

MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE
SCIENTIFIQUE

UNIVERSITÉ MOULOUD MAMMERI DE TIZI OUZOU

FACULTÉ DE GÉNIE ÉLECTRIQUE ET DE L'INFORMATIQUE



DÉPARTEMENT INFORMATIQUE

**Mémoire de fin d'études
de MASTER ACADÉMIQUE**

Domaine : Mathématique et informatique

Filière : Informatique

Spécialité : Réseau , Mobilité et systèmes embarqués

Thème :

**Développement d'un système biométrique multimodal
basé sur la fusion des scores de matching**

Président : Mr Mohammed-said HABET

Examineur : Mr Mohamed RAMDANI

Encadreur : Mme Chafia CHERIFI

Présenté par :

Boussa Rahim Ryad

Boussad Faouzi

Promotion: 2019-2020

Remerciements

*Nous tenons à témoigner notre reconnaissance à DIEU
tout
puissant, qui nous a aidé et bénit par sa volonté durant
toute cette année.*

*Nous tenons à exprimer nos vifs remerciements
accompagnés de toute notre gratitude, tout d'abord à
notre*

*Promotrice Mme CHERIFI, pour avoir accepté de nous
encadrer, diriger et orienter durant toute la durée de ce
projet ainsi que pour la marque de confiance qu'elle nous
a
manifesté et ses précieux conseils furent d'un apport
considérable.*

*A tous les enseignants de l'UMMTO qui ont contribué à
notre formation.*

*Nos plus vifs remerciements vont aussi aux membres du
jury pour avoir accepté d'honorer par leur jugement notre
travail.*

*Nos sincères sentiments vont à tous ceux qui, de près ou
de
loin, ont contribué à la réalisation de ce projet, en
particulier nos chères familles et nos amis.*

SOMMAIRE :

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

Chapitre I : BIOMETRIE : Applications, concepts et enjeux

I.1 Introduction.....	3
I.2 La biométrie.....	3
I.2.2 Définition.....	3
I.2.2 Historique.....	3
I.3 Les modalités biométrique.....	4
I.3.1 Méthodes morphologiques.....	4
I.3.2 Méthodes comportementales.....	8
I.3.3 Méthodes biologiques.....	11
I.3.4 Méthodes multimodales.....	12
I.4 Les caractéristiques de la biométrie.....	12
I.5 Domaine d'application de la biométrie.....	13
I.6 Marché de la biométrie.....	14
I.7 Le système biométrique.....	15
I.7.1 Définition.....	15
I.7.2 Architecture d'un système biométrique.....	15
I.7.3 Evaluation et mesure de performance.....	18
I.8 Les avantages et limites des systèmes biométriques.....	20
I.8.1 Les avantages.....	20
I.8.2 Les limites.....	20
I.9 Conclusion.....	21

Chapitre II : Système de reconnaissance de visages

II.1 Introduction.....	22
II.2 Pourquoi le visage ?.....	22
II.3 Système de reconnaissance du visage.....	22
II.3.1 Fonctionnement du système.....	22
II.3.1.1 Détection et acquisition de l'image.....	23
II.3.1.2 Prétraitement.....	23
II.3.1.3 Extraction des caractéristiques.....	23

II.3.1.4 Apprentissage.....	24
II.3.1.5 Classification.....	24
II.3.1.6 Comparaison et décision	24
II.4 Les difficultés de la reconnaissance faciale.....	24
II.5 Méthodes de reconnaissances.....	27
II.5.1 Les méthodes globales.....	28
II.5.2 Les méthodes locales.....	30
II.5.3 Les méthodes hybrides.....	31
II.5.4 Les méthodes de reconnaissance 3D.....	32
II.6 Conclusion.....	33

Chapitre III : Système de reconnaissance des empreintes digitales

III.1 Introduction.....	34
III.2 Pourquoi l'empreinte digitale ?.....	34
III.3 Définition et classification de l'empreinte digitale.....	34
III.3.1 La représentation globale.....	35
III.3.1 La représentation locale.....	36
III.4 Système de reconnaissance des empreintes digitales.....	37
III.4.1 Prétraitement des images empreinte.....	38
III.4.2 Les méthodes d'extraction de caractéristiques.....	39
III.4.3 Comparaison des empreintes.....	43
III.5 Conclusion.....	45

Chapitre IV : La fusion de modalités

IV.1 Introduction.....	46
IV.2 Pourquoi s'orienter vers la multimodalité?.....	46
IV.3 La fusion multimodale.....	46
IV.3.1 Conception d'un système biométrique multimodal	46
IV.3.2 Les différentes formes de multi-modalité.....	47
IV.4 Les différents niveaux de fusion	48
IV.4.1 Fusion avant matching.....	49
IV.4.2 Fusion après matching.....	49
IV.5 La fusion au niveau des scores.....	51

IV.6 Normalisation des scores.....	51
IV.7 Techniques de classification des scores.....	53
IV.8 Techniques de combinaison des scores.....	53
IV.9 Conclusion.....	55

Chapitre V : Conception et réalisation

V.1 Introduction.....	56
V.2 Conception.....	56
V.2.1 Les acteurs du systèmes	56
V.2.2 Diagramme de cas d'utilisation général.....	56
V.2.3 Diagrammes de séquence détaillée	58
V.2.4 Architecture et fonctionnement du système.....	61
V.3 Réalisation	68
V.3.1 Outils de développement et de test.....	68
V.3.2 L'implémentation du système.....	68
V.4 Conclusion.....	71

Chapitre VI : Résultats expérimentaux

V.1 Introduction.....	72
V.2 Le sous-système de reconnaissance de visages.....	72
V.2.1 La base de données ORL	72
V.2.2 Évaluation du sous-système.....	74
V.3 Le sous-système de reconnaissance des empreintes digitales	77
V.3.1 La base de données DB2.....	77
V.3.2 Évaluation du sous-système.....	77
V.4 Le système de reconnaissance multimodal.....	78
V.4.1 Évaluation du système.....	78
V.5 Conclusion.....	80
Conclusion générale.....	81

Liste des figures :

Chapitre I : BIOMETRIE : Applications, concepts et enjeux

Figure I.1 Système de mesures corporelles de Bertillon.....	4
Figure I.2 Empreinte digitale.....	5
Figure I.3 Reconnaissance de visage.....	6
Figure I.4 L'iris	6
Figure I.5 La rétine.....	7
Figure I.6 Spectre d'un signal voix.....	8
Figure I.7 Reconnaissance de la démarche.....	9
Figure I.8 un système de reconnaissance de la dynamique de la frappe	9
Figure I.9 Signature sur une tablette graphique.....	10
Figure I.10 L'ADN d'une cellule d'eucaryote est situé dans des chromosomes au sein du noyau..	11
Figure I.11 La thermographie faciale.....	11
Figure I.12 Marché de la biométrie par région	14
Figure I.13 Les parts de marché biométrique par technologie	15
Figure I.14 Architecture d'un système biométrique.....	15
Figure I.15 Enrôlement d'une personne dans un système biométrique	16
Figure I.16 Identification d'un individu dans un système biométrique	16
Figure I.17 Authentification d'un individu dans un système biométrique	17
Figure I.18 Distributions des scores authentiques et imposteurs.....	18
Figure I.19 Courbe ROC.....	19
Figure I.20 Exemple de courbes CMC pour différents algorithmes de reconnaissance faciale	19

Chapitre II : Système de reconnaissance de visages

Figure II.1 Architecture d'un système de reconnaissance faciale.....	23
Figure II.2 Exemple de normalisation.....	23
Figure II.3 Exemple d'un visage avec des changements de luminosité.....	24
Figure II.4 Exemple d'un visage avec des variations de pose.....	25
Figure II.5 Exemple d'un visage sans et avec une barbe.....	25
Figure II.6 Exemple de variations d'expressions faciales.....	26
Figure II.7 Variations dû à la présence d'occlusions partielles.....	26
Figure II.8 Exemple de changement d'apparence avec le temps.....	27
Figure II.9 Classification des algorithmes principaux utilisés en reconnaissance faciale.....	27

Figure II.10 Illustration du principe de séparation optimale des classes par le LDA.....	29
Figure II.11 Machines à Vecteur de Support (SVM)	31
Figure II.12 (a) Visage normalisé ; (b) 2D Image; (c) 2.5D Image.....	32

Chapitre III : Système de reconnaissance des empreintes digitales

Figure III.1 Caractéristiques d'une empreinte digitale	35
Figure III.2 Les principales classes d'empreintes digitales.....	36
Figure III.3 Les types de minuties.....	36
Figure III.4 Représentation des vecteurs de terminaison et de bifurcation.....	37
Figure III.5 Architecture générale d'un système complet de reconnaissance d'empreintes.....	37
Figure III.6 L'empreinte digitale en gris.....	38
Figure III.7. Orientation locale dans une image d'empreinte.....	38
Figure III.8 Binarisation de l'empreinte digitales.....	39
Figure III.9 Squelettisation de l'empreinte digitale	40
Figure III.10 Les cinq cas obtenus lors de processus d'extraction des minuties.....	40
Figure III.11 Processus d'extraction des minuties	41
Figure III.12 Type des fausses minuties.....	41
Figure III.13 L'image directionnelle.....	42
Figure III.14 Le suivi d'une crête.....	42
Figure III.15. Fingerprint dans une image	43
Figure III.16 Les variations intra-classe d'une même empreinte digitale.....	44
Figure III.17 La comparaison basée sur les minuties.....	45
Figure III.18 L'extraction des informations de texture basées sur l'orientation locale.....	45

Chapitre IV : La fusion de modalités

Figure IV.1 Sources d'informations dans un système de fusion biométrique.....	47
Figure IV.2 Schéma de répartition des différents niveaux de fusion biométrique.....	48
Figure IV.3 Fusion aux niveau du capteur.....	49
Figure IV.4 Fusion au niveau des caractéristiques.....	49
Figure IV.5 Fusion au niveau de la décision.....	50
Figure IV.6 La fusion au niveau des scores.....	50

Chapitre V : Conception et réalisation

Figure V.1. Diagramme de cas d'utilisation global.....	57
Figure V.2. Diagramme de séquence « Apprentissage ».....	58

Figure V.3. Diagramme de séquence « Identification ».....	59
Figure V.4. Diagramme de séquence « Authentification».....	60
Figure V.5. Diagramme de séquence « Tests de performance».....	61
Figure V.6. Diagramme de fonctionnement du système.....	62
Figure V.7. Représentation modulaire de la phase « Apprentissage ».....	62
Figure V.8. Les étapes de prétraitement des images du visage.....	62
Figure V.9. Les étapes de prétraitement des images de l’empreinte digitale.....	63
Figure V.10. Algorithme DWT.....	63
Figure V.11. Algorithme de détection de minuties.....	64
Figure V.12. Algorithme d’élimination des fausses minuties.....	64
Figure V.13. Calcul du FRR.....	67
Figure V.14. Calcul du FAR.....	67
Figure V.15. Interface pour l’enrollement d’un nouveau sujet.....	69
Figure V.16. Interface pour les tests de performances.....	69
Figure V.17. interface graphique de l’authentification.....	70
Figure V.18. interface pour l’identification.....	71

Chapitre VI : Résultats expérimentaux

Figure VI.1. Base de données ORL.....	73
Figure VI.2. Exemple de changements d’orientations du visage.....	73
Figure VI.3. Exemple de changements d’éclairage.....	73
Figure VI.4. Exemple de changements des expressions faciales.....	73
Figure VI.5. Exemple de port de lunettes.....	74
Figure VI.6. FAR en fonction du type d’ondelette et de la distance	74
Figure VI.7. FRR en fonction du type d’ondelette et de la distance.....	75
Figure VI.8. TID en fonction du type d’ondelette et de la distance.....	76
Figure VI.9. Exemple d’empreintes digitales de la base FVC2002 DB2.....	77
Figure VI.10. Variation du FAR (%) et du FRR (%) en fonction des règles de fusion.....	78
Figure VI.11. Variation du TID (%) en fonction des règles de fusion.....	79

Introduction générale

La nécessité de la sécurité civile et la lutte contre les fraudes d'une part et l'explosion de l'informatique et la croissance des moyens de communication d'autre part ont fait augmenter le besoin de sécurisé et de s'assurer l'identité des individus. Les systèmes d'authentification traditionnels (mots de passe, codes PIN, badges, clefs,...etc.) ne sont pas vraiment fiables (faciles à falsifier) à cause de leur inhabilité à différencier entre une personne autorisée (client) et une personne non autorisée (un imposteur), problème qui provoque l'apparition des systèmes biométriques.

En fait l'utilisation de la biométrie pour des fins de reconnaissance n'est pas vraiment récente, l'utilisation de caractères anthropométriques comme le visage, la voix, et la démarche afin de reconnaître les individus est le moyen le plus naturel chez les êtres humains. L'utilisation des empreintes digitales remonte à la plus haute antiquité, les premières traces d'utilisation de cette caractéristique ont été découvertes en Egypte (il y'a plus de 4000 ans). Les chinois ont aussi utiliser ce trait très tôt pour des fins de signature de documents. Depuis 1897, les empreintes digitales ont été adoptées par les services de police dans les enquêtes criminelles, cependant les procédures manuelles et la gestion des bases de données rendent le travail long et coûteux.

Aujourd'hui le développement technologique favorise l'apparition des systèmes de reconnaissance automatiques de plus en plus puissants, beaucoup d'autres caractéristiques d'authentification (comme le visage, la voix, la signature, la rétine, l'iris etc.) sont utilisées, la biométrie n'est plus limitée aux empreintes digitales. L'utilisation des systèmes de reconnaissance basés sur la biométrie augmente de manière significative, Les applications biométriques sont nombreuses et permettent d'apporter un niveau de sécurité supérieur dans plusieurs domaines, tels que, le contrôle d'accès physique à des lieux protégés, et le contrôle d'accès virtuel à des réseaux d'ordinateurs.

Un système biométrique typique doit au moins garantir les conditions suivantes : l'universalité, l'unicité, l'acceptabilité, la facilité d'utilisation, la stabilité, la mesurabilité et la robustesse face aux attaques frauduleuses. Bien que les techniques biométriques montrent leur vigueur, cependant Il est difficile de trouver un système biométrique unimodal basé sur une seule donnée biométrique ou signature unique qui permet de garantir avec certitude une bonne identification (un taux de reconnaissance de 100%) ou qui remplisse toutes les exigences d'un système biométrique typique.

Avec l'utilisation de la biométrie multimodale, toutes ces limitations peuvent être réduites ou bien supprimées, l'identification par cette biométrie consiste à combiner deux à plusieurs systèmes unimodaux tout en améliorant la performance de la reconnaissance.

Dans ce mémoire , l'objectif est le développement d'un système de reconnaissance biométrique multimodal basé sur deux des principales technologies biométriques (en termes de part de marché international de la biométrie) à savoir l'empreinte digitale et la reconnaissance faciale. Pour la fusion des informations issues de ces deux sources biométriques, nous avons opter pour la fusion aux niveaux des scores. Le manuscrit de ce mémoire est organisé autour de six chapitres, de la manière suivante :

- Dans le premier chapitre nous allons introduire la biométrie avec ces caractéristiques et les différente modalités, les systèmes biométriques avec les mesures de performances utilisées pour leur évaluation, ainsi que les avantages et les limitations de ces systèmes.
- Dans le deuxième chapitre nous allons introduire les systèmes de reconnaissance de visages, ces principales difficultés et enfin nous allons explorer les différentes techniques de reconnaissance.

- Dans le troisième chapitre nous allons voir un état de l'art sur les empreintes digitales et le fonctionnement des systèmes de reconnaissance basés sur cette même modalité (le prétraitement , les méthodes d'extraction et les méthodes de comparaison).
- Dans le quatrième chapitre nous allons voir un état de l'art de la multimodalité et nous allons introduire les différents niveaux de fusions en décrivant la fusion au niveau de scores.
- Dans le cinquième chapitre nous allons présenter la phase de conception et réalisation de notre système, les cas d'utilisation de notre système ainsi que toutes les méthodes utilisé pour le réaliser.
- Le sixième chapitre est dédié à l'évaluation des performances des systèmes de reconnaissance faciale et de reconnaissance d'empreintes digitales en fonction des méthodes mise en œuvre ainsi que les performances avec différentes règles fusion du système multimodal résultant de la fusion de deux modalités (visage et l'empreinte digitale).
- Nous terminons ce mémoire par une conclusion générale.

CHAPITRE I

BIOMETRIE : Applications, concepts et enjeux

I.1 Introduction :

La biométrie constitue l'ensemble des technologies qui exploitent des caractéristique biométriques (physiques, comportementales ou biologiques) comme des moyens d'identification des individus. Ces technologies exploitent les caractéristiques qui sont uniques chez les individus et ne peuvent être perdues ni volées ni reconstituées contrairement aux moyens classiques reposant sur des mots de passe ou des cartes magnétiques. C'est pour cette raison que la biométrie apparaît comme l'une des meilleures technologies contre la fraude à l'identité.

Le présent chapitre donne un aperçu sur les principales technologies biométriques qui sont disponibles ainsi que leurs comparatifs. Il décrit également le principe de fonctionnement des systèmes biométriques et les outils utilisés pour mesurer leurs performances ainsi que leurs avantages et limites.

I.2 La biométrie :

I.2.1 Définition

A. Définition : La biométrie désigne dans un sens très large l'étude quantitative d'une population à l'aide des mathématiques, et plus précisément dans le cas qui nous intéresse, la technologie qui analyse les caractéristiques physiques ou comportementales d'un individu et permettant la vérification de son identité.

B. Définition (Larousse) : En technologie, la biométrie désigne la technique qui permet d'associer à une identité une personne voulant procéder à une action grâce à la reconnaissance automatique d'une ou de plusieurs caractéristiques physiques et comportementales de cette personne préalablement enregistrées (empreintes digitales, visages, voix, etc).

I.2.2 Historique :

Les toutes premières formes d'utilisation de la biométrie remontent à bien plus longtemps que ce que la plupart des personnes croient. En effet, dès -3000 avant J-C, les historiens ont des traces d'échanges commerciaux babyloniens utilisant les empreintes digitales pour la transaction de biens, en office de signature, ou encore vers le 7^{ème} siècle en Chine antique pour les mêmes raisons [1].

C'est à partir du 17^{ème} siècle que des études scientifiques ont vraiment commencé, cas de Marcello Malpighi (1628-1694) un médecin italien, qui découvre la couche basale de l'épiderme (couche quasiment la plus à l'intérieur) suivi de plusieurs études effectués par plusieurs chercheurs avec le temps, de Johannes Evangelista Purkinje (1787 – 1869), le premier, en 1823, à avoir caractérisé les différences dans les empreintes digitales. Il les classe en 9 catégories de motifs jusqu'à Sir Francis Galton (1822-1911), physicien anglais où dans l'ouvrage «*Fingerprints*» il présente ses études et explique que les empreintes digitales sont propres à chaque humain, qu'elles sont uniques et permanentes [1].

A la fin du 19^{ème} siècle, Alphonse Bertillon (1853-1914) est un grand criminologue français, il a inventé un système (Bertillonnage 1882) qui identifie les criminels en mesurant les différentes parties du corps, leur morphologie et en notant les différentes marques d'un corps, que ce soit la taille, des cicatrices, des taches de naissance etc... (figure 1.3) [1].

Et ce n'est qu'aux débuts du 20^{ème} siècle, que des recherches sur d'autres formes de reconnaissance biométrique apparaissent (Rétine, Iris), et avec l'arrivée des systèmes informatique et le traitement du signal numérique à partir des années 60, l'approche algorithmique de la biométrie est apparue ce qui a conduit immédiatement à l'automatisation de l'identification humaine. Les systèmes de reconnaissance des locuteurs (1966) et de reconnaissance des empreintes digitales (1963) ont été parmi les premiers à être explorés [2].

Les années 1970 ont vu le développement et le déploiement de systèmes de géométrie de la main et le début des essais à grande échelle et l'intérêt croissant pour l'utilisation gouvernementale de ces technologies d'identification personnelle automatisée (1977). Les systèmes de vérification de signature (1983) sont apparus dans les années 1980, suivis par des systèmes de visage (1981). Les systèmes de reconnaissance de l'iris (1993) ont été développés dans les années 1990 [2].

Au 21^{ème} siècle d'autres systèmes biométriques plus innovants ont été développés tel que les battements de cœurs en 2012, le mouvement des yeux en 2013, la thermographie en 2014 ... etc.

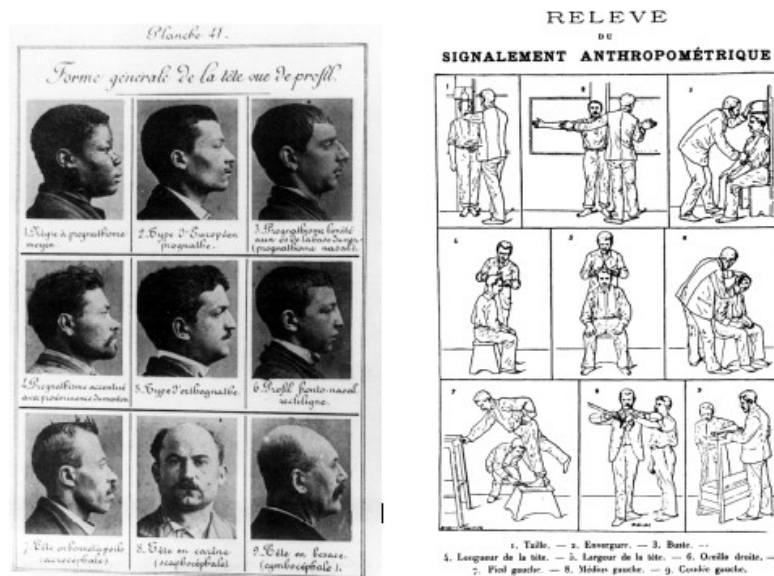


Figure 1.1 Système de mesures corporelles de Bertillon

I.3 Les modalités biométrique :

Il existe trois grandes familles de modalités biométriques permettant de vérifier ou de déterminer l'identité d'un individu. C'est des caractéristiques physiques, comportementales ou biologiques unique pour chaque individu et donc fiables et sécurisées pour la reconnaissance, elles surpassent les méthodes traditionnelles tel que les mots de passe, les signatures...etc.

I.3.1 Méthodes morphologiques :

C'est la plus répandue pour sa facilité de mise en œuvre et son acceptation par le public, elle traite les caractéristiques physiques d'un individu, parmi eux citons :

A. L'empreinte digitale :

L'empreinte digitale est le dessin formé par un doigt sur un support suffisamment lisse pour qu'y restent marqués, les dermatoglyphes et elles sont uniques à chaque individu et chaque doigt a son empreinte propre. La probabilité que deux personnes aient les mêmes empreintes digitales est infinitésimale : une chance sur 64 milliards [3].

L'identification par cette caractéristique est la technique la plus anciennement utilisée. En fait, c'était toujours le choix biométrique évident pour les services de police depuis plus de 100 ans. Il existe plusieurs types de système de capture d'empreinte digitale : optique, thermique, électromagnétique et ultrasons [4].



Figure I.2 Empreinte digitale [5]

Les avantages et les inconvénients de la reconnaissance par l'empreinte digitale :

Les avantages	Les inconvénients
• La plus ancienne et la plus connue des utilisateurs • Facile à mettre en œuvre • Faible coût • Technologie viable et exécution rapide.	• Besoin de la coopération de l'utilisateur • Moyennement accepté par la société . • Problème d'universalité (Certaines personnes ne possèdent ou pas d'empreinte digitales ou détruites dans le temps)

B. Le visage :

Le visage est le moyen le plus naturel pour identifier une personne, ce qui explique pourquoi cette caractéristique est bien acceptée par les utilisateurs. L'image du visage peut être captée par une caméra numérique, ou un appareil photo pour extraire un ensemble de facteurs considérés propres à chaque individu.

Ces dernières 25 années , la performance des systèmes de reconnaissance du visage s'est grandement améliorée mais les résultats sont encore loin d'être parfaits.

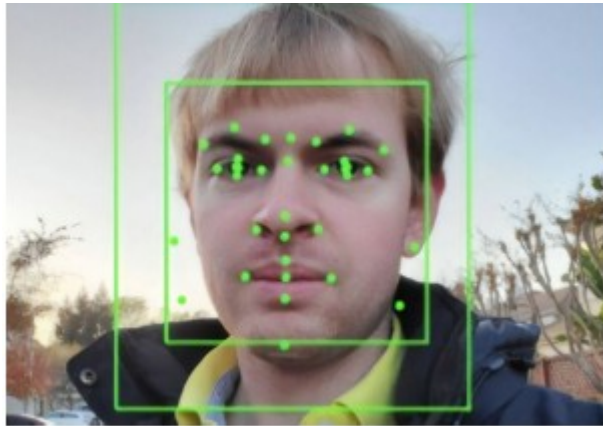


Figure I.3 Reconnaissance de visage

Les avantages et les inconvénients de la reconnaissance de visages :

Les avantages	Les inconvénients
• Aucun contact physique avec l'utilisateur • Faible coût • Très bien acceptées par les populations et très répandue • Performance élevées	• Sensible à l'environnement (éclairage, expression faciale ...) • Impossibilité de distinguer entre deux vrais jumeaux • Sensible au changement moustaches, lunettes, barbe)

C. L'iris :

L'iris est la région annulaire située entre la pupille et le blanc de l'œil. La biométrie par ce trait est récente puisqu'elle ne s'est véritablement développée que dans les années 80, et c'est une caractéristique très fiable, selon les estimations de Daugmann 1, la probabilité de trouver 2 iris suffisamment identiques est 1 sur 10^{72} environ, elle permet de différencier même entre jumeaux ou entre l'œil gauche et l'œil droit.

L'image de l'iris est capturée par une caméra standard contraignantes (exemple la distance entre la camera et l'iris ne dépasse pas un mètre), ce qui limite l'utilisation de cette modalité.

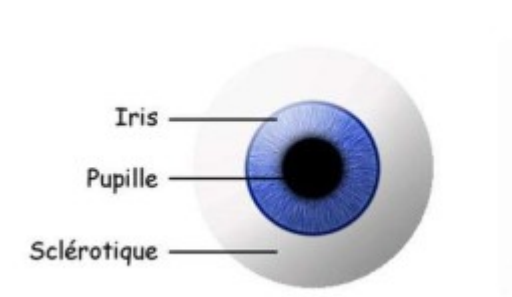


Figure I.4 L'iris [5]

Les avantages et les inconvénients de la reconnaissance de l'iris :

Les avantages	Les inconvénients
• Performance et fiabilité très élevée • La texture de l'iris est parfaitement stable au cours du temps et passe à travers les lunettes, lentilles • Différencie entre deux vrais jumeaux	• Technologie très coûteuse • Besoin de la coopération de l'utilisateur • La fiabilité diminue proportionnellement à la distance entre l'œil et le capteur

D. La rétine :

La rétine est la couche sensorielle de l'œil qui permet la vision, cette zone est parcourue par des vaisseaux sanguins dont leurs positions sont uniques et stables durant toute la vie de la personne. L'identification de la rétine n'est pas récente, elle remonte aux années 30. Cette technologie est considérée parmi les plus fiables toutefois elle est mal acceptée par les utilisateurs à cause des contraintes de l'acquisition.

