intérêts de la biométrie, une comparaison entre l'authentification par la biométrie et l'authentification par les moyens classique, les applications des systèmes biométrique, l'architecture des systèmes biométriques, les types de la biométrie ainsi que ses différentes modalités et la performance des systèmes biométriques.

La biométrie présente plusieurs modalités qui participe chacune dans des applications de sécurité avec un certain niveau de performance. Ces différentes biométries ne sont pas toutes

acceptées par le grand public du fait des contraintes du contacte avec les lecteurs comme l'iris.

La reconnaissance du visage est l'une des biométries les plus utilisées et qui consiste à reconnaitre les personnes par leurs visages. Ce qui fera l'objet du chapitre suivant.

II.1 Introduction :

La reconnaissance des visages a été développée par Benton et Van Allen en 1968 [24]. L'utilisation des techniques de reconnaissance faciale a connu un développement à grande échelle depuis le milieu des années 90, avec l'utilisation efficace de nouvelles technologies, notamment l'ordinateur et sa capacité de traitement d'images ce qui lui a donné des nouvelles applications, le contrôle de l'identité sous toutes ses formes. De plus, l'existence de bases de données de grande taille ont permis de mettre au point des algorithmes et des approches de plus en plus complexes et par conséquent, les performances de reconnaissance se sont trouvées améliorées.

II.2 Pourquoi choisir le visage ?

La reconnaissance faciale, en tant qu'une des technologies biométriques de base, a pris une part de plus en plus importante dans le domaine de la recherche, ceci étant dû aux avances rapides dans des technologies telles que les appareils photo numériques, Internet etc.

Malgré que certains disent que la reconnaissance des visages est une biométrie relativement peu sûre, sur le fait que le signal acquis est sujet à des variations beaucoup plus élevées que d'autres caractéristiques, comme la variation de l'éclairage, le changement de la position du visage, la présence ou l'absence de lunettes et autres, mais au cours de ces dernières années plusieurs techniques de traitements d'images sont apparues, telle que la détection du visage, la normalisation de l'éclairage, etc. Sans oublier le développement considérable des technologies des caméras numériques, ce qui néglige l'effet de ces problèmes.

La reconnaissance faciale possède plusieurs avantages sur les autres technologies biométriques : elle est naturelle, non intrusive et facile à utiliser, en plus les capteurs utilisés sont peu coûteux (une simple caméra), faciles à installer et acceptés 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, contrairement à l'empreinte digitale et l'iris où le sujet devra être très proche du capteur et devra coopérer pour l'acquisition de l'image sans oublier le coût de l'équipement nécessaire pour l'acquisition (équipement spécial coûteux). Appuyé par une deuxième place dans l'industrie de la biométrie avec une part de 15% du marché derrière l'empreinte digitale, la reconnaissance du visage s'avère le bon compromis entre le coût et la précision.

II.3 La reconnaissance automatique de visages :

Un système automatique de reconnaissance de visages est un système biométrique utilisant le visage à des fins d'identification et/ou de vérification de personnes à partir de leurs images de visages fixes (à l'aide d'un appareil photo) ou dynamique (séquences vidéo, à l'aide d'une camera) en comparant les caractéristiques de cet individu avec celles stockées dans une base de référence.

Ce système doit intégrer une étape d'apprentissage durant la quelle il associe l'allure du visage à l'identité d'une personne. Cette étape permet de construire une base de données des personnes connues, stockant des images étiquetées des identités.

Pour ce faire, un système automatique comporte deux modes de fonctionnement : un mode enrôlement et un mode identification. Le premier mode sert à extraire pour chaque personne les éléments caractéristiques et les met sous la forme d'un vecteur caractéristique, appelé par la suite signature. Cette dernière, associée à une étiquette d'identité, sera stockée dans une base de données dédiée. Le mode d'identification permet de reconnaitre une personne à partir de son image faciale, c'est-à-dire de retrouver l'identité associée à l'image.

Nous présentons dans la figure suivante une illustration générale d'un système de reconnaissance de visages dans ces deux modes de fonctionnement.

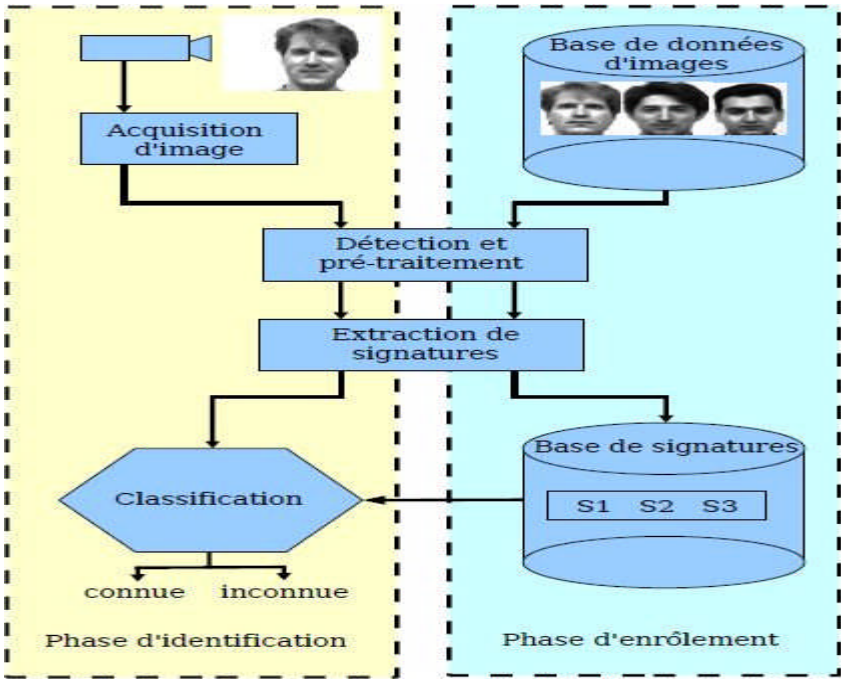


Figure II.1 : fonctionnement d'un système de reconnaissance automatique de visages [25].

Le système comporte deux modules qui appliquent les mêmes traitements dans les deux modes de fonctionnement.

Le premier module permet de détecter le visage dans l'image brute captée par le système d'acquisition ainsi que d'éliminer les parasites causés par la qualité des dispositifs optiques ou électroniques dans le but de ne conserver que les informations essentielles, il fournit ainsi au second module une image contenant seulement le visage. A partir de celle-ci, le second module extrait la signature discriminante et non redondante. Ce module constitue l'étape clé du processus de reconnaissance, car les performances du système entier dépendent de la précision avec laquelle les informations utiles sont extraites. La signature sera par la suite soit stockée soit utilisée pour la classification (distance de Mahalanobi). En mode hors-ligne (enrôlement), elle sera stockée dans une base de données dédiée. En mode enligne (identification), elle servira comme entrée à un troisième module qui s'occupe de la classification de cette signature et de fournir la décision finale : personne inconnue ou personne connue et qui ?

II.4 Principales difficultés de la reconnaissance de visage :

La reconnaissance faciale est une tâche que les humains effectuent naturellement et sans effort dans leurs vies quotidiennes. Ils peuvent 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 (conditions d'éclairage, d'expression faciales et d'orientations).

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. Les variations d'éclairage rendent la tâche de reconnaissance de visage très difficile. En effet, le changement d'apparence d'un visage du 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. La variation d'illumination constitue un défi majeur pour la reconnaissance faciale.

Figure II.2. Exemple de variation d'éclairage.

2. Variation de pose :

Le taux de reconnaissance de visage baisse considérablement quand des variations de pose sont présentes dans les images. La variation de pose est considérée comme un problème majeur pour les systèmes de reconnaissance faciale. Quand le visage est de profil dans le plan image (orientation < 30°), il peut être normalisé en détectant au moins deux traits faciaux (passant par les yeux). Cependant, lorsque la rotation est supérieure à 30°, la normalisation géométrique n'est plus possible [26].

Figure II.3 : Exemples de variation de poses.

3. Expressions faciales :

L'expression faciale modifie l'aspect du visage, elle entraîne forcément une diminution du taux de reconnaissance. 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.

Figure II.4 : Exemples de variation d'expressions.

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. Par exemple, une moustache ou une barbe modifie la forme du visage.

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 de visage, les systèmes proposés sont 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.

II.5 Les méthodes d'extraction des caractéristiques du visage :

L'étape de décision dans les systèmes de reconnaissance repose sur les différentes caractéristiques extraites de l'image du visage. Pour cela plusieurs méthodes d'extraction des caractéristiques ont été développées et qui sont subdivisées en trois catégories : les méthodes globales, les méthodes locales, les méthodes hybrides. Chacune de ces méthodes repose sur une représentation particulière du visage.

II.5.1 les méthodes locales :

Ce sont des méthodes géométriques, appelées aussi les méthodes à trais, à caractéristiques locales ou analytiques. Elles se basent 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, comme les yeux, le nez, la bouche, etc...

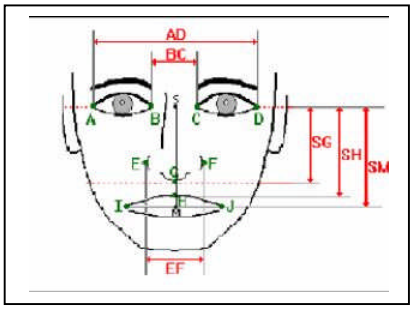


Figure II.5 : distances entre points caractéristiques

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 [27].

Les méthodes locales peuvent être classées en [26] :

- **Méthodes géométriques :** Elles sont basées sur l'extraction de la position relative des éléments qui constituent le visage (tel que le nez, la bouche et les yeux). La plupart des approches géométriques utilisent des points d'intérêt (comme les coins de la bouche et des yeux).
- **Méthodes graphiques :** elles se basent sur la représentation graphique des caractéristiques locales du visage.

Parmi ces méthodes on cite :

II.5.1.1 Elastic Bunch Graph Matching (EBGM) :

L'algorithme EBGM est né des travaux de Wiskott et al. de la Southern California University (USC, USA) et de la Rurh University (Allemagne) en 1997[28]. Il se base sur l'application d'un treillis élastique virtuel sur le visage en reliant ses points caractéristiques localisés manuellement ou automatiquement. Pour chaque point on associe un jeu de coefficients d'ondelettes complexes de gabor appelés jet.

Pour effectuer une reconnaissance avec une image test, on fait une mesure de similarité entre les différents Jets et les longueurs des segments du treillis de deux images.

Un Jet est basé sur une transformée en ondelettes [29], défini comme la convolution d'une image avec une famille de noyaux de Gabor.

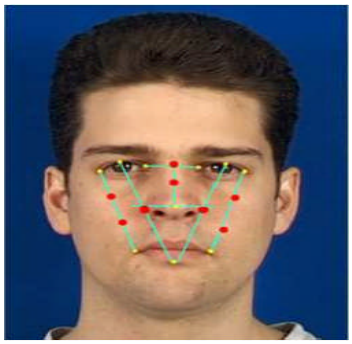


Figure II.6 : localisation des points caractéristique

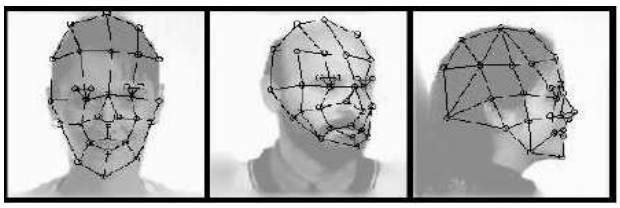


Figure II.7 : création du treillis

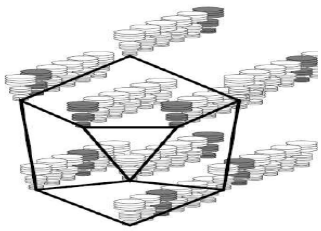


Figure II.8 : face Bunch Graph

II.5.1.2 La méthode de Markov caché (HMM) :

Hidden Markov Models [30] sont un ensemble de modèles statistiques utilisés pour caractériser les propriétés statistiques d'une image. L'image est divisée en N régions significatives qui sont, par exemple pour le visage, les cheveux, le front, les yeux, le nez et bouche. Chacune de ces régions est ensuite assignée à un état Si dans un HMM 1D :

S_1 ⟶ bouche

S_2 ⟶ nez

S_3 ⟶ yeux

S_4 ⟶ front

S_5 ⟶ cheveux

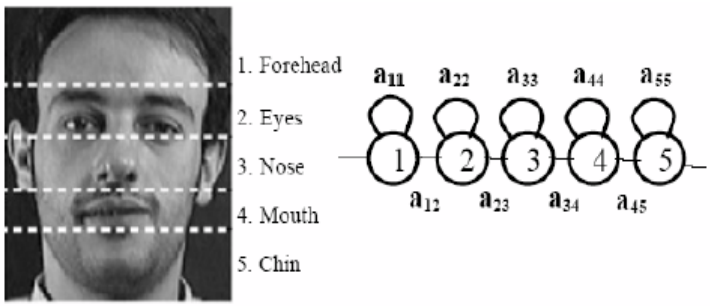


Figure II.9 : les 5 états du HMM de haut en bas d'une image du visage.

Un modèle de Markov caché (HMM) représente de la même façon qu'une chaîne de Markov un ensemble de séquences d'observations dont l'état de chaque observation est associé à une fonction de densité de probabilité. La probabilité de chaque état ne dépend que de l'état qui le précède immédiatement.

La reconnaissance est effectuée en assortissant une image de teste contre chaque modèle d'apprentissage (chaque HMM présente une personne différente). Et dans la fin de cette procédure, l'image est convertie en une séquence d'observation et la probabilité est calculée pour chaque modèle enregistré. Le modèle avec la probabilité la plus élevée indique l'identité de la personne inconnue [31] [32].

Le but de l'étape d'apprentissage est d'optimiser les paramètres pour mieux décrire l'observation.

II.5.2 Les méthodes globales ou holistiques :

Sont des méthodes basées sur la surface entière du visage comme entrée à l'algorithme de reconnaissance, sans tenir en compte les caractéristiques locales (yeux, bouche, etc…), et s'appuient sur des propriétés statistiques bien connues et utilisent l'algèbre linéaire.

Chaque image du visage est vue comme une matrice (n,m) de valeurs de pixels qui peut être transformé en vecteur de dimension (n*m), plus facile à manipuler. Ces méthodes sont rapide à mettre en œuvre et les calcules sont de complexité moyenne. Ainsi qu'elles sont très sensibles aux variations d'éclairage et d'expressions faciales, du fait qu'elle manipule directement les pixels de l'image.

II.5.2.1 Analyse en composante principale (ACP):

L'algorithme ACP est né des travaux de MA. Turk et MP. Pentland, en 1991[33]. Il est connu sous le nom d'eigenface, car il utilise des valeurs et des vecteurs propres, respectivement (eigenvalues, eigenvectors). Le but de l'ACP et de réduire l'espace de données de sorte à obtenir un sous espace de dimension raisonnable, tel que la projection sur ce dernier tient plus d'informations possible les plus précises.

L'ACP est utilisé pour représenter efficacement les images de visages tout en les projetant sur l'espace des visages propres (eigenface). Ces derniers sont des images de la même taille que les images de l'apprentissage qui montrent des visages ayant un aspect fantomatique. Mathématiquement ils sont les vecteurs propres de la matrice de covariance des images d'apprentissage. Chaque image d'apprentissage peut être présentée en termes de combinaison linéaire des eigenfaces et de l'image moyenne [31]. Son principe est de réduire les **P** variables de **n** individus en **M** (M<=P) composantes indépendantes.

Figure II.10 : exemple d'Eigenface

II.5.2.2 Analyse Linéaire Discriminante :

L'algorithme LDA est né des travaux de *Belhumeur et al.* de l'Université Yale (New Haven, USA), en 1997 [34]. Il est aussi connu sous le nom de *Fisherfaces*. Il permet de projeter les images dans un espace de dimension réduite de la même façon que les Eigenfaces, tout en effectuant une séparation des classes des images, chaque individu dans sa classe avec plusieurs images de cet individu.

LDA est une technique qui cherche les directions efficaces pour la discrimination entre les données. Elle est connue pour sa minimisation de l'éparpillement intra classe (les images du même individu), et sa maximisation de l'éparpillement inter classe (les images des différents individus).

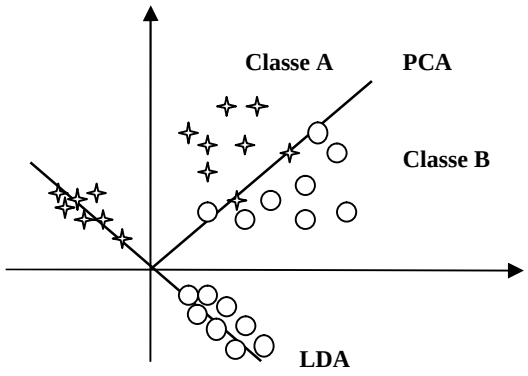


Figure II.11 : la projection PCA et LDA d'un ensemble de données [35]

II.5.2.3 Réseau de Neurones Artificiels :

Le réseau de neurones artificiels ou RNA est l'assemblage fortement connectés d'unités de calcul. Chacune des unités de calcul est un neurone formel qui est, en soit, une formule mathématique ou un modèle simplifié d'un neurone biologique. On classe généralement les réseaux de neurones en deux catégories: les réseaux faiblement connectés à couches que l'on appelle des réseaux «feedforward » ou réseaux directs et les réseaux fortement connectés que l'on appelle des réseaux récurrents. Dans ces deux configurations, on retrouve des connexions totales ou partielles entre les couches. Les réseaux de neurones peuvent être utilisé tant pour la classification, la compression de données ou dans le contrôle de systèmes complexes en automatisme.

L'idée est d'identifier à partir d'exemples un visage De manière plus formelle, l'apprentissage du réseau à pour but l'extraction des informations pertinentes [36] à l'identification. Une image brute (ou prétraitée) de dimensions fixes constitue habituellement la source d'entrée des réseaux. Les dimensions doivent être établies au préalable car le nombre de neurones sur la couche d'entrée en dépend. Le nombre de sorties du réseau dépend par ailleurs directement de la quantité d'individus à discriminer.

II.5.2.4 Les Séparateurs à vaste marges (SVM) :

SVM (Support Vector Machines) est une nouvelle technique d'apprentissage statistique, proposée par V. Vapnik en 1995. Elle permet d'aborder des problèmes très divers comme le classement, la régression, la fusion,…etc.

Depuis son introduction dans le domaine de la Reconnaissance de Formes (RdF), plusieurs travaux ont pu montrer l'efficacité de cette technique principalement en traitement d'image. L'idée essentielle consiste à projeter les données de l'espace d'entrée (appartenant à des classes différentes) non linéairement séparables, dans un espace de plus grande dimension appelé espace de caractéristiques, de façon à ce que les données deviennent linéairement séparables [37].

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

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

II.5.3 Les méthodes hybrides :

Sont des méthodes fusionnant les deux types précédents d'une manière à combiner leurs avantages et éviter les inconvénients afin d'améliorer les performances des systèmes de reconnaissance. Plusieurs fusions ont été proposées dont on trouve :

La fusion de trois classificateurs individuels faite par Acherman et Bunke, qui sont HMM et PCA pour les poses de visage frontal et le classificateur de forme sur des vues profil. Le taux maximum des résultats est de 97,7% contre 94,7% pour la PCA qui a donné le meilleur résultat individuellement parmi les autres classificateurs [38].

Nous avons vus quelques méthodes appliquées pour l'extraction des caractéristiques du visage et la reconnaissance des individus. Chaque méthode a un pourcentage de réussite et d'échec. Nous allons présenter la méthode que nous allons utiliser dans notre application qui est l'ACP.

II .6 L'Analyse en composante principale :

Introduction :

On dispose d'un nuage de points (données) dans un espace de dimension élevée, duquel on ne peut extraire l'information utile à l'analyse.

L'ACP (PCA pour Principal Component Analysis, en anglais) nous donnera un sous-espace de dimension inferieur, tel que la projection de données sur ce dernier retienne le plus d'information possible et que les données serait le plus dispersé possible.

Le contexte dans lequel on applique cette technique est le suivant : on observe sur n individus p variables explicatives $X_1, X_2, X_3, \ldots\ldots, X_p$ quantitatives, présentant des relations multiples qu'on veut analyser. Dans ce but, on désire réduire la dimension de ces données (réduire la complexité des calculs) et les rendre indépendants pour une interprétation simple et efficace. La PCA permet de résumer l'information apportée par ces P variables en M composantes indépendantes (M ≤ P) en la détruisant le moins possible.

L'ACP se base sur la matrice de covariance entre les variables pour trouver le sous-espace optimal pour représenter les données. Ainsi les composantes principales obtenues sont la projection des variables dans le nouvel espace.

Donc, son idée principale est de chercher la plus précise des représentations (projections) dans un sous-espace de dimension inférieure.

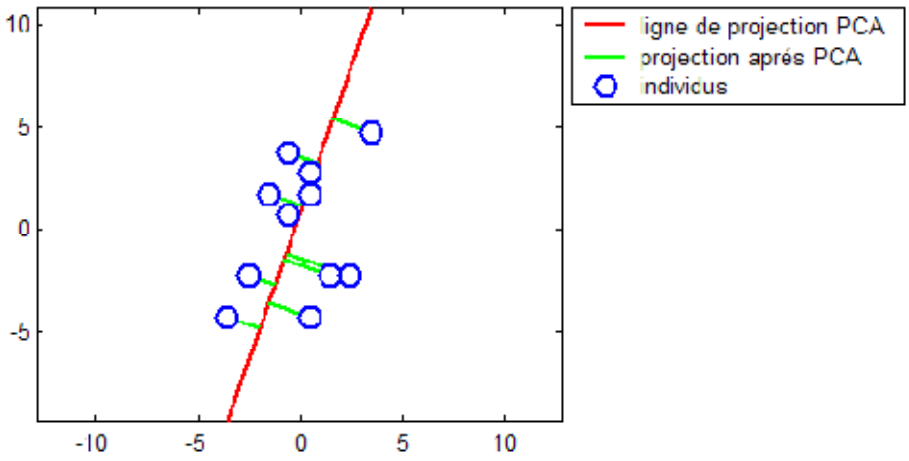


Figure II.12: Exemple de projection suivant PCA

II.6.1 Principe mathématique de la PCA :

On considère un vecteur **X** représentant une distribution de n données de dimension p (p variable explicatives) :

$$X = [X_1\ X_2\ X_3\ \ldots X_i \ldots X_n]$$

On désire représenter le plus exact possible cette distribution dans un espace E de dimension k ($k \leq p$) et tel qu'en sortie on aura les données indépendantes entre elles (matrice de covariance diagonale).

Soit $Y = [Y_1\ Y_2\ Y_3\ \ldots Y_i \ldots Y_n]$ la projection de X à travers W la matrice de projection, dans le nouveau sous-espace, alors $Y=W^T X$ (W^T est la matrice transposée de W).