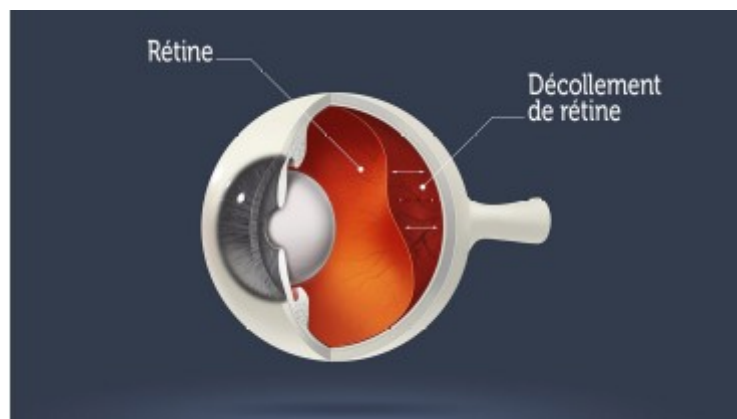


Figure I.5 La rétine

Les avantages et les inconvénients de la reconnaissance de la rétine :

Les avantages	Les inconvénients
• Performance et fiabilité très élevée • Durable dans le temps • Les risques de fraude sont quasi nuls, puisque la partie du corps exploitée n'est pas apparente.	• Technologie coûteuse • Système intrusif et peu agréable • Ne passent pas à travers des lunettes et peut, de plus, les réseaux sanguins peuvent être modifiés (forte alcoolémie, diabète)

I.3.2 Méthodes comportementales :

Ce sont des méthodes qui se basent sur des éléments comportementales qui sont propres à l'individu, parmi eux citons :

A. La voix :

La voix humaine est une caractéristique biométrique qui n'exige aucun contact physique avec le lecteur de système, elle dépend de la structure anatomique de l'individu, elle se constitue de composants physiologiques (tonalité, âge, sexe, fréquence, accent, harmoniques...) et comportementaux (vitesse, rythme, etc.).

En 1962 Lawrence Kersta [6] a prouvé que la voix de chaque personne est unique et qu'il est possible de la présenter graphiquement. Il existe deux principales méthodes de traitements de ce trait biométrique, la première dépend de texte prononcé, et la deuxième (la plus difficile) est indépendante de texte. Bien que cette modalité ne nécessite pas de matériel cher (microphone par exemple), cependant le bruit ambiant et les propriétés acoustiques telles que la réflexivité et l'absorption influencent son efficacité.



Figure I.6 Spectre d'un signal voix

Les avantages et les inconvénients de la reconnaissance de la voix :

Les avantages	Les inconvénient
• Système non intrusif • Faible coût • Très bien acceptées par les populations	• Sensible aux bruits ambiants • Fraude possible par enregistrement • Dépend de l'état de l'utilisateur (physique et émotionnel)

B. Analyse de la démarche :

Elle consiste à identifier les individus par leurs manières de marché (mouvement du corps, longueur de pas...), qui est supposée unique pour chaque individu.

Deux types de techniques d'identification de ce trait peuvent être distingués, l'approche "Model-based" qui dépend de quelques paramètres comme la longueur des parties du corps, la longueur de pas, la jointure d'angle etc. et l'approche "Appearance- based" qui est une analyse directe de l'image en extrayant les caractéristiques.

L'avantage majeur de cette biométrie consiste dans le fait qu'on peut identifier la personne à distance.



Figure I.7 Reconnaissance de la démarche

Les avantages et les inconvénients de la reconnaissance de la démarche :

Les avantages	Les inconvénients
• Système non intrusif • Très bien acceptées par les populations • Permet une reconnaissance à distance	• Très peu répandu et toujours en cours • Aucune preuve que la démarche est unique actuellement • Mise en œuvre difficile d'un tel système

C. Dynamique de frappe au clavier :

La dynamique de frappe au clavier est l'une de ces formes d'identification biométrique qui permet de vérifier l'identité d'un individu en analysant le rythme auquel cette personne tape. De la pression mise sur les touches en passant par les fautes régulières et la vitesse de frappe, chacun a une méthode supposée unique de taper au clavier. Un système basé sur cette dynamique ne nécessite aucun équipement particulier, seulement un ordinateur disposant d'un clavier [7].

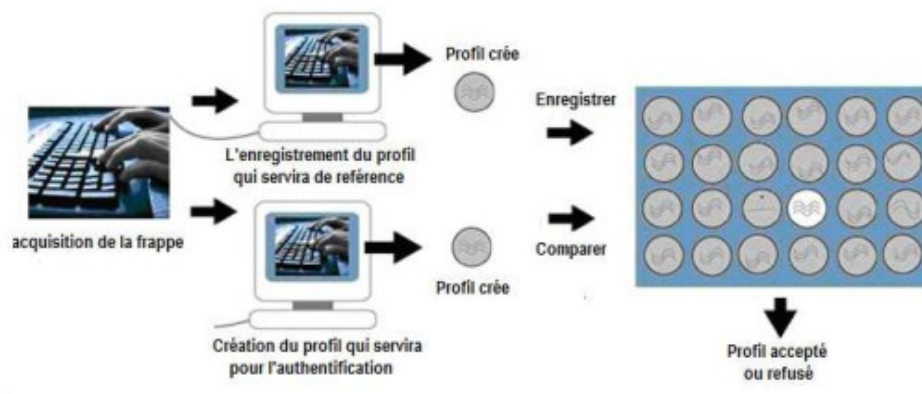


Figure I.8 un système de reconnaissance de la dynamique de la frappe [5]

Les avantages et les inconvénients de la reconnaissance de la démarche :

Les avantages	Les inconvénients
• Facile à mettre en œuvre et pas coûteuse	• Très peu répandue • Dépend de l'état de l'utilisateur (physique et émotionnel)

D. Dynamique de l'écriture (la signature) :

Chaque personne a un style d'écriture unique. On peut donc définir, à partir de la signature d'une personne, un modèle qui pourra être employé pour effectuer une identification. On distingue deux façons de capturer et de traiter une signature, soit avec des capteurs simples (scanners) et une analyse statique de la signature qui utilise la géométrie de la signature, soit par l'usage d'une palette graphique (ou équivalent) munie d'un stylo sensible à la pression et une analyse dynamique de la signature qui utilise les paramètres statiques ainsi que l'accélération, la vitesse et les profils de trajectoire de la signature [8].



Figure I.9 Signature sur une tablette graphique

Les avantages et les inconvénients de la reconnaissance de la dynamique de la signature :

Les avantages	Les inconvénients
• Une forme acceptable juridiquement et administrativement pour l'identification des personnes • Signer est un geste naturel et facile pour les populations	• Difficile d'atteindre une très haute exactitude d'identification en raison des grandes variations de signature pour une même personne

I.3.3 Méthodes biologiques :

Elle traite les composantes biologiques de l'individu comme :

A. L'ADN :

L'acide désoxyribonucléique ou ADN est une macromolécule biologique présente dans toutes les cellules d'un être vivant [9] et son analyse est une méthode extrêmement précise d'identification, issue directement de l'évolution de la biologie moléculaire. Cependant l'identification d'une personne grâce à son ADN est assez coûteuse à mettre en place et lente à réaliser.

L'information génétique d'un individu est unique (aucun membre de l'espèce ne possède la même combinaison de gènes codés l'ADN). Le profil génétique, aujourd'hui couramment utilisé pour des identifications judiciaires où il présente une percée majeure dans la criminalistique pour l'identification des personnes inconnues ou pour déterminer la source des échantillons biologiques laissés dans les lieux de crime. Le profil génétique fut introduit officiellement pour la première fois dans une affaire criminelle en 1986 par l'universitaire anglais Alec Jeffreys [10,11].

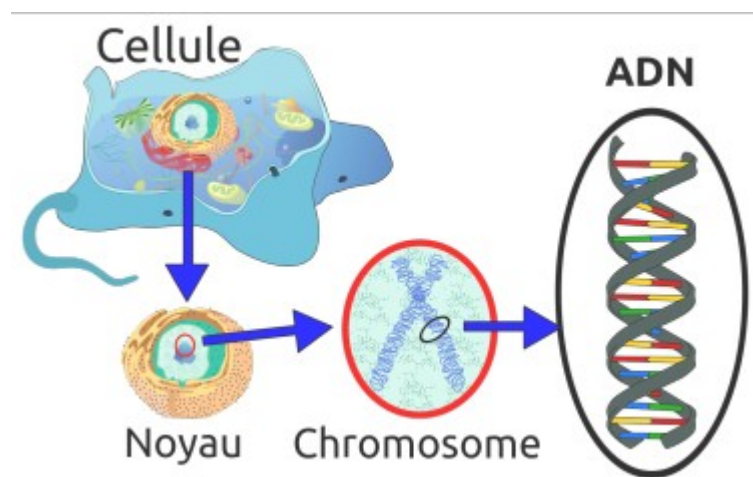


Figure I.10 L'ADN d'une cellule d'eucaryote est situé dans des chromosomes au sein du noyau[9].

B. La reconnaissance de la thermographie faciale :

La thermographie se définit comme une technique permettant d'obtenir une image thermique d'une scène au moyen d'un appareillage approprié comme utiliser un appareil photo ou une caméra numérique dans le domaine de l'infrarouge [12]. La quantité de chaleur émise par les différentes parties du visage qui est capturées dans n'importe quelle condition d'éclairage et même dans le noir complet caractérise chaque individu de façon unique. Elle dépend de la localisation des veines mais aussi de l'épaisseur du squelette, la quantité de tissus, de muscles, de graisses, etc.

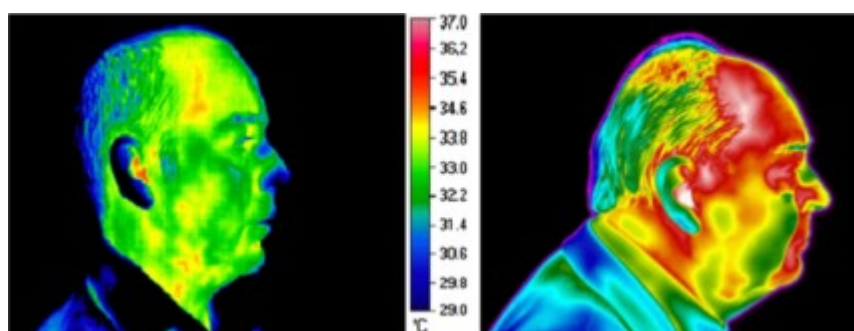


Figure I.11 La thermographie faciale

C. L'odeur corporelle :

La plupart des mammifères ont une odeur corporelle qui leur est propre, en tant qu'espèce, et en tant qu'individu. Chez les insectes, elle est un moyen courant d'identification de l'appartenance à l'espèce, à la colonie. Chez les mammifères, c'est un moyen courant d'identification des individus les uns par les autres au sein d'un groupe [13]. Cette odeur corporelle provient d'un mélange complexe de substances chimiques. Le parfum naturel du corps se compose du sébum (notre propre huile essentielle), de la sueur, de l'activité des bactéries sur notre peau et des hormones que contiennent le sébum et la sueur. Les systèmes biométriques qui exploitent cette technologie analysent ces composantes ensuite transformées en données comparatives pour la reconnaissance.

L'identification humaine à partir de l'odeur corporelle n'est pas nouvelle. Les polices s'en servent depuis plus d'un siècle en faisant appel à des chiens renifleurs, dont l'odorat est suffisamment puissant pour retrouver une personne à partir d'un échantillon qu'ils ont senti et En 1999, d'après un article de presse de CNR-Australia (Computer-News-Reseller) une société anglaise Mastiff-Electronics situé à Hampshire, des travaux entrepris sous le nom de code SCENTINEL, pour le développement d'un système biométrique d'identification d'individu s'appuyant sur l'odeur corporelle de la personne.

I.3.4 Méthodes multimodales :

Certaines méthodes unimodales possèdent un système d'identification difficile à contourner mais en contrepartie il est intrusif, et assez coûteux à mettre en place, d'autres quant à elles ont soit des performances pas très satisfaisantes ou sont susceptibles de fraude par enregistrement, copie ... etc.

Afin d'y remédier difficultés liées aux systèmes précédents, une première solution consiste à intégrer la biométrie avec l'identification basée sur une connaissance ou une possession tel qu'un mot de passe ou un code PIN (identification à deux facteurs). Cette méthode permet d'améliorer la sécurité du système, mais elle possède les faiblesses inhérentes à l'identification basée sur une connaissance ou une possession, la seconde solution est la multi modalité, une alternative qui permet de fusionner plusieurs systèmes biométriques afin d'améliorer de manière systématique la performance d'un système biométrique [14]. Par performance, nous entendons à la fois la précision du système mais aussi son efficacité, plus particulièrement en mode identification [15]. En effet, des classificateurs différents font en général des erreurs différentes, et il est possible de tirer parti de cette complémentarité afin d'améliorer la performance globale du système.

I.4 Les caractéristiques de la biométrie :

Une caractéristique biométrique (ou trait) est une caractéristique physique, comportementale ou biologique contenant l'essentiel d'informations permettant la distinction d'un individu. Chacune de cette caractéristique peut être considérée comme une caractéristique biométrique dans la mesure où elle respecte les exigences suivantes [16] :

A. Universalité : La caractéristique doit être possédée par chaque individu.

B. Unicité : la caractéristique doit être unique pour chaque individu pour pouvoir différencier entre les individus.

C. Permanence (durabilité) : Les caractéristiques biométriques devraient résister au changement dans le temps (invariante dans le temps).

D. Mesurabilité : Les caractéristiques biométriques doivent être quantitativement mesurables pour être ensuite traitées et utilisées pour la comparaison de deux individus.

E. Performance : Un système biométrique pratique doit avoir une précision acceptable et une vitesse de reconnaissance raisonnable vis-à-vis des ressources requises.

F. Acceptabilité : A quel degré les personnes visées à utiliser l'application acceptent de présenter leurs traits biométriques au système.

G. Infalsifiabilité : La caractéristique doit être difficilement falsifiable afin d'éviter une utilisation frauduleuse du système.

Les caractéristiques biométriques ne possèdent pas toutes ces propriétés, ou les possèdent mais à des degrés différents. Le tableau ci-dessous, extrait de [17], compare les principales modalités biométriques selon les propriétés suivantes : universalité (U), unicité (N), permanence (P), collectabilité (C), acceptabilité (A) et performance (E).

Information	U	N	P	C	A	E
ADN	Oui	Oui	Oui	Faible	Faible	xxxxx
Empreinte digitale	Oui	Oui	Oui	Oui	Moyenne	xxxx
Visage	Oui	Non	Faible	Oui	Oui	xxxx
Iris	Oui	Oui	Oui	Oui	Faible	xxxxx
Rétine	Oui	Oui	Oui	Oui	Faible	xxxxx
Géométrie de la main	Oui	Non	Oui	Oui	Oui	xxxx
Démarche	Oui	Non	Faible	Oui	Oui	xxx
Dynamique de frappe	Oui	Oui	Faible	Oui	Oui	xxxx
Voix	Oui	Oui	Faible	Oui	Oui	xxxx

Tableau I.1 comparaison des principales modalités biométriques

I.5 Domaine d'application de la biométrie :

Le champ d'application de la biométrie couvre potentiellement tous les domaines où la sécurité et/ou l'identification est nécessaire. Aujourd'hui, les principales applications sont la production de titres d'identité, le contrôle d'accès à des sites sensibles, le contrôle des frontières, l'accès aux réseaux, systèmes d'information, stations de travail et PC, le paiement électronique, la signature électronique et même le chiffrement de données. Cette liste n'est pas exhaustive, et de nouvelles applications vont très certainement voire rapidement le jour.

Ces principales applications sont divisées en trois grandes classes :

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

B. Applications gouvernementales : Telle que les titres d'identité (carte nationale d'identité, passeport, permis de conduire, carte de séjour) et les systèmes de vote électroniques.

C. Applications juridiques : Elles consistent généralement en l'identification de corps des victimes, la recherche criminelle, l'identification de terroriste ... etc.

I.6 marché de la biométrie :

La biométrie connaît une croissance et un engouement sans précédent, il existe peu d'informations publiques concernant ce marché. Cependant on peut considérer quelques chiffres pour évaluer son développement au fil des années suivantes.

Selon des prévisions, le marché de la biométrie passerait de 33 milliards de dollars en 2019 à 65.3 milliards de dollars en 2024, avec un taux de croissance annuel de 14.6% durant cette période 2019-2024.

Dans son rapport intitulé «Sensors for Biometry and Recognition 2016», l'Institut d'études Yole Développement estime que les technologies d'empreintes digitales dominantes évolueront progressivement vers des solutions multimodales [18].

Selon Yole, 525 millions d'unités de capteurs auraient été vendues en 2015 et ce chiffre devrait atteindre 1.500 millions d'unités d'ici 2021. A côté de la détection des empreintes digitales pour le déverrouillage et le paiement mobile, il faut compter avec les technologies de reconnaissance visuelle pour la sécurité basée sur les images combinées de l'œil et du visage. En outre, les assistants vocaux développés par Amazon et Google mettent en jeu des modules de reconnaissance vocale enregistrée [18].

Les facteurs majeurs de cette croissance sont le développement du secteur des applications smartphone (66% du marché total de la biométrie), et les initiatives ne prisent pas les gouvernements pour adopter des solutions biométriques [18].

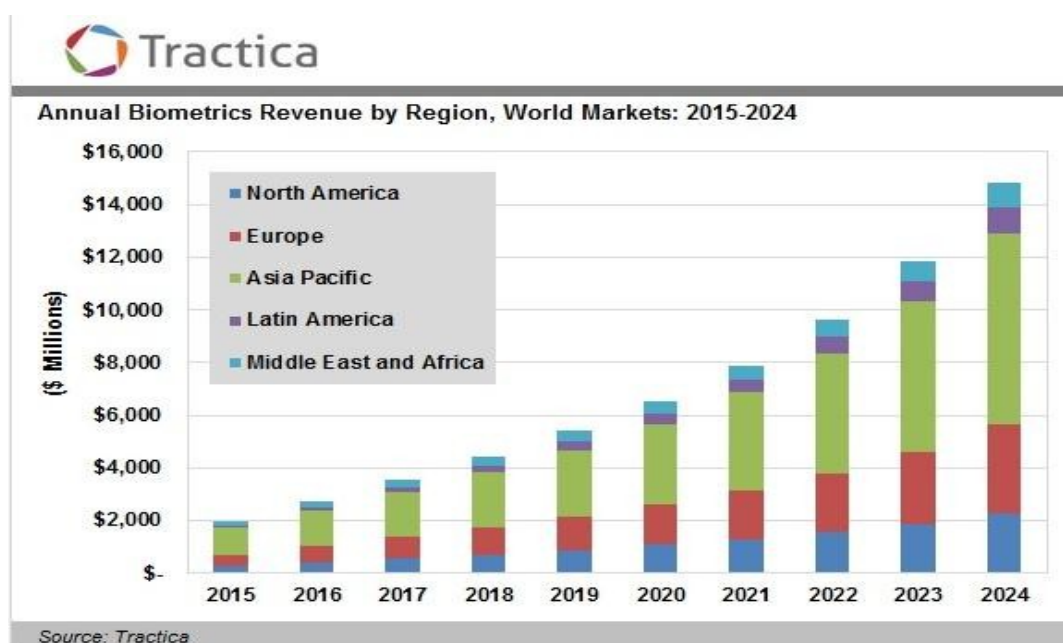


Figure I.12 Marché de la biométrie par région [19]

La plus grande part du marché est consacrée aux systèmes de reconnaissance par empreinte digitale (environ 31 % du chiffre d'affaires total). Le succès de ces systèmes est dû essentiellement à leur précision, popularité et leur coût relativement bas. Vient ensuite la reconnaissance par l'iris qui a gagné, durant ces dernières années (16 % de la part du marché), en dépassant la reconnaissance de du visage (15% de la part du marché) qui avait avant la deuxième place en termes de source de revenus après les empreintes digitales.

Biometrics Market Share

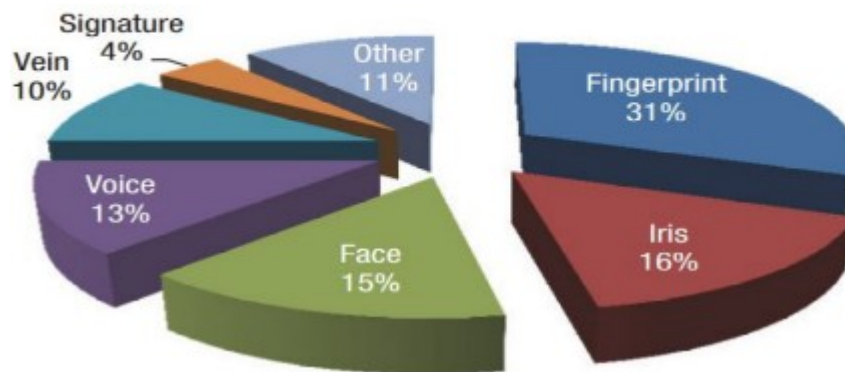


Figure I.13 Les parts de marché biométrique par technologie [18]

I.7 Le système biométrique :

I.7.1 Définition :

Un système biométrique est essentiellement un système qui acquiert des données biométriques d'un individu, puis compare un ensemble de caractéristiques extraites à partir de ces données à un ensemble de données stockées au préalable pour pouvoir enfin exécuter une action ou prendre une décision à partir du résultat de cette comparaison [20].

I.7.2 Architecture d'un système biométrique :

L'architecture d'un système biométrique se compose de six modules [25] (voir Figure 1.14).

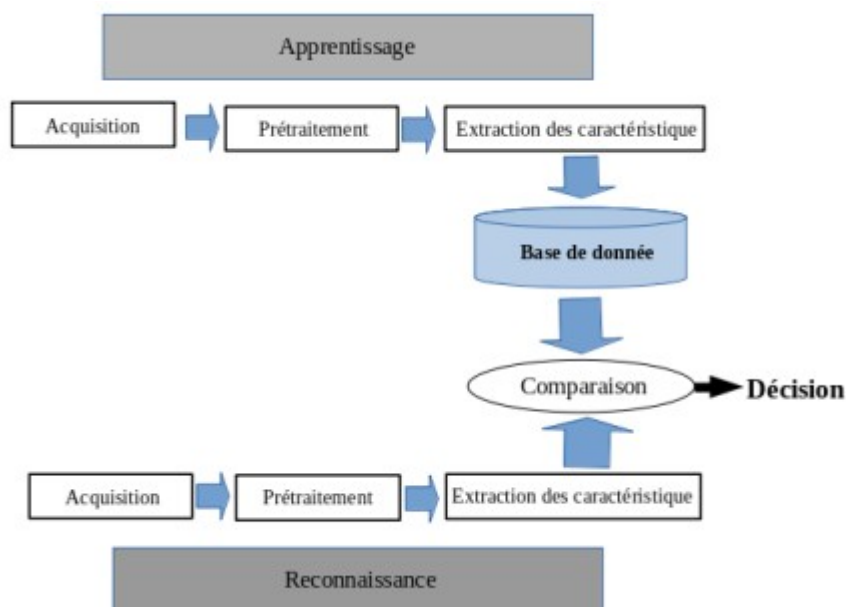


Figure I.14 Architecture d'un système biométrique

I.7.2.1 Fonctionnement d'un système biométrique :

Les systèmes biométriques peuvent fournir deux modes de fonctionnement, l'apprentissage (l'enrôlement), la reconnaissance (vérification et identification).

A. Apprentissage (enrôlement) : est la première phase de tout système biométrique, il s'agit du processus qui permet l'introduction d'un nouveau modèle dans le module de stockage (Base de données). Cet enregistrement peut s'accompagner par l'ajout d'information biographique.

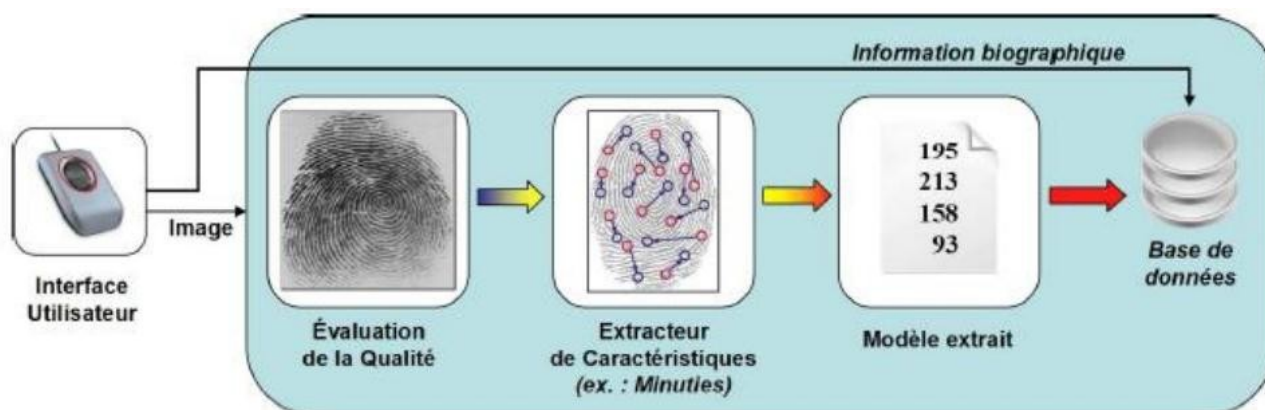


Figure I.15 Enrôlement d'une personne dans un système biométrique [16]

B. Reconnaissance : C'est le processus de vérification qu'un modèle est existant dans le module de stockage et qui permet l'identification de l'individu (comparaison). Les systèmes biométrique peuvent fonctionner sur deux modes distincts de reconnaissance, l'authentification et l'identification :

L'identification :

L'identification répond à la question « qui êtes-vous ? ». Dans ce cas, la personne est identifiée parmi d'autres (vérification 1: N) . Ses données personnelles sont comparées aux données d'autres personnes contenues dans la même base de données ou dans d'éventuelles bases de données reliées.

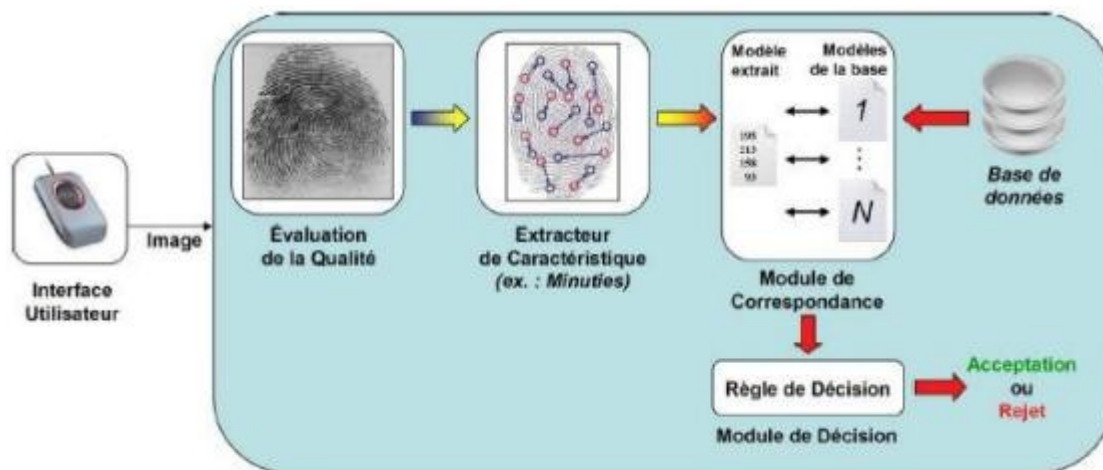


Figure I.16 Identification d'un individu dans un système biométrique [16]

L'authentification :

L'authentification répond à la question : «Etes-vous bien celui que vous prétendez être ?». Dans ce cas, la biométrie permet de certifier l'identité d'une personne en comparant les données qu'elle va présenter avec les données préenregistrées de la personne qu'elle prétend être (vérification 1:1).

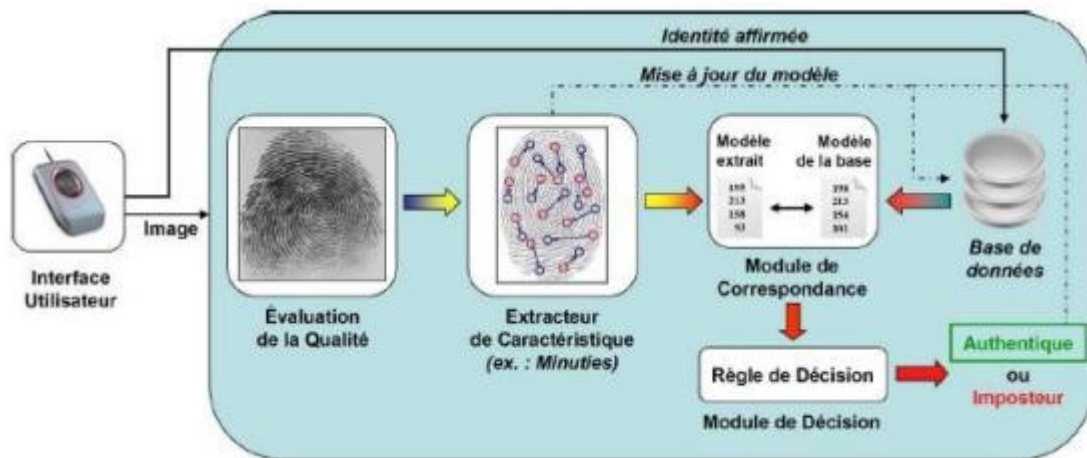


Figure I.17 Authentification d'un individu dans un système biométrique [16]

Ces deux procédés de reconnaissance font appel à des solutions techniques différentes.