Ainsi le problème est de trouver **W** tel que la matrice de covariance de **Y** soit diagonale (assurer l'indépendance des données) et avoir une concentration des données pour permettre la réduction de dimensionnalité.

Notons par $\sum X$ la matrice de covariance de X ($\sum X = XX^T$ avec X centré à sa moyenne), $\sum Y$ celle de **Y** et par **Λ** la matrice des valeurs propres de $\sum X$.

La PCA résout ce problème par la diagonalisation de $\sum X$, ce qui revient à calculer les vecteurs propres et valeurs propres de cette dernière et donc $\sum X\ \boldsymbol{W} = \Lambda\mathbf{W}$.

La matrice de projection **W** sera celle des vecteurs propres de $\sum X$.

On a :

dim(**X**) = (p*n). (dim (**X**) désigne la dimension de **X**)

dim(**Y**) = (p*n).

dim(**W**) = (p*p).

dim (**Λ**) = (p*p).

On peut choisir que k vecteurs propres de W (réduction de dimensionnalité), avec $k \leq p$ et donc Y aura k composantes principales (lignes) et W aura k colonnes (vecteurs propres).

Et donc :

$$\sum \boldsymbol{Y} = \boldsymbol{Y}\boldsymbol{Y}^{\boldsymbol{T}} = \boldsymbol{W}^{\boldsymbol{T}}\,\boldsymbol{X}\,\boldsymbol{X}^{\boldsymbol{T}}\,\boldsymbol{W} = \boldsymbol{W}^{\boldsymbol{T}}\sum \boldsymbol{X}\;\;\boldsymbol{W}$$

$\sum \boldsymbol{Y}$ est la rotation de $\sum \boldsymbol{X}$ par W.

On a aussi : $\sum \boldsymbol{X}\;\boldsymbol{W} = \boldsymbol{\Lambda}\,\boldsymbol{W} \Rightarrow \sum \boldsymbol{Y} = \boldsymbol{W}^{\boldsymbol{T}}\boldsymbol{\Lambda}\boldsymbol{W} = \boldsymbol{\Lambda}\boldsymbol{W}\boldsymbol{W}^{\boldsymbol{T}} = \boldsymbol{\Lambda}$, en effet $\sum \boldsymbol{Y}$ est la matrice des valeurs propres de $\sum \boldsymbol{X}$ et donc diagonale, ainsi la variance de chaque composante principale est maximisée à la valeur propre correspondante et elle est indépendante des autres k-1 composantes restantes.

II.6.2 Quelques Propriétés de la PCA :

II.6.2.1 Concentration de l'information et réduction de dimensionnalité :

Soit le vecteur $X = (X_1, X_2, X_3, \ldots\ldots, X_p)$ de matrice de covariance $\sum X$ avec les paires de valeurs propres vecteurs propres $(\lambda_1, \boldsymbol{e_1}), (\lambda_2, \boldsymbol{e_2}), \ldots, (\lambda_p, \boldsymbol{e_p})$ et $\lambda_1 \geq \lambda_2 \geq \lambda_3 \ldots \geq \lambda_p$, alors on a :

La variance totale de la population est égale à :

$$\sum_{I=1}^{P} Var(X) = trace\left(\sum X\right) = trace(W\Lambda W^T) = trace(\Lambda) = \lambda_1 + \lambda_2 + \cdots + \lambda_p$$

Ainsi la proportion de la variance totale expliqué par la k-ième composante est égale à :

$$\frac{\lambda_k}{\lambda_1 + \lambda_2 + \cdots + \lambda_p}$$

Et donc on peut réduire la dimensionnalité en gardant que les vecteurs propres correspondant aux valeurs propres suffisamment grandes. Pour cela, on prend m valeurs propres nécessaire pour une réduction sans perte d'information considérable, tel que :

$$\frac{\lambda_1 + \lambda_2 + \cdots + \lambda_m}{\lambda_1 + \lambda_2 + \cdots + \lambda_p} \geq 95\%$$

II.6.2.2 Indépendance de l'information :

Puisque $\sum \boldsymbol{y}$ est diagonale alors la $cov(y_i, y_j) = 0$ si $i \neq j$ et donc ceci assure l'indépendance des données en sortie. Ce point est capital dans l'analyse des données et en particulier la classification.

II.6.2.3 La PCA et la direction de la variance :

Les λ_i représente les variances dont les composantes principales et leurs valeurs déterminent la direction de la projection grâce aux vecteurs propres correspondants, alors la population en entrée est projetée en direction de la plus grande variance pour obtenir la nouvelle population.

II.6.3 PCA dans la reconnaissance de visages :

L'ACP a été introduite dans la reconnaissance de visages par MA.Turk et MP.Pentland, en 1991[33]. Il est aussi connu sous le nom d'Eigenfaces car il utilise les vecteurs et les valeurs propres (respectivement Eigenvectors et Eigenvalues en anglais).

Le but principal est d'extraire l'information pertinente de l'image visage et la coder le plus efficacement possible puis la comparer avec la base des modèles codés de la même manière.
En terme mathématique, c'est de calculer les composantes principales d'une distribution de visages, par le calcul des vecteurs propres (Eigen Face) de la matrice de covariance de l'ensemble des visages et les ordonnées suivant les valeurs propres correspondantes. Chaque vecteur propre suivant sa valeur propre capturera une grande ou petite variation des visages de la distribution étudiée et l'ensemble de ces vecteurs caractérisent les variations totales des images. Ainsi, ces vecteurs propres représenteront la base de projection des visages dans l'espace propre, soit dans l'apprentissage pour produire les modèles ou dans le test pour pouvoir classifier les images en comparant le modèle test avec ceux de la base d'entrainement.

II.7 Algorithme de reconnaissance PCA:

On considère un ensemble de n images de visages de taille (h, w) telles que chacune d'elles est représentée sous forme de vecteur de taille (h*w, 1). Par analogie à ce qu'on a défini précédemment, Le vecteur **X** de taille (h*w, n), représente la matrice des images d'apprentissage du système tel que chaque colonne est une image et chaque ligne est une valeur de pixel (qui correspond aux variables explicatives dans la PCA) dans l'image correspondante. On décompose l'algorithme en étapes comme suit :

1. Processus d'apprentissage :

1. Chaque image de visage (matrice de pixels) $I_{i_{(h*w)}}$ de l'espace d'apprentissage est transformée sous forme de vecteur colonne $X_{i_{(h*w,1)}}$ (par concaténation des colonnes de la matrice).

$$I_i = \begin{pmatrix} a_{1,1} & \cdots & a_{1,w} \\ \vdots & \ddots & \vdots \\ a_{h,1} & \cdots & a_{h,w} \end{pmatrix} \qquad X_i = \begin{pmatrix} a_{1,1} \\ \vdots \\ a_{h,1} \\ a_{1,2} \\ \vdots \\ a_{h,2} \\ \vdots \\ \vdots \\ a_{h,w} \end{pmatrix}$$

2. On rassemble les n vecteurs images de visages de l'espace d'apprentissage dans une unique matrice X, où chaque colonne représente un vecteur image X_i

$$X = \begin{pmatrix} a_{1,1} & b_{1,1} & \cdots & \cdots & z_{1,1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{h,1} & b_{h,1} & \cdots & \cdots & z_{h,1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{h,w} & b_{h,w} & \cdots & \cdots & z_{h,w} \end{pmatrix}$$

3. On calcule ensuite l'image moyenne Ψ à partir de n images d'apprentissage. Cette image peut être vue comme le centre de gravité du jeu d'images :

$$\Psi = \frac{1}{n}\sum_{I=1}^{n} X_i$$

4. On ajuste ensuite les données par rapport à la moyenne. L'image moyenne est soustraite de chaque image des images d'apprentissage (on élimine donc les

ressemblances pour se concentrer sur les différences), ce qui génère les vecteurs de différences :

$$\Phi_i = X_i - \Psi \quad , \qquad i = 1 \dots n$$

5. La matrice de covariance $\sum X$ est construite ainsi :

$$\sum X = \sum_{i=1}^{N} \Phi_i \Phi_i^T$$

$$\sum X = XX^T$$

La prochaine étape consiste à calculer les vecteurs propres et les valeurs de cette matrice de covariance $\sum X$ de taille (h*w,h*w), c'est-à-dire de l'ordre de la résolution d'une image. Le problème est que cela peut parfois être très difficile et très long ! En effet, si h*w > n (si la résolution est supérieure au nombre d'images), il y aura seulement n − 1 vecteurs propres qui contiendront de l'information (les vecteurs propres restants auront des valeurs propres associées nulles). Par exemple, pour 100 images de résolution 320×240, nous pourrions résoudre une matrice L de 100 × 100 au lieu d'une matrice de 76800 × 76800 pour ensuite utiliser l'algèbre linéaire pour trouver les vecteurs propres de la matrice$\sum X$. Le gain de temps de calcul serait considérable ! Typiquement, nous passerions alors d'une complexité de l'ordre du nombre de pixels dans une image à une complexité de l'ordre du nombre d'images [28].

Nous prenons donc en compte les deux cas suivants (h*w > n) ou (h*w < n) :

6. Cas ou h*w <= n
   - Calculer la matrice de covariance du jeu d'image X : $\sum X = XX^T$
   - Calculer la matrice des vecteurs propres W ordonnées suivant la matrice des valeurs propres $\boldsymbol{\Lambda}$ elle-même triée par ordre décroissant.

   Cas ou h*w > n
   - Calculer la matrice L= $X^T X$ de taille (n*n).
   - Calculer la matrice des vecteurs propres W' ordonnée suivant la matrice des valeurs propres $\boldsymbol{\Lambda}$ elle-même triée par ordre décroissant.
   - Pour revenir au cas normal, on fait cette transformation :

$$W = X * W'$$

Et on normalise les vecteurs propres obtenu (colonne de W) en les divisant par leurs normes euclidienne, ainsi on obtient notre matrice de projection W.

7. Projeter les images dans le nouvel espace qu'on appellera « Espace propre », en faisant :

$$Y = W^T X$$

On peut éventuellement choisir les k premier vecteurs propres dans W au lieu des P vecteurs propres (ou des n vecteurs) résultants des calculs pour réduire la dimensionnalité.

Ainsi nous avons obtenu la nouvelle représentation des images(les modèles) dans l'espace propre en garantissant l'indépendance entre les composantes principales obtenue et par conséquent on peut faire une discrimination.

Avant d'attaquer la phase deux de notre algorithme (processus de reconnaissance), attardons-nous un peut sur l'étape clé de la première phase de l'algorithme qui est l'étape de calcul des vecteurs propres.

En effet il faut d'abord que les vecteurs propres n'ont de sens que pour une matrice carrée, et une matrice carrée de taille (n*n) possède uniquement n vecteur propre (nous prenons la norme du vecteur propre à 1, par convention). Mais voila le problème c'est qu'une matrice qui est juste carrée peut avoir des valeurs et des vecteurs propres complexes ce qui serait vraiment problématique pour notre système. Mais heureusement, l'algorithme PCA recherche les vecteurs propres de la matrice de covariance du jeu d'image d'apprentissage, et on sait que la matrice de covariance est une symétrique ($mat=mat^T$), cette propriété représente un gros avantage du fait qu'il est mathématiquement définit qu'une matrice symétrique possède des valeurs et des vecteurs propres réelles [39].

La matrice étant symétrique le calcul des vecteurs propres se trouve accélérer grâce à des algorithmes qui prenne en compte cette propriété de symétrie. Dans notre système nous avons utilisé le célèbre algorithme de Jacobi qui utilise une suite de rotations orthogonales sur la matrice en entrée pour trouver une nouvelle base ou cette matrice sera diagonale, la matrice diagonale ainsi obtenu est la matrice des valeurs propres de la matrice en entrée, et la matrice de passage vers la nouvelle base est la matrice des vecteurs propres[40].

2. Processus de reconnaissance :

Lorsqu'un visage est présenté au système, la procédure d'identification consiste à :

1. l'image d'entrée $I_{i_{(h*w)}}$ contenant le visage à identifier est transformée en un vecteur $X_{i_{(h*w,1)}}$, qu'on nomme **Test.**
2. On soustrait l'image moyenne de l'image d'entrée.

$$\Phi_i = X_i - \Psi$$

3. Par la suite l'image d'entrée normalisée est Projetée dans l'espace des visages propres **Test-propre=W^T*Test.**
4. Comparer suivant qu'on est dans une identification ou une vérification avec les modèles obtenus dans l'apprentissage. La comparaison se fait par le calcul des distances entre vecteur de modèles et **Test-propre**.

Nous venons de voir que la phase de décision se résume à un simple calcul de distance entre l'image Test et les images d'apprentissages dans le nouvel espace propre, ce calcul va se faire grâce à la distance **Euclidienne**. Nous présentant brièvement cette distance dans ce qui suit.

La distance Euclidienne:

La méthode de calcul de distance s'applique pour déterminer des degrés de ressemblance.

Le plus populaire des indices de distance est la distance euclidienne. Cette distance représente la distance géographique la plus courte entre deux points dans un espace multidimensionnel. Soit deux points x et y dans un espace à n dimensions de coordonnées x = {x_1, x_2, . . . , x_n} et y = {y_1, y_2, . . . , y_n} de même dimension n. Alors la distance euclidienne entre x et y est donnée par :

$$D(X,Y) = \sqrt{\sum_{I=1}^{n}(x_I - y_i)^2}$$

Le principe de fonctionnement de la PCA est résumé dans le schéma suivant :

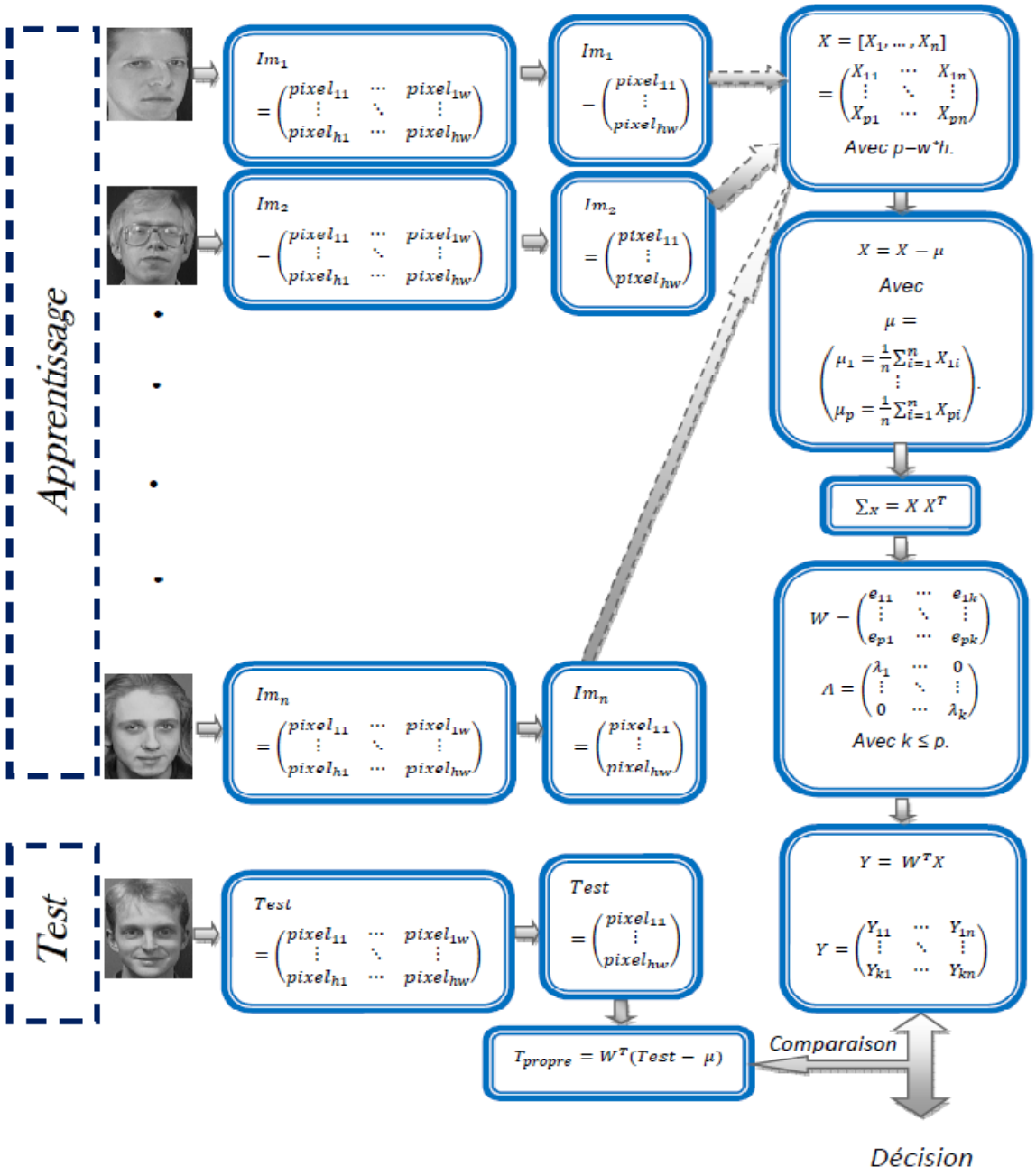


Figure II.13 : Processus de reconnaissance par PCA

II.8 Conclusion :

On a présenté dans ce chapitre, plusieurs méthodes pour faire de la reconnaissance de visages : méthodes locales, méthodes globales, méthodes hybrides. La méthode qu'on propose à l'intérêt dans le cadre de notre projet est l'ACP, qu'est une méthode globale utilisant en premier lieu les niveaux de gris des pixels d'une image. Le principe selon lequel on peut construire un sous-espace vectoriel en ne retenant que les « meilleurs »vecteurs propres, tout en conservant beaucoup d'information utile, fait du PCA un algorithme efficace et couramment utilisé en réduction de dimensionnalité. C'est un algorithme incontournable. La PCA est très célèbre en reconnaissance de visages, surtout par sa facilité d'implémentation et ses performances assez intéressantes.

Mais les problèmes que la PCA rencontre dans la reconnaissance de visages, c'est qu'en cas d'ajout d'une nouvelle personne à la base de données le système doit être recyclé (refaire l'apprentissage) car les résultats de la PCA (la matrice **W**) dépendent de l'ensemble total des images de l'échantillon d'apprentissage.

III.1 Introduction :

Ce chapitre est consacré à la partie conception de notre système. L'approche utilisée est l'approche objet. Elle consiste à modéliser informatiquement un ensemble d'éléments d'une partie du monde réel en un ensemble d'entités informatiques. Ces entités sont appelées objets. Cette approche présente plusieurs avantages dont les principaux sont : la modularité, l'extensibilité et la réutilisabilité.

La conception sera modélisée à l'aide du langage UML (Unified Modeling Language), en raison de son formalisme relativement simple.

III.2 Langage de modélisation :

III.2.1 Définition de l'UML :

(Unified modeling language) est un langage unifié pour la modélisation dans le cadre de la conception orienté objet. Il s'agit d'un langage graphique de modélisation objet permettant de spécifier, construire, visualiser et décrire les détails d'un système logiciel. Il est issu de fusion de plusieurs méthodes dont « bootch » et « omt » et adapté à la modélisation de tous types de système. Il devient aujourd'hui un standard dans le domaine d'analyse et de conception orienté objet [41].

Il propose plusieurs modèles qui sont des descriptions abstraites du système étudié et qui sont :

- Le modèle de classe qui capture la structure statique.
- Le modèle des cas d'utilisations qui décrit les besoins de l'utilisateur.
- Le modèle d'interactions qui décrit les scénarios et les flots de messages.
- Le modèle des états qui exprime le comportement dynamique des objets.
- Le modèle de réalisation qui montre les unités de travail.
- Le modèle de déploiement qui précise la répartition des processus.

Ces modèles sont regardés et manipulés par les utilisateurs au moyen de vue graphiques qu'on appel diagrammes.

III.2.2 Les différents types de diagrammes UML :

Il existe 2 types de vues du système qui comportent chacune leurs propres diagrammes [42]:

- **les vues statiques :**
  - diagrammes de cas d'utilisation : ils permettent de structurer les besoins des utilisateurs et les objectifs correspondants d'un système.
  - diagrammes d'objets : le diagramme d'objets permet de mettre en évidence des liens entre les objets. A l'exception de la multiplicité, qui est explicitement indiquée, le diagramme d'objets utilise les mêmes concepts que le diagramme de classes. Ils sont essentiellement utilisés pour comprendre ou illustrer des parties complexes d'un diagramme de classes.
  - diagrammes de classes : le diagramme de classes exprime la structure statique du système en termes de classes et de relations entre ces classes. L'intérêt du diagramme de classe est de modéliser les entités du système d'information.
  - diagrammes de composants.
  - diagrammes de déploiement.
- **les vues dynamiques :**
  - diagrammes de collaboration : le diagramme de collaboration permet de mettre en évidence les interactions entre les différents objets du système. Un diagramme de collaboration fait apparaître les interactions entre des objets et les messages qu'ils échangent.
  - diagrammes de séquence : le diagramme de séquence est une variante du diagramme de collaboration. Par opposition aux diagrammes de collaboration, les diagrammes de séquence possèdent intrinsèquement une dimension temporelle mais ne représente pas explicitement les liens entre les objets.

  - diagrammes d'états-transitions : Ils ont pour rôle de représenter les traitements (opérations) qui vont gérer le domaine étudié. Le diagramme d'états-transition est associé à une classe pour laquelle on gère différents états : il permet de représenter tous les états possibles ainsi que les événements qui provoquent les changements d'état.
  - diagrammes d'activités : le diagramme d'activité est attaché à une catégorie de classe et décrit le déroulement des activités de cette catégorie. Le déroulement

s'appelle "flot de contrôle". Il indique la part prise par chaque objet dans l'exécution d'un travail. Il sera enrichi par les conditions de séquencement.

III.2.3 les acteurs d'un Système:

Un acteur représente un rôle joué par une personne ou une chose qui interagit avec un système. Les acteurs se déterminent en observant les utilisateurs directs du système, ceux qui sont responsables de son exploitation ou de sa maintenance, ainsi que les autres systèmes qui interagissent avec le système en question. La même personne physique peut jouer le rôle de plusieurs acteurs.

Les acteurs de notre système :

1. L'Administrateur:

C'est la personne qui gère le système et qui choisit la configuration la plus efficace pour le rendre robuste et performant.

- Il prend à sa charge la gestion de la base de données ; il enregistre les nouvelles personnes.
- Il met à jour les informations des personnes et supprime ceux qui quittent le système.
- Il teste également les paramètres de chaque méthode et observe les avantages et les inconvénients de chacune, pour choisir la meilleure configuration.

2. Utilisateur (la Personne teste):

C'est un individu qu'on veut identifier pour avoir des informations sur lui, ou dans un autre cas une personne qui demande une autorisation d'accès (authentification).

III.3 quelques diagrammes de notre système :

III.3.1 Les diagrammes de cas d'utilisation :

Un cas d'utilisation (use case) modélise une interaction entre le système informatique à développer et un utilisateur ou acteur interagissant avec le système. Plus précisément, un cas d'utilisation décrit une séquence d'actions réalisées par le système qui produit un résultat observable pour un acteur.

Liens entre cas d'utilisation : include et extend.

1. Extends : On dit qu'un cas d'utilisation X étend un cas d'utilisation Y lorsque le cas d'utilisation X peut être appelé au cours de l'exécution du cas d'utilisation Y.
2. Include : la relation d'include n'a pour seul objectif que de factoriser une partie de la description d'un cas d'utilisation qui serait commune à d'autres cas d'utilisation. Le cas d'utilisation inclus dans les autres cas d'utilisation n'est pas à proprement parlé un vrai cas d'utilisation car il n'a pas d'acteur déclencheur ou receveur d'évènement. Il est juste un artifice pour faire de la réutilisation d'une portion de texte.

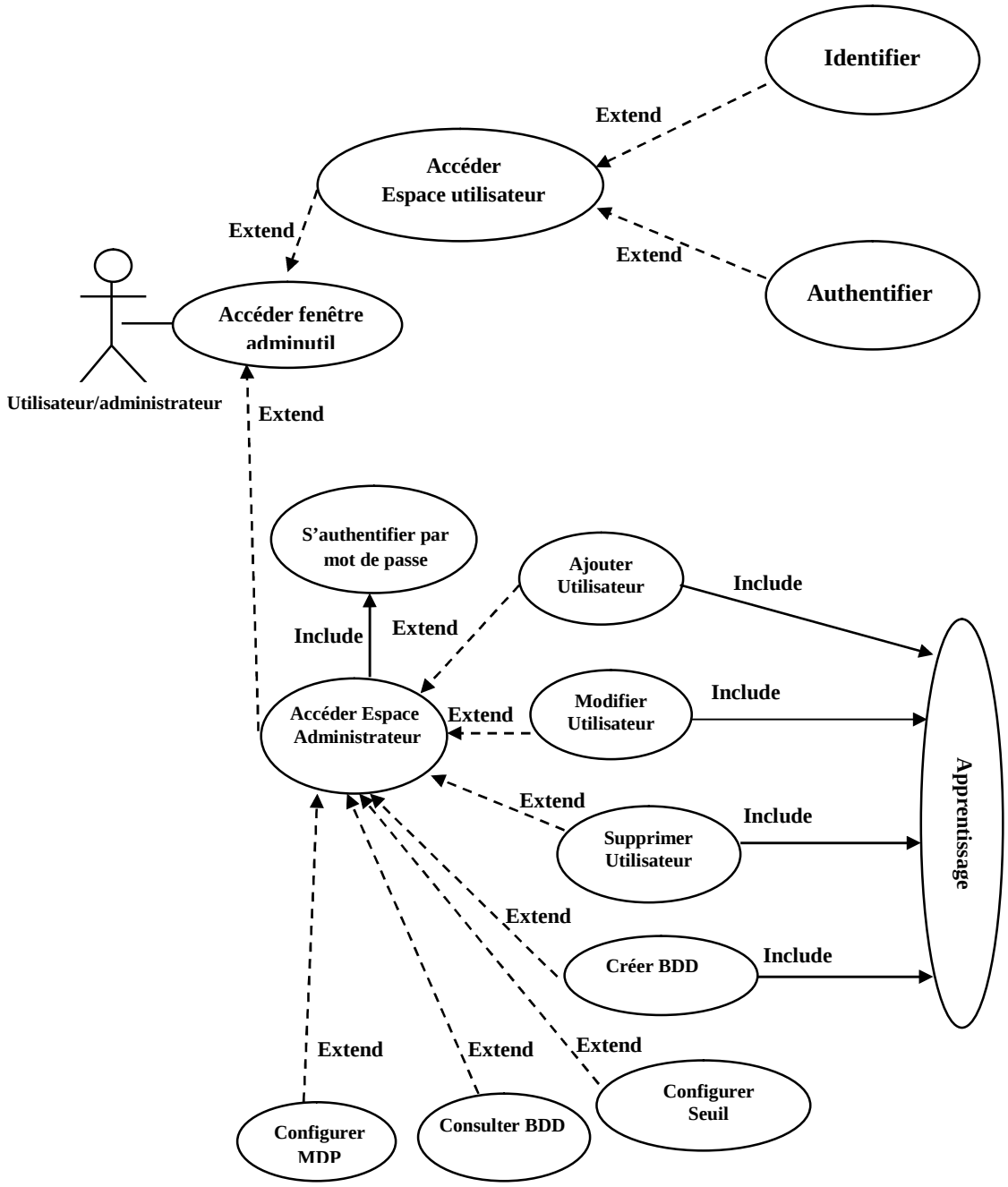


Figure III.1 : Diagramme des cas d'utilisations

III.3.2 Diagrammes de séquences :

Les diagrammes de séquences mettent en valeur les échanges de messages (déclenchant des événements) entre acteurs et objets (ou entre objets et objets) de manière chronologique, l'évolution du temps se lisant de haut en bas.

Accéder à l'espace administrateur :

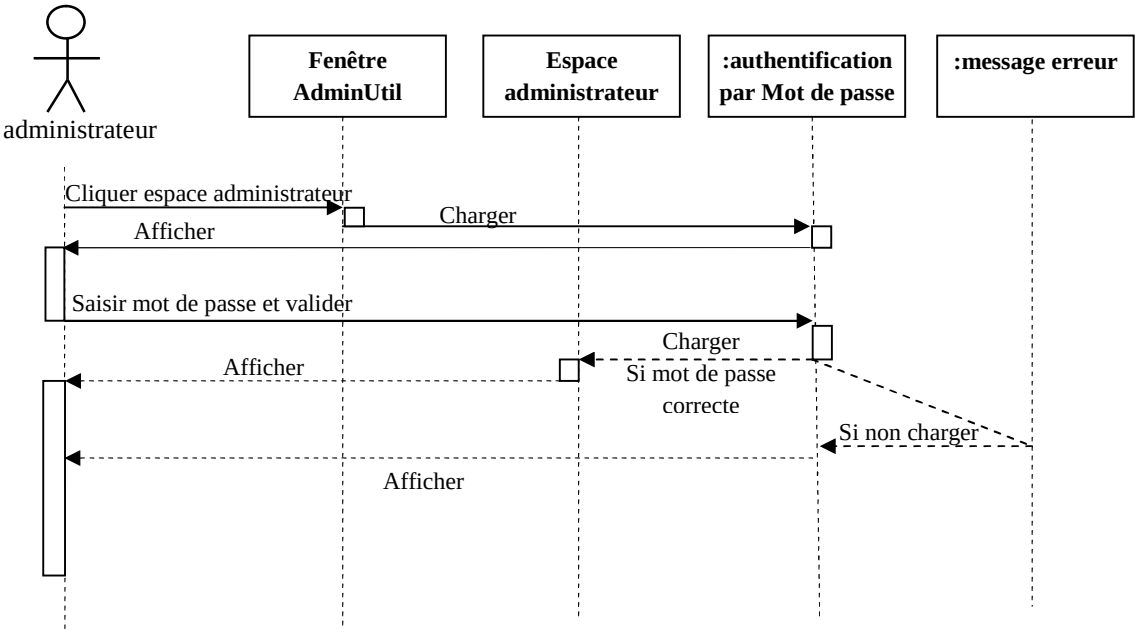


Figure III.2 : Diagramme de séquence du cas d'utilisation accéder espace administrateur

Ajout d'un utilisateur :

Pour ce cas d'utilisation l'administrateur remplis le formulaire de l'utilisateur en définissant ses différents attributs (ID, nom, prénom, date de naissance, lieu de naissance, profession) et joint à ce formulaire l'image de visage de l'utilisateur qui sera utilisé dans la reconnaissance, après validation les attributs de l'utilisateur et l'image de son visage sont sauvegardés dans la base de données, et un nouvel apprentissage de la nouvelle base d'image est effectué.

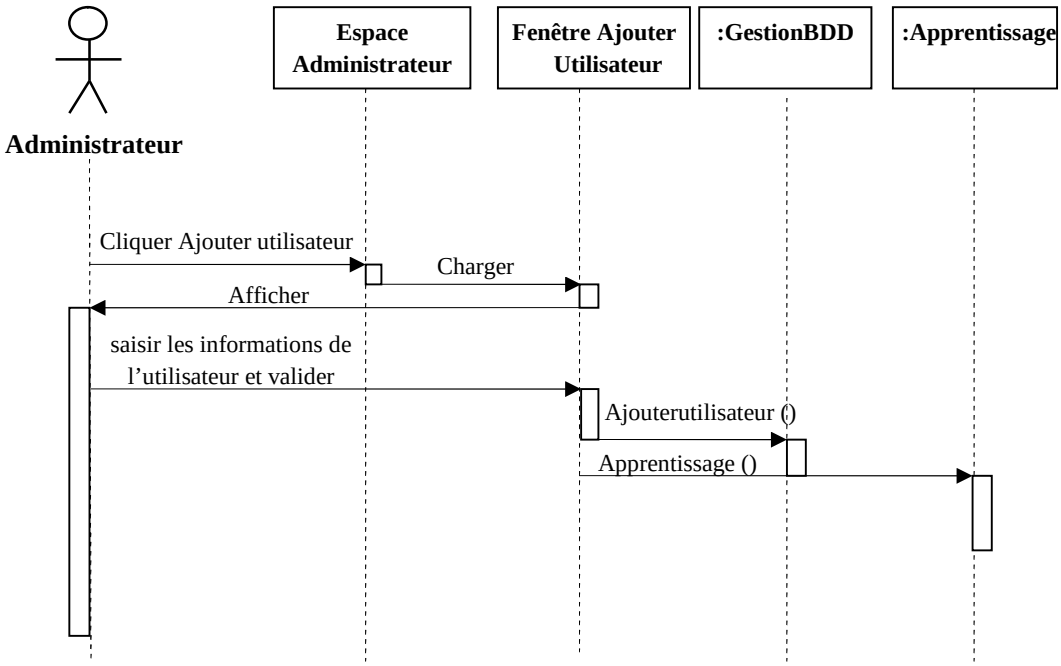


Figure III.3 : Diagramme de séquence du cas d'utilisation Ajouter Utilisateur

Suppression d'un utilisateur :

Pour ce cas d'utilisation l'administrateur entre l'identificateur de l'utilisateur à supprimer, puis il lance la recherche de cet utilisateur, ce qui va permettre de charger les attributs de l'utilisateur (ID, nom, prénom, date de naissance, lieu de naissance, profession) et son image depuis la base de données. Après validation les attributs de l'utilisateur et l'image de son visage sont supprimés dans la base de données, et un nouvel apprentissage de la nouvelle base d'image est effectué.

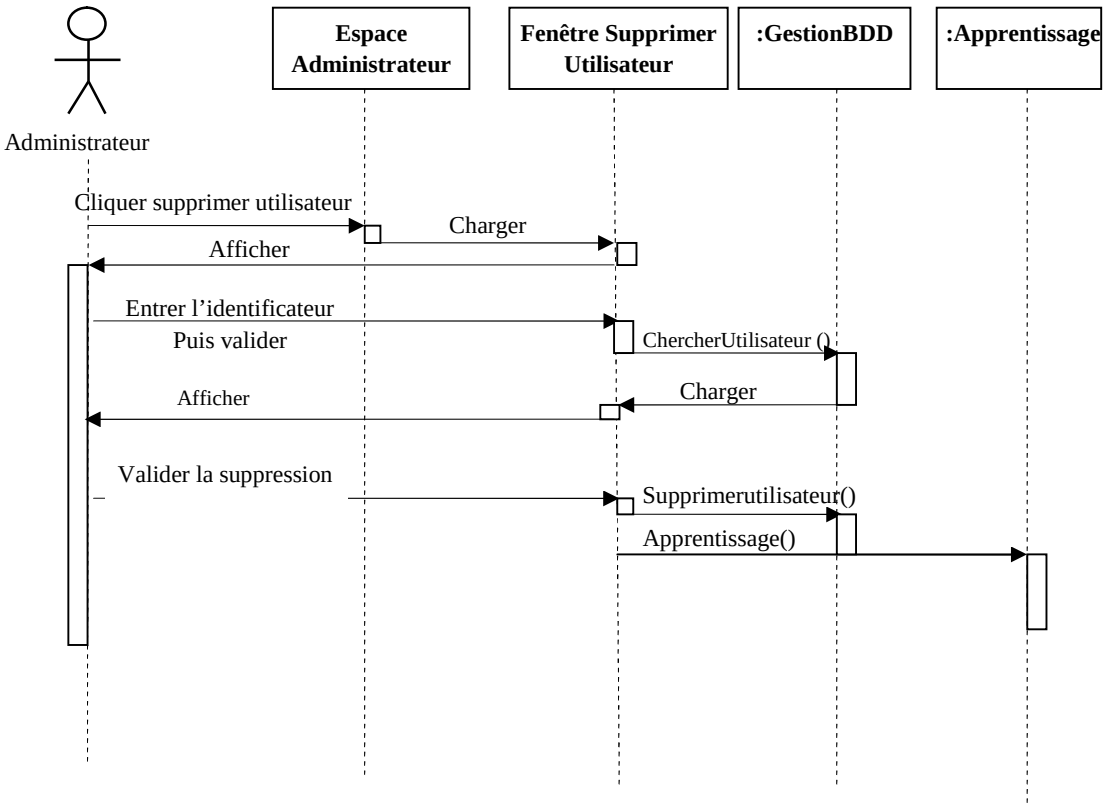


Figure III.4 : Diagramme de séquence du cas d'utilisation Supprimer Utilisateur

Consulter la base de données :

Pour ce cas d'utilisation l'administrateur clique sur le bouton suivant ou bien précédent pour visualiser les utilisateurs qui existent dans la base de données.

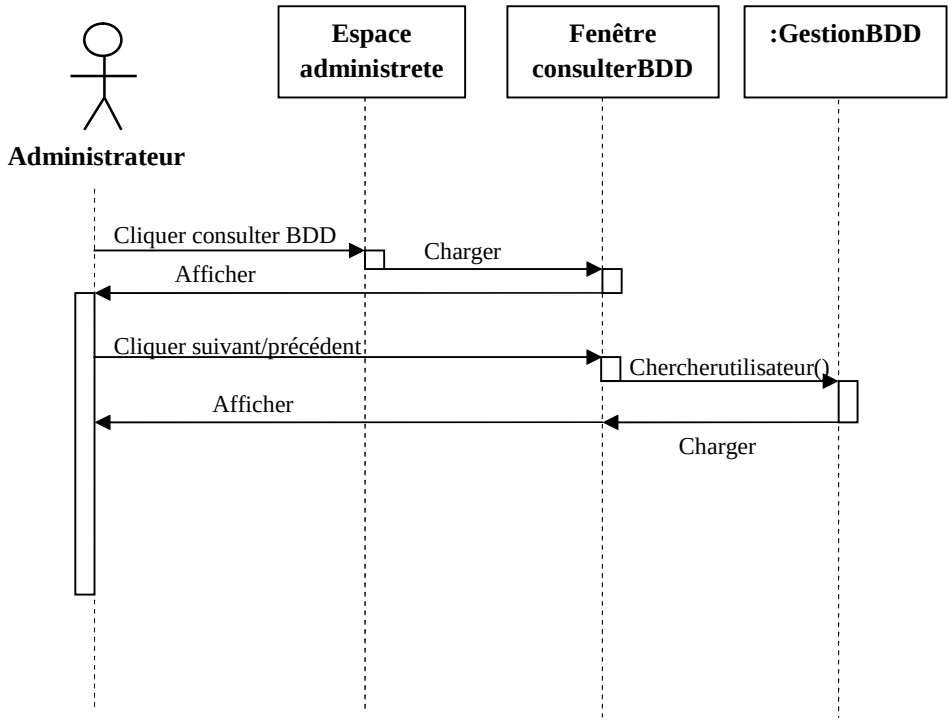


Figure III.5 : Diagramme de séquence du cas d'utilisation consulterBDD

Configurer seuil :

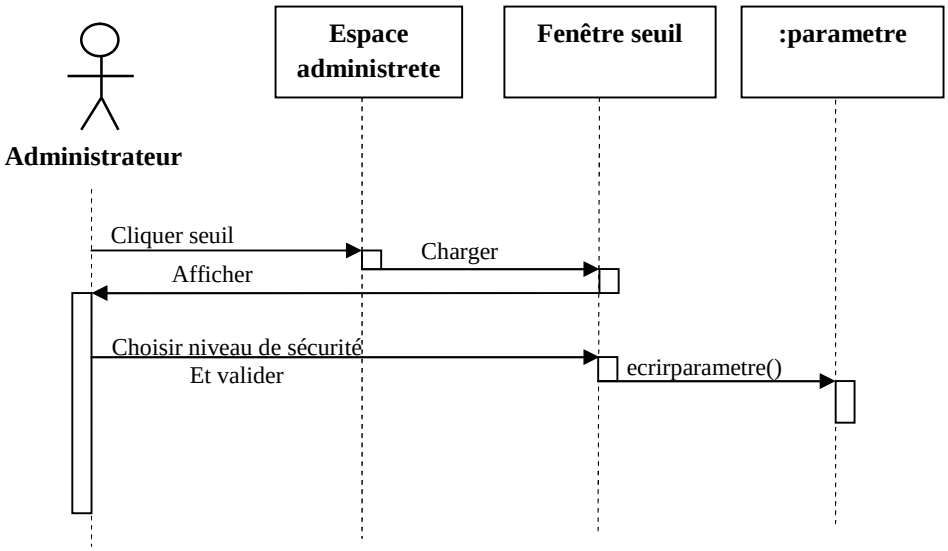


Figure III.6 : Diagramme de séquence du cas d'utilisation configurer seuil

Apprentissage :

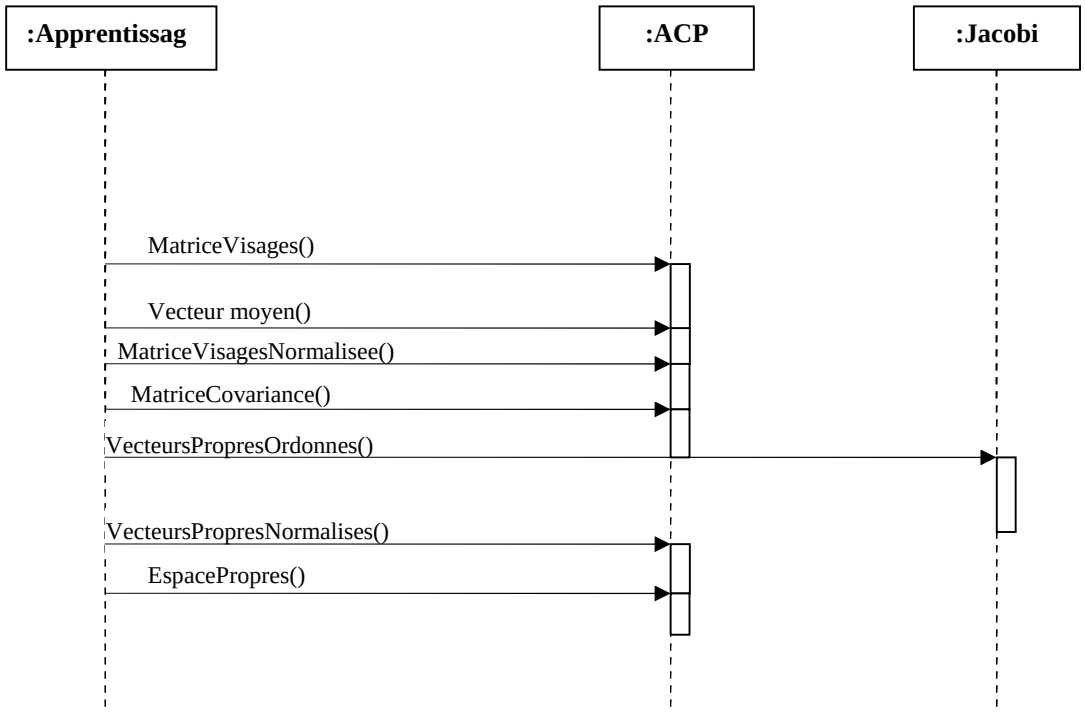


Figure III.7 : Diagramme de séquence du cas d'utilisation Apprentissage

Authentification :

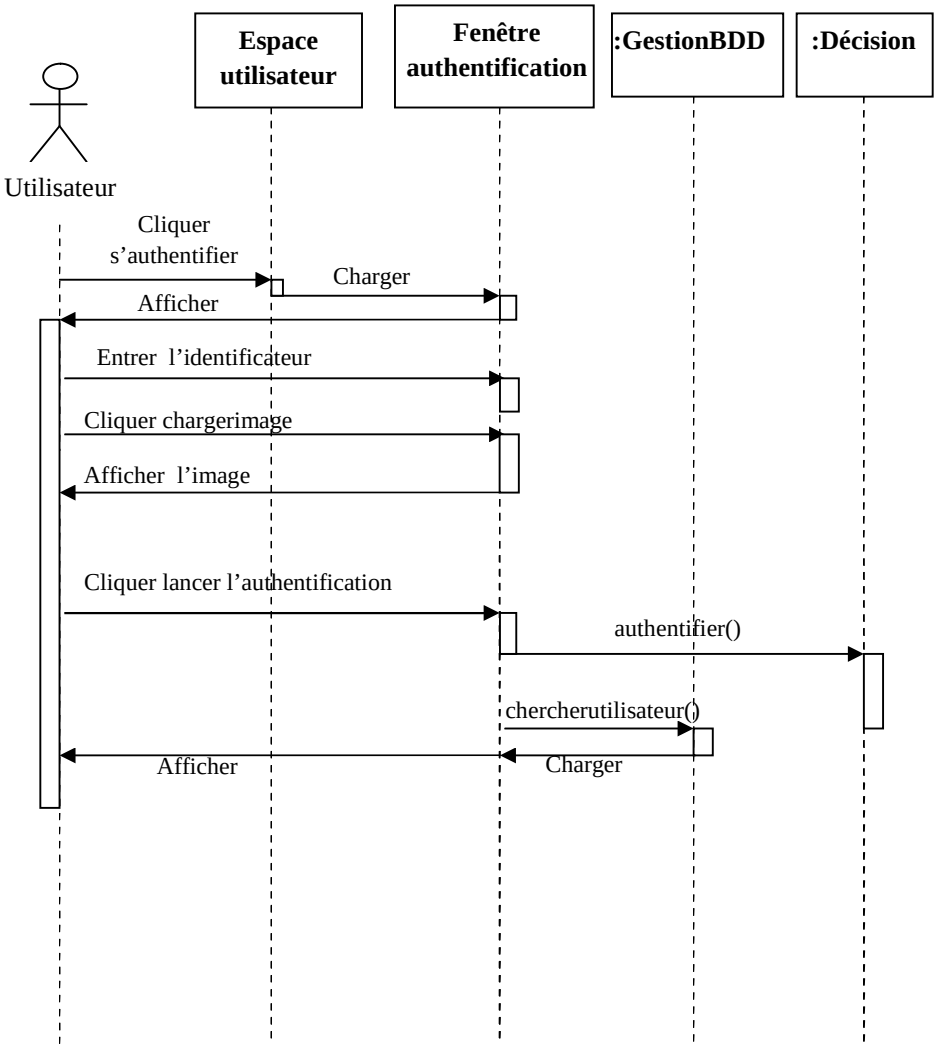


Figure III.8 : Diagramme de séquence pour le cas d'utilisation authentification

Identification :