- L'identification nécessite en général une **base de données centralisée** qui permet de comparer les données biométriques de plusieurs personnes.
- L'authentification peut se passer d'une telle base de données centralisée. On peut simplement enregistrer des données sur un **support décentralisé**, du type de nos cartes à microprocesseur.

Sur le plan de la protection des données, on privilégiera plutôt un procédé d'authentification avec un support décentralisé. Un tel procédé présente moins de risques. Le support décentralisé est en la possession de l'utilisateur lui-même et ses données ne figurent pas nécessairement dans une base de données.

A l'inverse, dans l'hypothèse d'un procédé d'identification nécessitant une base de données externe, l'utilisateur n'a pas la maîtrise physique de ses données, avec tous les risques que cela présente.

I.7.2.2 Les modules d'un système biométrique :

A. Module d'acquisition ou capture: Il s'agit d'un capteur biométrique (avec ou sans contact) qui permet d'acquérir une modalité spécifique d'une personne (caméra, microphone...etc.).

B. Module de prétraitement: Les données brutes acquises sont prétraitées pour améliorer leurs qualité et faciliter l'extraction des données discriminatoires pertinentes (caractéristiques).

C. Module d'extraction de caractéristiques : Il détermine à partir de la donnée prétraitée la nouvelle représentation des données dite modèle ou Template. Cette nouvelle représentation doit être pertinente et idéalement unique pour chaque personne.

D. Module de stockage: Contient les modèles biométriques des utilisateurs enrôlés du système. Le système de stockage peut être par exemple, un simple fichier ou bien une base de données. La figure 1.15 montre l'enregistrement d'une personne dans le système.

E. Module de comparaison/similarité (Matching) : Compare les données extraites par le module d'extraction de caractéristiques à un ou plusieurs modèles préalablement enregistrés (Template). Ce module détermine ainsi le degré de similarité (ou de divergence).

F. Le module de décision : Il détermine si le degré de similitude retourné par le module de similarité est suffisant pour déterminer l'identité d'un individu. Généralement le degré est un nombre compris entre 0 (différence totale) et 1 (correspondance parfaite).

I.7.3 Evaluation et mesure de performance :

En biométrie, nous distinguons deux types populations : les véritables clients (Genuine) qui sont autorisés à accéder dans la zone protégée et les imposteurs (Imposters) qui n'ont aucune autorisation, mais qui vont quand même essayer de rentrer d'où la performance d'un système biométrique est un élément essentiel à prendre en compte dans le choix d'un système.

Il existe deux manières de présenter les performances d'un système biométrique selon le mode de fonctionnement l'application soit du type authentification ou identification :

A. Authentification :

Les indicateurs de performances dans ce mode sont [5]:

1. Le taux de faux rejet (« False Reject Rate » ou FRR) : Ce taux représente le pourcentage d'individus censés être reconnus par le système mais qui sont rejetés. Notons que le taux d'acceptations véritables (« Genuine Accept Rate » ou GAR) est égal à 1-FRR.

$$FRR = \frac{\text{nombre des imposteurs acceptés}}{\text{nombre total de test imposteurs}}$$

2. Le taux de faux accepté (« False Acceptance Rate » ou FAR) : Ce taux représente le pourcentage d'individus reconnus par le système biométrique alors qu'ils n'auraient pas dû l'être.

$$FAR = \frac{\text{nombre des clients rejetés}}{\text{nombre total de test clients}}$$

3. Le taux d'égale erreur (« Equal Error Rate » ou EER) : Ce taux représente un point de mesure de performance. Ce point correspond à L'endroit où FAR = FRR, il représente un compromis entre le nombre de faux acceptés et le nombre de faux rejetés.

La figure 1.16 illustre les taux de faux accepté et de faux rejet à partir des distributions des scores d'un système (authentiques et imposteurs).

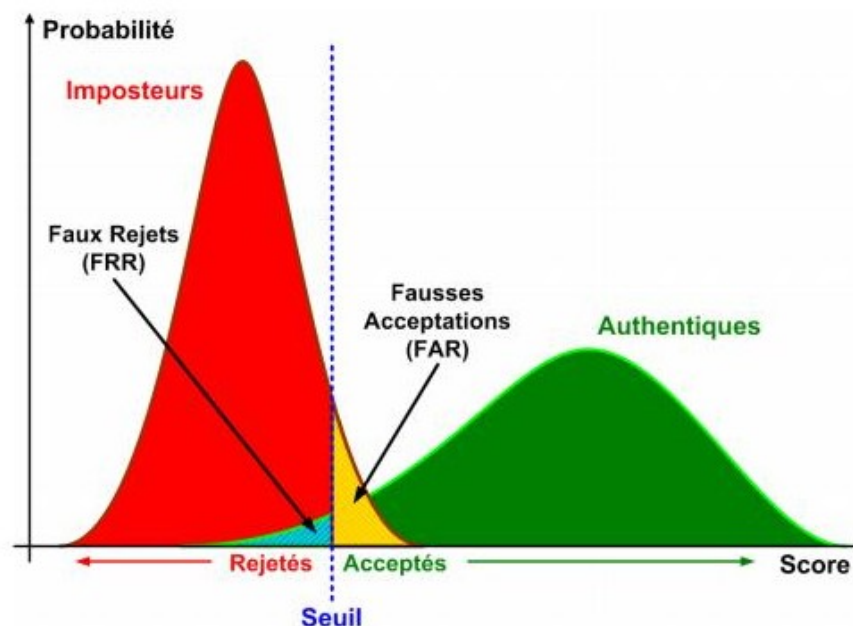


Figure I.18 Distributions des scores authentiques et imposteurs

Lorsque le système dans ce mode, la courbe la plus couramment utilisée est appelée **courbe ROC** (Receiver Operating Characteristic). Une courbe ROC (voir la figure 1.6) présente le taux de faux rejeté en fonction du taux de faux accepté. Le taux d'égale erreur peut être facilement identifiable puisqu'il s'agit de l'intersection de cette courbe avec la droite d'équation $y = x$.

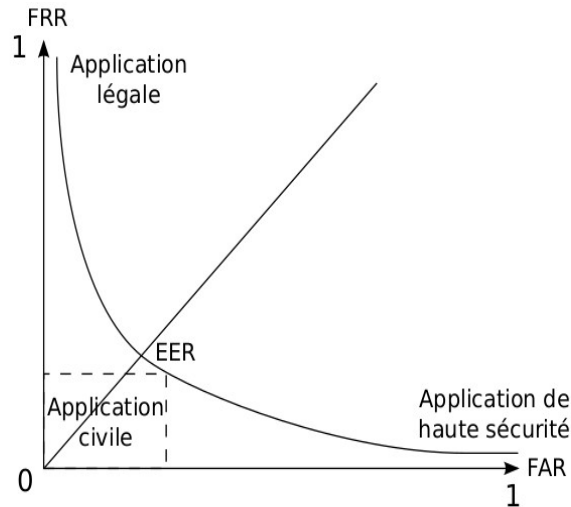


Figure I.19 Courbe ROC

B. Identification :

Lorsque le système opère dans ce mode on peut évaluer ses performance grâce à un seul indicateur, **le TID (Taux d'identification)**, c'est le pourcentage des personnes bien reconnus, il est défini par la formule suivante [5]:

$$TID = \frac{\text{Nombre de test ayant conduit à une identification correct}}{\text{Nombre total des tests}}$$

La courbe la plus utilisée un teste d'identification est appelée **courbe CMC** (Cumulative Match Characteristic). La courbe CMC donne le pourcentage de personnes reconnues en fonction du rang [26]. Le rang est une variable définissant à partir de quand l'identification d'un individu est réalisée avec succès. On dit qu'un système reconnaît au rang 0 (ou 1 selon les conventions) lorsqu'il choisit la plus proche image comme résultat de la reconnaissance. On peut donc dire que plus le rang augmente, plus le système est moins fiable. La figure suivante montre un exemple d'une courbe CMC.

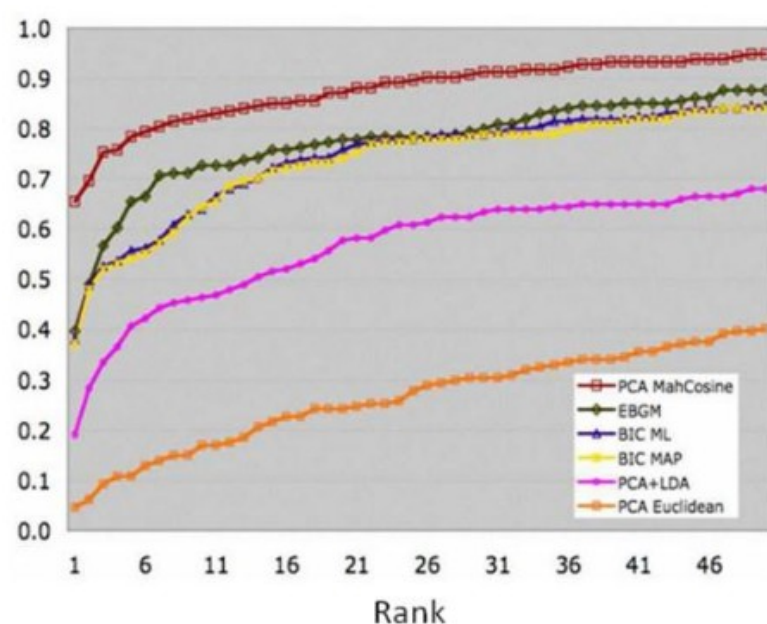


Figure I.20 Exemple de courbes CMC pour différents algorithmes de reconnaissance faciale [27].

I.8 Les avantages et limites des systèmes biométriques :

I.8.1 Les avantages :

La biométrie est une technologie récente et adoptée par de grands constructeurs de matériel informatique [23]. L'usage de la biométrie est un complément ou une alternative de l'utilisation des méthodes d'authentification comme des mots de passe, des badges ... etc. parmi les avantages de cette technique [24], citons :

A. Vitesse et précision : L'utilisation de mots de passe et de codes pour accéder de manière sécurisée à un site physique ou virtuel est assez simple, mais générique. En revanche, la technologie de sécurité biométrique désigne les mots de passe biologiques qui ne peuvent être falsifiés. En d'autres termes, l'identification et l'authentification d'un individu donné sont fiables. La reconnaissance d'iris ou faciale est de plus en plus souvent intégrée aux processus de sécurité, du fait de la rapidité et de la simplicité de la détection.

B. Sécurité et rentabilité : Une fois le système de contrôle biométrique intégré, il n'y a plus besoin d'investissements infrastructurels supplémentaires. Les coûts d'investissement initiaux et récurrents chutent par conséquent de manière très nette. Ces systèmes contribuent en outre à prévenir les pertes dues à la fraude et aux entrées illégales. À lui seul, cet avantage permet d'économiser de l'argent et d'accroître la rentabilité.

C. Évolutif pour accompagner la croissance : Au fur et à mesure que les entreprises grandissent, la sécurité doit impérativement évoluer avec elles. L'évolutivité constitue d'ailleurs l'un des principaux avantages des contrôles biométriques. La flexibilité de ces systèmes leur permet d'accepter facilement des données supplémentaires sur les employés. En clair, la sécurité grandit avec l'entreprise.

D. L'aspect pratique : L'un des principaux avantages d'un système de contrôle biométrique tient à sa commodité. Les mots de passe n'ont pas besoin d'être réinitialisés. Une fois le test biométrique activé, la reconnaissance des empreintes digitales, de l'iris et du visage peut s'effectuer et les employés vaquer à leurs occupations. On peut même enregistrer les données et les vérifier selon les besoins.

I.8.2 Les limites :

Bien que les applications biométriques soient constamment améliorées, ces derniers souffrent de plusieurs limites. Parmi les limites des systèmes biométriques [25], citons :

A. Le bruit sur la donnée capturée : Les données biométriques capturées peuvent être bruyantes ou endommagées, ces données bruitées risquent alors d'être mal appariées avec les modèles de la base de données aboutissant à un rejet incorrect d'un utilisateur autorisé. Des exemples de données bruitées sont une empreinte digitale avec une cicatrice, une voix altérée par un rhume mais généralement dues à des capteurs défectueux ou mal entretenus.

B. Les variations d'intra-classe : Les données biométriques d'un individu acquises pendant l'authentification peuvent être très différentes des données enrôlées (Template) dans la base de données. Cette variation peut être causée par une mauvaise interaction entre l'utilisateur et le capteur (changement de pose), une variation des conditions de l'environnement ambiant (changements d'éclairage) ou même par une variation de la constitution psychologique de l'individu (expression faciale).

C. Unicité : Alors qu'un trait biométrique est censé être unique et variable d'un individu à l'autre, il peut y avoir de grandes similitudes interclasses par rapport à ce trait (apparence faciale des vrais jumeaux), ce qui risque d'augmenter le taux de fausse acceptation du système.

D. Non-universalité : L'utilisation d'un système biométrique unimodal suppose que chaque individu de la population ciblée possède la modalité en question. Or, ce n'est pas toujours vrai et une partie de cette population (malades ou de handicapés) risquent d'être exclus.

E. Les attaques : Il est vrai que les traits biométriques sont beaucoup plus difficiles à contrer que les moyens d'identification classiques (les mots de passe et les cartes d'accès). Cependant, les impostures existent en particulier dans les modalités comportementales telles que la signature et la voix. Les traits physiologiques sont également sensibles aux attaques d'usurpation (l'utilisation de silicone pour reproduire des empreintes digitales).

I.9 Conclusion

Dans ce chapitre nous avons présenté la biométrie. Nous avons vu en premier une définition de la biométrie et son historique, ensuite quelques modalités biométriques les plus connues par famille et les caractéristiques biométriques ensuite l'évolution du marché de la biométrie et ses domaines d'application et à la fin, nous avons vu l'architecture et le principe de fonctionnement des systèmes biométriques, ainsi que l'évaluation et la Mesure de performance, les avantages et les limites de ces systèmes.

Dans le chapitre qui suit nous allons voir un état de l'art sur la reconnaissance faciale.

CHAPITRE II

Système de reconnaissance de visages

II.1 Introduction :

La facilité de reconnaissance des personnes par leur visage et les développements technologiques qui ont connu ces dernières années spécialement en informatique et en intelligence artificielle ont suscité un énorme intérêt auprès des scientifiques et des chercheurs pour développer des systèmes de reconnaissances automatiques du visage, en effet depuis le début des années 90, un tel système de reconnaissance est devenu possible à mettre en place [5][28].

Bien que cette technologie soit performante et bénéfique pour certaines applications à des fins de sécurité elle rencontre certaines difficultés techniques ou des problèmes éthiques selon certaines personnes ou organisations, le respect de la vie privée n'est plus garanti vu que des images du visage doivent être mémorisées dans des bases de données pour assurer les fonctions du système de reconnaissance [5].

Dans ce chapitre nous allons expliquer le principe de fonctionnement d'un système de reconnaissance automatique du visage, nous verrons par la suite les méthodes de reconnaissance de visage avec quelques techniques les plus connues pour chaque méthode.

II.2 Pourquoi le visage ?

Le visage reste le moyen et la modalité la plus naturelle pour la reconnaissance, elle reste la plus acceptée parmi les autres modalités par les populations puisqu'elle permet une reconnaissance à distance (non intrusive) et ne demande aucune coopération de l'utilisateur, d'une autre part elle surpasse les autres modalités d'un point de vue économique, les capteurs sont très peu coûteux et faciles à mettre en place (une simple caméra suffit). Cependant il faut prendre en compte les difficultés des systèmes actuels (changement de position, illumination, présence de composants structuraux) pour maximiser les performances de ces derniers [29].

II.3 Système de reconnaissance du visage :

La reconnaissance faciale est une technologie de plus en plus répandue, apparue avec l'une des premières tentatives faite en 1973 par Takeo Kanade lors de sa thèse de doctorat à l'Université de Kyoto [30]. Basée sur l'intelligence artificielle, la reconnaissance de visages permet d'identifier une personne sur une photo ou une vidéo en comparant son visage avec ceux sauvegardés dans une base de données.

Le principe de fonctionnement de base d'un système de reconnaissance faciale peut être résumé en quatre étapes, les deux premières (module de détection et module de normalisation du visage) s'effectuent en amont du système, et les deux dernières représentent la reconnaissance (module d'extraction et module de comparaison des caractéristiques).

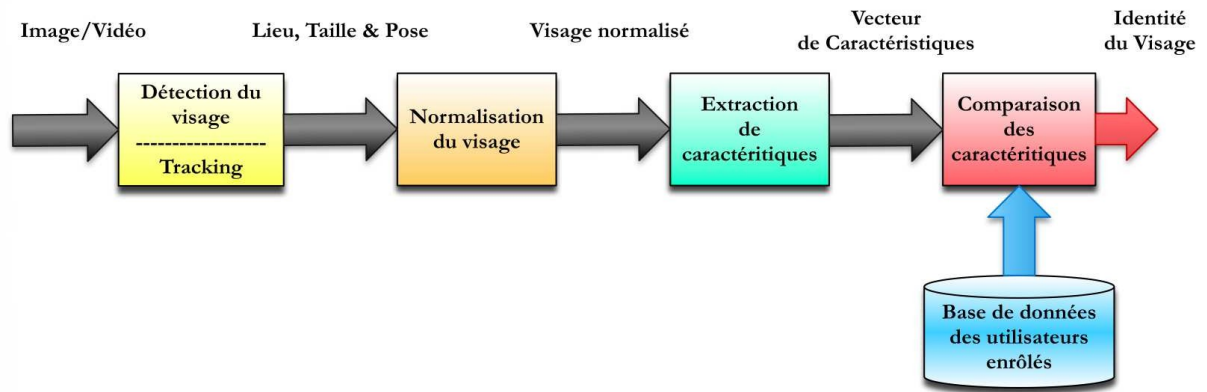


Figure II.1 Architecture d'un système de reconnaissance faciale [26]

II.3.1 Détection et acquisition de l'image :

Cette étape consiste à détecter et extraire l'image du monde physique (réel), elle permet d'avoir une représentation matricielle de l'image (matrice de niveau de gris), l'opération peut être statique ou dynamique selon le capteur utilisé [29].

II.3.2 Prétraitement :

La phase de prétraitement quant à elle permet de préparer l'image du visage de telle sorte qu'elle soit exploitable en éliminant le bruit engendré lors de la capture et les zones non informatives . Cette étape est aussi appelée étape de normalisation puisque elle ramène à un format prédéfini toutes les images extraites de l'image brute grâce à différentes méthodes de traitements : normalisation géométrique, égalisation d'histogramme ...etc [29].

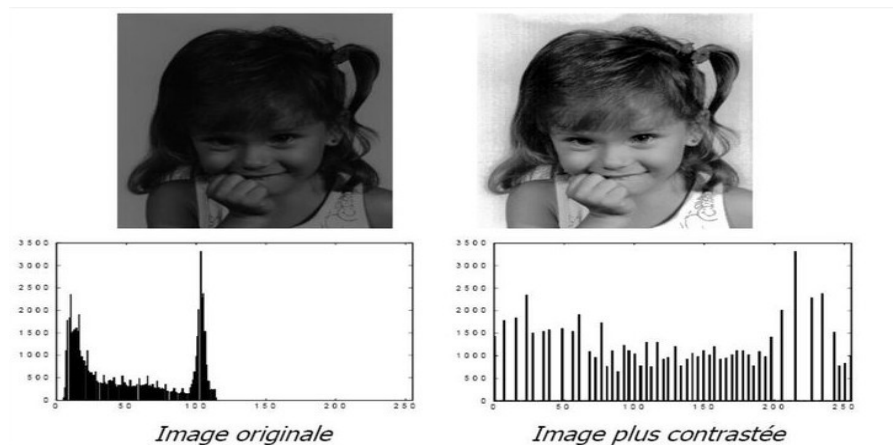


Figure II.2 Exemple de normalisation

II.3.3 Extraction des caractéristiques :

Cette étape vise à transformer le contenu d'une image en un ensemble de vecteurs de caractéristiques, ou des descripteurs, qui devraient être discriminatifs, informatifs, et non redondants avec une taille raisonnable et non sensibles aux variations de l'image (position, échelle, éclairage, etc.).

II.3.4 Apprentissage :

C'est une étape qui consiste à enregistrer les paramètres (caractéristiques) d'un individu après leurs extractions dans un module de stockage (base de donnée). Ce processus permet de faire apprendre les individus au système pour une éventuelle reconnaissance, cette étape est considérée en quelque sorte la mémoire du système.

II.3.5 Classification :

Cette étape consiste à classer les paramètres (caractéristiques) extraits. Les individus ayant des similarités sont regroupés dans la même classe. Ces classes varient selon le type de décision. L'efficacité de cette étape à une influence directe sur la performance du système de reconnaissance de visage [29].

II.3.6 Comparaison et décision :

Cette étape consiste à comparer entre les données extraites dans la phase extraction et les modèles des individus déjà mémorisés dans la base de données afin de vérifier la correspondance entre deux visages, cependant il faut introduire une mesure de similarité pour prendre une décision si oui ou non l'individu est reconnu par le système [29].

II.4 Les difficultés de la reconnaissance faciale :

De nombreuses propriétés du visage ainsi que les conditions dans lesquelles ils ont été capturés rendent le traitement automatique difficile. Dans le cadre de la reconnaissance le principal problème d'un système automatique de reconnaissance du visage est dû à la variation d'acquisition des images, notamment la variation inter-classe causée par la ressemblance physique entre les individus et la variation intra-classe comme la variabilité que peut prendre le visage d'une même personne, les conditions d'éclairage ou les caractéristiques des capteurs [31]. Les difficultés de la reconnaissance faciale peuvent être attribuées aux facteurs suivants [21] :

II.4.1 Illumination :

Lors de la prise de vue, un facteur tel que l'éclairage (spectres, distribution de source de luminance et intensité) influence énormément sur l'apparence de visage. On distingue deux types d'éclairage peuvent influencer sur l'apparence d'un visage : l'illumination globale affecte tout le visage de manière uniforme (ou presque) et l'illumination locale entraîne la création d'ombre et de zones éclairées.

Notons que de nombreuses approches ont été proposées pour gérer ces problèmes de luminosité comme une modélisation implicite de la luminosité dans la création d'un modèle de visage, l'extraction de caractéristiques invariantes aux changements de luminosité et certain nombre d'approches traitent le problème par une étape de prétraitement dont l'objectif principal est de corriger ces problèmes dûs aux variations de luminosité.



Figure II.3 Exemple d'un visage avec des changements de luminosité [21]

II.4.2 La pose et orientation :

lors de la capture, la pose d'un visage définit la rotation qu'a pu subir un visage. On distingue selon le type de rotation deux types de variations de pose : rotation dans le plan (le visage de profil dans le plan) où l'apparence du visage n'est pas déformée, et une bonne estimation de l'angle de la rotation peut suffire à recalculer l'image par simple rotation inverse et dans le cas de la rotation hors plan c'est souvent bien plus complexe, sauf si les visages utilisés pour l'enrôlement et la reconnaissance présentent la même pose.

Les variations de pose affectent grandement les systèmes de reconnaissance automatique de visages, c'est pourquoi nombreux d'entre eux se limitent aux poses frontales, ou à des poses spécifiques requérant cependant une estimation au préalable.

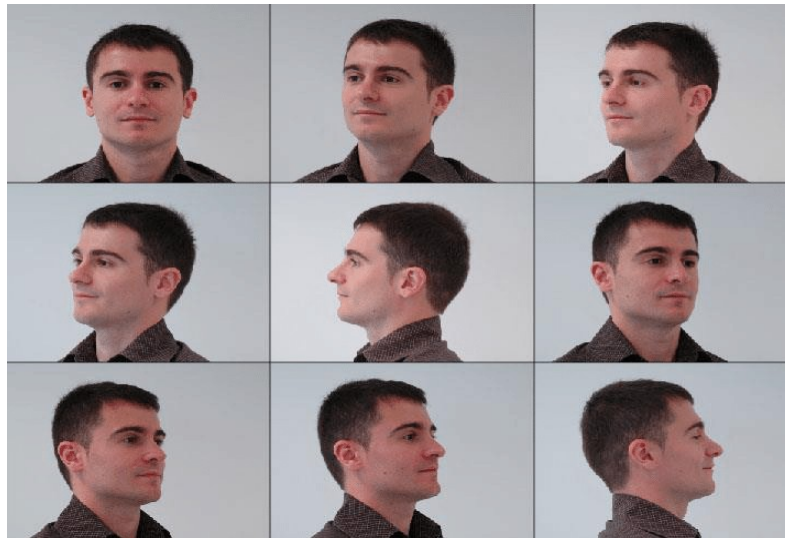


Figure II.4 Exemple d'un visage avec des variations de pose

II.4.3 Présence ou absence des composants structuraux :

Les dispositifs faciaux tels que les barbes, les moustaches, et les verres peuvent ou ne peuvent pas être présents et il y a beaucoup de variabilité parmi ces composants qui peuvent influencer énormément les caractéristiques faciales telles que la forme, la couleur, et la taille du visage.



Figure II.5 Exemple d'un visage sans et avec une barbe

II.4.4 Expression faciale :

L'aspect des visages est directement affecté par l'expression faciale d'une personne. Les éléments faciaux tels que la bouche ou encore les yeux peuvent alors subir des déformations importantes, pouvant faire échouer un système de reconnaissance faciale en diminuant le taux de reconnaissance.



Figure II.6 Exemple de variations d'expressions faciales

II.4.5 Occlusion :

Les occlusions partielles apparaissent fréquemment dans des applications réelles où des visages peuvent être partiellement occlus par d'autres objets comme des cheveux longs, des lunettes de vue, de soleil, par tout autre objet (foulard...) ou dans une image avec un groupe de personnes, quelques visages peuvent partiellement occlure d'autres visages.



Figure II.7 Variations dû à la présence d'occlusions partielles

II.4.6 Autres difficultés :

D'autres types de difficultés à part ceux cités ci-dessus peuvent influencer un système de reconnaissance faciale comme par exemple les opérations de chirurgie esthétique qui engendrent généralement des changements considérables dans l'apparence faciale des individus ou l'âge des captures (le moment où les captures du visage sont prises). En effet, l'apparence d'un visage peut changer avec le temps (l'âge de l'individu) notamment lors du passage de l'adolescence à l'âge adulte, et un écart de temps important entre deux captures peut engendrer des difficultés de reconnaissance.



Figure II.8 Exemple de changement d'apparence avec le temps

II.5 Méthodes de reconnaissances :

Durant ces vingt dernières années, de nombreuses approches ont été proposées, elles se répartissent en trois catégories : les méthodes globales et les méthodes géométriques et hybride.

La figure suivante illustre les différents algorithmes de reconnaissance faciale par méthode.