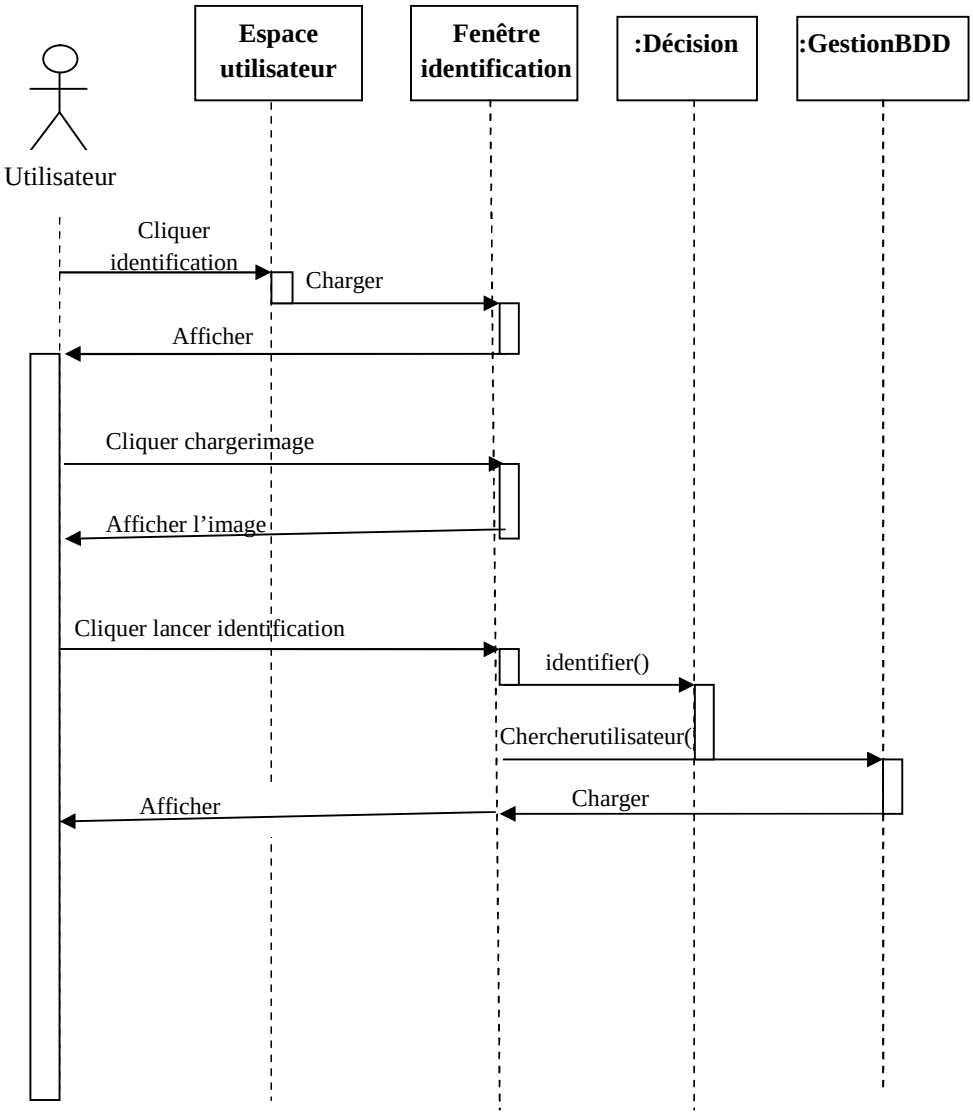


Figure III.9 : Diagramme de séquence du cas d'utilisation identification

III.3.3 les diagrammes d'activité :

Un diagramme d'activités est une variante des diagrammes d'états-transitions, organisé par rapport aux actions et principalement destiné à représenter le comportement interne d'une méthode (la réalisation d'une opération) ou d'un cas d'utilisation.

Le diagramme d'activité permet de présenter les transitions conditionnelles et les transitions de synchronisation.

Cas suppression :

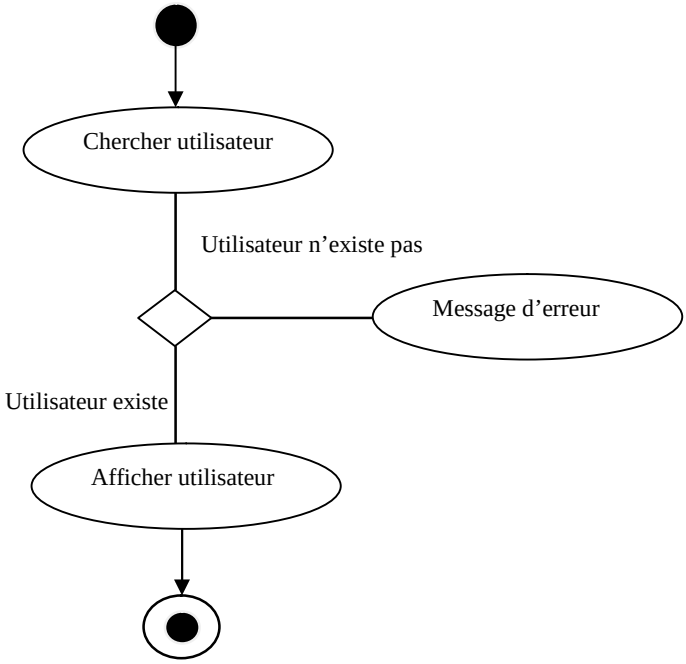


Figure III.10 : Diagramme d'activité pour le cas de suppression

Cas authentification et identification:

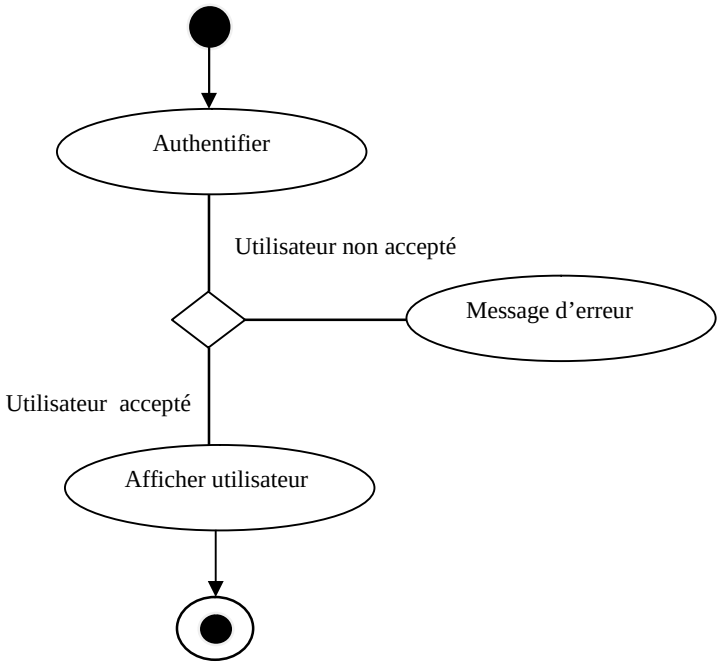


Figure III.11 : Diagramme d'activité pour le cas d'authentification

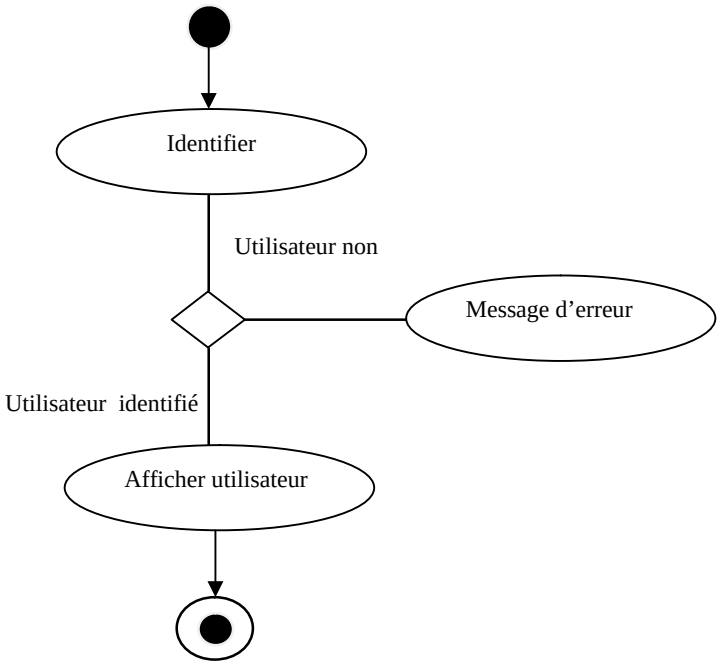


Figure III.12 : Diagramme d'activité pour le cas d'identification

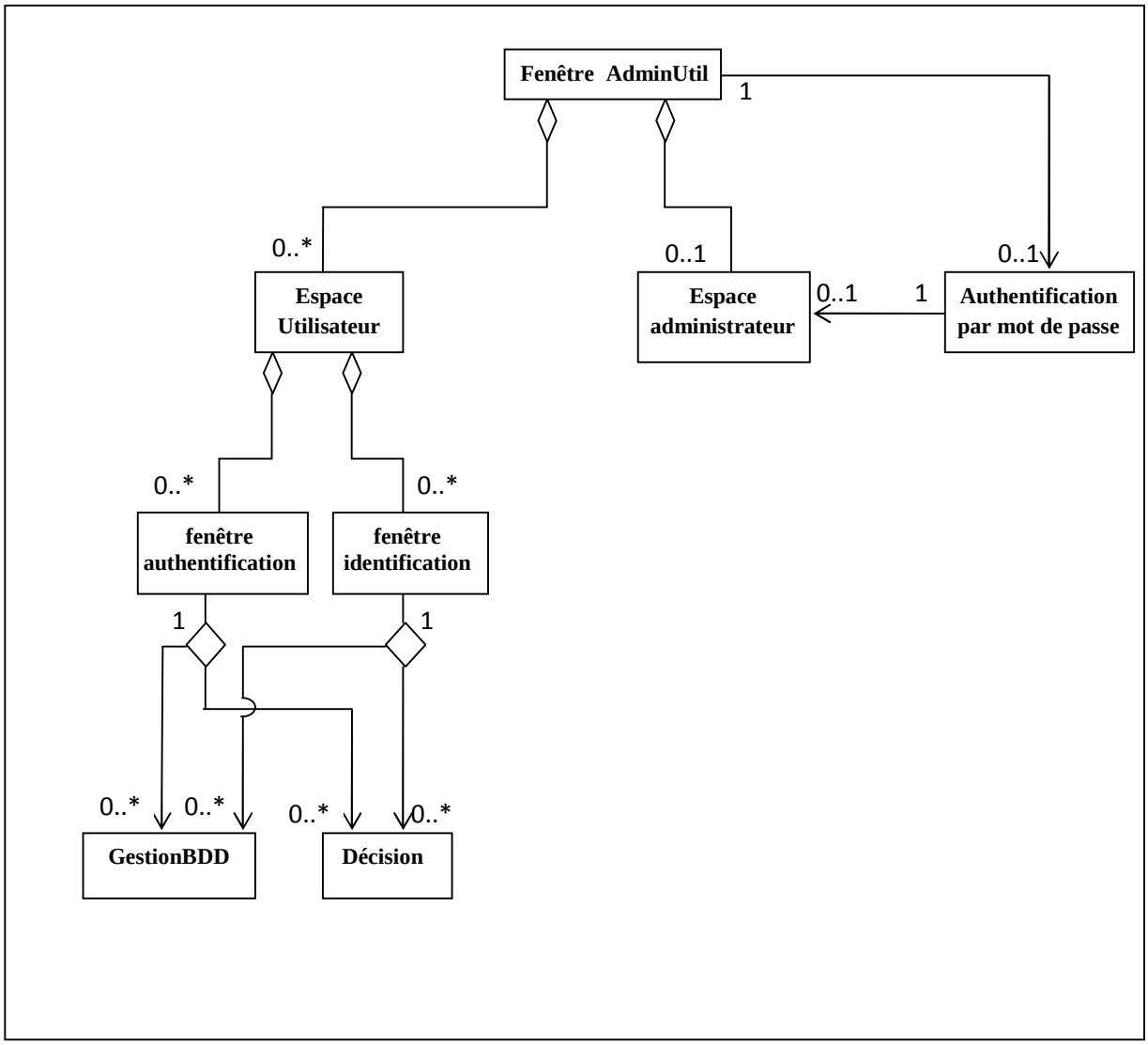
III.3.4 Les diagrammes de classes :

Les diagrammes de classes expriment de manière générale la structure statique d'un système, en termes de classes et de relations entre ces classes. De même qu'une classe décrit un ensemble d'objets, une association décrit un ensemble de lien, les objets sont des instances des classes et les liens sont des instances des relations. Un diagramme de classes n'exprime rien de particulier sur les liens d'un objet donné, mais décrit de manière abstraite les liens potentiels d'un objet vers d'autres objets.

L'ensemble des diagrammes de séquence représentés a permis de mettre en évidence les classes suivantes :

1. Classe espace Administrateur.
2. Classe fenêtre Ajout Utilisateur.
3. Classe fenêtre Supprimer Utilisateur.
4. Classe fenêtre Modifier Utilisateur.
5. Classe fenêtre consulter BDD.
6. Classe fenêtre créer BDD.
7. Classe fenêtre changer MDP.
8. Classe fenêtre seuil.
9. Classe espace utilisateur.
10. Classe fenêtre identification.
11. Classe fenêtre authentification.
12. Classe apprentissage.
13. Classe jacobi.
14. Classe acp.
15. Classe décision.
16. Classe paramètre.

Nous donnons ci-dessous le diagramme de classe qui nous offre une vue global de la composition interne de notre système.



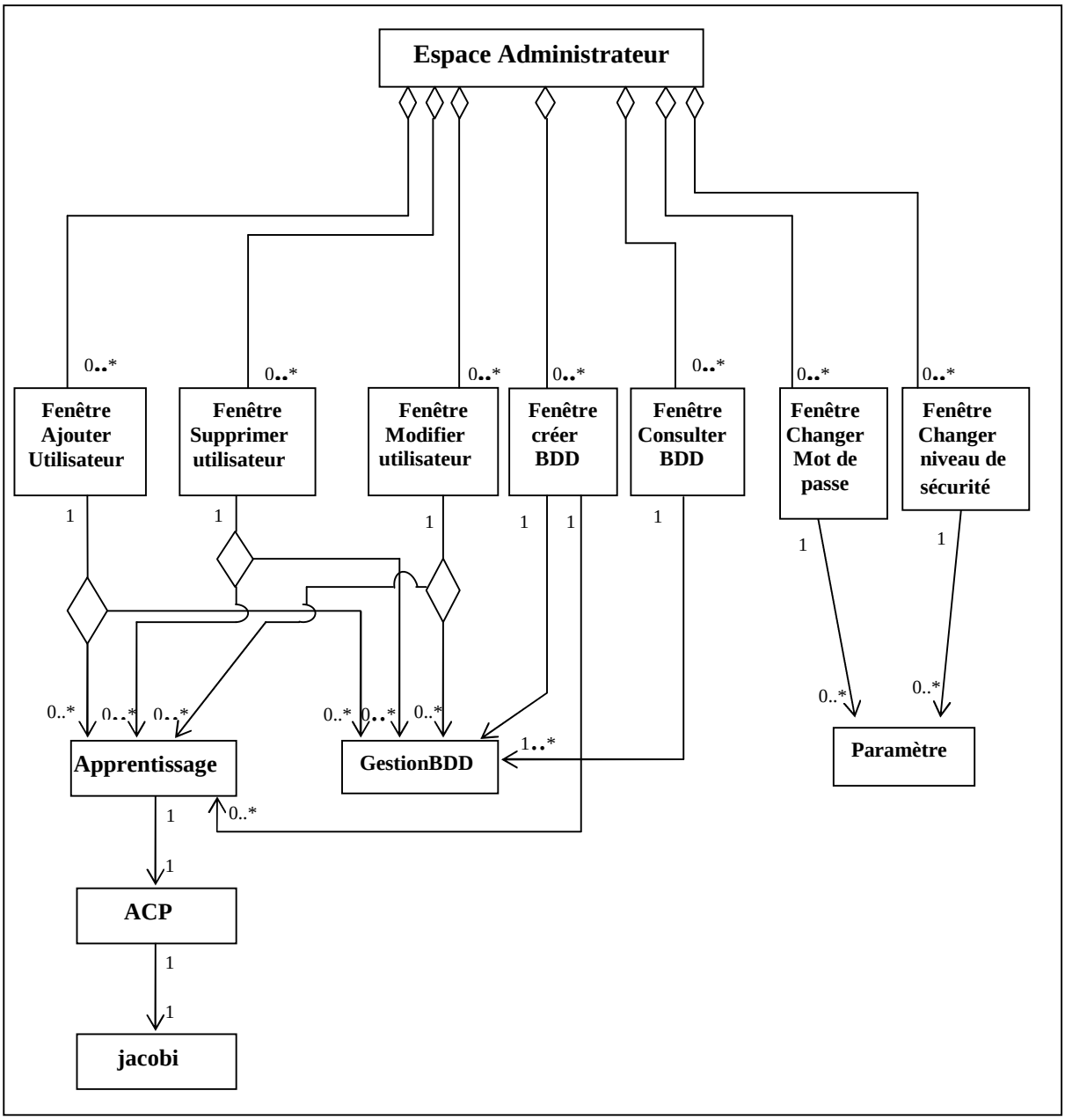
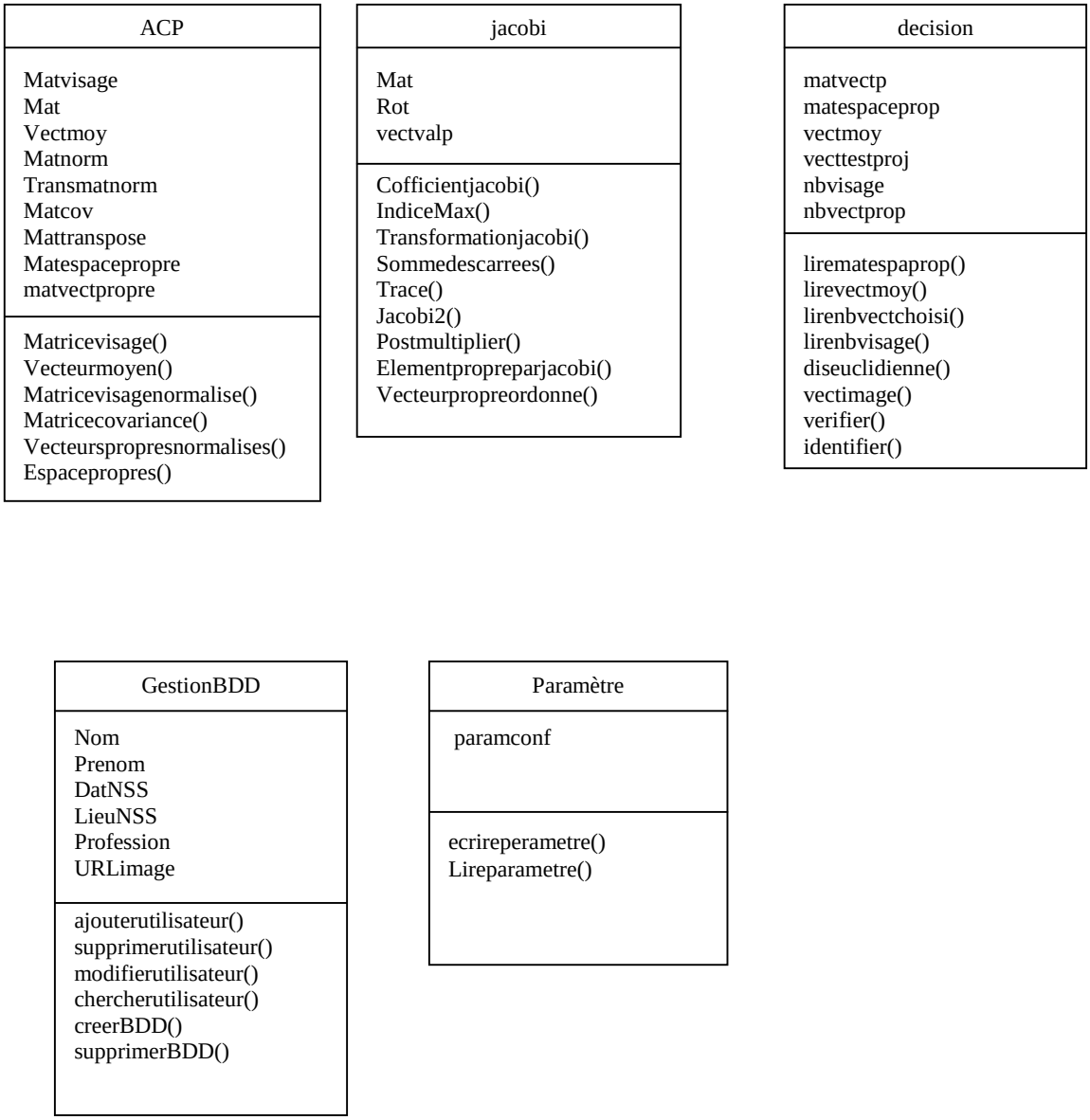


Figure III .13: Diagramme de classe du système



III.4 Conclusion :

Dans ce chapitre nous avons pu modéliser le fonctionnement du système. Ceci est fait à travers différents diagrammes permettant de bien spécifier la composition et le comportement de l'application. Dans le chapitre suivant, on procède à la réalisation de notre système.

IV.I Introduction :

Après avoir défini la conception de notre système dans le chapitre précédent, nous passons dans ce qui suit à la réalisation. Pour ce faire, nous allons commencer par la description du langage et des outils de programmation utilisée pour la réalisation du système. Par la suite, nous illustrerons les principales fonctionnalités de notre système en donnant divers illustrations de ces interfaces.

IV.2 Langage de programmation :

Le C++ est l'un des langages de programmation les plus utilisés actuellement. Il est à la fois facile à utiliser et très efficace.