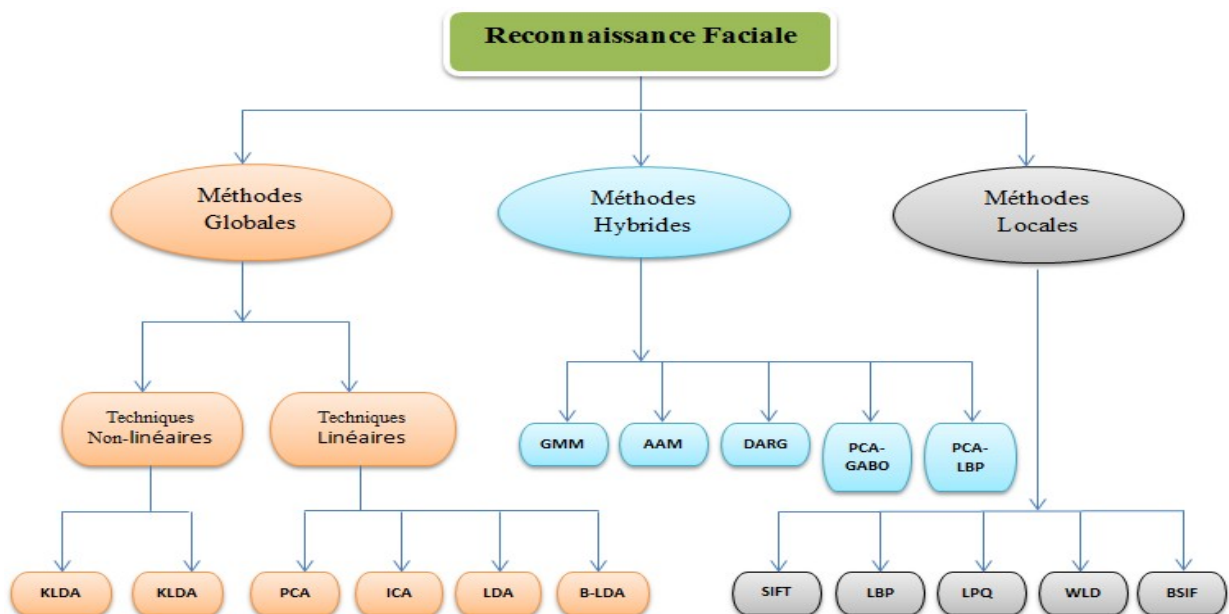


Figure II.9 Classification des algorithmes principaux utilisés en reconnaissance faciale [25]

II.5.1 Méthodes globales :

Dans ces approches, également appelées méthodes basées sur l'apparence, les images de visage sont globalement traitées, c'est-à-dire qu'il n'est pas nécessaire d'extraire des points caractéristiques ou des régions faciales (bouche, yeux, ...etc). Ainsi, l'image du visage est représentée par une matrice de pixels, et cette matrice est souvent transformée en vecteurs de pixels pour faciliter leur manipulation.

L'avantage principal des méthodes globales est qu'elles sont faciles à mettre en œuvre, bien qu'elles soient sensibles aux variations (pose, éclairage, expressions faciales et orientation). En effet, tout changement dans l'image du visage entraîne un changement des valeurs de pixels. Ces méthodes utilisent principalement une analyse de sous-espaces de visages. Cette expression repose sur un fait relativement simple : une classe de "formes" qui nous intéresse (dans notre cas, les visages) réside dans un sous-espace de l'espace de l'image d'entrée. Selon la technique utilisée pour modéliser les sous-espaces de visages, cette catégorie peut elle-même être divisée en approches linéaires et non linéaires. Les algorithmes globaux s'appuient sur des propriétés statistiques bien connues et utilisent l'algèbre linéaire.

A. Techniques linéaires :

Les techniques linéaires réalisent une projection linéaire des visages (espace dont la dimension est égale à la dimension des images, donc grande) sur un espace de plus faible dimension. Cependant, ces techniques linéaires sont sensibles aux conditions de luminosité notamment, et plus généralement aux variations non convexes. Ainsi, l'utilisation de distances classiques dans l'espace projeté ne permet pas toujours de réaliser une bonne classification entre les classes « visages » et « non visages ». Et parmi les approches les plus importantes réunies au sein de cette méthode, citons :

L'Analyse en Composantes Principales (PCA ou Eigen Faces) :

La plus connue de ces approches est la technique dite Eigenfaces présentée par Turk et Pentland [32], nommée Eigenfaces car elle utilise des vecteurs propres et des valeurs propres (respectivement Eigen vectors et Eigen values en anglais). L'idée principale consiste à exprimer les images de départ selon une base de vecteurs orthogonaux particuliers ces fameux vecteurs propres contenant des informations indépendantes d'un vecteur à l'autre. Ces nouvelles données sont donc exprimées d'une manière plus appropriée à la reconnaissance du visage.

De nombreux travaux ont été réalisés sur le choix des vecteurs propres à retenir pour définir le nouvel espace, comme [21] :

- Kirby et al. [33] proposent un critère basé sur l'énergie des valeurs propres, le principe est de retenir les vecteurs propres correspondant aux plus grandes valeurs propres jusqu'à ce que la somme des valeurs propres dépasse un certain seuil de l'énergie totale (90%).
- Martinez et al. [34] montrent que les taux de reconnaissance peuvent être améliorés en ignorant les premiers vecteurs propres (ceux dont les valeurs propres associées sont les plus grandes), ceux-ci encodant souvent les variations d'illumination.

L'Analyse Discriminante Linéaire (LDA ou Fisherfaces) :

La LDA est une méthode d'analyse numérique qui permet de chercher la combinaison linéaire des variables qui représentent au mieux les données, elle est très utilisée dans le domaine de la reconnaissance des formes à savoir la reconnaissance de visage [12].

Présentée par Belhumeur et al en 1997 [35], la LDA (souvent nommée Fisherfaces) consiste à diviser les visages en classes selon le critère de Fisher ensuite elle analyse les vecteurs propres de la matrice de dispersion des données, pour maximiser les variations inter-classes (les images de différents individus) tout en minimisant les variations intra-classes (les images d'un même individu), Cette technique est une variante de PCA, mais contrairement à celle-ci où la meilleure représentation (celle maximisant la variance) est recherchée, le but est ici une meilleure séparation des classes [5].

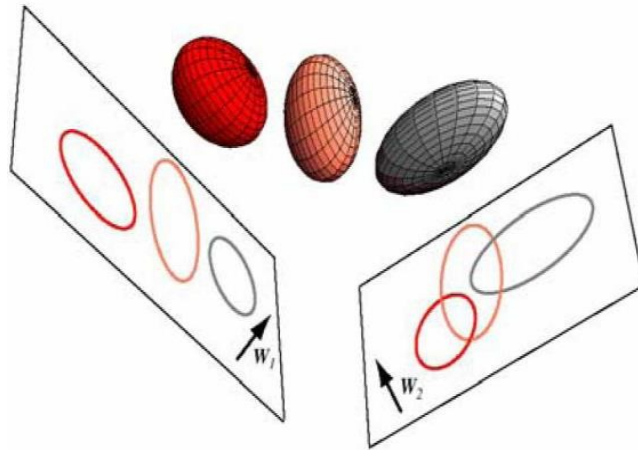


Figure II.10 Illustration du principe de séparation optimale des classes par le LDA. Trois distributions 3D sont projetées sur deux sous-espaces 2D décrits par les vecteurs w_1 et w_2 . Puisque le LDA essaye de trouver la plus grande séparation parmi les classes, on voit bien que w_1 est ici le vecteur optimal [36].

D'autres techniques linéaires ont également été utilisées pour le calcul de vecteurs caractéristiques :

- l'analyse en composantes indépendantes (**ICA**) [37]
- la factorisation de matrices non négatives (**NMF**) [38][39]
- l'analyse discriminante bilinéaire (**BDA**) [40]
- la technique dite de « Vecteurs communs discriminants » (**DCV**) [41]

Bien que ces méthodes linéaires soient assez efficaces, elles manquent de précision dès que les images de visages subissent des transformations non linéaires. Une simple modification de la luminosité transforme celui-ci de façon non linéaire étant donné la complexité de la forme.

B. Techniques non linéaires :

Des techniques globales non linéaires ont été développées, souvent à partir des techniques linéaires. Ainsi l'Analyse en Composantes Principales à Noyaux (ou « Kernel-PCA »)[42] et l'Analyse Discriminante Linéaire à Noyaux (ou « Kernel-LDA »)[43] utilisent la notion mathématique des noyaux pour étendre les techniques linéaires que sont l'ACP et la LDA.

D'autres techniques non linéaires ont également été utilisées dans le contexte de la reconnaissance faciale :

- le MultiDimensional Scaling (**MDS**) [44][45]
- les approches neuronales [46][47]
- l'Isomap [48]
- les diffusion maps [49]

L'utilisation de ces méthodes de projection de l'espace des images sur l'espace de caractéristiques est non linéaire et permet ainsi dans une certaine mesure de réduire la dimension des images de meilleure façon.

II.5.2 Méthodes Locales :

Appelées aussi les méthodes à traits, à caractéristiques locales, ou analytiques. Elles s'appuient en général sur des points caractéristiques du visage. Les méthodes d'extraction de caractéristiques locales analysent les informations de texture dans une région partielle du visage, et représentent de manière compacte les caractéristiques de l'ensemble du visage.

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. Mais leur difficulté se présente lorsqu'il s'agit de prendre en considération plusieurs vues du visage ainsi que le manque de précision dans la phase "extraction" des points constituent leur inconvénient majeur. Précisément, ces méthodes extraient les caractéristiques locales de visage, puis utilisent leur géométrie et/ou l'apparence comme donnée d'entrée du classificateur. On peut distinguer deux pratiques différentes :

- La première repose sur l'extraction de *régions* entières du visage, elle est souvent implémentée avec une approche globale de reconnaissance de visage.
- La deuxième pratique extrait des *points particuliers* des différentes régions caractéristiques du visage, tels que les coins des yeux, de la bouche et du nez.

Parmi les approches de cette méthode, citons :

Les ondelettes (wavelet) :

La transformée en ondelettes a été introduite par Morlet au début des années 80, utilisées pour l'évaluation des données sismiques. Sous l'impulsion de personnalités scientifiques telles que le physicien A. Grossman ou le mathématicien Y. Meyer, les ondelettes se sont imposées comme des outils fondamentaux de l'analyse harmonique moderne et elles sont largement appliquées aux domaines de l'ingénierie comme traitement du signal et de l'image où elles ont connu un grand succès pour des problèmes tels que l'estimation de mouvement, la reconnaissance de formes, la recherche dans des bases de données et la transmission progressive d'informations [5].

Le but de la transformée en ondelettes est de changer les données du domaine espace-temps en domaine fréquence-temps qui est utile dans le traitement du signal numérique et la compression d'image. Dans le traitement du signal, les ondelettes sont utiles pour récupérer les signaux faibles du bruit [50].

Machines à Vecteurs de Support (SVM) :

C'est une technique qui a été proposée par V.Vapnik en 1995 [51], elle est utilisée dans plusieurs domaines statistiques (classement, régression, fusion,... etc.). depuis son introduction dans le domaine de efficacité et principalement dans le traitement d'images.

L'idée essentielle de cette approche consiste à projeter les données de l'espace d'entrée (appartenant à différentes classes) non linéairement séparables, dans un espace de plus grande dimension appelé espace de caractéristiques, de façon à ce que les données deviennent linéairement séparables [52].

Dans cet espace, la technique de construction de l'hyperplan optimal est utilisée pour calculer la de classement séparant les classes tels que : Les vecteurs appartenant aux différentes classes se trouvent de différents côtés de l'hyper plan, et la plus petite distance entre les vecteurs et l'hyperplan (la marge) soit maximale.

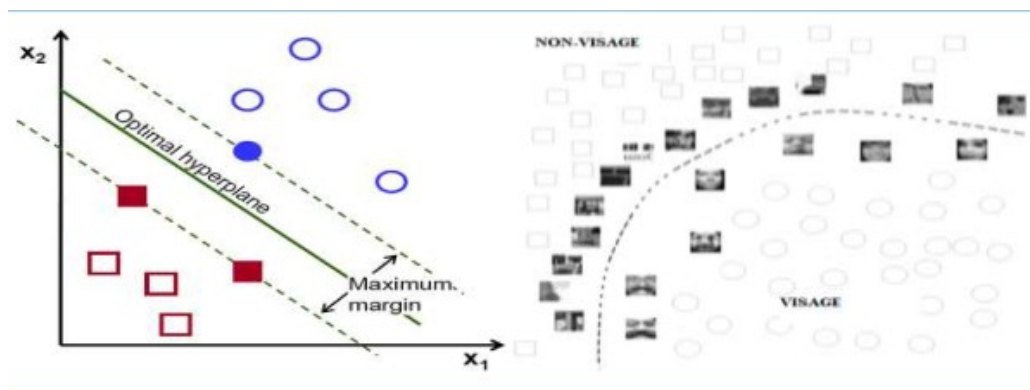


Figure II.11 Machines à Vecteur de Support (SVM) [5]

Réseaux de Neurones :

Un réseau de neurones artificiels ou RNA est un système dont la conception est à l'origine schématiquement inspirée du fonctionnement des neurones biologiques, et qui par la suite s'est rapproché des méthodes statistiques. L'unité de base du réseau de neurones est le perceptron où chaque perceptron effectue un travail relativement simple : il reçoit des données pondérées des voisins ou des sources externes et calcule sur cette base un signal de sortie qui est propagé à d'autres unités [5].

Les réseaux de neurones peuvent être utilisés tant pour la détection, la classification, la compression de données ou dans le contrôle de systèmes complexes en automatique, et généralement ils sont optimisés par des méthodes d'apprentissage de type probabiliste, en particulier bayésien. Ils sont placés d'une part dans la famille des applications statistiques, qu'ils enrichissent avec un ensemble de paradigmes permettant de créer des classifications rapides (réseaux de Kohonen en particulier), et d'autre part dans la famille des méthodes de l'intelligence artificielle auxquelles ils fournissent un mécanisme perceptif indépendant des idées propres de l'implémenteur, et des informations d'entrée au raisonnement logique formel (*Deep Learning*) [53].

II.5.3 Méthodes hybrides :

Les méthodes hybrides permettent d'associer les avantages des méthodes globales et locales en combinant la détection de caractéristiques géométriques (ou structurales) avec l'extraction de caractéristiques d'apparence locales. Elles permettent d'augmenter la stabilité de la performance de reconnaissance lors de changements de pose, d'éclairement et d'expressions faciales. Les méthodes les plus connues sont basées sur des modèles statistiques comprenant le modèle actif d'apparence.

Parmi les approches de cette méthode, citons :

LogGabor PCA :

LogGabor PCA présenté par Perlibakas [54]. Une convolution par des ondelettes de Gabor orientées est réalisée autour de certains points caractéristiques du visage. Les vecteurs ainsi créés contiennent à la fois la localisation ainsi que les amplitudes des énergies locales. Une analyse en Composantes Principales est ensuite réalisée afin de réduire la dimension de ces vecteurs [21].

Les Modèles Actifs d'Apparence (*Active Appearance Models* ou AAM) :

Une méthode proposée par Cootes et al [55]. Cette modélise indépendamment la forme et la texture d'un visage en appliquant une Analyse en Composantes Principales. Les vecteurs obtenus pour la forme et la texture sont ensuite utilisés pour la reconnaissance. Un nouveau visage qui doit être identifié est adapté au modèle par un processus d'optimisation itératif. Les paramètres de forme et de texture obtenus sont ensuite comparés à ceux de la base [21].

Le tableau ci-dessous récapitule qualitativement la différence entre les deux types de caractéristiques locale et globale.

Facteurs de variations	Caractéristiques locales	Caractéristiques globales
• Illuminations	Très sensible	Sensible
• Pose	Sensible	Très sensible
• Expressions	Pas sensible	Sensible
• Bruit	Très sensible	Sensible
• Occlusion	Pas sensible	Très sensible

Tableau II.1 Comparaison entre les caractéristiques locales et globales

II.5.4 Méthodes de reconnaissances 3D :

Cette méthode est considérée comme une amélioration de la reconnaissance 2D. En effet, elle crée un modèle 3D depuis plusieurs photos effectuées successivement ou depuis une vidéo, cela permettant d'avoir différents points de vue de la personne à reconnaître afin de créer le modèle 3D.

En plus des techniques de reconnaissance du visage 3D, il existe aussi d'autres approches comme l'utilisation de la technologie infrarouge où elle permet en outre à un système biométrique de fonctionner, même lorsque la capture dans le domaine visible est impossible ou de mauvaise qualité [29], ou bien il existe aussi des techniques de reconnaissance du visage 2.5D où L'image 2.5D (image de profondeur) correspond à une représentation bidimensionnelle d'un ensemble de points 3D (x,y,z) où chaque pixel dans le plan (x,y) stocke la valeur de sa profondeur z . La figure suivante illustre un exemple d'une transformation 2.5D :

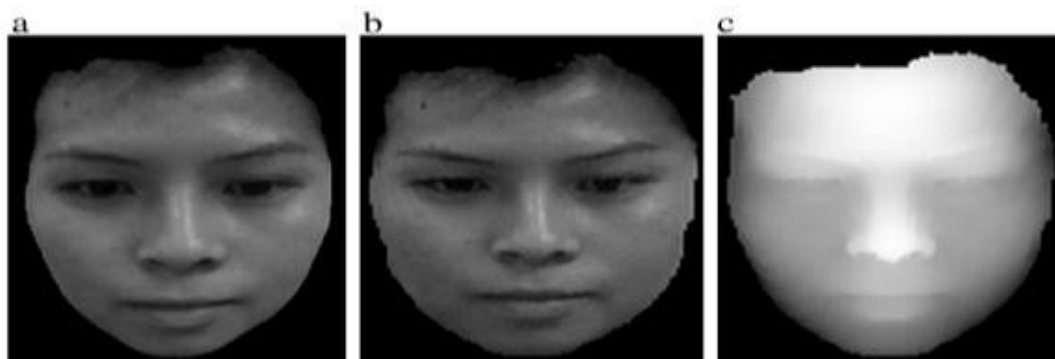


Figure II.12 (a) Visage normalisé ; (b) 2D Image; (c) 2.5D Image

II.6 Conclusion :

Dans ce chapitre nous avons présenté l'état de l'art sur le fonctionnement d'un système de reconnaissance automatique de visages, ces difficultés comme l' Illumination de la capture, la pose et l'orientation du visage, l'expression faciale...etc, ensuite nous avons vu les principales approches utilisées dans la littérature pour la reconnaissance (les méthodes globales, locales et hybrides).

Dans le chapitre qui suit nous allons voir un état de l'art sur la reconnaissance automatique des empreintes digitales.

CHAPITRE III

La reconnaissance par empreintes digitales

III.1 introduction :

L'utilisation de l'empreinte digitale comme moyen d'identification est très ancienne, son histoire remonte au moins à 6000 av. JC. L'empreinte digitale est unique pour chaque individu [1]. *Francis Galton* a démontré (en 1888) la permanence de sa forme tout au long de la vie de la personne, ainsi que son inaltérabilité. Depuis longtemps le seul moyen de l'acquisition de cette modalité consiste à utiliser l'encre, les avancées technologiques ont permis l'apparition des appareils numériques basés sur la capture optique, thermique, électromagnétique ou sur les ultrasons [56].

Dans ce chapitre nous allons voir une définition de l'empreinte digitale et ses caractéristiques, ensuite nous allons expliquer le principe de fonctionnement d'un système de reconnaissance automatique des empreintes digitales dans lequel nous verrons les méthodes de prétraitement, d'extraction des caractéristique et enfin les méthodes de comparaison des empreintes digitales.

III.2 Pourquoi l'empreinte digitale ?

En étant la modalité la plus connue dans le domaine de la reconnaissance biométrique et aussi l'une des premières à être utilisée dans les systèmes de reconnaissance automatique, l'empreinte digitale détient la plus grande part du marché de la reconnaissance biométrique et elle est considérée comme l'une des modalités les plus acceptées par l'ensemble de la population. Les différentes propriétés qui permettent aux empreintes digitales d'être si puissantes c'est qu'elles sont uniques et immuables, elles ne se modifient pas au cours du temps sauf par accident (brûlure par exemple), une analyse poussée permet de différencier entre de vrai jumeaux [57], les capteurs utilisés sont très peu coûteux et enfin la facilité de la mise en place d'un tel système.

III.3 Définition et classification de l'empreinte digitale :

L'empreinte digitale est le modèle du relief cutané des doigts formée à environ sept mois du développement du fœtus, scientifiquement est composée des crêtes qui contiennent des pores et des sillons, et les pores permettent de sortir 80% d'eau et 20% de matières organiques, ces matières laissent des marques sous formes des lignes [58].



Figure III.1 Caractéristiques d'une empreinte digitale [59]

L'empreinte digitale possède un ensemble de propriétés globale (les centres et les deltas) et locales (les minuties). Typiquement, les représentations globales sont des attributs entiers des doigts, elles sont employées pour la classification des empreintes digitales tandis que les représentations locales se composent de plusieurs points, chaque point est dérivé d'une région dans l'espace limitée de l'empreinte, ils sont employées pour la comparaison des empreintes digitales.

III.3.1 La représentation globale :

Le modèle entier d'empreintes digitales est classé par un certain nombre des classes et typiquement les empreintes digitales sont subdivisées par Francis Galton en trois grandes familles [60] : loops, whorls, archs, ensuite Edward Henry les a classées [61] en six sous-classes principales selon : arch, tented arch, left loop, right loop, et whorl. Les empreintes digitales sont aussi distinguées par l'épaisseur des rides, la séparation des rides, la profondeur des rides et les locations des points critiques (les noyaux et les deltas) (Figure III.2).

Les classes proposées par Francis Galton :

A. Les Boucles (Loops) : une empreinte est de classe boucle si ses stries rentrent d'un côté et ressortent du même côté et si elle possède un point singulier de type boucle et un point singulier de type delta. Les boucles représentent 65% des empreintes des doigts humains.

B. Les Spires (Whorls) : une empreinte appartient à la classe spire si elle possède au moins une strie qui fait 360°. Elle peut aussi contenir jusqu'à deux régions singulières de type boucles et deux régions singulières de type deltas. Les spires représentent 30% des empreintes des doigts humains.

C. Les Arches (Archs) : une empreinte est de classe arche si elle possède des stries qui rentrent d'un côté et ressortent du côté opposé et si elle ne contient ni boucle ni delta comme points singuliers. Les arches ne représentent que 5% des empreintes des doigts humains.

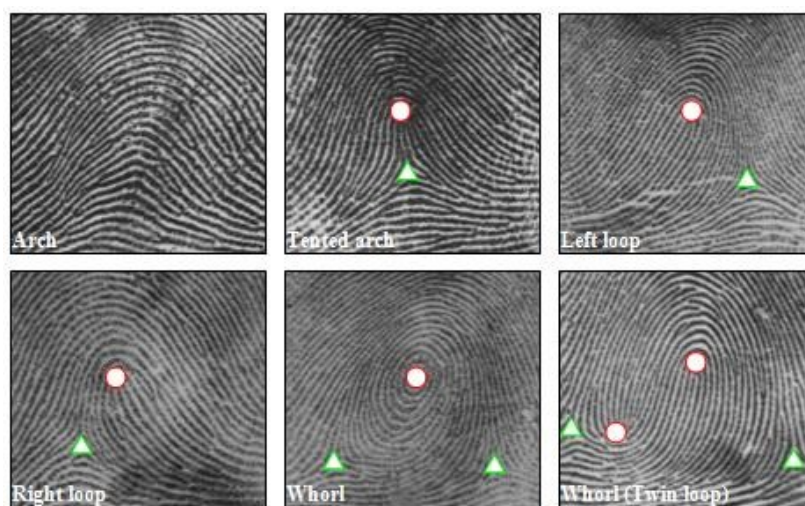


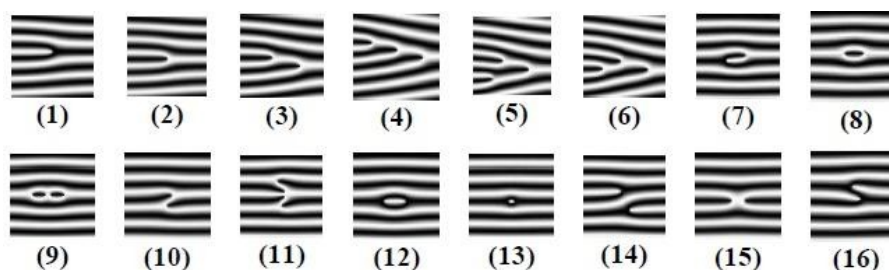
Figure III.2 Les principales classes d'empreintes digitales selon la classification de Galton-Henry

III.3.2 La représentation locale :

Les caractéristiques locales les plus utilisées sont basées sur les minuties des rides. les minuties désignent les différentes discontinuités des lignes des empreintes. Un ensemble des minuties extraites d'une empreinte digitale peut caractériser cette empreinte digitale.

Nous pouvons distinguer jusqu'à seize types de minuties différentes (voir la figure III.3), mais en général dans les algorithmes on n'en s'intéresse qu'aux deux types suivants parce qu'ils sont facilement détectables :

- **La bifurcation** : c'est le point où la strie se divise en deux
- **La terminaison** : c'est le point où la strie s'arrête



1	Terminaison	9	Boucle double
2	Bifurcation simple	10	Pont simple
3	Bifurcation double	11	Pont jumeau
4	Bifurcation triple 1	12	Intervalle
5	Bifurcation triple 2	13	Point isolé
6	Bifurcation triple 3	14	Traversée
7	Crochet	15	Croisement
8	Boucle simple	16	Tête bêche

Figure III.3 Les types de minuties

En fait les autres types de minuties ne sont que les résultats des combinaisons des minuties de terminaison et de bifurcation. Par exemple, les boucles peuvent être visualisées en tant que deux bifurcations.

Chaque minutie est représentée par les coordonnées (x, y) de sa position dans l'image, et l'angle θ qui est la direction associée à la strie (figure III.5). Donc chaque minutie de l'empreinte est repérée par un vecteur de la forme : (Type de minutie, x, y, θ).

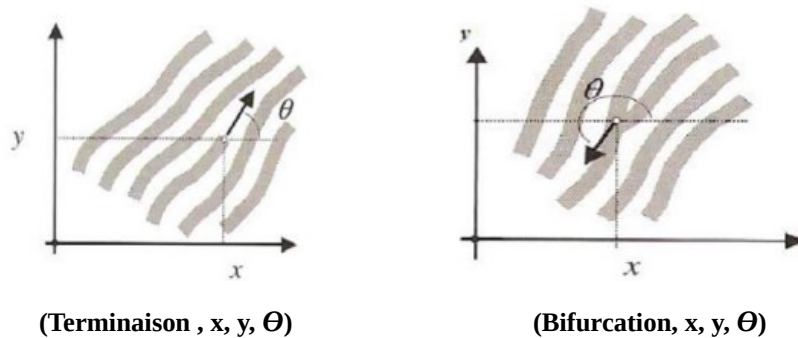


Figure III.4 Représentation des vecteurs de terminaison et de bifurcation [62]

III.4 Système de reconnaissance des empreintes digitales :

Le principe de fonctionnement de base d'un système de reconnaissance par empreintes digitales (Figure III.5) peut être résumé en quatre étapes , les deux premières (l'acquisition de l'image à l'aide d'un capteur et le module de prétraitement de l'image), et les deux dernières représentent la reconnaissance (module d'extraction des caractéristiques avec un post-traitement et le module de comparaison des empreintes).

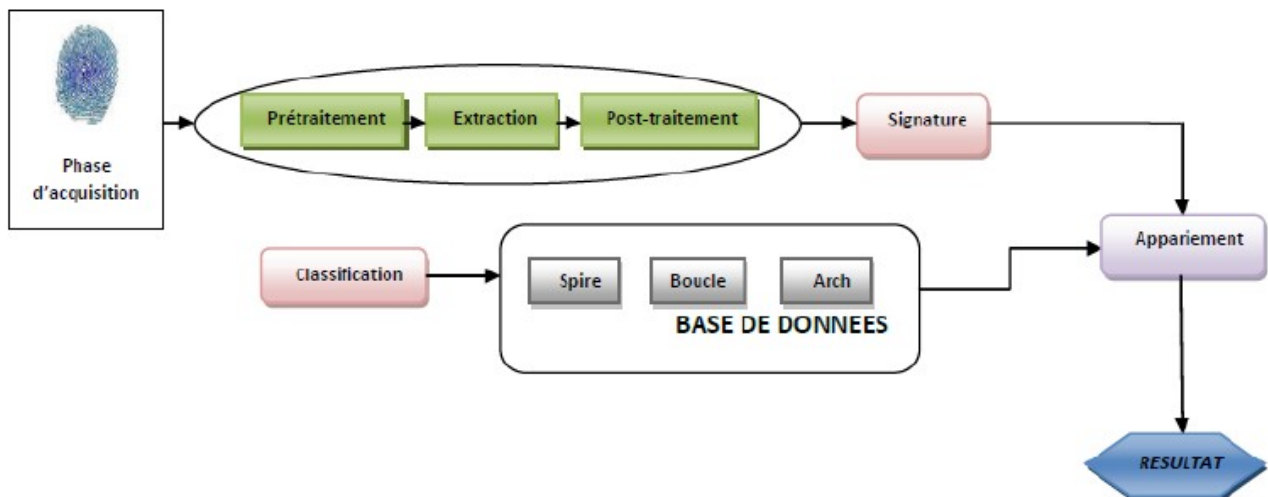


Figure III.5 Architecture générale d'un système complet de reconnaissance d'empreintes [63].

III.4.1 Prétraitement des images empreintes :

Lors de l'acquisition de l'empreinte l'image obtenue contient souvent beaucoup caractéristiques ayant des origines diverses :

- Les substances parasites présentes sur le doigt (encre, graisse, saletés).
- La personne (cicatrices, métiers manuels, âge).
- L'environnement où se produit l'acquisition (température de l'air, degré d'humidité).
- Les caractéristiques spécifiques du moyen d'acquisition utilisé.

Pour permettre une reconnaissance fiable, un prétraitement est alors nécessaire pour améliorer la qualité de l'image obtenue et éviter les erreurs.

A. Niveau de gris :

une image en niveaux de gris s'oppose d'une part à une image en noir et blanc, dans laquelle chaque pixel est soit noir, soit blanc, et d'autre part à une image en couleurs. Le nombre de nuances de gris varie, de 16 (codé sur 4 bits) à 256 (un octet par pixel) et plus, selon l'usage envisagé.

Pour convertir une image couleur en niveau de gris il faut remplacer, pour chaque pixel les trois valeurs représentant les niveaux de rouge, de vert et de bleu, par une seule valeur représentant la luminosité [64].



Figure III.6 L'empreinte digitale en gris

B. Calcul de l'image orientation :

C'est une étape essentielle pour déterminer les rides et trouver la région d'intérêt d'empreinte digitale. L'orientation locale d'un point (x,y) est la valeur de l'angle $\theta_{xy} \in [0^\circ \dots 180^\circ]$ [parallèle au flux de crêtes sur le voisinage local centré en (x,y) comme le montre la figure suivante [65] :

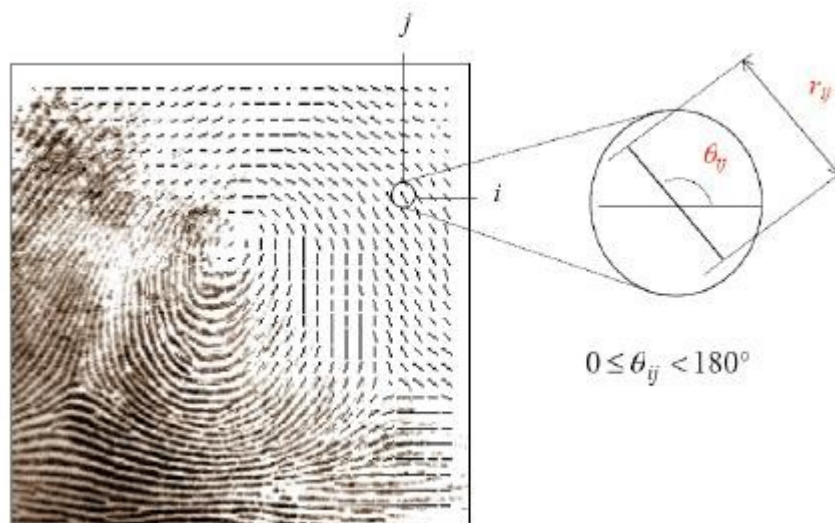


Figure III.7. Orientation locale dans une image d'empreinte [65]

C. Segmentation de l'image :

Après avoir estimé le champ d'orientation d'une image d'empreinte digitale, un algorithme de segmentation doit être utilisé pour localiser des zones d'intérêt et des zones de bruit afin de ressortir le plus d'informations utiles au système.

D. Extraction des points singuliers :

Ces points permettent de faciliter le processus d'enregistrement (registration) dans le but de combler les problèmes de translation ou de rotation.

E. Détection du point core :

Le point core est le centre de l'empreinte digitale et sa localisation est essentielle dans le processus d'authentification. Le point core d'une empreinte digitale est considéré comme le point de courbure maximale des crêtes dans une image empreinte. Donc pour le détecter il suffit de calculer les courbures des crêtes et prendre la plus grande (courbure maximale) [65].

III.4.2 Méthodes d'extraction des caractéristiques :

Bien qu'il existe plusieurs méthodes d'extraction des minuties nous pouvons les classer en deux catégories : celles qui se basent sur la binarisation de l'image de l'empreinte digitale (c.à.d. la conversion de l'image en une image noir et blanc) dites les méthodes classiques, et celles qui travaillent directement sur l'image filtrée dites méthodes directes.

A. Méthodes classiques ou méthode basée sur la binarisation :

La méthode la plus répandue consiste à extraire les minuties à partir d'un squelette de l'image. D'abord préparé à l'étape d'extraction au moyen d'une binarisation et d'une squelettisation, ensuite un fichier signature est extrait de l'empreinte avec la détection et l'extraction des minuties [66].

- **Binarisation :** La binarisation permet d'augmenter la visibilité des minuties (caractéristique), il s'agit de donner une intensité aux crêtes et une autre intensité différente aux vallées.

Plusieurs techniques de binarisation ont été proposées, la plus utilisée consiste à comparer chaque pixel à un seuil S , en lui assignant la valeur un (blanc) si son intensité est supérieure à S sinon il prend la valeur zéro (noir). Le seuil S peut être global fixé dès le départ ou local adaptatif obtenu en calculant la moyenne des pixels de chaque bloc de l'image de l'empreinte digitale [67].



Figure III.8 Binarisation de l'empreinte digitales

- **Squelettisation** : La squelettisation permet une détection rapide des minuties et il existe plusieurs algorithmes de squelettisation dans la littérature.

En général la squelettisation c'est une sorte d'amincissement basée sur des opérations morphologiques itératives, dans le but d'obtenir une image plus schématique de l'empreinte dans laquelle toutes les crêtes ont un pixel de largeur tout en conservant la connexité (c.à.d. respecter la continuité des stries) [68].



figure III.9 Squelettisation de l'empreinte digitale

- **Détection de minuties** : Lorsque les rides sont bien déterminées après la binarisation et la squelettisation de l'empreinte, les minuties seront facilement détectées, Il existe plusieurs méthodes de détection mais en général c'est un processus lié aux nombre de voisins :

- Les pixels avec trois pixels voisins sont identifiés comme bifurcations.
- Les pixels avec un pixel voisin sont identifiés comme arêtes de ride.

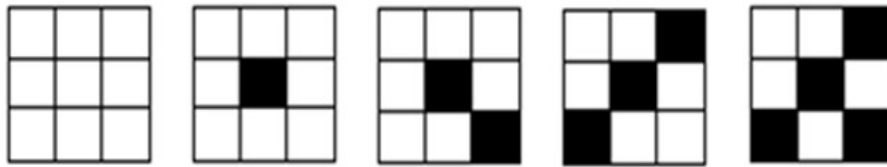


Figure III.10 Les cinq cas obtenus lors de processus d'extraction des minuties. Les pixels de valeur 1 et de valeur 0 correspondent respectivement aux les carrés noirs et les carrés blancs.

Explication de la figure :

- $I(i, j) = 0$, une vallée de l'empreinte.
- $I(i, j) = 1$ et aucun voisin, un point isolé.
- $I(i, j) = 1$ et un voisin, une terminaison.
- $I(i, j) = 1$ et deux voisins, une ligne continue.
- $I(i, j) = 1$ et trois voisins, une bifurcation.

À la fin de ce processus, nous acquérons un grand nombre des minuties, 100 minuties en moyenne. Parmi lesquelles environ 60% sont des minuties érronées, y compris celles introduites lors des étapes de binarisation et de squelettisation. Donc un post-traitement éliminant les fausses minuties est nécessaire avant de passer à l'étape suivante. le processus entier d'un algorithme d'extraction des minuties est montré dans la figure III.10.

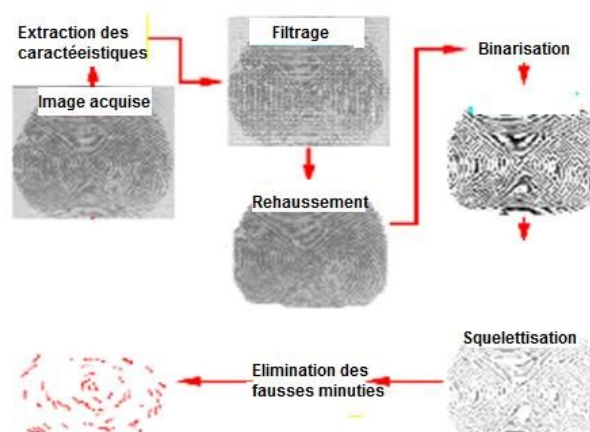


Figure III.11 Processus d'extraction des minuties [69].

- **L'élimination des fausses minuties (post-traitement) :** l'extraction peut engendrer ces deux types d'erreur, *un oubli de minuties* où l'algorithme d'extraction échoue dans la détection de vraies minuties existantes sur l'empreinte, en général parce que cette minutie est dans une région bruitée ou parce que la structure des crêtes est assez endommagée. Deuxième type d'erreurs, *un ajout de minuties* où l'algorithme d'extraction identifie faussement une structure de crêtes altérée comme étant une minutie.

Les méthodes existantes qui filtrent les fausses positives reposent généralement sur l'utilisation d'heuristiques [70] [71] (basées sur le fait que la distance entre deux minuties voisines ne doit pas dépasser un certain seuil).

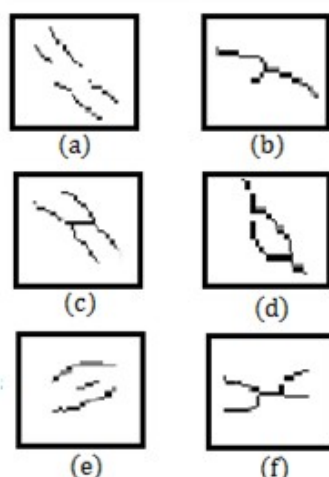


Figure III.12 Type des fausses minuties, (a) coupure dans les crêtes, (b) segment court, (c) pont, (d) îlot, (e) segment court, (f) segment court.

Bien que les méthodes basées sur la binarisation soient faciles à mettre en place et moins coûteuses, elles ont quelques défauts qui résident principalement dans la possibilité de perdre beaucoup d'informations due au bruit introduit lors de binarisation. De plus la binarisation et la squelettisation exigent un temps de calcul important vient de plusieurs balayage de l'image, ce qui diminue la performance des méthodes classiques.

B. Méthodes directes :

La méthode d'extraction directe (*Direct gray-scale methods*) est proposée par D. Maio et D. Maltoni [72]. Elle consiste à extraire l'ensemble des minuties directement sur l'image filtrée en niveau de gris sans passer par les étapes de binarisation et de squelettisation. Le principe de cette approche se base sur le suivi des crêtes (stries) de l'image directionnelle selon le maximum local.

- **L'image directionnelle :** C'est l'estimation de l'orientation de lignes de l'empreinte digitale. Soit I l'image de l'empreinte en noir et blanc, $I(i, j)$ représente le pixel (i, j) . L'image directionnelle (ou l'orientation de l'empreinte) c'est la matrice notée D dont chaque case (i, j) contient l'orientation locale $\Theta(i, j)$ entre l'axe horizontal et l'orientation (approximative) des lignes de l'empreinte dans le voisinage du pixel (i, j)

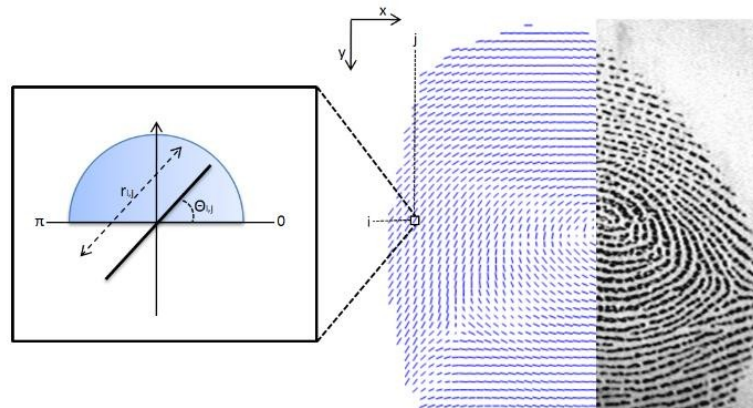


Figure III.13 L'image directionnelle [73]

- **Le suivi des crêtes :** Le suivi des stries nécessite l'estimation du champ d'orientation de l'empreinte. Soit le point (i_a, j_a) appartenant à une strie, pour la parcourir nous avançons de μ pixels dans la direction Θ_a afin d'atteindre un point soit x_a . Ensuite nous cherchons le maximum local le plus proche de x_a sur la section orthogonale à la direction Θ_a centrée en x_a de longueur en obtenant un autre point (i_b, j_b) de la strie (voir la figure III.13). Nous recommençons le même processus en prenant comme nouveau point de départ le point (i_b, j_b) , on s'arrête lorsqu'on détecte une bifurcation ou une terminaison. On refait les mêmes opérations avec toutes les stries de l'empreinte digitale. Pour assurer qu'une crête n'est parcourue qu'une seule fois, nous adoptons la stratégie d'étiquetage, c'est ainsi nous détectons toutes les minuties de l'empreinte.

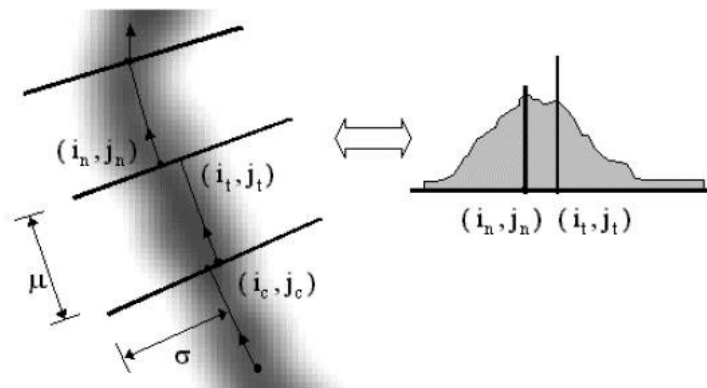


Figure III.14 Le suivi d'une crête [72]

Bien que l'extraction des minuties directement à partir de l'image filtrée soit plus rapide et produit très peu de fausses minuties par rapport à celles générées par les méthodes basées sur la binarisation, cependant l'ajustement des paramètres μ et Θ est très sensible aux fortes variations locales de la distance inter-strie.

C. Traitement de texture :

La texture est la répétition spatiale d'un élément de base dans l'image. Elle est caractérisée par des propriétés telles que la direction locale des crêtes, les composantes fréquentielles locales de la texture de l'empreinte ou l'isotropie. Cette méthode de traitement de la texture est une alternative aux méthodes basées sur les minuties et aujourd'hui elle fait l'objet d'un véritable axe de recherche.

L'étude de la texture locale utilise des algorithmes basés sur la corrélation qui divise l'empreinte en petits secteurs (ou blocs) où la direction, la fréquence, le pas des lignes ou autres descripteurs de texture sont extraits puis stockés. Elle permet un traitement très rapide, et donc un temps de réponse très court.

L'approche la plus connue et la plus reprise dans différents travaux repose sur le calcul du FingerCode [74] voir figure III.15.

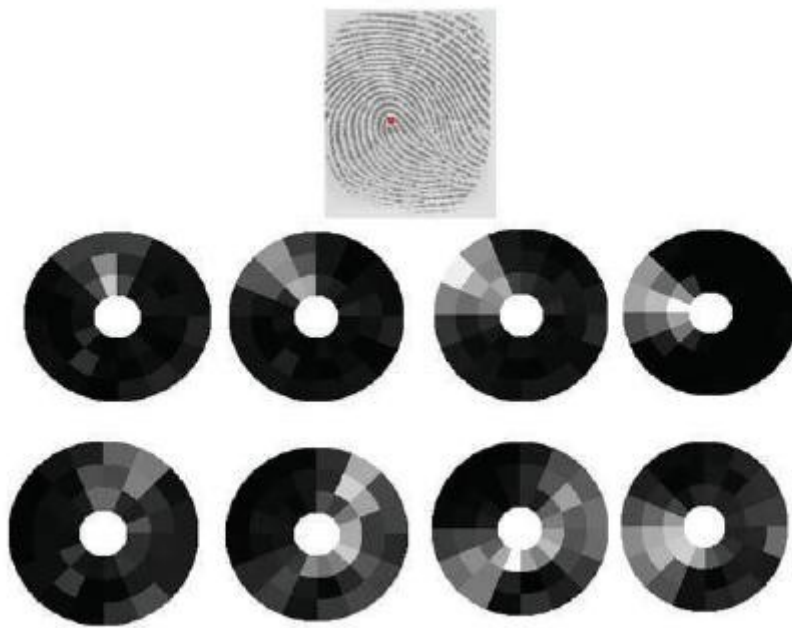


Figure III.15. Fingercode dans une image [74]

III.4.3 Comparaison des empreintes (phase d'appariement) :

Un système de reconnaissance automatique d'empreinte digitale renvoie une réponse soit positive ou négative après avoir comparé l'empreinte à identifier à toutes les autres empreintes qu'il possède dans sa base de données. Cependant cette tâche n'est pas facile, notamment à cause de la variabilité dans les différentes impressions d'une même empreinte (variation intra-classe). Les facteurs principaux responsables des variations intra-classe sont : l'état de la peau (exemple le doigt n'est pas propre entaché de graisse ou de sueur), la variation de la pression du doigt sur le capteur d'empreinte, le déplacement, la rotation c'est ainsi qu'un déplacement du doigt de 2mm qui est imperceptible à l'œil humain provoque une translation d'à peu près 40 pixels dans une image scannée à une résolution de 500 dpi [62]. Donc les algorithmes de comparaison doivent prendre en compte tous ces paramètres [66].

La figure III.14 illustre quelques exemples des images d'une même empreinte digitale extraites de la base de données FVC2002.



Figure III.16 Les variations intra-classe d'une même empreinte digitale, **(a)** le doigt est incliné à gauche sur le capteur d'empreinte, **(b)** le doigt est incliné à droite, **(c)** le doigt est plus pressé, **(d)** le doigt est légèrement pressé, **(e)** une partie du doigt n'est pas apposée sur le capteur d'empreinte, **(f)** le doigt est correctement apposé sur le capteur d'empreinte, **(g)** le doigt est sale, **(h)** le doigt est propre [62].

les différentes approches de comparaison des empreintes sont classées en trois grandes familles : la comparaison basée sur la corrélation , la comparaison basé sur les minuties et la comparaison basées sur les singularité des lignes d'empreintes digitales.

A. La comparaison basée sur la corrélation :

Elle consiste à comparer tout simplement les pixels de deux empreintes digitales , et calculer la corrélation de pixels. Cette approche est assez facile à réaliser. Cependant Les techniques basées sur la corrélation de pixels ne sont pas efficaces car elles sont sensibles à la variation intra-classe.

En fait les différentes impressions d'une même empreinte peuvent donner des images très différentes, ce qui rendent les valeurs de leurs pixels différents. De plus ces approches sont coûteuses en temps de calcul, ce problème peut être résolu en calculant seulement la corrélation de certaines régions locales déterminées suivant quelques critères, toutefois les comparaisons basées sur la corrélation de pixels ne sont pas assez rigoureuses.

B. La comparaison basées sur les minuties :

Ce sont les approches les plus utilisées. Les minuties sont extraites de deux empreintes digitales et représentées sous forme d'un ensemble de points dans un plan à deux dimensions selon le modèle des coordonnées (figure III.4). L'assortiment basé sur les minuties consiste à trouver un bon alignement entre les minuties de deux empreintes à comparer qui donne un maximum de paires de minuties semblables. Une marge de tolérance afin de compenser les erreurs introduite par le bruit et la distorsion sera définie (figure III.15).

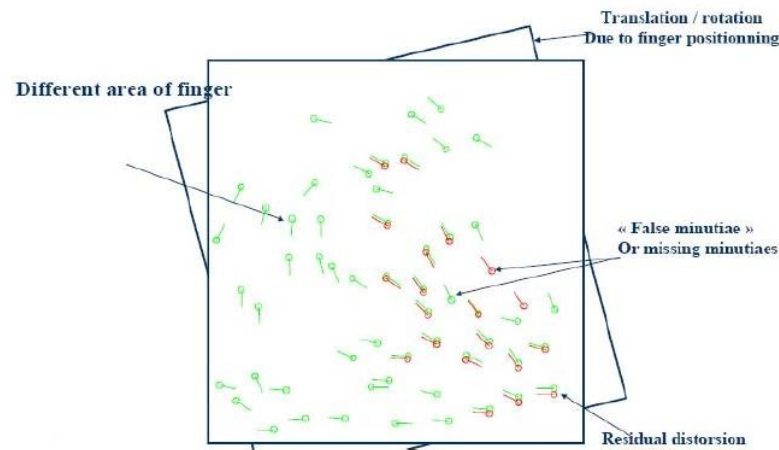


Figure III.17 La comparaison basée sur les minuties [75]

C. La comparaison basées sur les singularités de ligne d'empreinte digitale :

Lorsqu'on dispose d'une image de mauvaise qualité, il est très difficile de réaliser l'extraction de minutie, en revanche, d'autres singularités de lignes d'empreinte telles que l'orientation locale, la taille, la position géométrique, la fréquence, la texture locale peuvent être plus facilement extraites que les minuties. Ces singularités sont cependant très instables et très variables d'une personne à une autre et d'un doigt à une autre (d'une même personne). Ces techniques sont donc très peu utilisées.

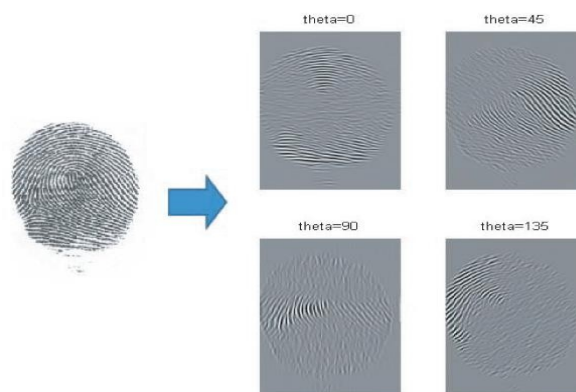


Figure III.18 L'extraction des informations de texture basées sur l'orientation locale de l'empreinte digitale [76]

III.5 Conclusion

Dans ce chapitre nous avons présenté un état de l'art sur les empreintes digitales avec leurs caractéristiques globales et locales, ensuite nous avons vu le fonctionnement d'un système de reconnaissance automatique basé sur cette même modalité avec ses méthodes de prétraitement, les méthodes d'extraction des caractéristiques et enfin nous avons présenté les différentes méthodes d'appariement ou de comparaison de ces empreintes.

Dans le chapitre qui suit nous allons voir la fusion de modalités.

CHAPITRE IV

La fusion de modalités

IV.1 Introduction :

La biométrie multimodale désigne l'utilisation de plus d'une source d'information pour la reconnaissance d'un individu [77] [78]. Par exemple, un système biométrique multimodal peut utiliser plus d'une modalités (empreinte digitale et le visage...etc) pour confirmer l'identité d'un utilisateur. Cette technique permet d'améliorer les performances de la reconnaissance et aide à résoudre certains des problèmes et limitations rencontrés précédemment par les systèmes unimodaux.

Dans ce chapitre nous allons voir en premier la fusion multimodale et les différents niveaux de fusion, nous expliquerons par la suite la fusion au niveau des scores et les différentes techniques de normalisation de ces scores et enfin nous allons voir les techniques de combinaison et les techniques de classification des scores.

IV.2 Pourquoi s'orienter vers la multimodalité ?

Les technologie et les techniques concernant les systèmes biométriques unimodaux (utilisant un seul trait biométrique) ne permettent actuellement pas d'avoir un taux de reconnaissance élevé car ces derniers sont limités et rencontrent plusieurs problèmes tel que :

Le bruit sur la donnée capturée,La variation intra-classe,les problème d'unicité,la non-universalité,la vulnérabilité aux attaques. Ces derniers sont cités en détails le premier chapitre.

Avec tous ces problèmes la fiabilité et les performances des systèmes unimodaux sont remise en question ,Pour surpasser ces limites il est possible d'avoir recours à la combinaison de plusieurs modalités d'où le terme Multimodalité.

Dans ce mémoire on a opter pour un système à deux traits biométriques, en l'occurrence le visage et l'empreinte digitale pour les avantages qu'ils présentent : faible coût, facilité de mise en œuvre, acceptée par la population tout en atteignant des performances élevée.

IV.3 La fusion multimodale :

IV.3.1 Conception d'un système biométrique multimodal :

Pour la conception d'un système biométrique multimodal, une variété de facteurs doit être prise en compte sur le design et la structure d'un tel système, parmi ces facteurs, citons :

A. L'Interface Homme-Machine (IHM) :

Permettre une acquisition efficace des informations biométriques d'un individu, tout en minimisant l'inconvenance pour l'utilisateur [79]. par exemple une seule camera pour obtenir l'image de l'iris et du visage en même temps.

B. Le facteur de coût :

Un compromis entre le coût correspondant à l'amélioration de la performance du système, au nombre de capteurs déployés, au temps pris pour acquérir les données biométriques, aux exigences de stockage, et au degré de commodité perçue par l'utilisateur.

C. La détermination des sources d'information biométrique :

Pour un type d'application donné on choisit les différentes sources d'information biométrique les plus pertinentes.

D. L'acquisition et séquence de traitement :

L'acquisition simultanée ou en série des modalités biométriques, et la manière dont les informations ou les données sont traitées, en même temps ou séquentiellement.

E. Le type d'information :

Définit le types d'informations ou d'attributs qui doivent être fusionnés et qui sont fournies par multiples sources biométriques (caractéristiques, scores de correspondance, décision, etc.).

F. La méthode de fusion :

Le schéma de fusion optimal à choisir pour combiner les informations présentées par de multiples sources biométriques.

Finalement, l'évaluation d'un système biométrique multimodal est souvent lié à sa précision de reconnaissance, du nombre d'utilisateurs qui peuvent être pris en compte par ce système, du coût résultant par l'ajout de nouveaux capteurs et du temps supplémentaire requis pour acquérir et traiter plusieurs modalités.