Il peut être considéré comme un successeur de C. Tout en gardant les points forts de ce langage, il corrige certains points faibles et permet l'abstraction de données. De plus, il permet la programmation objet. Les caractéristiques du C++ en font un langage idéal. Il est incontournable dans la réalisation des grands programmes. Les optimisations des compilateurs actuels en font également un langage de prédilection pour ceux qui recherchent les performances.
Les principaux avantages du C++ sont les suivants :

- langage orient´e objet.
- écriture du code très rigoureuse.
- grand nombre de fonctionnalités ;
- performances du C ;
- facilité de l'utilisation des langages objets ;
- portabilité des fichiers sources ;
- facilité de conversion des programmes C en C++, et, en particulier, possibilité d'utiliser toutes les fonctionnalités du langage C ;
- contrôle d'erreurs accru.

Voire également la rapidité de C++ grâce à la disponibilité d'une large collection d'APIs (Application Programming Interface), ce langage nous semble le plus adéquat pour le développement de notre application.

IV.3 Les outils de développement :

Du point de vue logiciel, nous avons travaillé sur une plateforme Windows XP sur laquelle sont installés les outils nécessaires à la réalisation de notre travail :

IV.3 .1 L'environnement de développement (Microsoft Visual Studio):

Visual Studio 2010 est un IDE permettant le développement de différentes applications. La version finale de Visual Studio 2010 est apparue le 12 Avril 2010, cette version utilise le .NET Framework 4 et c'est la version qu'on va utiliser pour développer notre application.

Microsoft Visual Studio est une suite de logiciels de développement pour Windows conçu par Microsoft. C'est un ensemble complet d'outils de développement permettant de générer des applications Web ASP.NET, des Services Web XML, des applications bureautiques et des applications mobiles.
Microsoft Visual Studio 2010 intègre de nouvelles fonctionnalités qui simplifient le processus de développement d'application, de la conception au déploiement, il permet la création d'applications puissantes, hautes performances.

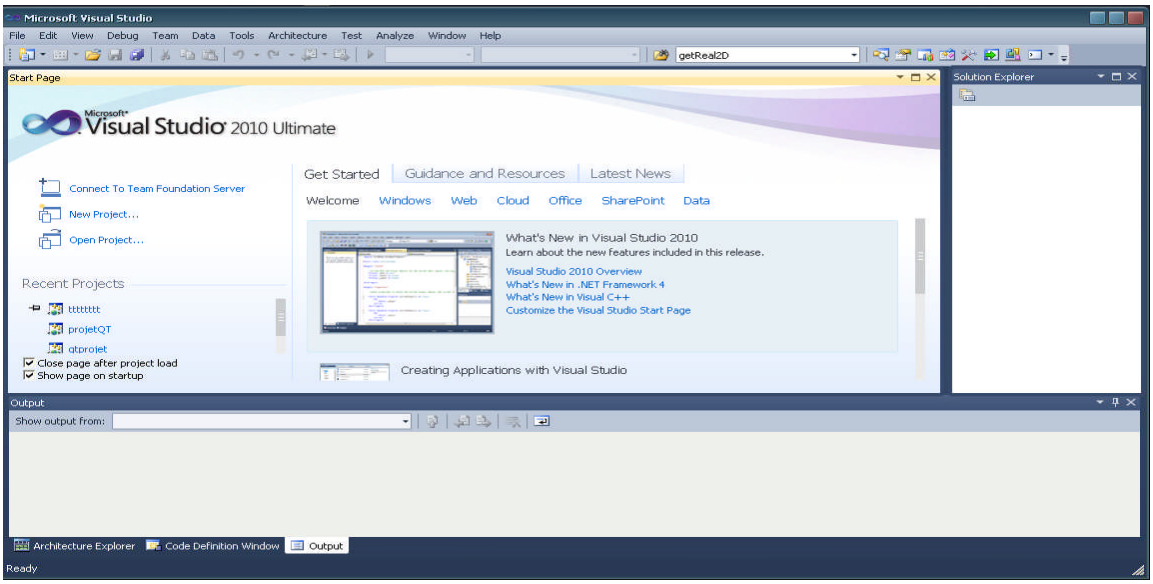


Figure IV.1 : Vue général de l'interface de l'environnement Microsoft Visual Studio

IV.3.2 La bibliotheque Qt :

Qt est une bibliothèque logicielle qui offre essentiellement des composants d'interface graphique (communément appelés widgets), mais également d'autres composants non-graphiques permettant entre autre l'accès aux données, les connexions réseaux, la gestion des files d'exécution, etc. Elle a été développée en C++ par la société Trolltech et est disponible pour de multiples environnements Unix utilisant X11 (dont Linux), Windows et Mac OS. Qt est un toolkit qui présente de nombreux avantages.

Le fait d'être une bibliothèque logicielle multiplate-forme attire un grand nombre de personnes qui ont donc l'occasion de diffuser leurs programmes sur les principaux OS existants.

Qt est notamment connu pour être la bibliothèque sur laquelle repose l'environnement graphique KDE, l'un des environnements de bureau les plus utilisés dans le monde Linux.

Figure IV.2 : Logo de la bibliothèque QT

IV.4 Description des interfaces :

Dans ce qui suit, nous présenterons les principales interfaces de notre système.

IV.4.1 Page accueil :

C'est la première fenêtre qui apparaît lors de lacement du système de reconnaissance faciale.

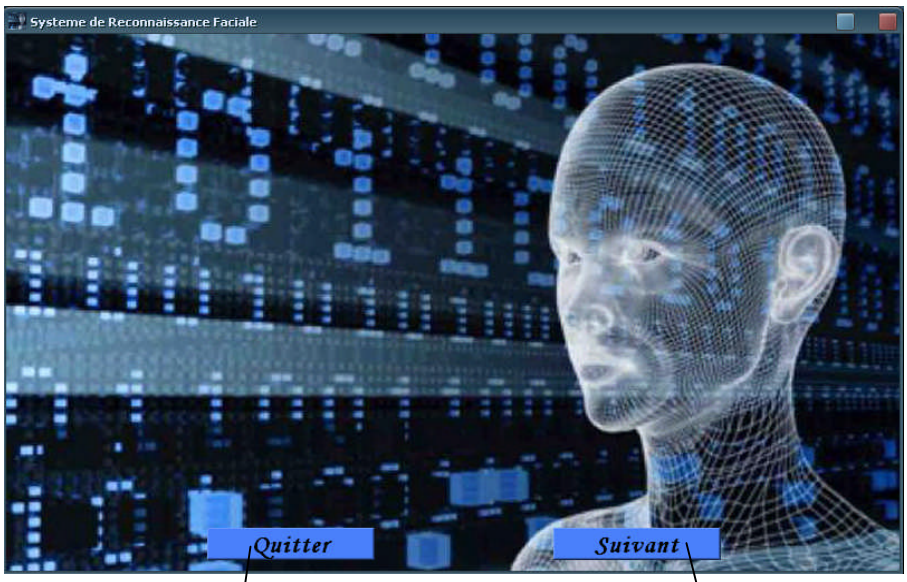


Figure IV.3 : Page d'accueil

Quitter Le système de reconnaissance faciale

Atteindre la fenêtre de choix Utilisateur/ Administrateur

IV.4.2 Fenêtre Utilisateur/administrateur :

Figure IV.4 : Fenêtre espace Utilisateur/administrateur

Atteindre espace Utilisateur

Quitter le système

Atteindre espace Administrateur

L'espace administrateur est protégé par un mot de passe. En cliquant sur le bouton Espace Administrateur la fenêtre d'authentification par mot de passe apparait.

IV.4.2.1 Fenêtre d'authentification par mot de passe :

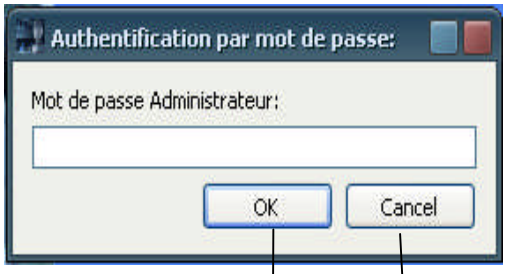


Figure IV .5 : Fenêtre d'authentification par mot de passe

Si le mot de passe est correct, accès a l'espace administrateur si non le message d'erreur suivant va apparaitre

Fermer la fenêtre d'authentification

Figure IV.6 : Message d'erreur

IV.4.3 Espace Administrateur :

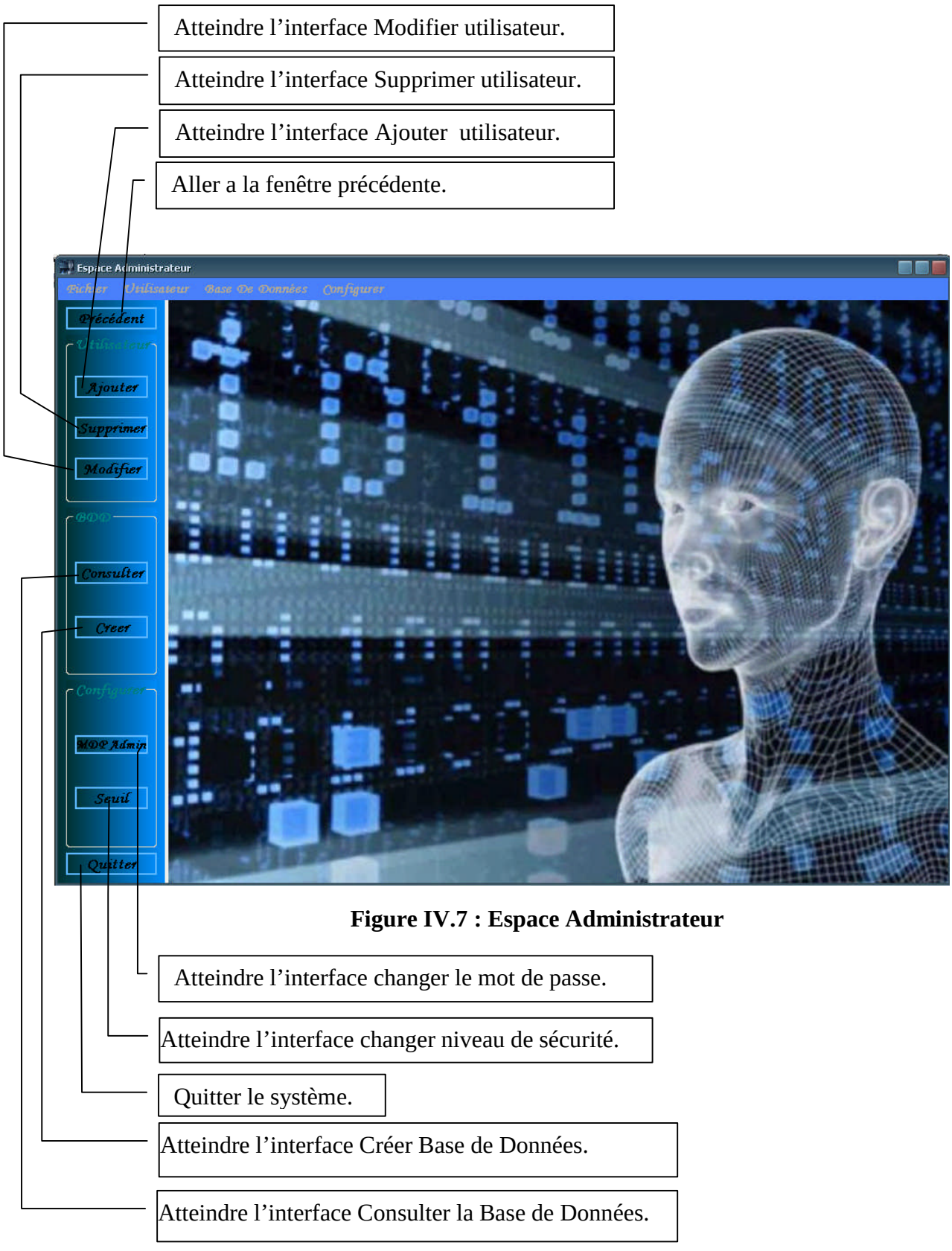


Figure IV.7 : Espace Administrateur

IV.4.3.1 Fenêtre Ajouter Utilisateur :

Cette interface permet à l'administrateur d'ajouter des utilisateurs au système.

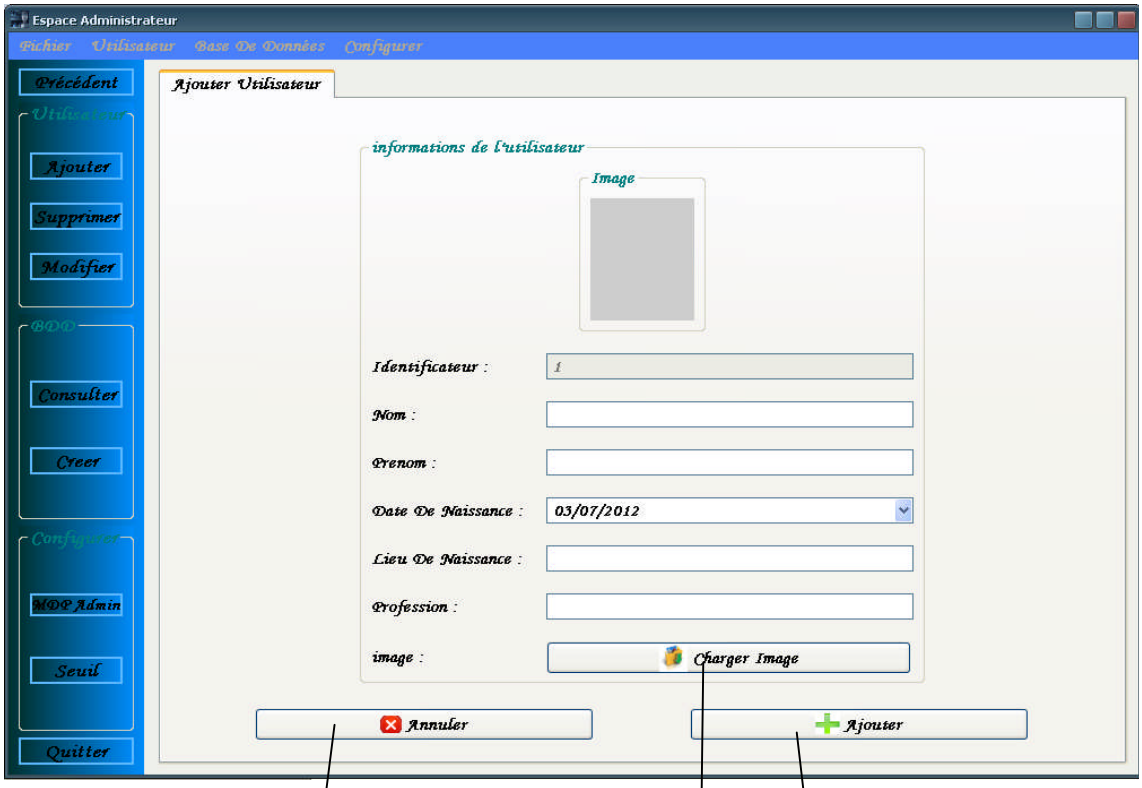


Figure IV.8 : Fenêtre Ajout Utilisateur

Annuler l'ajout de l'utilisateur a la base de données

Charger l'image de visage de l'utilisateur à ajouter, c'est cette image qui va être utilisé dans la reconnaissance.

Ajouter le nouveau utilisateur a la base

IV.4.3.2 Fenêtre Supprimer Utilisateur :

Cette interface permet à l'administrateur de supprimer des utilisateurs dans la base de données.

Chercher dans la base de données l'utilisateur dont l'identificateur correspond l'identificateur entré et l'affiché dans la partie utilisateur à supprimer.

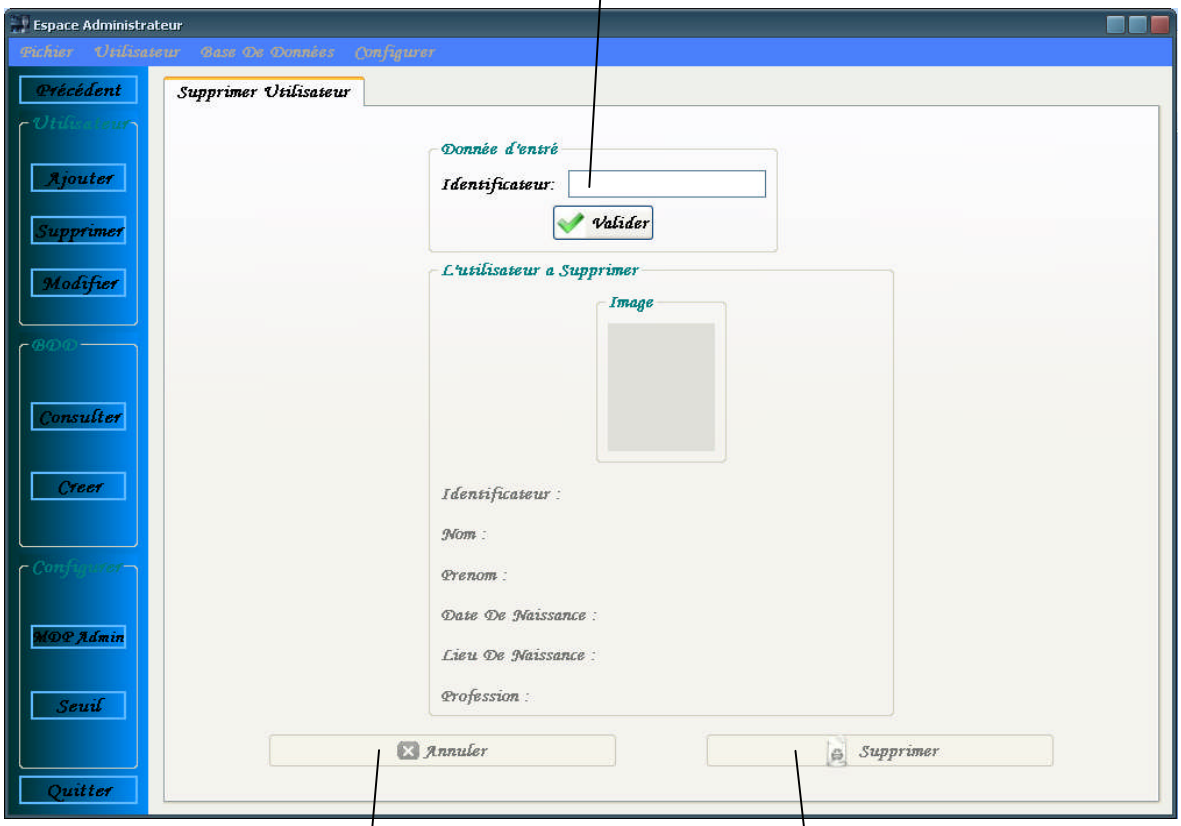


Figure IV.9 : Fenêtre Supprimer Utilisateur

Annuler la suppression du l'utilisateur.

Confirmer la suppression du l'utilisateur.

IV.4.3.3 Fenêtre Modifier Utilisateur :

Cette interface permet à l'administrateur de modifier les attributs d'un utilisateur ainsi que son image dans la base de données.

Chercher dans la base de données l'utilisateur dont l'identificateur correspond a l'identificateur entré et l'affiché dans la partie utilisateur à modifier.

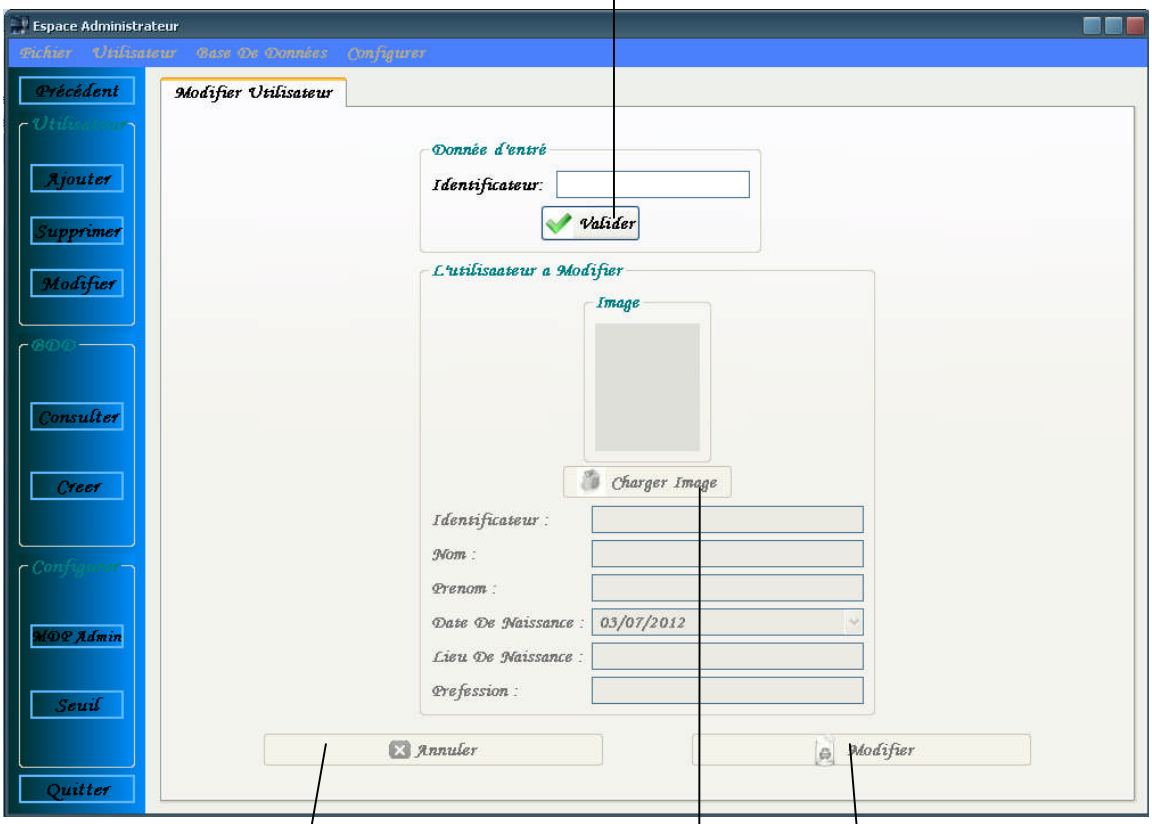


Figure IV.10 : Fenêtre Modifier Utilisateur.

Annuler la modification de l'utilisateur

Permet de modifier l'image de l'utilisateur dans la base de données en chargeant une autre.

Confirmer la modification du l'utilisateur

IV.4.3.4 Fenêtre consulter base de données :

Cette interface permet à l'administrateur de consulter la base de données.