IV.3.2 Les différentes formes de multimodalité :

Selon les sources d'information qui peuvent être considérées dans un système biométrique multimodal, il existe de nombreux scénarios possibles [26] :

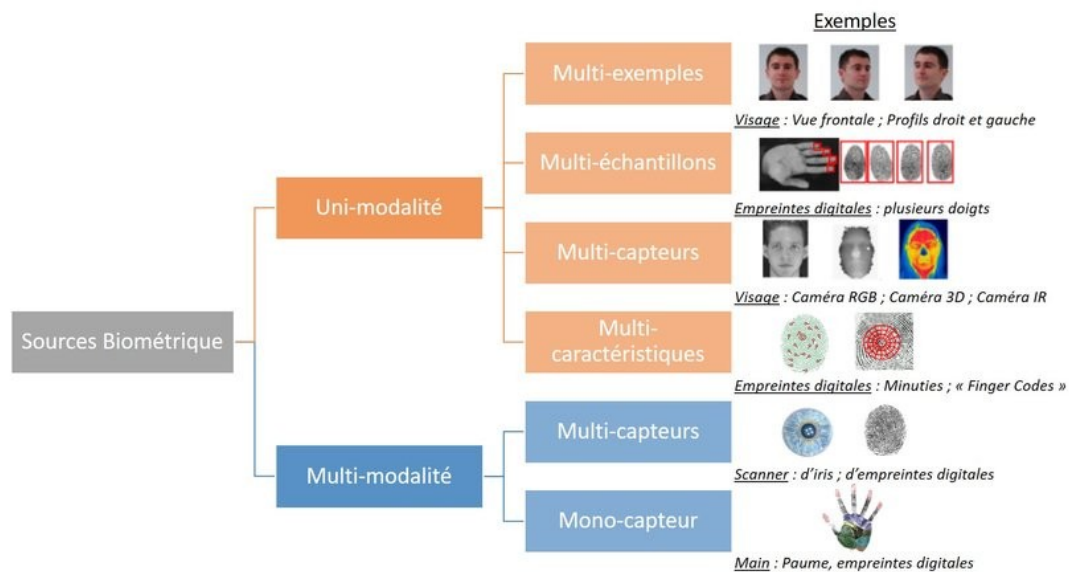


Figure IV.1 Sources d'informations dans un système de fusion biométrique [80]

A. Systèmes multi-échantillons :

L'utilisation de plusieurs échantillons du même trait biométrique dans le but de prendre en compte les variations qui peuvent se produire au sein de ce trait, par exemple, l'acquisition du profil frontal du visage et les profils gauches et droits afin de tenir compte des variations de la pose faciale.

B. Systèmes multi-capteurs :

L'utilisation de deux à plusieurs capteurs pour capturer un même trait biométrique d'un individu, par exemple l'utilisation d'une caméra classique et une caméra plus sophistiquée pour l'acquisition d'une image 2D et une autre 3D d'un visage.

C. Systèmes multi-algorithmes :

L'utilisation de plusieurs algorithmes pour le traitement d'une seule donnée biométrique afin d'extraire diverses caractéristiques qui peuvent améliorer la performance du système, par exemple, l'utilisation des algorithmes d'analyse de texture et de minuties sur l'empreinte digitale.

D. Systèmes multi-instances :

L'utilisation de plusieurs instances d'un même trait biométrique, par exemple, l'utilisation des empreintes digitales des dix doigts d'un individu.

E. Systèmes multimodaux :

L'utilisation de plusieurs traits biométriques, par exemple les veines, l'empreinte digitale et l'empreinte d'articulation.

En combinant des informations issues d'une seule et même modalité, les quatre premiers systèmes permettent d'améliorer les performances de la reconnaissance en réduisant la variabilité intra-classe, Cependant ces systèmes ne permettent pas de traiter le problème de la non-universalité ainsi que leurs résistance aux fraudes, contrairement aux systèmes "multi-biométries" [25].

Enfin, on peut noter que l'utilisation du terme de systèmes hybrides [81] est pour se référer aux systèmes qui intègrent un sous-ensemble des 5 scénarios que nous venons d'évoquer.

IV.4 Les différents niveau de fusion :

Dans un système typique de reconnaissance de formes, nous suivons une chaîne de traitement qui comporte quatre modules (module de capture, d'extraction des caractéristiques, de comparaison et le module de décision). Dans un système biométrique multimodal, la fusion peut être accomplie en utilisant l'information disponible dans l'un de ces modules (niveaux). Selon *Sanderson and Paliwal* [82], deux grandes familles de fusions peuvent être distinguées, la fusion avant correspondance (matching) et la fusion après correspondance.

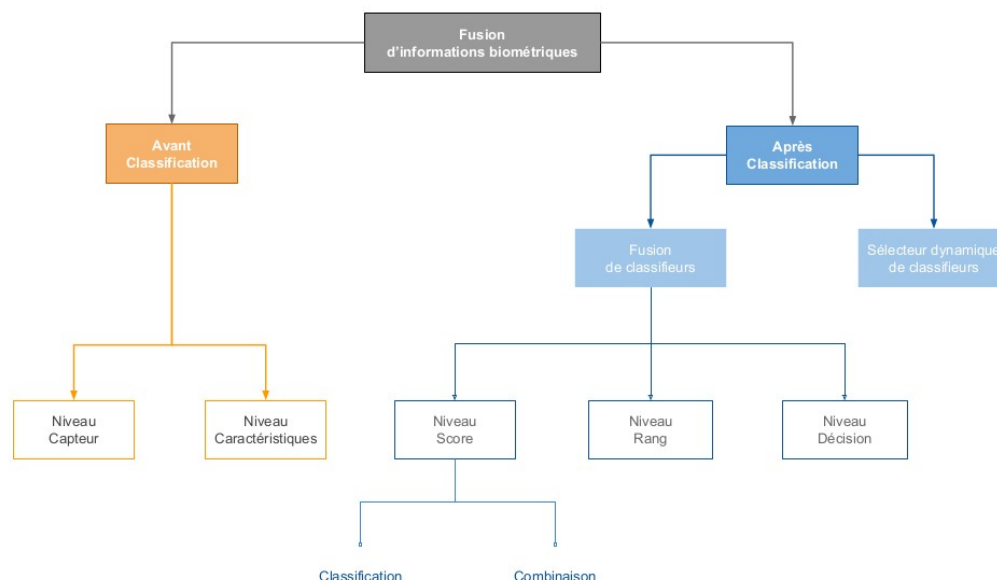


Figure IV.2 Schéma de répartition des différents niveaux de fusion biométrique [80]

IV.4.1 Fusion avant le matching :

Avant la correspondance (matching), l'intégration d'informations peut avoir lieu soit au niveau du module de capture ou au niveau du module d'extraction des caractéristiques.

A. Niveau Capteur (Sensor Level) :

Il s'agit de la fusion au niveau capteur des données brutes ("raw data") provenant d'un à plusieurs capteurs, ce type de fusion peut se faire uniquement si les diverses captures sont obtenues à partir de plusieurs capteurs compatibles ou d'un seul capteur pour permettre une homogénéité des informations acquises. Par exemple, les images de visage obtenues à partir de plusieurs caméras peuvent être combinées pour former un modèle 3D du visage. La figure 4.3 illustre la fusion au niveau du capteur.

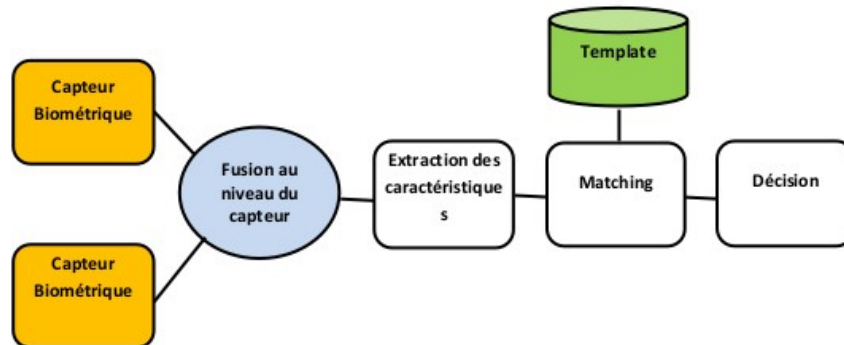


Figure IV.3 Fusion aux niveau du capteur [25]

B. Niveau Caractéristiques (Feature Level) :

La fusion au niveau caractéristiques consiste à combiner plusieurs données caractéristiques issues de différent traits biométriques. Contrairement à la fusion au niveau capteur, cette fusion ne nécessite pas une homogénéité entre les données. Le vecteur caractéristiques résultant de cette fusion est calculé soit comme une somme pondéré si les vecteurs de caractéristiques en entrée sont homogènes, ou comme une concaténation si les vecteurs de caractéristiques à fusionner sont hétérogènes, par exemple la fusion des caractéristiques de modalité visage et d'empreinte palmaire [83], toutefois la concaténation augmente l'espace de classification, ce qui pose le problème de la malédiction de la dimension [84].

La figure 3.4 illustre la fusion au niveau des caractéristiques.

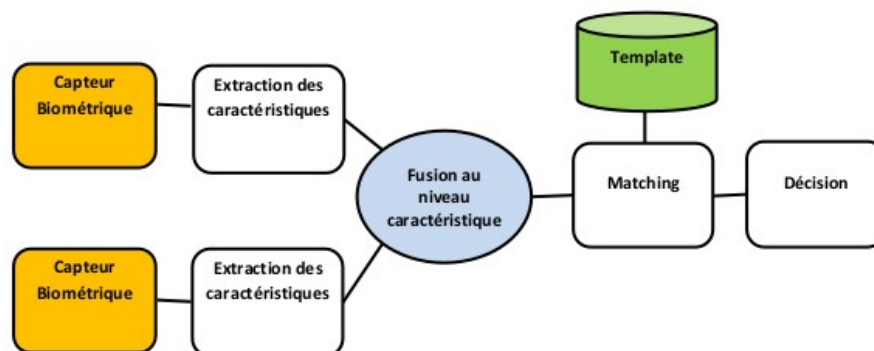


Figure IV.4 Fusion au niveau des caractéristiques [25]

IV.4.1 Fusion après le matching :

L'intégration de l'information après classification ou correspondance (fusion après le matching) peut être divisée en quatre catégories : fusion au niveau décision, fusion au niveau rang, fusion au niveau score et une sélection dynamique de classifieurs qui choisit les résultats d'un classifieur qui est le plus à même de donner la décision correcte d'un modèle d'entrée spécifique [85].

A. Niveau Décision (Decision Level) :

L'intégration d'information au niveau décision est simple et abstraite. En effet chaque sous-système décide individuellement de la meilleure correspondance possible selon l'entrée qui lui est présentée. Les méthodes les plus utilisées pour ce type de fusion sont le majority voting [86] (si la majorité des systèmes ont décidé 1 alors la décision finale est "accepté"), les règles ET (si tous les systèmes ont décidé 1 alors la décision finale est "accepté") et OU (si un système a décidé 1 alors la décision finale est "accepté") [87], le behavior knowledge space [88], et le weighted voting [89]. La figure 4.5 illustre la fusion au niveau décision.

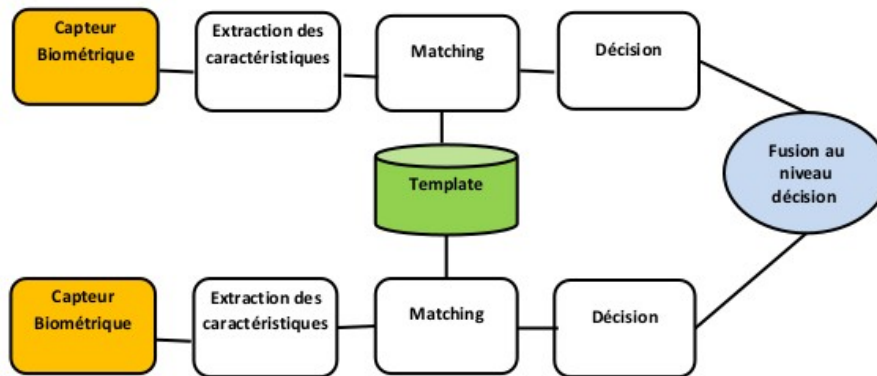


Figure IV.5 Fusion au niveau de la décision [25]

B. Niveau Rang (Rank Level) :

La fusion au niveau du rang est la méthode qui consolide plusieurs résultats d'identification pour améliorer la fiabilité du système. Quand la sortie de chaque "matcher" (module de reconnaissance) biométrique est un sous-ensemble de correspondances possibles triées dans un ordre décroissant de confiance, alors la fusion peut se faire au niveau rang. Ho et al. [90] décrivent un système multimodal fondé sur la fusion au niveau du rang en utilisant les approches *highest rank method* (assigner à chaque correspondance possible le meilleur (minimum) rang calculé par différents matchers), *Borda count* (utiliser la somme des rangs assignés par les matchers individuels afin de calculer les rangs combinés) et *logistic regression* (une somme pondérée des rangs individuels est calculée et les poids sont déterminés par régression logistique) [26].

C. Niveau Score (Score Level) :

L'intégration d'information au niveau score est l'approche la plus courante dans les systèmes biométriques multimodaux vu que ce niveau de fusion peut être appliqué à tous les types de biométries dans un espace de dimension limité (le vecteur de scores résultant a une dimension égale au nombre de sous-systèmes). En fait, la fusion au niveau score donne un meilleur compromis entre la richesse d'informations et la facilité d'implémentation où les scores (de correspondance) donnés en sortie par les matchers contiennent l'information la plus riche à propos du modèle d'entrée, après les vecteurs de caractéristiques et il est relativement facile d'accéder et de combiner les scores générés par les différents matchers. Dans le reste de ce chapitre nous allons détailler la fusion au niveau des scores. La figure 4.6 illustre la fusion au niveau décision.

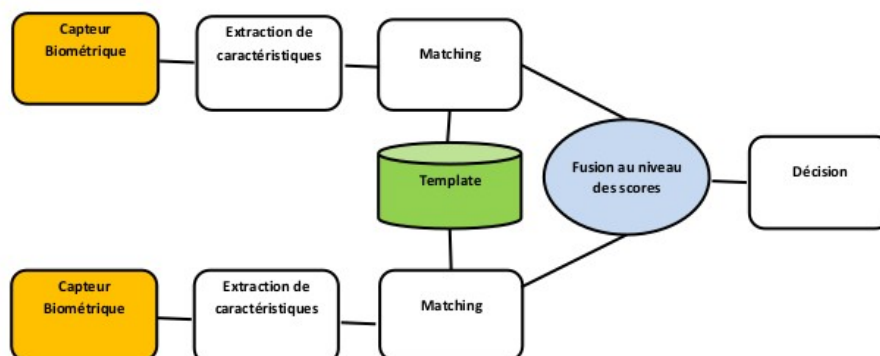


Figure IV.6 La fusion au niveau des scores [25]

IV.5 La fusion au niveau des scores:

Cette méthode consiste à fusionner les scores de correspondance en sortie par les matchers, ces derniers contiennent une information pertinente à propos du modèle d'entrée, c'est l'approche la plus utilisée dans les systèmes biométrique multimodaux pour sa facilité d'implémentation et sa richesse en information [26].

Il existe deux approches principales pour fusionner les scores, il a été démontré que la méthode la plus performante est de traiter cela comme un problème de combinaison, l'autre approche consiste à voir ça comme un problème de classification [26].

Classification, dans cette approche un vecteur de caractéristique est construit en utilisant les scores de correspondance en sortie des matchers puis il est attribué à l'une des deux classes : « Genuine user », « Imposer user ». En général cette méthode ne nécessite pas de normalisation des scores avant de les envoyer dans le classifieur .

Combinaison, dans cette approche un seul score est formé en combinant les scores de correspondance individuels , ce dernier est utilisé pour la décision finale. En général il est important que les scores soient normalisés avant la combinaison.

IV.6 Normalisation des scores :

C'est l'ensemble des méthodes qui permettent de ramener des scores dans un domaine commun , il est indispensable de normaliser les scores avant leur combinaison dans les cas suivants :

Si, les scores de correspondance ne sont pas homogène (dissimilarité, similarité), si les scores de correspondance ne sont pas inclus dans le même interval, ou si les scores de correspondance ne suivent pas la même distribution statistique. Parmi les techniques de normalisation des scores citons [26] :

A. La normalisation Min-Max:

Cette technique de normalisation est la technique de normalisation la plus simple, et la plus adaptée lorsque les bornes (minimales et maximales) des scores sont connues. Dans ce cas on translate les scores minimum vers 0 et les scores maximum vers 1. si les scores minimum et maximum ne sont pas connus nous pouvons les estimer à partir d'un jeu d'entraînement de scores de correspondance donné et appliquer ensuite la normalisation Min-Max, cependant la technique reste valable mais pas robuste (sensible aux valeurs aberrantes dans les données utilisées pour l'estimation). La formule de normalisation Min-Max est :

$$S'_i = \frac{S_i - \min(S_i)}{\max(S_i) - \min(S_i)} , \quad (4.1)$$

S_i représente les scores de correspondance de sortie de chaque sous système.

B. La normalisation Decimal scaling:

Cette technique de normalisation peut être appliquée lorsque les scores de différents matchers évoluent selon une échelle logarithmique. Par exemple, si un matcher a des scores dans l'intervalle [0, 1] et l'autre matcher a des scores dans l'intervalle [0,1000], La formule de normalisation Decimal scaling est :

$$S'_i = \frac{S_i}{10^n} , \quad (4.2)$$

Où $n = \log_{10} \max(S_i)$. Les problèmes de cette technique sont le manque de robustesse et l'hypothèse sur l'évolution des scores de différents matchers selon une échelle logarithmique.

C. La normalisation Z-Score:

Cette technique de normalisation est la technique la plus couramment employée, elle utilise de chaque matcher deux paramètres (la moyenne et l'écart-type de la distribution des scores) qui peuvent être déduits de l'algorithme de reconnaissance. Si on n'a pas connaissance sur la nature de ce dernier, on estime la moyenne et l'écart-type à partir d'un jeu de scores de correspondance donné. La formule de normalisation Z-Score est :

$$S'_i = \frac{S_i - \mu}{\sigma} , \quad (4.3)$$

Où μ est la moyenne de la distribution calculée ou estimée et σ est l'écart-type des données. Cependant les deux paramètres de cette technique sont sensibles aux valeurs aberrantes donc un manque de robustesse. De plus, Si la distribution des scores n'est pas gaussienne, cette normalisation ne garantit pas un intervalle commun pour les scores normalisés provenant de différents matchers.

D. La normalisation médiane et l'écart absolu médian (MAD):

Cette technique de normalisation basée sur la médiane et l'écart-type absolu n'est pas sensible aux valeurs aberrantes et aux points aux extrémités d'une distribution. La formule de normalisation médiane et l'écart absolu médian (MAD) est :

$$S'_i = \frac{S_i - \text{median}}{\text{MAD}} , \quad (4.4)$$

Où $\text{MAD} = \text{median}(|S_i - \text{median}(S_i)|)$. Cependant lorsque la distribution de scores n'est pas gaussienne la médiane et l'écart-type absolu médian sont des estimateurs pauvres en paramètres de position et d'échelle (une faible efficacité par rapport aux estimateurs issus de la moyenne et de l'écart-type). Ainsi cette technique ne conserve pas la distribution originale.

E. La normalisation tanh (tangente hyperbolique):

Cette technique de normalisation introduite par *Hampel* et al [91] est généralement efficace et robuste dans la gestion des valeurs aberrantes. La normalisation tanh est donnée par :

$$S'_i = \frac{1}{2} \left\{ \tanh\left(0,01 \left(\frac{S_i - \mu_{GH}}{\sigma_{GH}}\right)\right) + 1 \right\} , \quad (4.5)$$

Où μ_{GH} et σ_{GH} sont respectivement estimateurs de la moyenne et l'écart-type de la distribution des scores clients, tels qu'ils sont donnés par les estimateurs de *Hampel*. Les estimateurs de Hampel sont basés sur la fonction d'influence (ψ) suivante :

$$\psi(u) = \begin{cases} u & 0 \leq |u| < a \\ a * \text{sign}(u) & a \leq |u| < b \\ a * \text{sign}(u) * \left(\frac{c - |u|}{c - b}\right) & b \leq |u| < c \\ 0 & |u| < a \end{cases} , \quad (4.6)$$

La méthode tanh est peu sensible aux valeurs aberrantes car la fonction de Hampel réduit l'influence des points aux bords d'une distribution (identifiés par a, b et c) pendant l'estimation des paramètres de position et d'échelle.

Les caractéristiques des différentes techniques de normalisation que nous venons de détailler sont résumées dans le tableau 4.1.

Technique de normalisation	Robustesse	Efficacité
Min/Max	Non	N/A
Decimal scaling	Non	N/A
Z-Score	Non	Élevée (optimale pour des données gaussiennes)
Médiane et MAD	Oui	Modérée
Estimateurs tanh	Oui	Élevée

Tableau IV.1 : Résumé Des Techniques de Normalisation de Scores [26]

IV.7 Techniques de classification des score :

Les méthodes de fusion à base de classifieurs cherchent à combiner les scores de correspondance afin d'arriver à une décision. Plusieurs classifieurs peuvent être utilisés [26].

Wang et al. [92] utilisent l'analyse discriminante linéaire de Fisher (LDA) et un classifieur de réseau de neurones associé à une fonction de base radiale (RBF) pour combiner les scores issus de système de reconnaissance faciale et de système de reconnaissance de l'iris.

Verlinde et Chollet [93] utilisent trois classifieurs : un premier utilisant la méthode des "k plus proches voisins" ("k-NN") avec une quantification vectorielle, un deuxième basé sur un arbre décisionnel et un dernier basé sur un modèle de régression logistique. Cette technique combine les scores issus de deux modules de reconnaissance faciale et d'un module de reconnaissance de la parole.

Chatzis et al. [94] utilisent une méthode de regroupement ("clustering") appelée "fuzzy k-means" et une quantification vectorielle floue ("fuzzy vector quantization"), couplée à un classifieur de réseau de neurones de RBF médiane pour fusionner les scores issus des systèmes biométriques basés sur des caractéristiques visuelles (visage) et acoustiques (voix).

Sanderson et al. [95] utilisent un classifieur basé sur une Machine à Vecteurs de Support (SVM) pour combiner les scores issus d'un module de reconnaissance faciale et d'un module de reconnaissance de la parole. Afin de surmonter un problème lié à la présence de bruit en entrée, ils implémentent des classifieurs résistants au bruit structurel comme un classifieur linéaire défini par morceau ("piece-wise linear classifier") et un classifieur Bayésien modifié.

Ross et Jain [96] utilisent un arbre décisionnel et des classifieurs discriminants linéaires pour combiner les scores issus des systèmes de reconnaissance de visage, d'empreintes digitale et de géométrie de la main.

IV.8 Techniques de combinaison des scores :

Les méthodes de combinaison de scores sont des méthodes simples permettant de produire un score final c à partir des scores s_i de R matchers. Parmi les méthodes les plus utilisés : le produit, la somme, le maximum, le minimum et la médiane [97].

A. La règle produit ("product rule") :

La règle consiste à calculer un nouveau score c en faisant le produit des scores s_i de chaque matcher :

$$C = \prod_{i=1}^R s_i , \quad (4.7)$$

Cette méthode est susceptible aux valeurs aberrantes si la normalisation adoptée n'est pas robuste. nous pouvons obtenir un score final égale à 0 si un des scores normalisés en entrée égale à 0.

B. La règle somme ("sum rule") :

La règle consiste à calculer un nouveau score c en faisant la somme des scores s_i de chaque matcher :

$$C = \sum_{i=1}^R s_i , \quad (4.8)$$

Cette méthode est plus efficace que la méthode produit car elle est robuste aux valeurs aberrantes et au bruit. De plus le score normalisé à 0 n'annule pas les autres scores.

C. La règle maximum ("max rule") :

La règle consiste à définir un nouveau score c comme étant le score maximal des scores s_i de chaque matcher :

$$C = \max_i (s_i) , \quad (4.9)$$

Cette méthode n'est pas robuste aux valeurs aberrantes.

D. La règle minimum ("min rule") :

La règle consiste à définir un nouveau score c comme étant le score minimal des scores s_i de chaque matcher :

$$C = \min_i (s_i) , \quad (4.10)$$

Cette méthode n'est pas robuste aux valeurs aberrantes.

E. La règle somme pondérée :

La méthode somme pondérée nécessite un réglage de paramètres à la différence des méthodes cités ci-dessus. Par exemple Jain et Ross [98] ont proposé l'utilisation de poids w_i spécifiques à chaque utilisateur pour réaliser la somme pondérée de scores issus de différentes modalités. L'idée de cette méthode est que certains individus ont certains traits biométriques de qualité moins bonne que ceux des autres individus. Par exemple, certaines personnes peuvent avoir des empreintes digitales endommagées à cause d'un travail manuel prolongé. Pour de tels utilisateurs on affecte un faible poids au score d'empreinte digitale et un poids plus élevé aux scores d'autres modalités, la règle est :

$$C = \sum_{i=1}^R w_i s_i , \quad (4.11)$$

Cette methode permet de réduire les probabilités de faux rejet, cependant cette méthode exige un apprentissage de poids spécifiques pour chaque utilisateur.

IV.9 Conclusion :

Dans ce chapitre, nous avons introduit la fusion de modalités, nous avons présenté la fusion multimodale en citant une variété de facteurs nécessaire pour la conception d'un tel système biométrique (multimodale) ainsi que les différentes forme de multimodalité, ensuite nous avons vu les quatre niveaux de fusion : la fusion au niveau du capteur, la fusion au niveau des caractéristiques, la fusion au niveau des décisions et la fusion au niveau des scores sur la quelle nous avons détaillé avec les différentes techniques de normalisation des scores. Et enfin nous avons présenté deux approches de fusions des scores, l'approche à base de classifieurs, et l'approche de combinaison de scores.

CHAPITRE V

Conception et réalisation

V.1 Introduction:

Ce chapitre est consacré à l'étude analytique de notre système et son fonctionnement. Nous allons commencer par la conception où nous allons présenter les différents cas d'usages, l'architecture générale du système, en passant par les méthodes de mesure de performance, et enfin, nous verrons les détails d'implémentation des différents modules.

V.2 Conception:

Dans cette première partie, nous allons présenter les différentes approches adoptées, l'architecture des différents modules et classes de notre système, et enfin nous allons montrer les interactions entre ces derniers à travers plusieurs diagrammes.

V.2.1 Les acteurs du systèmes :

Le système comporte deux acteurs (L'administrateur et l'individu Test), chacun de ces acteurs est amené à effectuer un certain nombre de tâches qui sont résumées ci-dessous :

A. L'Administrateur :

C'est la personne responsable de la gestion et du bon fonctionnement du système, les tâches effectuées par cet acteur sont :

- Gestion de la base de données.
- Enregistrement des nouveaux clients dans le système.
- Test et réglage des différents paramètres du système.

B. L'individu Test :

C'est le client du système, c'est une personne qui interagit avec le système soit en l'identifiant ou en lui donnant un accès (authentification).

V.2.2 Diagramme de cas d'utilisation général :

Les cas d'utilisation vont nous permettre de préciser le contexte fonctionnel de notre système. La figure ci-dessous, nous montre les différentes façons d'utilisation du système proposé avec une description textuelle de chaque cas :

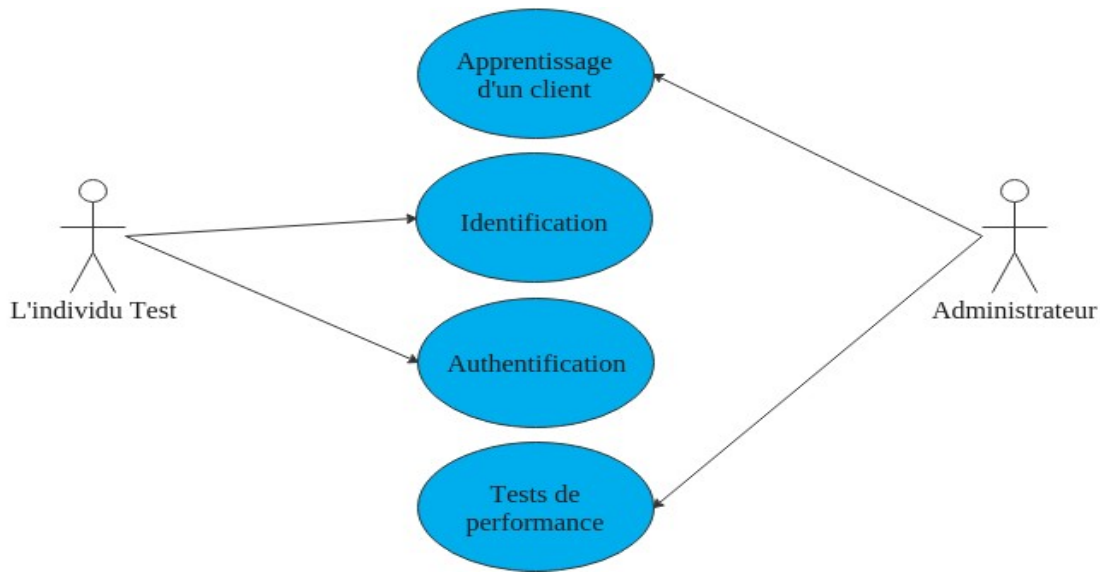


Figure V.1 Diagramme de cas d'utilisation global

A. Apprentissage d'un client : Ce cas d'utilisation permet à l'administrateur d'ajouter un nouveau client dans le système, pour ce nouveau client huit images du visages et huit autres de son empreinte digitale sont acquises, puis un modèle unique de chaque modalité sera généré à partir de ces images, pour enfin stocker ces derniers avec les informations personnelles dans une base donnée pour une utilisation ultérieure. Un scénario nominal (ajout d'un nouveau client) se présente comme suit :

- introduire au système des images du visage et de l'empreinte digitale du client
- Saisir les informations personnelles du client
- Enregistrement des informations du client avec ces images dans la base de données
- Prétraitement des images acquises
- Génération des modèles du client avec l'extraction des paramètres (application de la DWT pour les images du visage et la méthode basée sur les minuties).
- Enregistrement des modèles caractéristiques du client

B. Identification : Ce cas d'utilisation permet à un utilisateur (client) de s'identifier, le système utilise des données récupérées du client (image de son visage et de son empreinte digitale), et à partir de ces données et de l'ensemble des modèles stockés dans la base de données, il définit l'identité de l'utilisateur. Un scénario nominal se présente comme suit :

- Acquisition des données du client (image du visage et de l'empreinte digitale)
- Prétraitement des images acquises
- Génération des modèles test avec l'extraction des paramètres (application de la DWT pour les images du visage et la méthode basée sur les minuties).
- Parcourir la base de données à la recherche d'une correspondance des modèles générés
- Afficher l'identité de l'utilisateur reconnu.

C. Authentification : Ce cas d'utilisation permet à un utilisateur de s'authentifier (par exemple, avoir une autorisation d'accès), le système récupère les données du client (une image de son visage et de son empreinte digitale) et il vérifie si ces données correspondent à l'identité proclamée. Un scénario nominal se présente comme suit :

- Introduire les informations du client (le nom et le prénom)
- Acquisition des données du client (image du visage et de l'empreinte digitale)
- Prétraitement des images acquises
- Génération des modèles test avec l'extraction des paramètres (application de la DWT pour les images du visage et la méthode basée sur les minuties).
- Chargement du modèle proclamé à partir de la base de données à l'aide des informations acquises (le nom et le prénom) du client
- Comparer les modèles (les modèles chargés et les modèles test générés), si ils se correspondent alors l'utilisateur est authentifié sinon il s'agit d'un imposteur

D. Tests de performance : Ce cas d'utilisation permet à l'administrateur de faire des tests sur une base d'images donnée, en variant un ou plusieurs paramètres du système. Ceci, afin d'évaluer le système et de mesurer ces performances (TID, FAR et FRR). Un scénario nominal se présente comme suit :

- Introduire les paramètres de configuration
- Sélectionner la base de données (visages, empreintes digitales ou bien les deux)
- Chargement des modèles d'apprentissage et des modèles tests déjà enregistrés
- Calculer les mesures de performances (TID, FAR et FRR) pour la configuration choisie
- Afficher les résultats du calcul

V.2.3 Diagrammes de séquence détaillée :

Les diagrammes de séquences nous permettent de détailler et de décrire le fonctionnement du système avec ces différentes phases, et aussi de décrire comment les éléments du système interagissent entre eux et avec les acteurs.

A. Diagramme de séquences du cas d'utilisation « Apprentissage d'un client » :

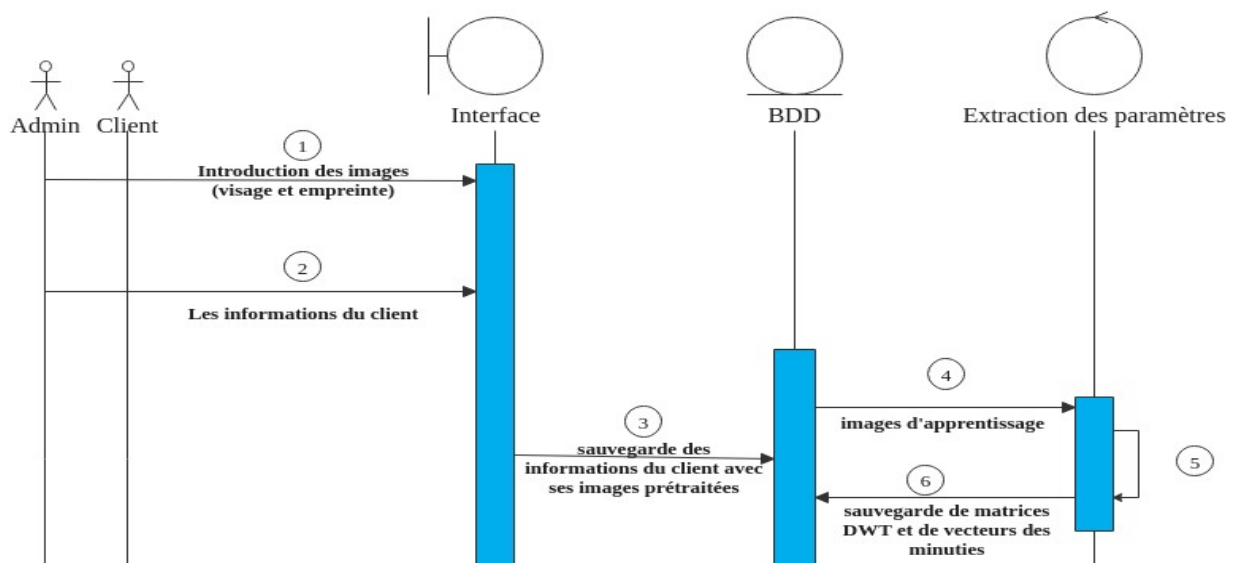


Figure V.2 Diagramme de séquence « Apprentissage »

Description du scénario d'apprentissage :

- Introduction d'un ensemble d'images du visage et de l'empreinte digitale du client au système.
- Introduction du nom et du prénom du client
- Le système enregistre les informations du client et l'ensemble de ses images dans la base de données
- Faire l'apprentissage avec N images de la base de données
- L'application de la DWT pour extraire les caractéristiques du visage et utiliser la méthode basé sur les minuties pour extraire le vecteur caractéristique des empreinte digitale
- Sauvegarder les matrices DWT résultantes et les vecteurs de minuties extraits

B. Diagramme de séquences du cas d'utilisation « Identification » :

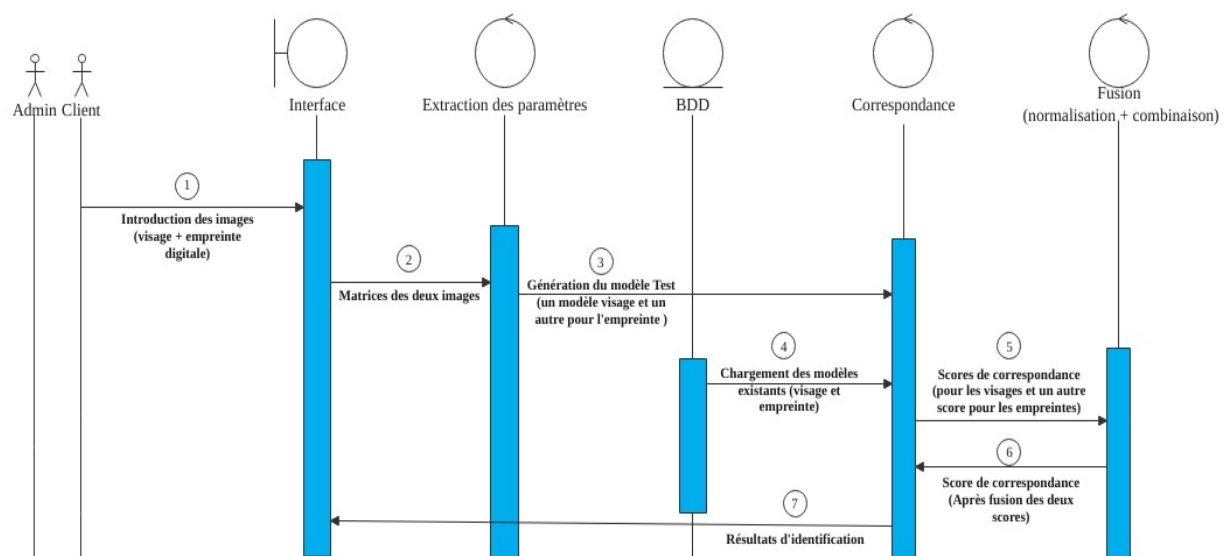


Figure V.3 Diagramme de séquence « Identification »

Description du scénario d'identification :

- Introduction des images du visage et de l'empreinte digitale de l'individu test
- Application des prétraitements nécessaires sur ces les images et les transformer en matrice 2D
- Extraction des caractéristiques et génération du modèle test en appliquant la DWT pour le visage et la méthode basée sur les minuties pour l'empreinte digitale
- Calculer le score de correspondance pour chaque modalité avec tout les modèles (de la même modalité) déjà enregistrés dans la base de données
- Fusion des scores de correspondance (le score du visage et le score empreinte) en leur appliquant une normalisation puis une combinaison
- Résultat de la fusion, un seul score pour les deux modalités
- Trier les scores résultants et afficher la personne la plus proche à l'individu test

C. Diagramme de séquences du cas d'utilisation « Authentification » :

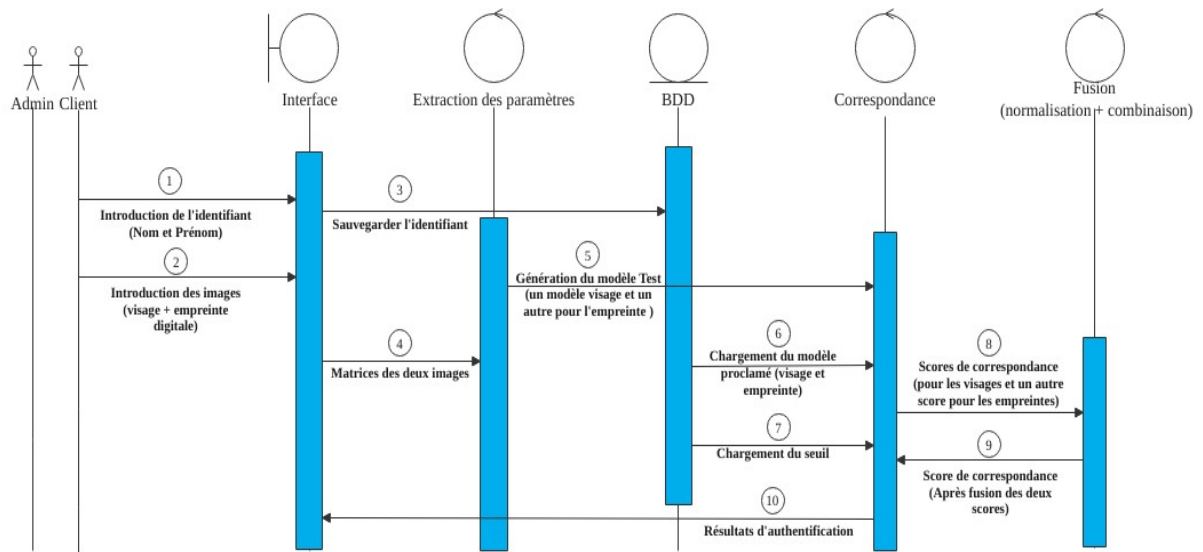


Figure V.4 Diagramme de séquence « Authentification »

Description du scénario d'authentification :

- Le client introduit son identifiant
- Introduction des images du visage et de l'empreinte digitale du client
- Le système sauvegarde l'identifiant et applique des prétraitements sur les images et les transforme en matrices 2D
- Génération du modèle Test en appliquant la DWT sur le visage et la méthode d'extraction de minuties basé sur les minuties pour l'empreinte digitale
- Chargement du modèle proclamé de la base de données à l'aide de l'identifiant du client et chargement du seuil de correspondance
- Calculer le score de correspondance pour chaque modalité avec le modèle proclamé (de la même modalité)
- Fusion des scores de correspondance (le score du visage et le score empreinte) en leur appliquant une normalisation puis une combinaison
- Résultat de la fusion, un seul score pour les deux modalités
- Comparer le score au seuil déjà chargé (si le score inférieur au seuil alors l'individu est un imposteur sinon c'est un client) et afficher le résultat de l'authentification

D. Diagramme de séquences du cas d'utilisation « Tests de performance » :

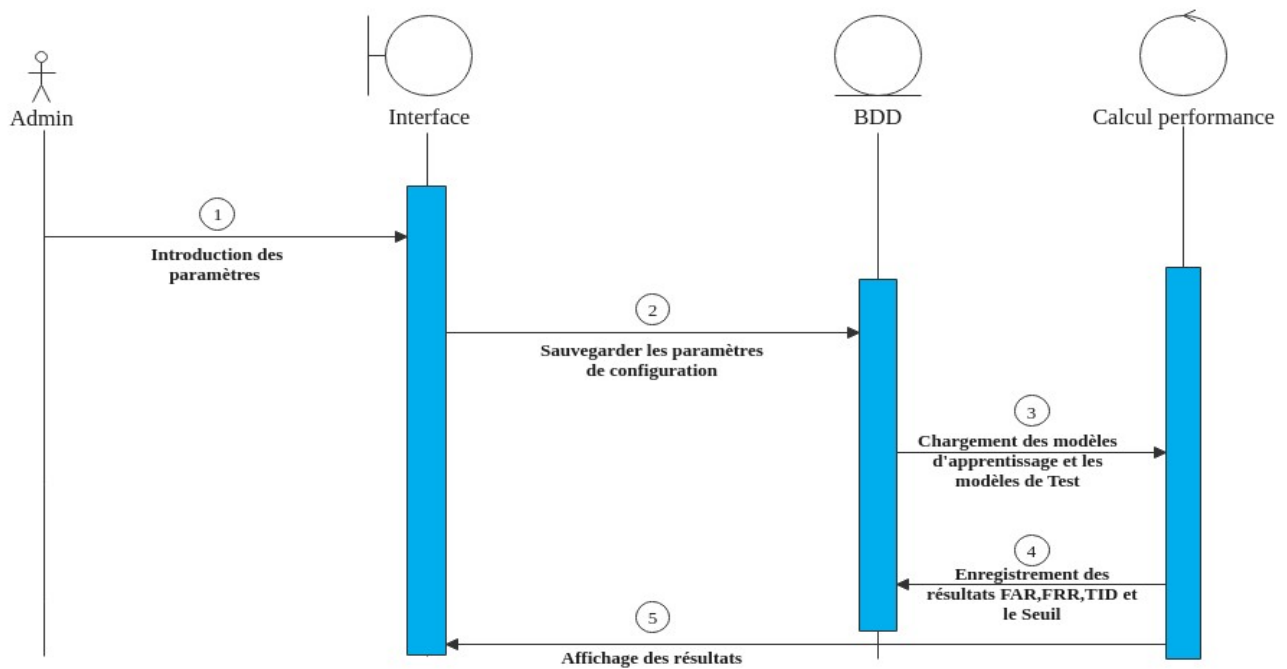


Figure V.5 Diagramme de séquence « Tests de performance»

Description du scénario de Tests de performance :

- Introduction des paramètres de configuration par l'administrateur
- La sélection de la base de données pour faire les tests
- Sauvegarder la configuration choisie pour le calcul
- Chargement des modèles d'apprentissage et de teste déjà enregistrés de la base de données choisie
- Enregistrement des résultats trouvés (FAR,FRR,TID et le Seuil)
- Affichage des résultats du test

V.2.4 Architecture et fonctionnement du système :

Les systèmes biométriques uni-modaux qui ont été développés intègrent globalement la même procédure de traitement, qui est composée de deux étapes : une étape d'apprentissage et une étape de reconnaissance. Le schéma suivant illustre le fonctionnement de notre système biométrique multimodale qui est une fusion de deux système uni-modal (système de reconnaissance de visages et celui des empreintes digitales).

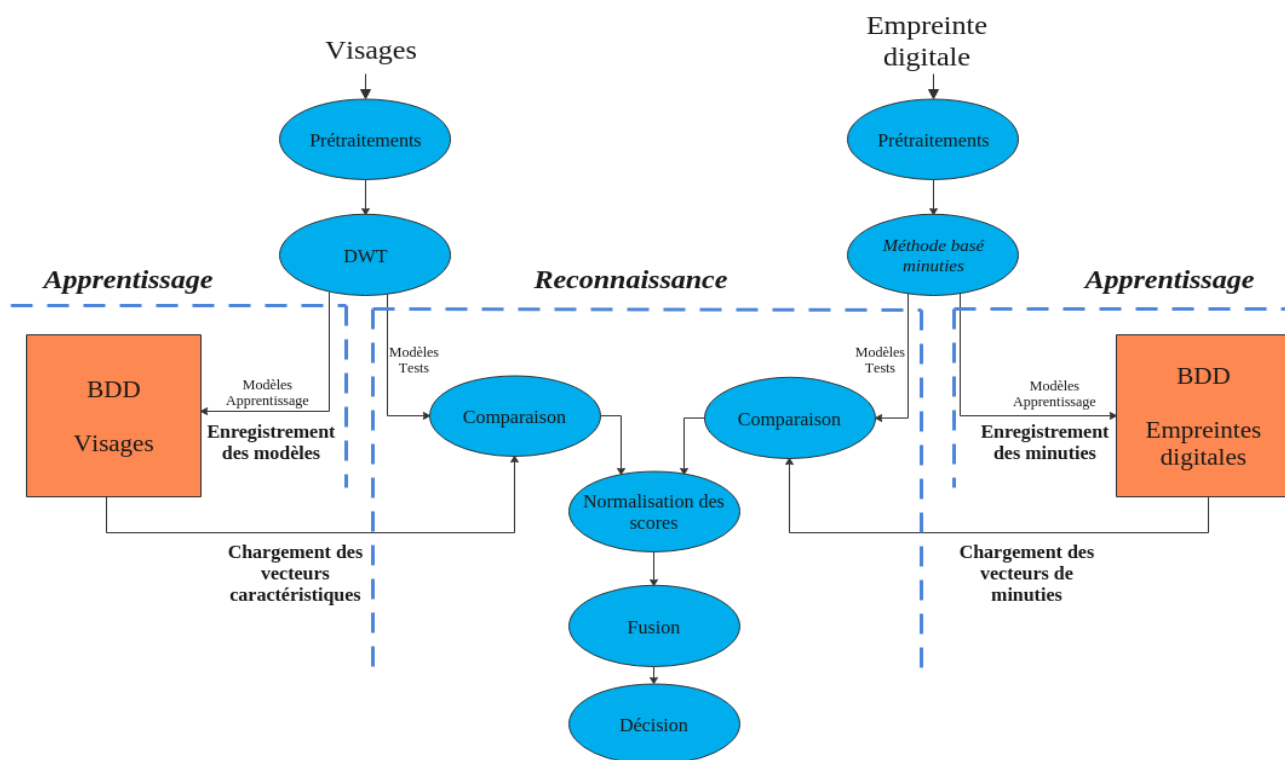


Figure V.6 Diagramme de fonctionnement du système

Nous détaillerons ci-dessous les modules qui constituent chaque unité, ainsi que les algorithmes utilisés, enfin le calcul des performances du système.

A. Phase d'apprentissage :

Le processus d'apprentissage de notre système avec les différents modules qui le composent sont illustrés et détaillés ci-dessous :

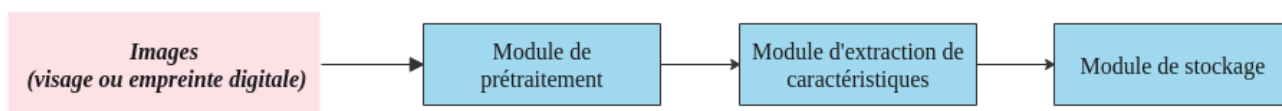


Figure V.7 Représentation modulaire de la phase « Apprentissage »

1. Module de prétraitement :

Le prétraitement est une étape nécessaire effectuée sur l'image acquise (originale) et elle consiste à éliminer le bruit et préparer l'image pour l'étape d'extraction.

La figure ci-dessous illustre les étapes à suivre pour le prétraitement des images du visage :

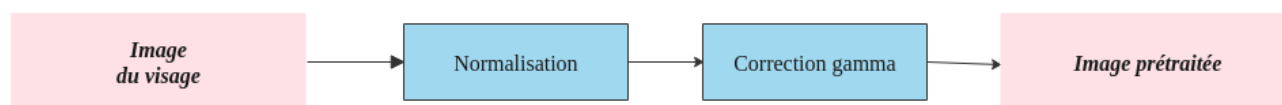


Figure V.8 Les étapes de prétraitement des images du visage

Pour le visage ce module se charge de redimensionner l'image à une taille homogène pour toutes les images (112*92) puis applique une correction gamma qui permet de réduire l'écart entre les zones sombres et claires du visage, et étaler la gamme totale de façon à rendre l'image plus ou moins linéaire visuellement.

La figure ci-dessous illustre les étapes à suivre pour le prétraitement des images de l'empreinte digitale pour l'approche basée sur les minuties :

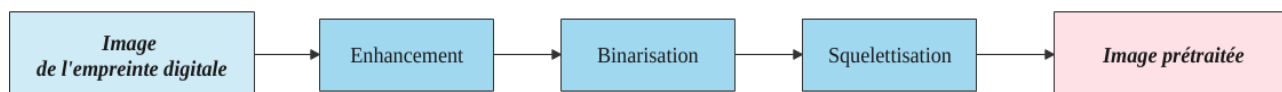


Figure V.9 Les étapes de prétraitement des images de l'empreinte digitale

2. Module d'extraction de caractéristiques :

L'extraction des paramètres est une phase importante dans un système de reconnaissance automatique. Elle permet d'extraire les caractéristiques pertinentes de chaque image de visage ou d'empreinte digitale.

L'approche utilisée pour l'extraction sur le visage *DWT(wavdec2)* :

Algorithme DWT

Une décomposition en ondelettes bidimensionnelle à un ou plusieurs niveau.

1. Découpe l'image en quatre blocs de pixels, les 3 derniers blocs concernent les détails de l'image (vertical, horizontal, diagonal), le premier bloc correspond à l'image détaillée.
2. Appliquer deux filtre (passe bas, passe haut) issue du choix d'ondelette à chaque bloc de pixel.
3. Les résultats sont le vecteur de décomposition C et la matrice comtable correspondante S qui sert à réduire les coefficients de la matrice C.

Figure V.10 Algorithme *DWT*

L'approche utilisée pour l'extraction sur l'empreinte digitale :

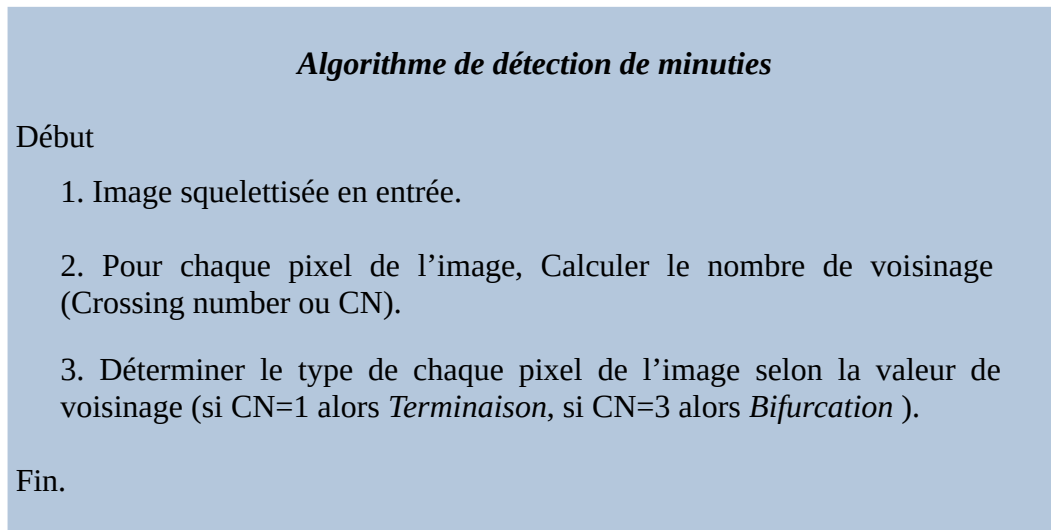


Figure V.11 Algorithme de détection de minuties

Pour l'empreinte digitale, l'algorithme de détection provoque la détection d'un nombre très important de minuties (quelques centaines) introduites pour la plupart lors des étapes de binarisation et de squelettisation (fausses minuties), afin de remédier à ce problème on effectue un post-traitement pour diminuer le nombre de minuties et d'éviter de trouver de fausses minuties :

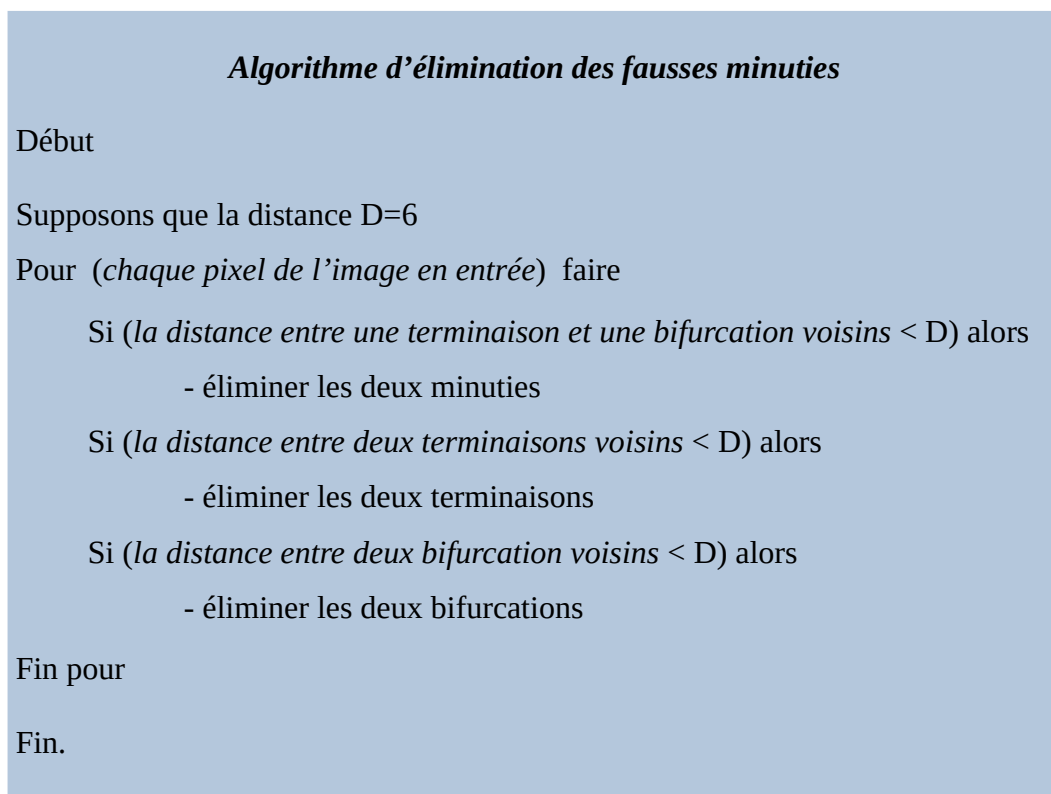


Figure V.12 Algorithme d'élimination des fausses minuties

3. Module de stockage :

Dans cette phase chaque client à un modèle unique (visage et empreinte digitale) avec ces informations personnelles, qui seront stockées dans une base de données multimodal (ou dans une base données pour chaque modalité) pour une utilisation ultérieure.