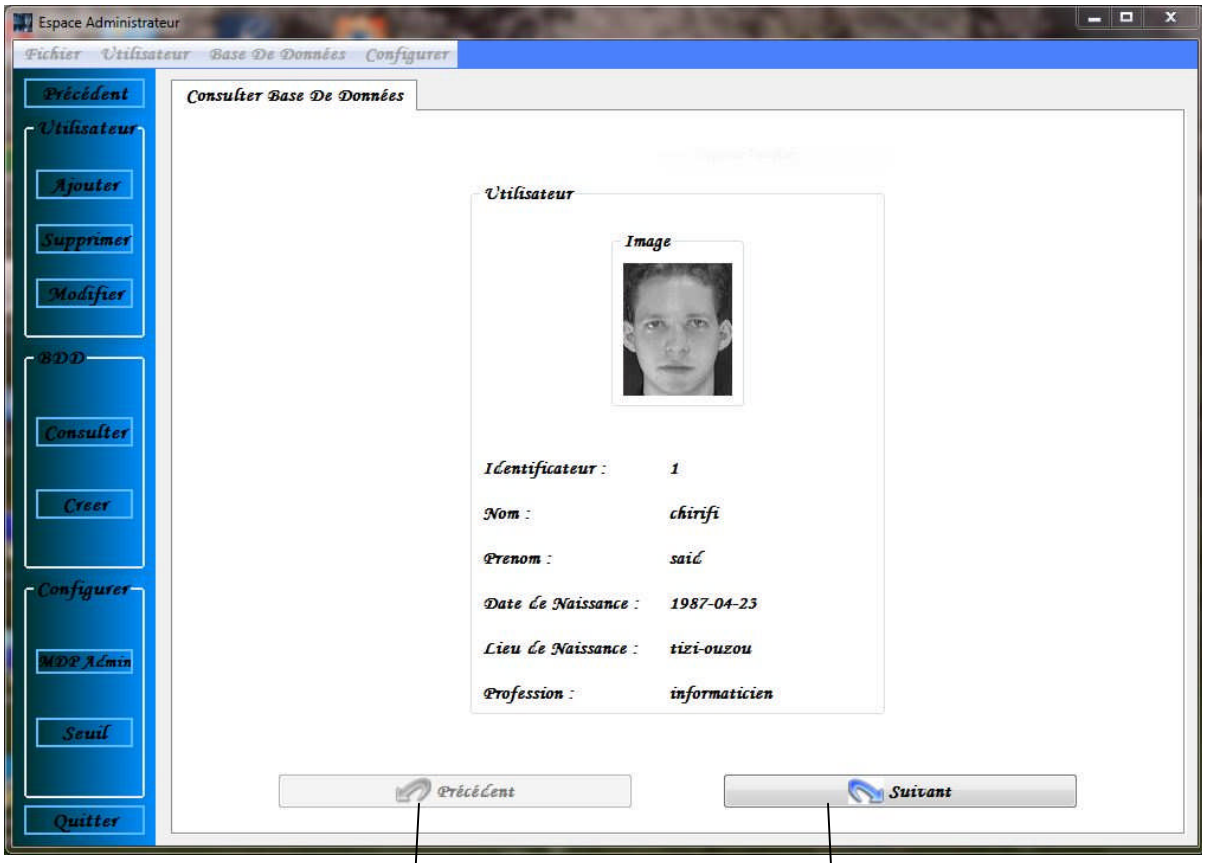


Figure IV.11 : Fenêtre Consulter Base de Données.

Client précédent

Client suivant

IV.4.3.5 Fenêtre créer la base de données :

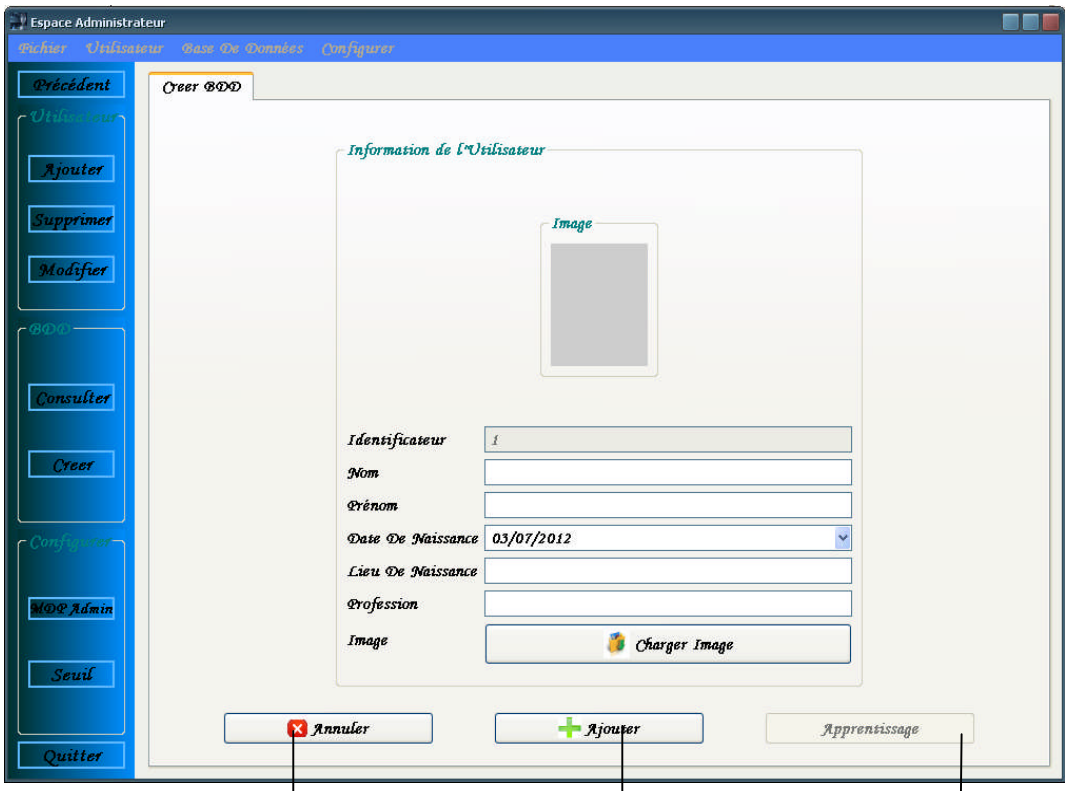


Figure IV.12 : Fenêtre Créer Base de Données.

Annuler l'ajout de l'utilisateur

Ajouter le nouveau utilisateur à la base de données

Ce bouton permet de lancer le processus d'apprentissage.

IV.4.3.6 Changer le mot de passe :

Cette interface permet à l'administrateur de changer le mot de passe.

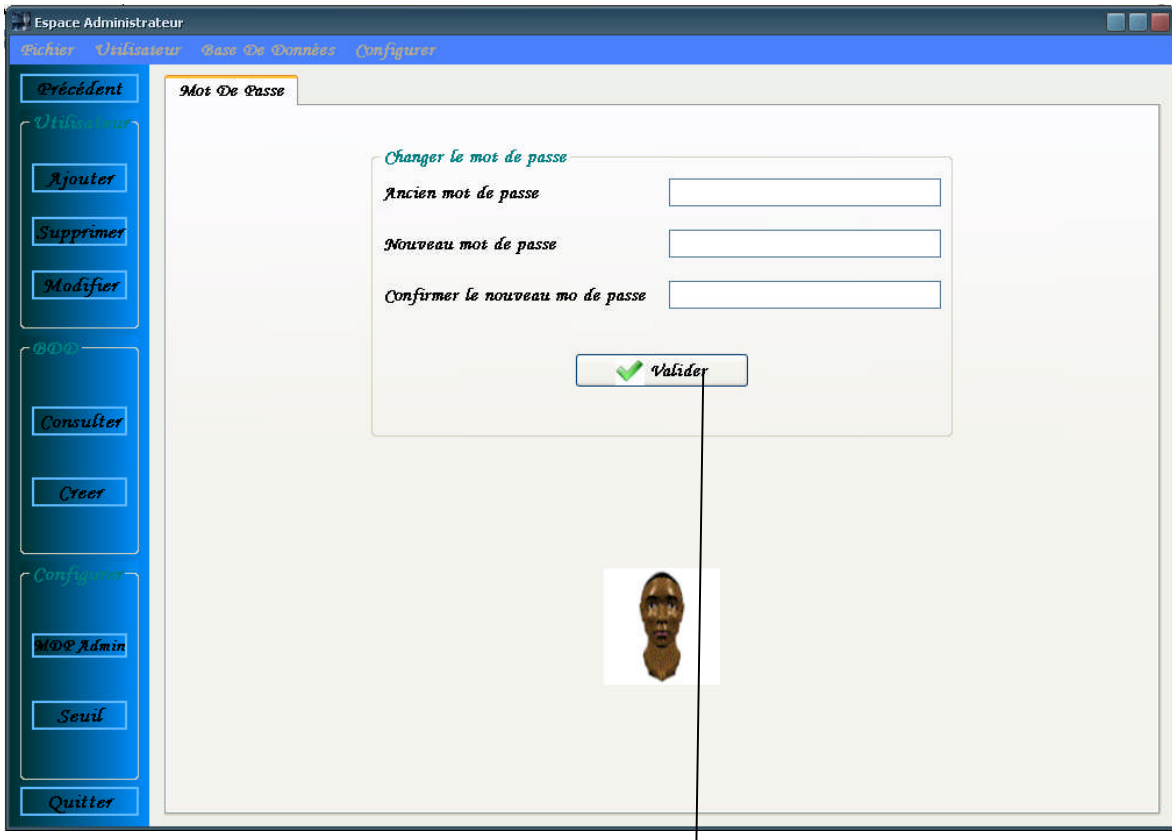
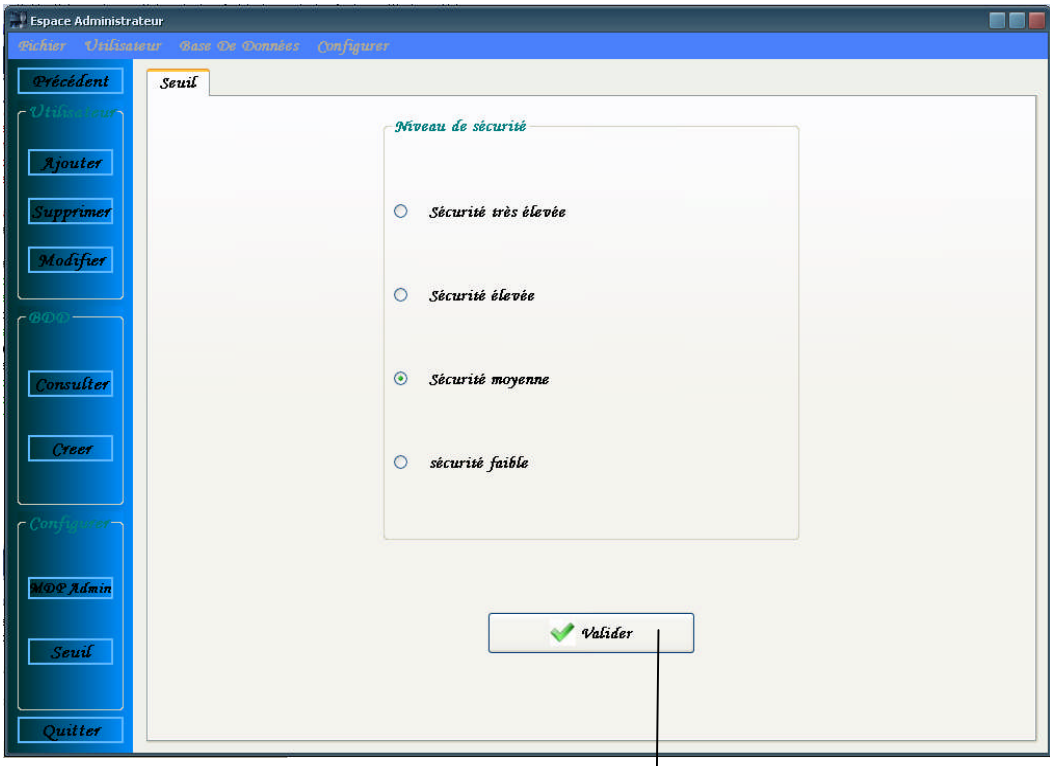


Figure IV.13 : Changer le mot de passe.

Ce bouton permet de valider le changement de mot de passe si l'ancien mot de passe est correct et la confirmation de nouveau mot de passe.

IV.4.3.7 : Changer le niveau de sécurité du système :

Cette interface permet à l'administrateur de changer le niveau de sécurité du système.



IV.14 : Changer le niveau de sécurité du système.

Ce bouton permet de valider le changement de niveau de sécurité.

IV.4.4 Espace Utilisateur :

Figure IV.15 : Espace Utilisateur.

IV.4.4. 1 Fenêtre D'identification :

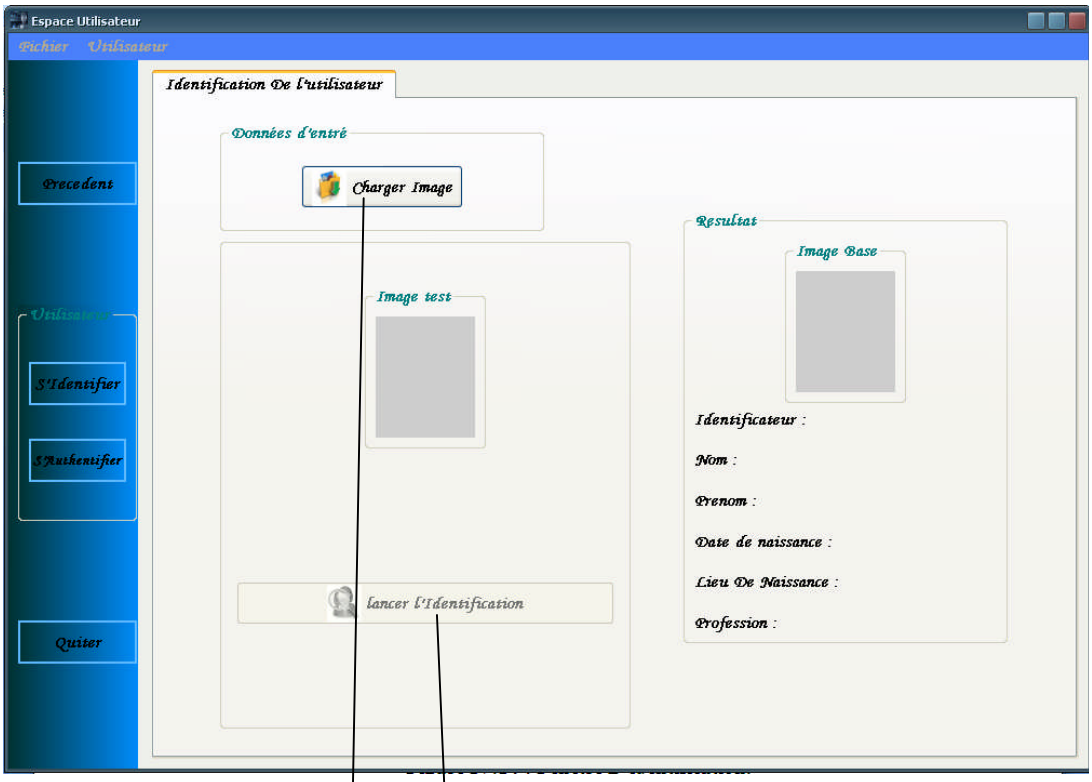


Figure IV.16 : Fenêtre D'identification.

Charger l'image de l'utilisateur a identifié.

Ce bouton permet de lancer le processus d'identification. Si l'utilisateur est reconnu ces attributs vont être affichés dans la fiche résultat si non un message d'erreur va être affiché.

IV.4.4.2 Fenêtre d'authentification :

Chercher dans la base de données l'utilisateur dont l'identificateur correspond a l'identificateur entré.

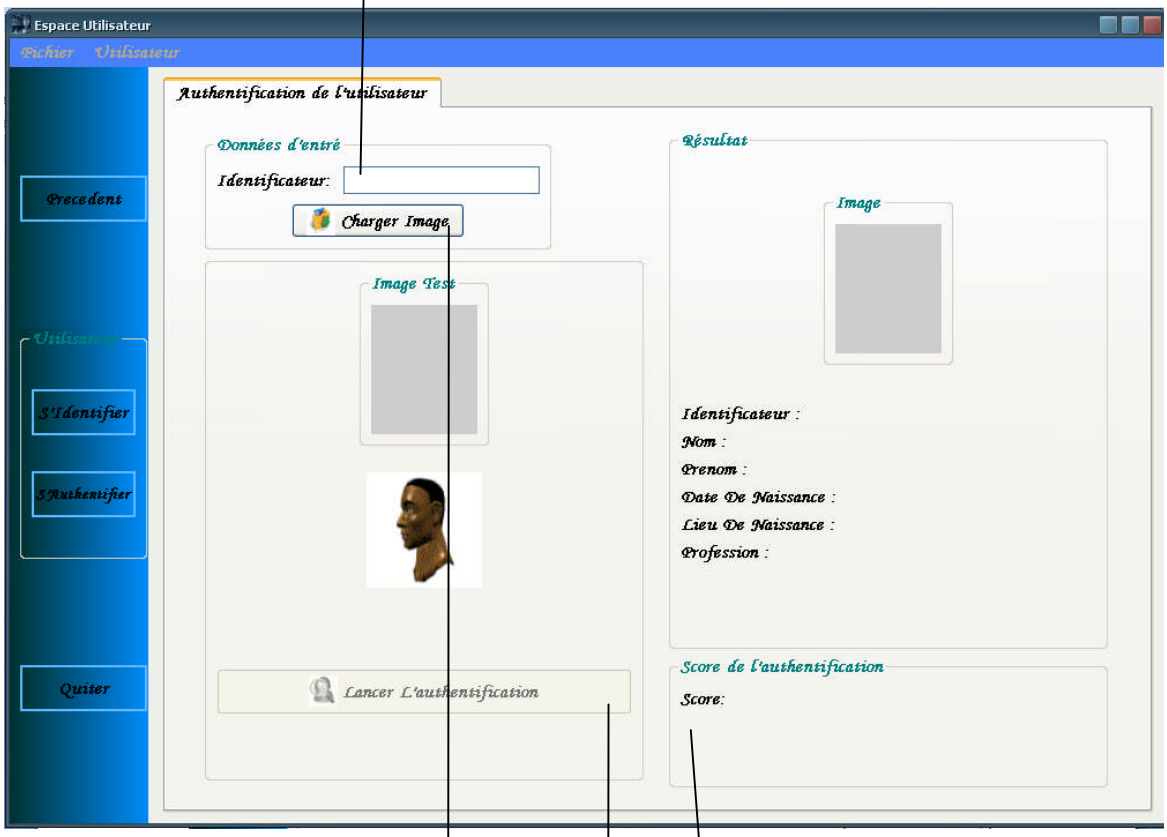


Figure IV.17 : Fenêtre d'authentification.

Charger l'image de l'utilisateur a qui on vérifié son identité.

Ce bouton permet de lancer le processus d'authentification. Si l'utilisateur est reconnu ces attributs vont être affichés dans la fiche résultat si non un message d'erreur va être affiché.

Si l'utilisateur est reconnu un score de reconnaissance va être affiché.

IV. 5 Evaluation du système :

Pour l'évaluation de notre système nous avons utilisé la base de données ORL.

IV.5.1 La base ORL :

La base ORL (Olivetti Research Laboratory) [43] a été collectée entre avril 1992 et avril 1994 par un laboratoire de AT&T, basé à Cambridge. La base contient 40 personnes, chacune étant enregistrée sous 10 vues différentes. Les images sont de taille 112 × 92 pixels. Pour quelques sujets, les images ont été collectées à des dates différentes, avec des variations dans les conditions d'éclairage, les expressions faciales (expression neutre, sourire et yeux fermés) et des occultations partielles par les lunettes. Toutes les images ont été collectées sur un fond foncé. Les poses de la tête présentent quelques variations en profondeur par rapport à la pose frontale.

Figure IV.18 : Extrait de la base ORL. Pour chacune des 40 personnes enregistrées, on dispose de 10 vues avec des changements de pose, d'expression et d'éclairage.

Quelques exemples de teste :

Effet de variation de pauses :

Image base

Image teste1

Image teste2

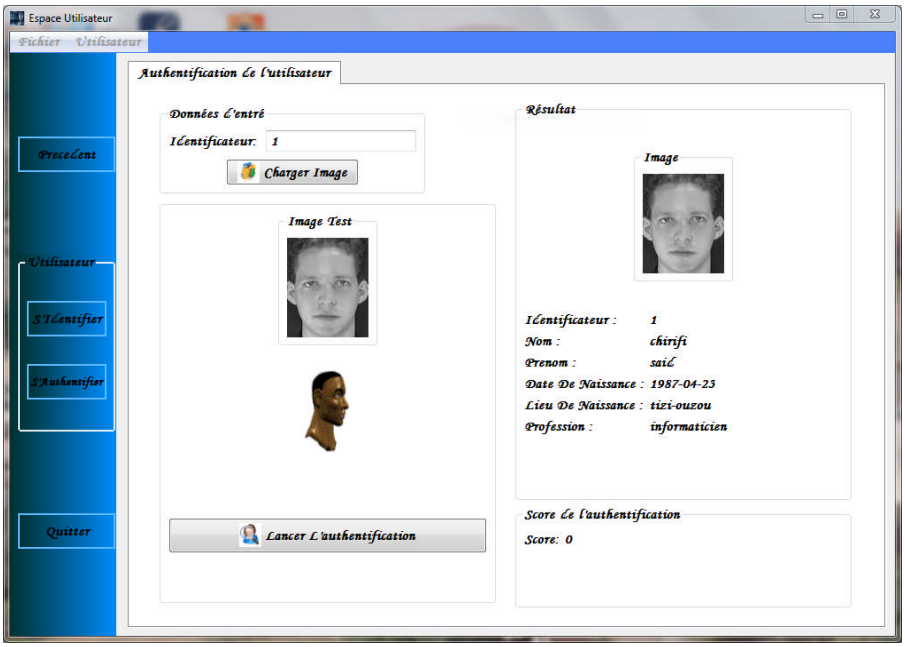


Figure IV.19 : Résultat du teste avec la même image que celle de la base de données

Pour la même image que celle de la base de données, la personne est acceptée avec un score de zéro.

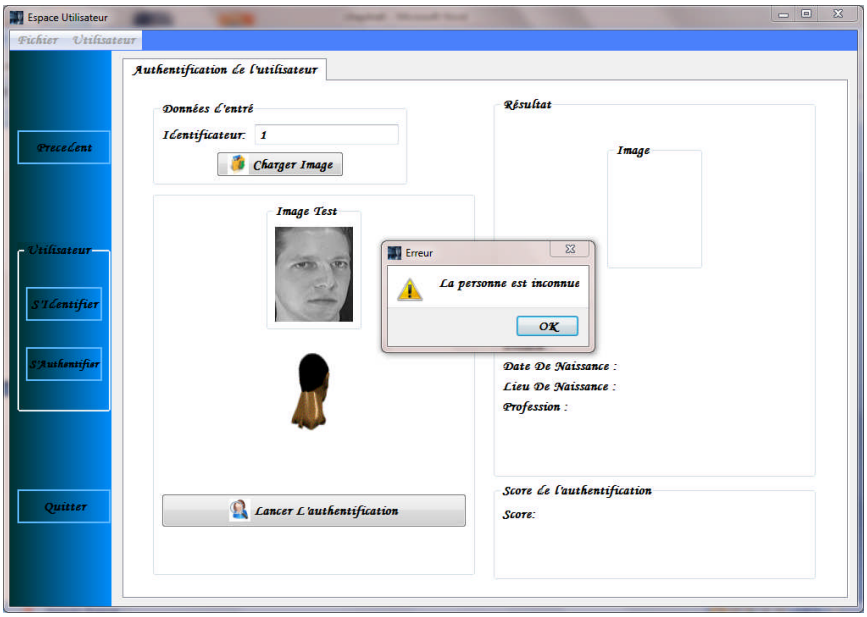


Figure IV.20 : Résultat du teste d'une image avec une pause différente

La même personne est rejetée avec un score de 3957 pour un seuil de 3305.

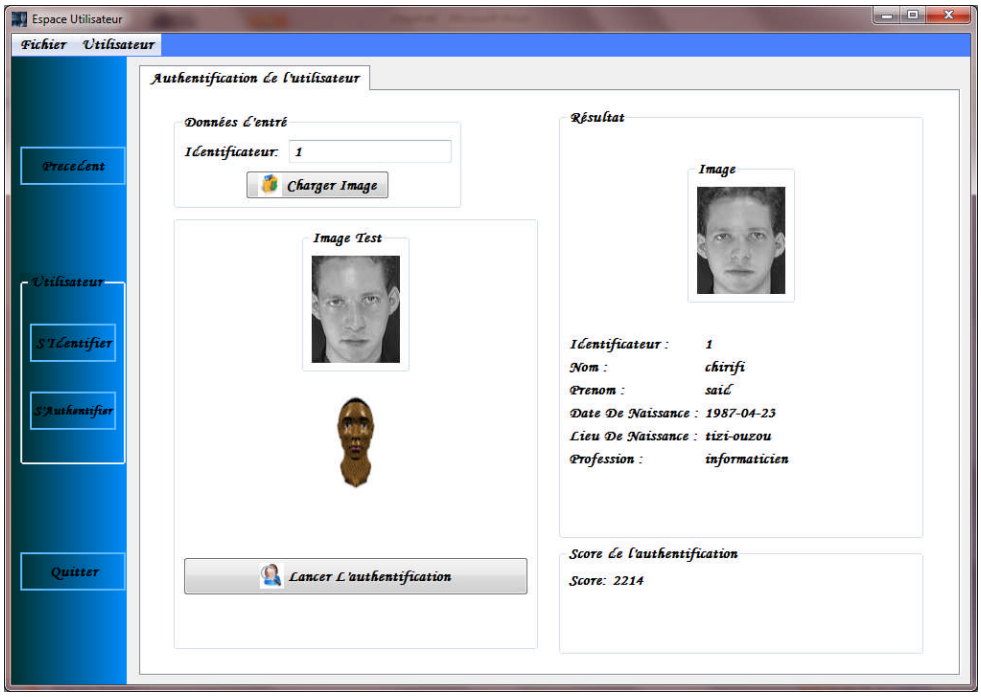


Figure IV.21 : Résultat du teste d'une image avec une autre pause

La personne est acceptée avec un score de 2214 pour un seuil de 2245.

Effet de port de lunettes :

Image base

Image teste

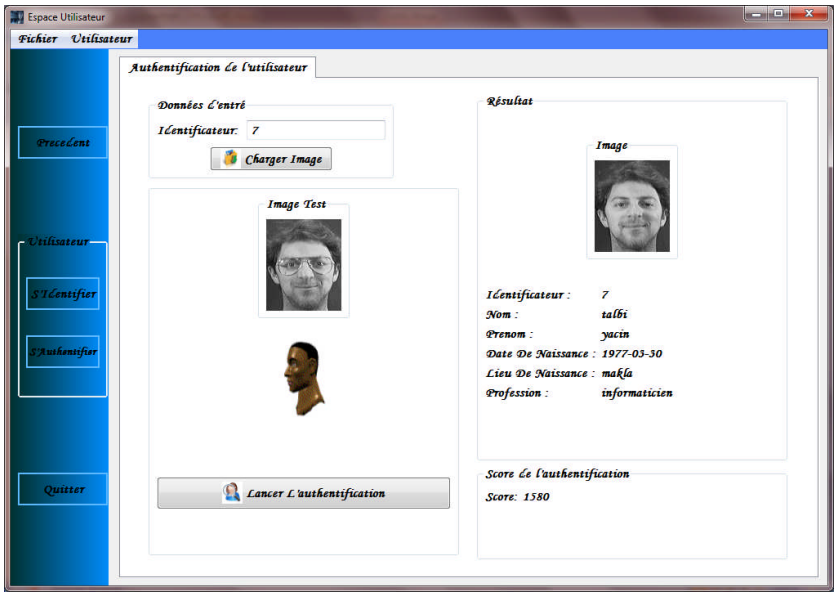


Figure IV.22 : Résultat du teste d'une image d'une personne portant des lunettes avec un seuil de 2245

La personne est reconnue avec un score de 1580 pour un seuil de 2245 mais rejetée pour un seuil de 1185.

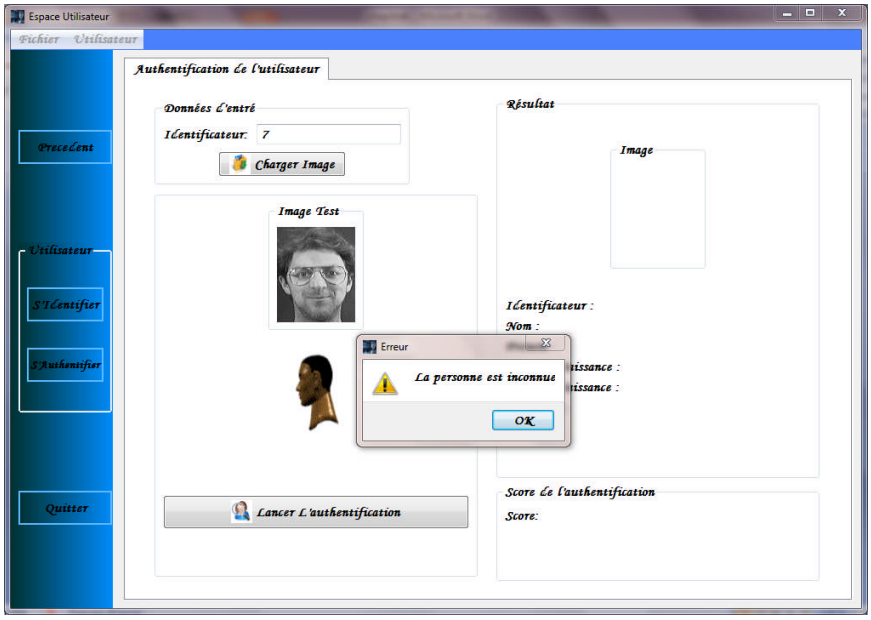


Figure IV.23 : Résultat du teste d'une image d'une personne portant des lunettes avec un seuil de 1185

Effet d'expression faciale :

Image base

Image teste

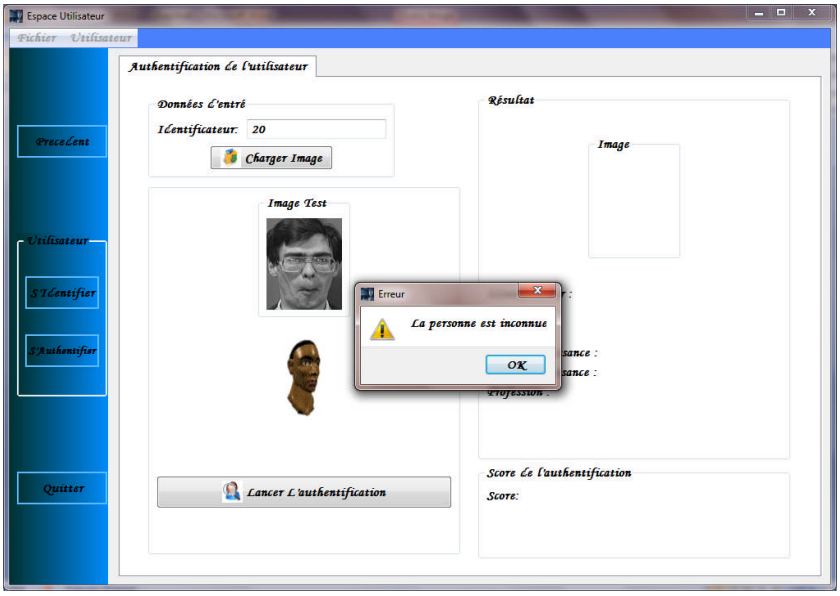


Figure IV.24 : Résultat du teste d'une image d'une personne avec une expression faciale différente

La personne est rejetée pour un seuil de 1185 avec un score de 1259.

Effet de changement d'éclairage

Image base

Image teste

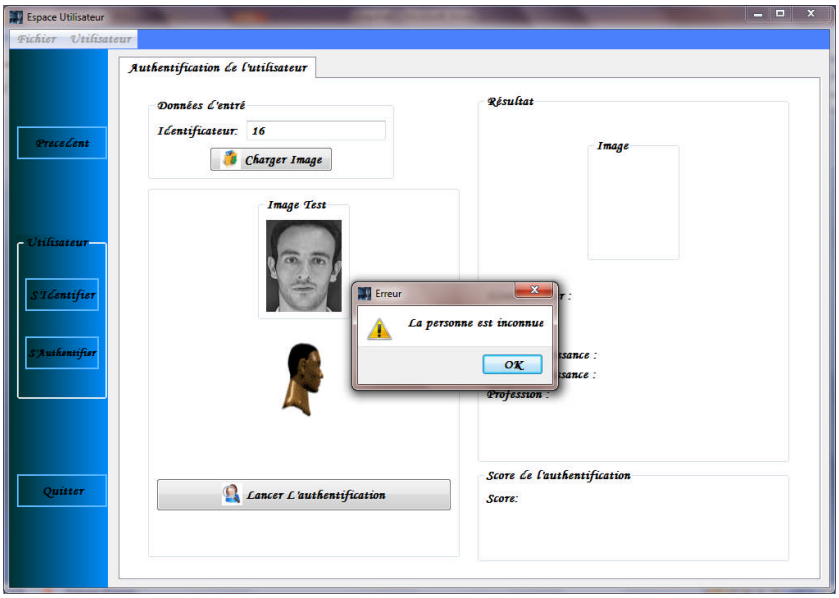


Figure IV.25 : Résultat du teste d'une image d'une personne dans un environnement avec un éclairage différent

La personne est rejetée avec un score de 3270 pour un seuil de 2245.

D'après tous ces testes effectués, nous remarquons que le système est sensible à la variation de pauses, changement d'éclairage et à l'expression faciale.

IV.5.2 La courbe roc de notre système :

La courbe roc représente la variation du taux de faux rejet en fonction du taux de fausse acceptation lorsque le seuil de décision varie.

Pour faire la courbe roc de notre système il faut calculer les taux d'erreur FAR et FRR tout en variant le seuil de décision. Les seuils pris sont : 1185, 2245, 3305, 4364, 5424.

Pour le calcule de FRR et FAR nous avons d'abord réorganisé la base de données ORL comme suit :

Nous avons considéré 10 dossiers (il y a 10 vues différentes pour chaque personne), dans chaque dossier nous avons pris 40 images des 40 personnes. En suite nous avons enregistré les 25 premières personnes du premier dossier dans la base de données et les 9 autres dossiers sont pris pour les testes.

Pour chaque dossier nous avons calculé les taux FRR et FAR pour chaque seuil des 5 précédents, puis nous avons fait la moyenne des 9 résultats obtenus.

Les résultats finals sont présentés par le tableau suivant :

Seuils	FRR	FAR
1185	0,87	0
2245	0,43	0
3305	0,17	0,063
4364	0,004	0,33
5424	0	0,77

Tableau VI.1 : Les taux d'erreur FAR et FRR de notre système

On peut présenter les résultats du tableau précédent à l'aide des deus courbes suivantes :

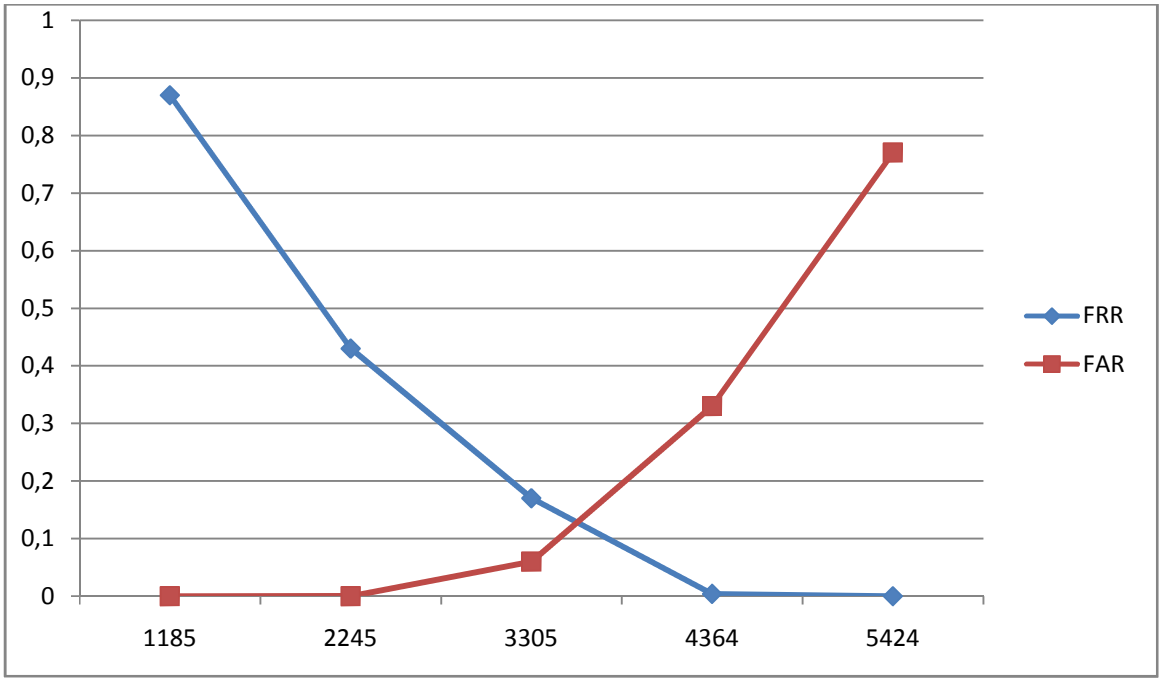


Figure IV.26 : Graphe représente la variation des taux de FRR et FAR en fonction du seuil

Ainsi on obtient la courbe roc suivante :

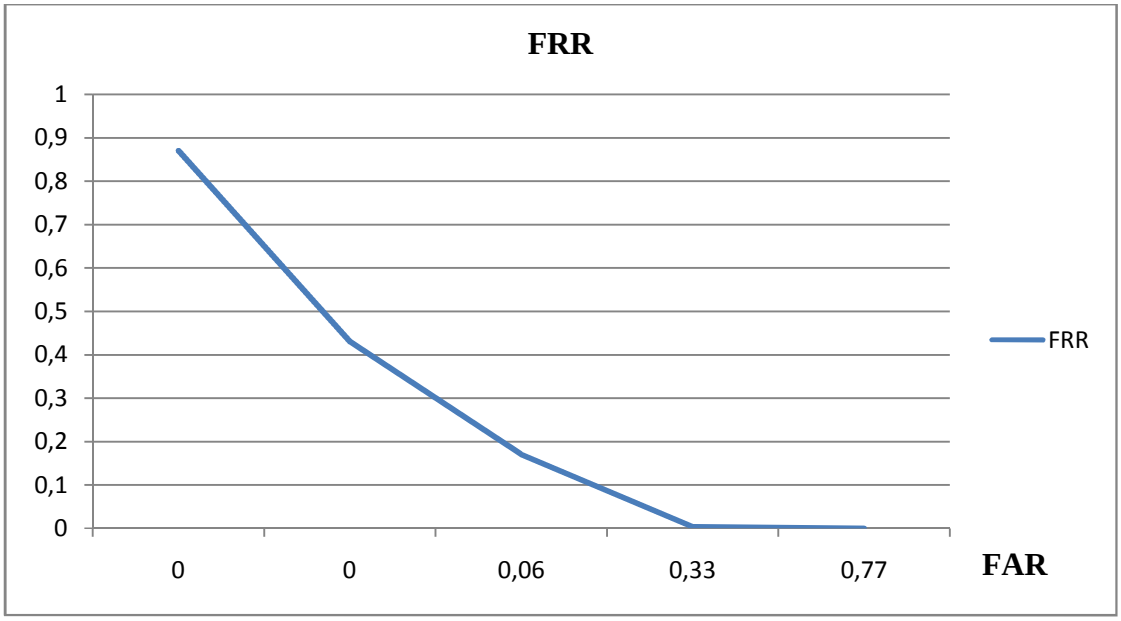


Figure IV.27 : La courbe roc de notre système

Nous remarquons d'après ces courbes, que les deux taux FRR et FAR varient en fonction du seuil de décision. Pour un seuil trop petit nous avons un taux de FRR trop élevé et un taux de FAR trop petit et plus le seuil augmente le taux de FRR diminue et le taux de FAR augmente.

Les résultats représentés par ces courbes sont ceux attendus, parce que pour un seuil petit (sécurité élevé) le taux de FRR est trop élevé et le taux de FAR est trop petit. Mais si on veut diminuer le taux de FRR le taux de FAR augmente pour un seuil plus grand, c'est-à-dire on va diminuer dans la sécurité du système. En effet, les deux taux d'erreur ne décroissent pas simultanément, si l'un croit l'autre décroit.

Le point d'intersection entre la courbe du taux de FAR et la courbe du taux de FRR présente le point d'équivalence des erreurs (EER). Bien que l'EER corresponde à un seuil où le système est plus performant, ce seuil n'est pas toujours celui considéré dans le cas pratique. En réalité, le seuil est choisi selon le niveau de la sécurité attendue de l'application. Si on veut un système très sécurisé, on minimise les fausses acceptations. Par conséquence, le taux des faux rejets augmente. Par contre, si la sécurité du système n'est pas assez critique, on minimise les faux rejets.

IV.6 Conclusion :

Dans ce chapitre nous avons présenté le langage de programmation ainsi que les différents outils utilisés pour la réalisation de notre système. Nous avons ensuite décrit toutes les principales fenêtres de notre application, et son fonctionnement général. Ainsi nous avons effectué quelques testes de notre application d'où nous avons montré l'effet de variation de poses, l'expression faciale, le changement d'éclairage et le port des lunettes sur le système. Ensuite, nous avons évalué la performance du système par le calcule des taux FRR et FAR pour faire la courbe roc.

Conclusion générale :

Ce travail s'inscrit dans le domaine de la reconnaissance automatique des visages. Celui-ci consiste à vérifier l'identité d'une personne à partir de son visage. Utilisé principalement pour des raisons de sécurité.

Dans ce travail, il était question d'implémenter un système biométrique de reconnaissance de visages basé sur la méthode globale PCA (Eigenfaces). L'algorithme PCA est l'une des approches les plus fiables et les plus simples.

Tout au long de la réalisation de ce projet, on a approché un domaine de biométrie très intéressant et d'avenir, avec tous les domaines qui lui sont attachés comme le traitement d'images, vision par ordinateur, reconnaissance de formes et l'analyse de données.

Jusqu'à maintenant il n'existe pas de système de reconnaissance de visages performant à 100%, de part la multitude de contraintes à qui l'image du visage est confrontée, en plus de la contrainte de l'environnement d'acquisition de l'image du visage qui doit être conditionné.

La méthode appliquée dans notre système (mesure de similarité) consiste à déterminer la différence entre l'image teste et celle de la base de données, et cette différence n'est pas nulle sauf si l'image teste est la même que celle de la base, et pour chaque image qui aura un grand changement la différence augmente et la chance de reconnaitre la personne diminue et cela est aussi en fonction du seuil fixé qui détermine le niveau de sécurité du système. Si le niveau de sécurité est trop élevé, la chance d'une personne d'être reconnue est faible ce qui engendre un grand nombre de faux rejet et à force que le niveau de sécurité baisse la chance de reconnaissance augmente c'est à dire le nombre de faux rejet diminue mais le nombre de fausse acceptation augmente.

Notre système ne contient pas un module de détection et de localisation du visage, et comme nous l'avons cité précédemment le système se base sur la méthode PCA, qui souffre de la sensibilité au changement d'éclairage et à la variation de pose.

Ainsi, et comme perspectives d'améliorations, on peut envisager l'étude et la réalisation d'un système de détection et de localisation du visage avec des performances assez hôtes, et pour palier aux problèmes de changement d'éclairage et de variation de pose on peut planifier une fusion avec une autre méthode (exemple : LDA).

Nous pouvons aussi penser qu'il serait très intéressant de réaliser un système bimodale combinant à la fois le visage et une autre technologie biométrique comme les empreintes digitales pour utiliser au maximum les avantages de ces deux modalités biométrique.

[1] John D.Woodward, Jr.,Christopher Horn, Julius Gatune , and Aryn Thomas, " Biometrics A Look at Facial Recognition" documented briefing by RAND Public Safety and justice for the Virginia State Crime Commission, 2003.

[2] http://Biometrie.online.fr.

[3] Anis CHAARI "Nouvelle approche d'identification dans les bases de données biométriques basée sur une classification non supervisée", thèse doctorat, Préparé au sein des laboratoires IBISC et RIADI, Octobre 2009.

[4] Vinh DANG Hoang Vu "Biométrie pour l'Identification" Promotion X - IFI, Hanoï, Vietnam 2005.

[5] **www.clusif.asso.fr/fr/.../pdf/ControlesAccesBiometrie.pdf**

[6] F.Perronnin et J.Dugelay. Introduction à la biométrie : "Authentification des Individus par Traitement Audio-Vidéo ", revue traitement du signal, volume 19, 2002.

[7] PHAN Viet Anh " Développement d'un module de segmentation pour un système de reconnaissance biométrique basé sur l'iris". Mémoire de fin d'étude, département Électronique et Physique de l'Institut National des Télécommunications. ÉVRY, France, Novembre 2008.

[8] C. Fredouille, J. Mariethoz, C. Jaboulet, J. Hennebert, J.-F. Bonastre, C. Mokbel, F. Bimbot, "Behavior of a Bayesian Adaptation Method for Incremental Enrollment in Speaker Verification", International Conference on Acoustics, Speech, and Signal Processing, p. 1197-1200, Istanbul, Turquie, 5-9 Juin 2000.

[9] Anthony LARCHER " Modèles acoustiques à structure temporelle renforcée pour la vérification du locuteur embarquée " thèse Doctorat, Université d'Avignon et des Pays de Vaucluse en collaboration avec Swansea University, septembre 2009.

[10] S. A. Israel, J. M. Irvine, A. Cheng, M. D. Wiederhold, et B. K. Wiederhold" ECG to identify individuals". Pattern Recognition 38(1), 133–142. 27), 2005.

[11] S. Marcel et J. del R. Millan, "Person Authentication using Brainwaves (EEG) and Maximum A Posteriori Model Adaptation", IEEE transactions on Pattern Analysis and Machine intelligence 29(4), 743–748. 27), 2007.

[12] **http://www.pierreau.fr/Dossier/Biometrie.pdf**

[13] Latila Acharya,Tomasz Kasprzykcki " La biométrie et son usage par l'Etat", Publication N°06-30-F, Révisé le16 Avril 2010.

[14] Sylvain Hocquet " Authentification biométrique adaptative Application à la dynamique de frappe et à la signature manuscrite", thèse doctorat, Université François Rabelais Tours ,2007.

[15] http://www.cai.gouv.qc.ca/06_documentation/01_pdf/biom_enj.pdf

[16] P. Jonathon Phillips, Alvin Martin, C. l. Wilson, and Mark Przybocki, "An introduction to evaluating biometric systems", Computer, 33(2) :56_63, 2000.

[17] BOUTELLAA Elhocine "Système biométrique de vérification de signatures manuscrites en ligne", thèse doctorat, École Doctorale Sciences et Technologies de l'Information et de la Communication (STIC), Oued-Smar Alger.

[18] ALLANO Lorène," La Biométrie multimodale : stratégies de fusion de scores et mesures de dépendance appliquées aux bases de personnes virtuelles ", thèse doctorat, l'universite d'evry-val d'essonne, Janvier 2009.

[19] JOURANI Reda "Reconnaissance de Visage", Université Mohammed V-Agdal, La faculté des sciences de Rabat, novembre 2006.

[20] Vinh DANG Hoang Vu "Biométrie pour l'Identification", Promotion X - IFI, Hanoï, Vietnam 2005.

[21] D.Mahmoudi "Biometrie Et Authentification", Rapport Technique, Suisse, 2000.

[22] Technique de Contrôle d'Acces par biometrie, technique CLUSIF, 2004, http://www.clusif.asso.fr,dossier

[23] IDENTIFICATION ET AUTHENTIFICATION BIOMETRIQUES ,Dossier d'architecture,ARS 2003-2004Pierre ROYER, http://www.pierreau.fr

[24] R. Brunelli and T. Poggio, "Face recognition: Features vs. templates" IEEE Trans. Pattern Anal. Mach. Intell., vol. 15, no. 10, pp. 1042–1053, Oct. 1993.

[25] Ahmed Chaari "Reconnaissance de visage par réseaux d'ondelettes de Gabor", these doctorat, Université Lille1, 08 decembre 2009 .

[26] Souhila Guerfi Ababsa, "Authentification d'individus par reconnaissance de caractéristiques biométriques liées aux visages 2D/3D", thèse doctorat, l'Université Evry Val d'Essonne, 03 octobre 2008.

[27] 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.

[28] Nicolas MORIZET, "Reconnaissance Biométrique par Fusion Multimodale du Visage et de l'Iris", thèse doctora, École Doctorale d'Informatique, Télécommunications et Électronique de Paris, Mars 2009.

[29] B. Hubbard, "Ondes et ondelettes. La Saga d'un outil mathématique. Pour la Science", July 2000.

[30] Fabrice Vermont, "LOCALISATION DE VISAGES", Projet de Diplôme, Lausanne, Février 2005.

[31] A.S. Tolba, A.H.El-Baz, and A.A. El-Harby, "face recognition : A literature Review", INTERNATIONAL JOURNAL OF SIGNAL PROCESSING VOLUME 2 NUMBER 2 2005 ISSN 1304-4494.

[32] Wen Geo, shiguang shan, face verification for access control, " Biometrics solutions for authentication in an E-World", Edited by David Zhang, Kuwer academic publishers, chapter 13, pp339-376, 2002.

[33] Turk, M.A., Pentland, A.P, "Eigenfaces for recognition". J. Cognit. Neurosci. Vol .3, p.71–86, 1991**.**

[34] Belhumeur, P.N., Hespanha, J.P., Kriegman, D.J. "Eigenfaces versus fisherfaces:recognition using class specific linear projection". IEEE Trans. Pattern Anal. Mach. Intell. Vol. 19 , No. 7 :p.711–720,1997.

[35] REDA Jourani, "reconnaissance des visages", Thèse des études supérieures approfondies, Faculté des Sciences de Rabat, 2006.

[36] S. palanivel, B. S. Venkatesh and B. Yegnamarayana, "Real time face recognition system using auto associative neural network models", Speech and vision laboratory Dpt of computer science and engineering, Indian institute of technology madras, India.

[37] Adjout Mohamed, Benaissa Abdelhak, "Fusion de la DCT-PCA et la DCT-LDA appliquée à la reconnaissance de visages", thèse d'ingénieur d'état, Institut National de formation en Informatique (I.N.I) Oued-smar Alger, 2007.

[38] B. Achermann and H. Bunke, "Combination of Classifiers on the Decision Level for Face Recognition", Technical Report IAM-96-002, Institut für Informatik und angewandte Mathematik, Universität Bern, January 1996.

[39] http://www.aiaccess.net/French/Glossaires/GlosMod/f_gm_matrice_symetrique.html

[40] William H. Press et al. "NumericalRecipes : the Art of scientific Computing 3rd Edition", chapitre 11, Eigensystems, Cambridge University Press, 2007.

[41] Pascal Roques" Modéliser un site e_commerce " Editions Eyrolles. Années d'édition 2002 .

[42] J.STEFFE , ENITA de Bordeaux, COURS UML ,Mars 2005.

[43] http://www.cam-orl.co.uk/facedatabase.html.

Annexe

UML *(unified modeling language):*

1. Historique :

C'est a la fin de l'année 1994 que lames rembauche et Grady Booch décident de travailler ensemble a l'élaboration d'une méthode unifier d'analyse et de conception objet.
En 1995, Ivar Jacobson les rejoints en apportant notamment le concept des cas d'utilisation, les premiers bases d'UML résulte de l'union de trois méthodes OMT (James rembauche).OOD (grady booch) et OOSE (Ivar Jacobson). [A2]

2. Définition :

UML (Unified Modeling Language) est un langage unifié pour la modélisation dans le Cadre de la conception orienté objet. Il s'agit d'un langage graphique de modélisation objet Permettant de spécifier, de construire, de visualiser et de décrire les détails d'un système Logiciel. Il est issu de la fusion de plusieurs méthodes dont « Booch » et « OMT » et adapté à La modélisation de tous types de systèmes. Il devint aujourd'hui un standard dans le domaine D'analyse et de conception orientée objet. [A1]

3. Présentation des modèles et diagrammes d'UML :

UML définit plusieurs modèles pour la représentation des systèmes :

- **Le modèle des classes** : le modèle de classe n'est plus utile c'est un formalisme pour représenter les concepts**.**
- **Le modèle des cas d'utilisation** : le modèle de cas d'utilisation décrit les besoins des utilisateurs.
- **Le modèle des états** : le modèle des états permet de représenter la dynamique des objets.
- **Le modèle d'interaction** : il représente de point de vue dynamique l'évolution des objets au cours de temps.
- **Le modèle de réalisation** : ce modèle moins important que les autres modèles d'UML, il montre les unités du travail.
- **Le modèle de déploiement** : il précise la préparation des processus.

Remarque :

Les modèles sont regarder et manipuler par les utilisateurs au moyen de vues graphique, a chaque vue correspondant un ou plusieurs diagrammes. UML définit neuf diagrammes :

- **Vus statique :**
    - Les digrammes de classes
    - Les digrammes D'objet
    - Les digrammes De cas d'utilisation
    - Les digrammes De composants
    - Les digrammes De déploiement
- **Vue dynamique :**
    - Les digrammes de séquence
    - Les diagrammes de collaboration
    - Le diagramme d'état de transition
    - Les diagrammes d'activités

4. Les diagrammes d'UML :

Un diagramme UML donne a l'utilisateur un moyen de visualiser et manipuler des éléments de modélisation.UML définit neufs sorte de diagramme pour représenter les différents points de vue de modélisation.

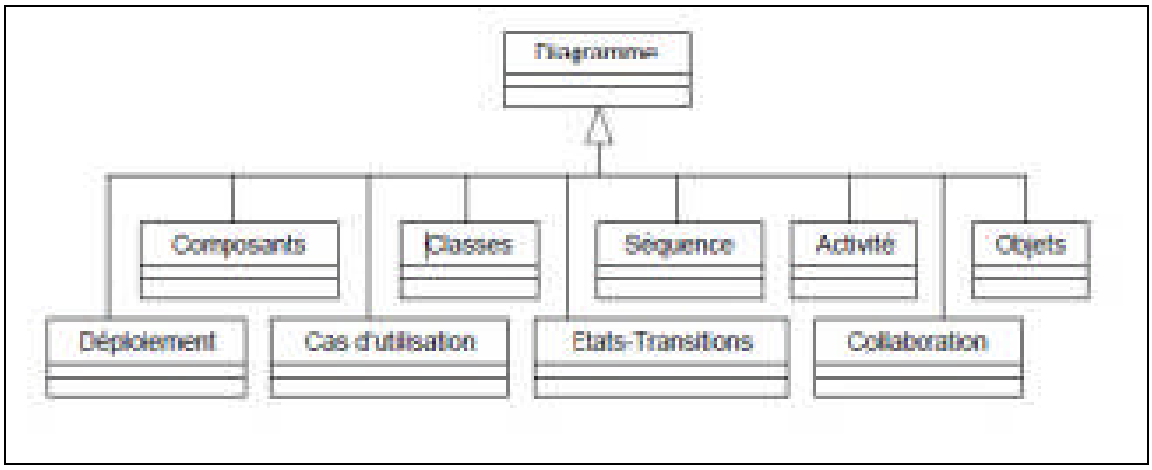


Figure A.1 : **Les diagrammes d'UML**

Voici les différents diagrammes :

4.1 Diagramme des cas d'utilisation :

4.1.1 Définition :

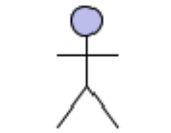
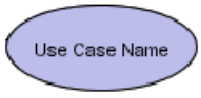
Les diagrammes des cas d'utilisation identifient les fonctionnalités fournies par le système (cas d'utilisation), les utilisateurs qui interagissent avec le système (acteurs), et les interactions Entre ces derniers. Les cas d'utilisation sont utilisés dans la phase d'analyse pour définir les Besoins de "haut niveau" du système.

Les objectifs principaux des diagrammes des cas d'utilisation sont:

- fournir une vue de haut-niveau de ce que fait le système.
- Identifier les utilisateurs ("acteurs") du système.
- Déterminer des secteurs nécessitant des interfaces homme-machine.

Les cas d'utilisation se prolongent au delà des diagrammes imagés. En fait, des descriptions textuelles des cas d'utilisation sont souvent employées pour compléter ces derniers et représentent leurs fonctionnalités plus en détail.

4.1.2 Représentation Graphique : Les composants de base des diagrammes des cas d'utilisation sont l'acteur, le cas d'utilisation, et l'association.

	Définition	**Représentation**
Acteur	un acteur est un utilisateur du système, et est représenté par une figure filaire. Le rôle de l'utilisateur est écrit sous l'icône, Les acteurs ne sont pas limités aux humains, Si le système communique avec une autre application, et effectue des entrées/sorties avec elle, alors cette application peut également être considérée comme un acteur	
Cas d'utilisation	un cas d'utilisation représente une fonctionnalité fournie par le système, typiquement décrite sous la forme Verbe+objet**,** ***Les*** cas d'utilisation sont représentés par une ellipse contenant leur nom.	
Association	les associations sont utilisées pour lier des acteurs avec des cas d'utilisation. Elles indiquent qu'un acteur participe au cas d'utilisation sous une forme	

	quelconque. Les associations sont représentées par une ligne reliant l'acteur et le cas d'utilisation. L'image suivante montre comment ces trois éléments de base collaborent pour former un diagramme de cas d'utilisation.	

4.1.3 Représentation textuelle : Chaque cas d'utilisation, est associé à une série d'actions représentant la fonctionnalité voulue, ainsi que les stratégies à utiliser dans l'alternative où la validation échoue, ou des erreurs se produisent, Ces actions peuvent être également définies dans la description de cas d'utilisation il n'y a donc aucune norme pour représenter ces cas textuellement. Cependant, il y a quelques règles communes que vous pouvez suivre:

4.1.4 Règles communes de description textuelle des cas d'utilisation:

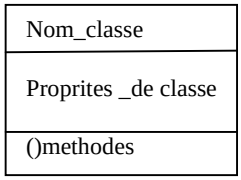
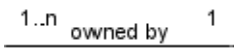
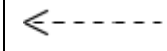
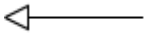
- Lister deux colonnes comprenant d'une part les actions de l'acteur et d'autre part les réponses du système.
- Utiliser un patron identifiant les acteurs, les conditions préalables, les post conditions, les scénarios principaux de réussite du processus, .etc.
- Rappelez-vous, le but du processus de modélisation est de pouvoir illustrer le mieux possible.
- les besoins du système, aussi n'hésitez pas à employer toutes les méthodes qui permettront une meilleurs compréhension des membres du projet.

4.2 Diagramme des Classes :

4.2.1 Définition :

Le diagramme des classes identifie la structure des classes d'un système, y compris les propriétés et les méthodes de chaque classe. Le diagramme des classes est le diagramme le plus largement répandu dans les spécifications D'UML.

4.2.2Représentation : Les éléments d'un diagramme des Classes sont les classes et les relations qui les lient.

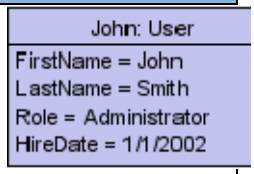
	Définition	Représentation
Classes	les classes sont les modules de base de la programmation orientée objet. Une classe est représentée en utilisant un rectangle divisé en trois sections. La section supérieure est le nom de la classe. La section centrale définit les propriétés de la classe.	
Association	une association est une relation générique entre deux classes. Elle est modélisée par une ligne reliant les deux classes. Cette ligne peut être qualifiée avec le type de relation, et peut également comporter des règles de multiplicité (par exemple un à un, un à plusieurs, plusieurs à plusieurs) pour la relation.	
Composition	si une classe ne peut pas exister par elle-même, mais doit être un membre d'une autre classe, alors elle possède une relation de composition avec la classe contenant. Une relation de composition est indiquée par une ligne avec un "diamant" rempli.	
Dépendance	quand une classe utilise une autre classe, par exemple comme membre ou comme paramètre d'une de ces fonctions, elle "dépend" ainsi de cette classe. Une relation de dépendance est représentée par une flèche pointillée.	
Agrégation	les agrégations indiquent une relation de contenant contenu. Elle décrite par une relation "possède". Une relation d'agrégation est représentée par une ligne avec un "diamant" creux.	
Généralisation	Une relation de généralisation est indiquée par une flèche creuse se dirigeant vers la classe "parent ".	

4.3 Diagramme des Objets :

4.3.1 Définition :

Les diagrammes des objets modélisent des exemples de classes. Ce type de diagramme est Employé pour décrire le système à un instant particulier

4.3.2 Représentation : Souvent, le diagramme des objets utilise une notation plus simple que le diagramme des classes correspondant, se focalisant sur les instances des objets et non sur les relations entre leurs classes (héritage compris). Beaucoup de diagrammes des objets représentent seulement les objets et les associations.

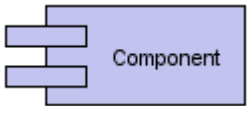
	Définition	**Représentation**
Objet	des objets sont identifiés en plaçant le nom d'instance suivi des deux points (:) devant le nom de l'Objet des objets sont identifiés en plaçant le nom d'instance suivi des deux points (:) devant le nom de la classe. Les valeurs de propriété sont écrites comme des paires " nom=valeur ". L'icône représentant un objet est un rectangle divisé en sections.	
Association	le diagramme des objets peut contenir également des associations. Souvent, les contraintes, le détail des relations et les règles de multiplicité trouvées dans le diagramme de classe ne sont pas représentés pour ne se concentrer que sur les objets et leurs propriétés. Les associations entre les objets sont représentées simplement en utilisant une ligne les joignant.	

4.4 Diagramme des composants :

4.4.1 Définition :

Le diagramme des composants est principalement employé pour décrire les dépendances entre les divers composants logiciels tels que la dépendance entre les fichiers exécutables et les fichiers source.

4.4.2 Représentation :

	Définition	**Représentation**
Composant	un composant représente une entité logicielle d'un système. (Fichier de code source, programmes, documents, fichiers de ressource .etc.). Un composant est représenté par une boîte rectangulaire, avec deux rectangles dépassant du côté gauche.	
Dépendance	une dépendance est utilisée pour modéliser la relation	

	entre deux composants. La notation utilisée pour cette relation de dépendance est une flèche pointillée, se dirigeant d'un composant donné au composant dont Il dépend	

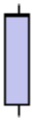
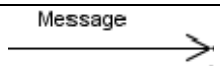
4.5 Diagramme des séquences :

4.5.1 Définition :

Les diagrammes des séquences documentent les interactions à mettre en œuvre entre les Classes pour réaliser un résultat, tel qu'un cas d'utilisation, UML étant conçu pour la programmation orientée objet, ces communications entre les classes sont reconnues comme Des messages. Le diagramme des séquences énumère des objets horizontalement, et le temps Verticalement. Il modélise l'exécution des différents messages en fonction du temps.

4.5.2 Représentation : Dans un diagramme des séquences, les classes et les acteurs sont énumérés en colonnes, avec leurs lignes de vie verticales indiquant la durée de vie de l'objet.

	Définition	**Représentation**
Objet	les objets sont des instances des classes, et sont rangés horizontalement. La représentation graphique pour un objet est similaire à une classe (un rectangle) précédée du nom d'objet (facultatif) et d'un point-virgule (:) .	
Acteur	les acteurs peuvent également communiquer avec des objets, ainsi ils peuvent eux aussi être énumérés en colonne. Un acteur est modélisé en utilisant le symbole habituel: Stick man.	
Ligne de vie	les lignes de vie, LifeLine, identifient l'existence de l'objet par rapport au temps. La notation utilisée pour une ligne de vie est une ligne pointillée verticale partant de l'objet.	

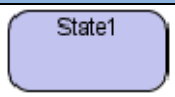
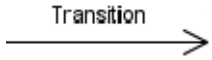
Activation	les activations, sont modélisées par des boîtes rectangulaires sur la ligne de vie. Elles indiquent quand l'objet effectue une action.	
Message	les messages, modélisés par des flèches horizontales entre les activations, indiquent les communications entre les objets.	

4.6 Diagramme d'état :

4.6.1 Définition :

Les diagrammes d'état sont utilisés pour documenter les divers modes ("état") qu'une classe peut prendre, et les événements qui causent une transition d'état.

4.6.2 Représentation :

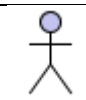
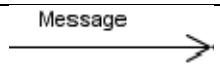
	Définition	**Représentation**
Etat	la notation de l'état décrit le mode de l'entité. Elle est représentée par rectangle avec les coins arrondie, contenant le nom de l'état.	
Transition	une transition décrit le changement de l'état d'un objet, provoqué par un événement. La notation utilisée pour représenter une transition est une flèche, avec le nom d'événement écrit au-dessus, au-dessous, ou à côté.	
Etat initial	l'état initial est l'état d'un objet avant toutes transitions. Pour des objets, ceci pourrait être l'état lors de leur instanciation. L'état initial est représenté par un cercle plein. Un seul état initial est autorisé sur un diagramme.	
Etat final	l'état final représente la destruction de l'objet que nous modélisons. Ces états sont représentés par un cercle plein entouré d'un cercle.	

4.7 Diagramme de collaboration:

4.7.1 Définition :

La collaboration est un mécanisme compose d'éléments structurel et comportementaux. Elle englobe deux constructions : une description de contexte statique des objets et une interaction représentée par les messages échanger. [A2]

4.7.2 Représentation :

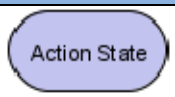
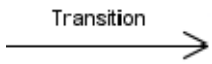
	Définition	**Représentation**
Objet	les objets, instances des classes, représentent une des entités impliquées dans les communications. La représentation graphique pour un objet est similaire à une classe (un rectangle) précédée du nom d'objet (facultatif) et de deux points (:).	
Acteur	les acteurs peuvent également communiquer avec des objets, aussi peuvent ils être présents sur des diagrammes de collaborations. Un acteur est modélisé en utilisant le symbole habituel: Stick man.	
Message	les messages, modélisés par des flèches entre les objets, sont affectés d'un numéro et indiquent les communications entre les objets.	

4.8 Diagramme d'activité :

4.8.1 Définition :

Les diagrammes d'activité sont utilisés pour documenter le déroulement des opérations dans un système, du niveau commercial au niveau opérationnel (de haut en bas).

4.8.2 Représentation :

	Définition	**Représentation**
Etat d'activité	l'état d'activité marque une action faite par un objet. Il est représenté par un rectangle arrondi.	
Transition	quand un état d'activité est accompli, le traitement passe à un autre état D'activité. Les transitions sont utilisées pour marquer ce passage. Les transitions sont modélisées par des flèches.	

Couloir (*Swimlane)*	Dans un diagramme d'activité, on peut placer les activités dans des couloirs (*Swimlanes*) qui représentent des systèmes. Les objets sont énumérés au dessus de la colonne, et les barres verticales séparent les colonnes pour former les swimlanes.	
Etat initial	l'état initial marque le point d'entrée la première activité. Il est représenté, comme dans le diagramme d'état, par un cercle plein. Il ne peut y avoir qu'un seul état initial sur un diagramme.	
Etat final	L'état final marque la fin du déroulement des opérations	
Barre de Synchronisation	Souvent, certaines activités peuvent être faites en parallèle. Pour dédoubler le traitement "Fork", ou le reprendre quand des activités multiples ont été accomplies ("join"), des barres de synchronisation sont utilisées. Celles ci sont modélisées par des rectangles pleins, avec des transitions multiples entrantes ou sortantes.	

5. Conclusion :

UML est un moyen d'exprimer des modèles objet en faisant abstraction de leur implémentation, c'est-à-dire que le modèle fourni par UML est valable pour n'importe quel langage de programmation.

Les différents digrammes d'UML permettre de faire une bonne modélisation pour un projet et une bonne structuration des données.