B. Phase de reconnaissance et la prise de décision :

1. Classification :

- **Les empreintes digitales :** La comparaison des empreintes digitales consiste à trouver une correspondance entre l'empreinte digitale à identifier et les empreintes déjà stockées dans la base de données. Cependant cette tâche n'est pas facile, notamment à cause de la variation intra-classe .

dans le cadre de notre application on a opté pour une approche basées sur les minuties ,cette méthode consiste à comparer les minuties extraites de deux empreintes dans un plan bidirectionnel et de retourner le nombre des paires de minuties "matchées" c.à.d. les paires possédant le même emplacement et la même orientation.

Considérons les deux ensembles de minuties suivants :

$$\begin{aligned} I &= \{m_1, m_2, \dots, m_m\} & m_i &= \{x_i, y_i, \theta_i\} & i &= 1..m. \\ T &= \{m'_1, m'_2, \dots, m'_n\} & m'_j &= \{x'_j, y'_j, \theta'_j\} & j &= 1..n. \end{aligned}$$

m et n représentent respectivement le nombre de minuties de I et T

Une minutie de T est considérée appariée avec une minutie de I si la distance *sd* (pour *spatial distance*) entre elles est inférieure ou égale à un seuil et la différence d'angle entre leurs orientations *dd* (pour *direction difference*) est inférieure ou égale aussi à une certaine seuil θ_0 :

$$sd(m'_j, m_i) = \sqrt{(x'_j - x_i)^2 + (y'_j - y_i)^2} \leq r_0 \quad (5.1)$$

$$dd(m'_j, m_i) = \min(|\theta'_j - \theta_i|, 360 - |\theta'_j - \theta_i|) \leq \theta_0 \quad (5.2)$$

plusieurs alignements sont effectués pour essayer d'avoir un nombre maximum de minuties assorties.

Deux empreintes sont considérées identiques si un certain nombre de minuties identiques est atteint. Soit une fonction *mm* (pour *munitiae matcher*) de comparaison de minuties :

$$mm(m_j, m_i) = \begin{cases} 1 & \text{Si } sd(m_j, m_i) \leq r_0 \text{ et } dd(m_j, m_i) \leq \theta_0 \\ 0 & \text{Sinon} \end{cases} \quad (5.3)$$

Le nombre de minuties matchées est donné par :

$$nb = \sum_{i=1}^m mm(m'_i, m_i) \quad (5.4)$$

Le score de similarité entre deux minuties est calculé grâce à la formule suivante :

$$S = \frac{\sqrt{(nb^2)}}{n * m} \quad (5.5)$$

où *nb* est le nombre de minuties matchées, *m* est le nombre de minuties de I et *n* est le nombre de minuties de T

- **Les visages :** Pour la reconnaissance du visage la méthode la plus courante et la plus simple pour la comparaison entre un modèle test et un modèle apprentissage utilise des classificateurs par mesure de dissimilarité ,c'est une distance qui est calculé entre deux images de visage.

Les métriques de distances les plus courante : « *Euclidienne* » , « *Mahalcov* » , « *Cosine* » , « *Ctb* » .

La distance calculé est ensuite normalisée dans la phase qui suit avant d'être fusionnée puis utilisée dans la prise de décision.

2. Normalisation des scores :

Dans notre système les résultats de la comparaison entre deux visages (distances) et ceux de la comparaison entre deux empreinte digitales (nombre de minuties matchées) ne sont pas homogène (dissimilarité pour les visages et similarité pour les empreintes digitales). Les méthodes de normalisation (Min-Max, Z-score,...voir Chapitre IV) permettent de ramener ces résultats (ou ces scores) dans un domaine commun, dans notre cas on ramène les scores (les distances) des images de visages dans un intervalle [0,1] en appliquant la normalisation Min-Max, ainsi pouvoir les fusionner avec ceux de l'empreinte digitale qui sont déjà dans cette intervalle.

3. Fusion des scores :

Cette étape consiste à fusionner un score obtenu à partir d'une comparaison entre deux images du visage et un score obtenu de la comparaison entre deux images d'empreinte digitale en appliquant l'une des règles de fusion (voir Chapitre IV) à savoir la règle « Somme », « Produit », « Maximum »...etc, cette étape nous permet d'avoir au final un seul score de correspondance pour les deux modalités.

4. Identification :

Cette étape consiste à chercher l'identité d'une personne parmi plusieurs sauvegardées au préalable (clients) dans une base de données.

On l'appelle « un parmi plusieurs ou 1-N », parce que le système doit accomplir une comparaison entre le modèle de l'individu test et tous les modèles sauvegardées dans la base de données. Le système peut soit prendre la « meilleure » ressemblance, soit donner tous les utilisateurs possibles qui conviennent et les ordonnées par ordre de similarité.

5. Authentification :

Cette méthode consiste à vérifier si l'identité de la personne testée est la même que celle proclamée par cette dernière. On l'appelle « un à un ou 1-1 », comme le système doit accomplir une comparaison entre le modèle de l'individu test et un seul modèle choisi enregistré dans la base de données.

C. Calcul des performances du système :

L'objectif ou l'intérêt de ce module est de calculer et d'optimiser les performances du système en jugeant l'efficacité des méthodes sur lesquelles il se base. Cela se fait en estimant un ensemble d'indicateurs, des indicateurs qui diffèrent selon le mode de reconnaissance :

1. Mode identification :

Pour ce mode de reconnaissance, mesurer les performances du système consiste à calculer le taux d'identification (TID), un taux qui représente la proportion du nombre de personnes identifiées sans erreurs. Le principe est : Pour toutes les personnes qui ont un modèle dans la base de données (client), l'administrateur effectue un test d'identification et compte le nombre de personnes bien identifiées. Puis, il divise ce dernier sur le nombre de personne testées et on multiplie tout par 100 pour obtenir un pourcentage.

$$TID = \frac{\text{Nombre de test ayant conduit à une identification correct}}{\text{Nombre total des tests}} \times 100$$

Ainsi, plus le TID est proche de 100, plus le système est performant (d'où la configuration est intéressante).

2. Mode authentification :

Pour ce mode de reconnaissance, mesurer les performances du système se fait en trois étapes qui consistent à calculer le seuil et les deux taux (taux de faux rejets (FRR) et le taux de fausse acceptation (FAR)).

Le seuil est donné comme suivant :

$$\text{Seuil} = (\max(\text{Scores_intra}) + \min(\text{Scores_extra})) / 2$$

Le taux de faux rejets (FRR) est le rapport entre le nombre de faux rejets et le nombre total de test clients. Le taux FRR est donné par l'algorithme suivant :

Algorithme de calcul du FRR

```
Début
  Pour i=1 à Nombre_test_intra
    si (Scores_intra(i) > Seuil)
      Faux_rejet = Faux_rejet + 1
    Finsi
  Fin pour
   $FRR = (Faux\_rejet / Nombre\_test\_intra) * 100$ 
Fin.
```

Figure V.13 Calcul du FRR

Le taux de fausse acceptation (FAR) est le rapport entre le nombre de fausse acceptation et le nombre total de test clients. Le taux FAR est donné par l'algorithme suivant :

Algorithme de calcul du FAR

```
Début
  Pour i=1 à Nombre_test_extra
    si (Scores_extra(i) <= Seuil)
      Fausse_acceptation = Fausse_acceptation + 1
    Finsi
  Fin pour
   $FRR = (Fausse\_acceptation / Nombre\_test\_extra) * 100$ 
Fin.
```

Figure V.14 Calcul du FAR

Remarques :

- Les tests extra consistent à comparer un modèle (de la base de données apprentissage) d'un individu avec d'autres modèles (de la base de données test) d'autres individus.
- Les tests intra consistent à comparer un modèle (de la base de données apprentissage) d'un individu avec d'autres modèles (de la base de données test) du même individu.
- Dans un système idéal $FRR + FAR = 0$, mais ce n'est pas le cas dans la pratique ; quand FRR augmente FAR diminue et vice versa. Par conséquent il faut trouver un compromis entre les deux taux.

V.3 Réalisation :

Dans cette partie et après avoir présenté les différentes conceptuelles de notre système, nous allons voir nos choix techniques (outils utilisés et langages de programmation). Enfin nous allons présenter les interfaces de notre système avec une description de chacune d'elles.

V.3.1 Outils de développement et de test :

Le choix des outils de programmation se fait par plusieurs facteurs : La puissance, La disponibilité de plusieurs fonctionnalités, etc. Dans le cadre de notre projet, nous avons utilisé Matlab.

A. MATLAB :

MATLAB est une abréviation de Matrix LABoratory. Écrit à l'origine, en Fortran, par Cleve Moler à la fin des années 1970, optimisé pour le traitement des matrices, d'où son nom. MATLAB est un environnement puissant, complet en plus de sa disponibilité est assurée sur plusieurs plateformes. C'est un environnement performant, ouvert et programmable qui permet de remarquables gains de productivité et de créativité. Matlab Contient également une d'interface graphique puissante. Ce qui prouve son utilisation dans différents domaines tels que l'éducation, la recherche et l'industrie.

Nous avons implémenté notre système de reconnaissance dans l'environnement de programmation MATLAB 2018 qui offre une grande simplicité de manipulation des images. Ce langage possède des avantages très intéressants pour les applications sur l'image tel que :

1. La portabilité de logiciel (la simplicité du processus de programmation).
2. L'utilisation des bases de données.
3. Facilité de manipulation des matrices ce qui est fort important dans le cas de notre application.
4. Un large choix de bibliothèques qui prennent en charge tous les outils mathématiques utiles au traitement et à l'analyse des images.

B. FingerPrint Matching :

Un open source pour le matching des empreintes basé sur les minuties , un outil développé par Vahid K. Alilou de 'University of Semnan' en Iran.

et partagé dans le MATLAB File_exchange, ce programme contient plusieurs fonctionnalités : l'extraction de minuties , appariement d'empreintes , calcul des indicateurs de performances etc ...

V.3.2 L'implémentation du système :

L'implémentation de notre système est composée de plusieurs bibliothèques de classes ; chacune contient plusieurs classes :

A. Présentation des interfaces de notre application :

Dans cette partie, on présentera les interfaces de notre application, ainsi que ses différentes fonctionnalités et leur correspondance avec les modules illustrés dans les sections précédentes.

1.Enrôlement :

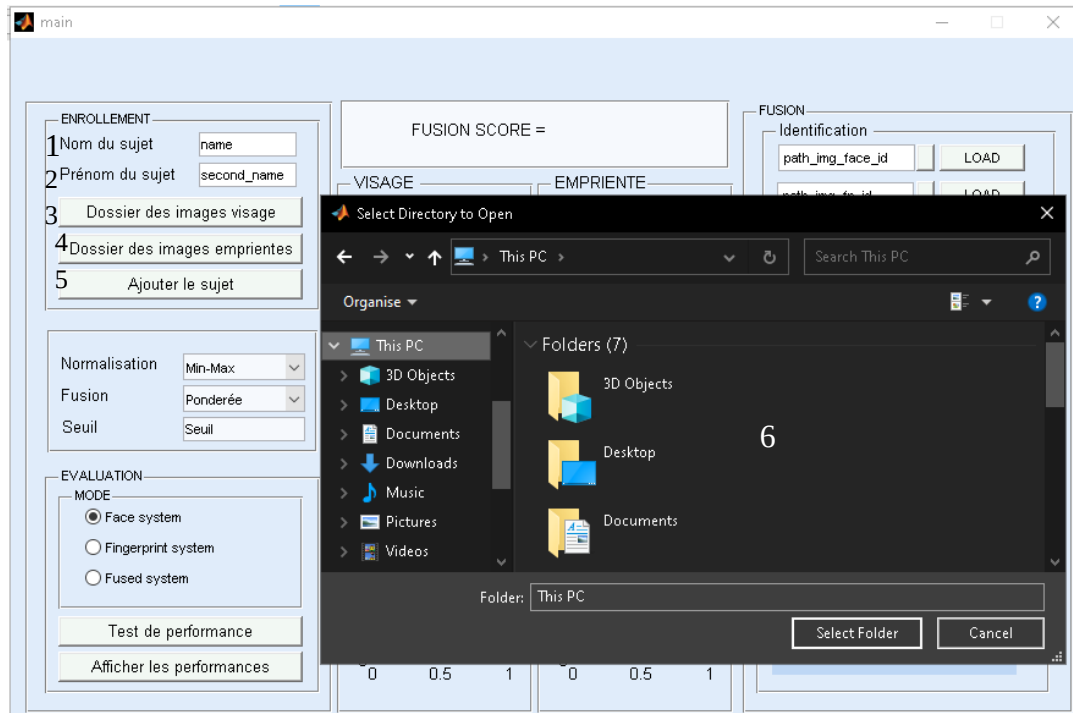


Figure V.15 Interface pour l'enrôlement d'un nouveau sujet

Explication de la figure :

- 1 Nom du sujet à ajouter
- 2 Prénom du sujet à ajouter
- 3 Spécifier le dossier des images du visage du sujet 4images
- 4 Spécifier le dossier des images des empreintes du sujet 4 images
- 5 Bouton pour ajouter le sujet dans la base de données
- 6 Boite de dialogue

L'administrateur doit d'abord rentrer le nom et le prénom du client à ajouter , puis spécifier le chemin des images du visage et ensuite de l'empreinte avant de cliquer sur le bouton « Ajouter le sujet ».

2. Evaluation du système :

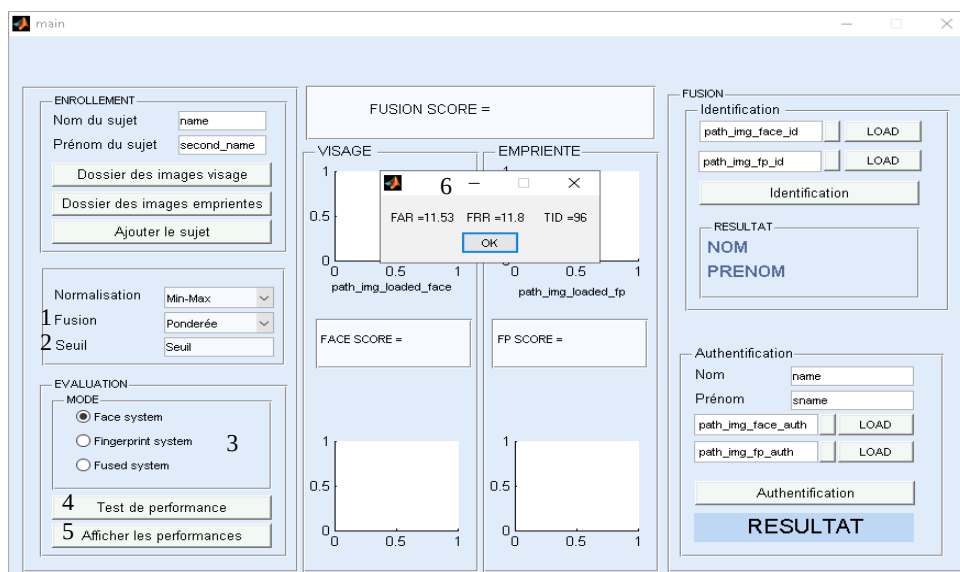


Figure V.16 Interface pour les tests de performances

Explication de la figure :

- 1 Choix du type de fusion
- 2 Choix du seuil , enter 0 et 1
- 3 Choix du mode système
- 4 Bouton pour les test de performances (calcul les performances avec le nouveau Seuil,type de Fusion)
- 5 Bouton pour afficher les indicateurs de performances FAR, FRR, TID
- 6 Affichage des indicateurs de performances

Le bouton « test de performances » lance des tests selon le mode et les paramètres d'évaluation choisi par l'administrateur .

Le bouton « afficher les performances » affiche les performances déjà enregistrées dans la base de donnée selon le mode d'évaluation choisi « face system » pour le visage , « fingerprint system » pour l'empreinte digitale et « fused system » pour la multi-modalité .

3. Authentification :

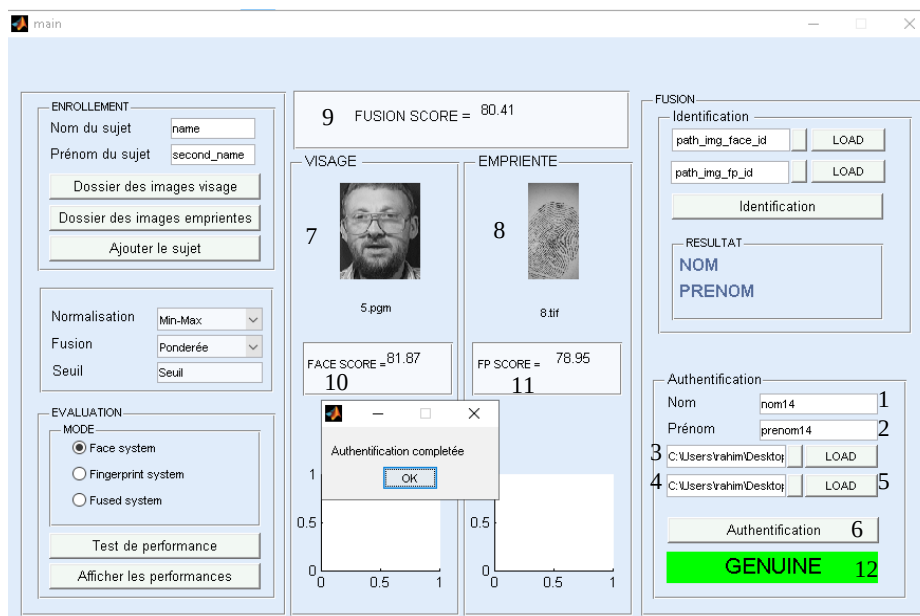


Figure V.17 interface graphique de l'authentification

Explication de la figure :

- 1 Nom du sujet à authentifier
- 2 Prénom du sujet à authentifier
- 3 Chemin de l'image visage du sujet à authentifier
- 4 Chemin de l'image empreinte du sujet à authentifier
- 5 Bouton pour charger les images du sujet à identifier
- 6 Bouton pour lancer l'authentification
- 7 L'image du visage en entrée
- 8 L'image de l'empreinte en entrée
- 9 Score en mode Fusion
- 10 Score du visage
- 11 Score de l'empreinte
- 12 Résultat de l'authentification (Genuine ou Imposteur)

Le client fournit son nom et prénom ainsi qu'une image du visage et une de l'empreinte puis lance l'authentification avec le bouton « Authentification ».Le système fait une vérification et retourne le résultat « Genuine » ou « Imposteur » dans le champ juste en dessous du bouton et les scores de chaque modalité en plus du score de la fusion.

4. Identification :

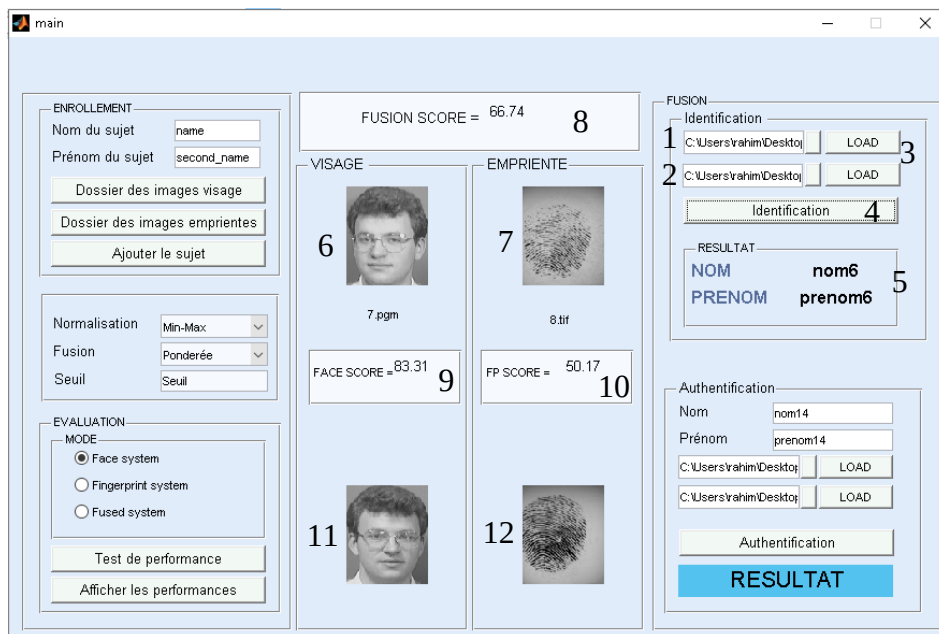


Figure V.18 interface pour l'identification

Explication de la figure :

- 1 Chemin de l'image du visage du sujet à identifier
- 2 Chemin de l'image empreinte du sujet à identifier
- 3 Bouton pour charger les images du sujet à identifier
- 4 Bouton pour lancer l'identification
- 5 Résultat de l'identification (Nom du sujet , Prénom du sujet)
- 6 L'image du visage en entrée
- 7 L'image de l'empreinte en entrée
- 8 Score en mode Fusion
- 9 Score du visage
- 10 Score de l'empreinte
- 11 L'image du visage identifiée
- 12 L'image de l'empreinte identifiée

Pour l'identification le client spécifie le chemin vers l'image du visage et un autre chemin vers celle de l'empreinte puis lance l'identification avec le bouton « Identification », le système parcourt la base de donnée en recherche de correspondance et retourne le nom et prénom du sujet identifié en plus des scores de chaque modalité et celui de la fusion.

V.4 Conclusion :

A travers ce chapitre, nous avons vu les étapes de la conception et la réalisation du système de reconnaissance multimodal (fusion du visage et de l'empreinte digitale), sa représentation modulaire et aussi les outils de développements utilisés pour l'implémenter, dans le chapitre suivant nous allons voir les tests et les résultats obtenus par ce système.

CHAPITRE VI

Résultats expérimentaux

VI.1 Introduction :

Pour évaluer l'efficacité des méthodes utilisées dans notre système, nous avons opté pour une validation sur des bases de données standard « ORL »[99] pour les visages et « FVC2002 DB2 »[100] pour les empreintes digitales. Les tests effectués concernent les deux modes de reconnaissance à savoir l'identification et la vérification. Dans un premier temps, nous allons exposer les tests effectués pour chaque sous-système ,le système de reconnaissance de visages et le système de reconnaissance des empreintes digitales, enfin nous allons exposer les tests et les résultats effectués sur notre système multimodal avec la fusion de ces deux derniers sous-systèmes.

Afin de comparer les résultats des nos deux sous-système (système de reconnaissance de visages et de reconnaissance des empreintes digitales) avec ceux de notre système multimodal , nous relevons les mesures suivantes :

- **Taux d'identification (TID)** : le pourcentage des personnes bien reconnues par le système .
- **Taux Faux rejet (FRR)** : le pourcentage de personnes censées être reconnues mais qui sont rejetées par le système.
- **Taux Faux accepter (FAR)** : le pourcentage de personnes censées ne pas être reconnues mais qui sont tout de même acceptées par le système.

VI.2 Le Sous-système de reconnaissance de visages :

VI.2.1 La base de données ORL :

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

Les données utilisées pour réaliser les tests sur notre sous-système proviennent de la base ORL , cette base de donnée est constituée de 40 individus, chaque individu possède 10 poses, donc la base contient 400 images. Les poses ont étaient prises sur des intervalles de temps différents pouvant aller jusqu'à trois mois. L'extraction des visages à partir des images a été faite manuellement. Nous présenterons dans ce qui suit les figures montrant les spécificités de la base de donnée de référence ORL

Les images ont été collectées à des dates différentes, avec de différentes conditions d'éclairage, de différentes expressions faciales (expression neutre, sourire et yeux fermés) et des occultations partielles par les lunettes...etc



Figure VI.1 Base de données ORL

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



Figure VI.2 Exemple de changements d'orientations du visage

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



Figure VI.3 Exemple de changements d'éclairage

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

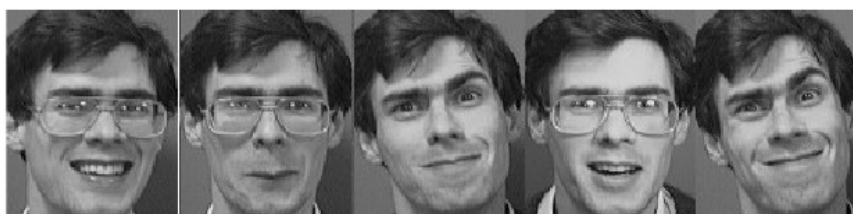


Figure VI.4 Exemple de changements des expressions faciales

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



Figure VI.5 Exemple de port de lunettes

Enfin la base de données ORL prends aussi en considération certaines particularités comme porter une barbe ou changer de coiffure, et elle comprend des individus de différents ages, sexe et couleurs de peaux.

VI.2.2 Évaluation des performances :

Dans cette section nous allons présenter les performances du sous-système dans les deux modes (identification & authentification).

Le système a été soumis à une série de tests avec comme approche d'extraction des caractéristiques la DWT(wavdec2) où on a utiliser la décomposition à 3 niveaux après avoir constater qu'elle donne de meilleurs résultats dans les travaux précédents. Et enfin on a utiliser les distances pour la classification de ces caractéristiques.

VI.2.2.1 Résultats des tests :

Pour l'évaluation de ce sous-système on utiliser différentes type d'ondelette pour l'extraction de caractéristiques et plusieurs métrique de distances pour le calcul de dissimilarité afin de pouvoir comparer les résultat de chaque combinaison et prendre celle qui donne de meilleurs résultat pour notre système multimodal. Enfin pour faire ces tests on a diviser la base de données ORL en deux sections comme suit :

- 200 images pour l'apprentissage , on prend les 5 premières images de chaque individu de la base de données.
- 200 images pour les tests, on prend les 5 dernières images de chaque individu de la base de données.

A. Mode authentification (FAR & FRR) :

1. FAR (%) :

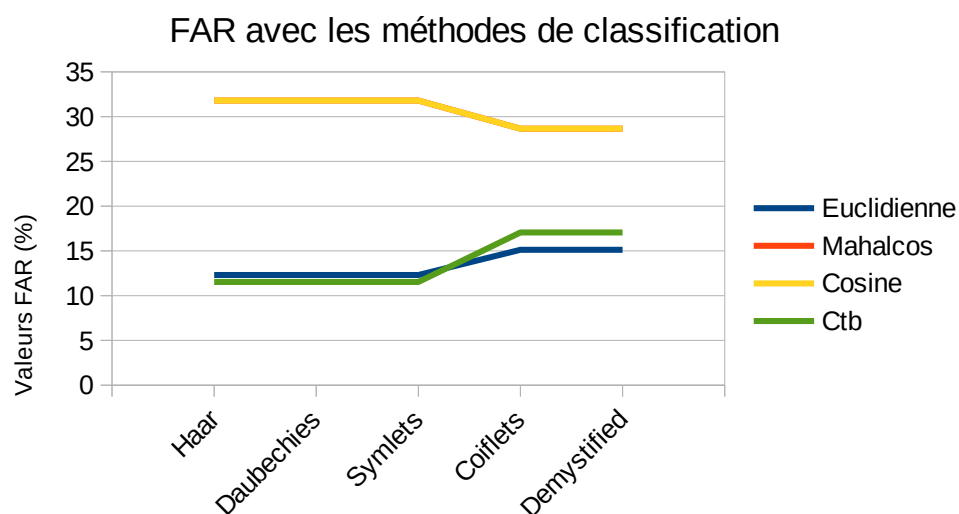


Figure VI.6 FAR en fonction du type d'ondelette et de la distance

	Haar	Daubechies	Symlets	Coiflets	Demystified
Euc	12,3	12,3	12,3	15,12	15,12
Mahalcos	31,79	31,79	31,79	28,65	28,65
Cosine	31,79	31,79	31,79	28,65	28,65
Ctb	11,53	11,53	11,53	17,05	17,05

Tableau VI.1 FAR en fonction du type d'ondelette et de la distance

A travers les résultats des tests voir (tableau VI.1) et la figure ci-dessus on remarque qu'on atteint le Taux de fausse acceptation (FAR) le plus bas avec la distance « Ctb » et les ondelettes de « Haar », « Daubechies » et « Symlets ».

2. FRR (%) :

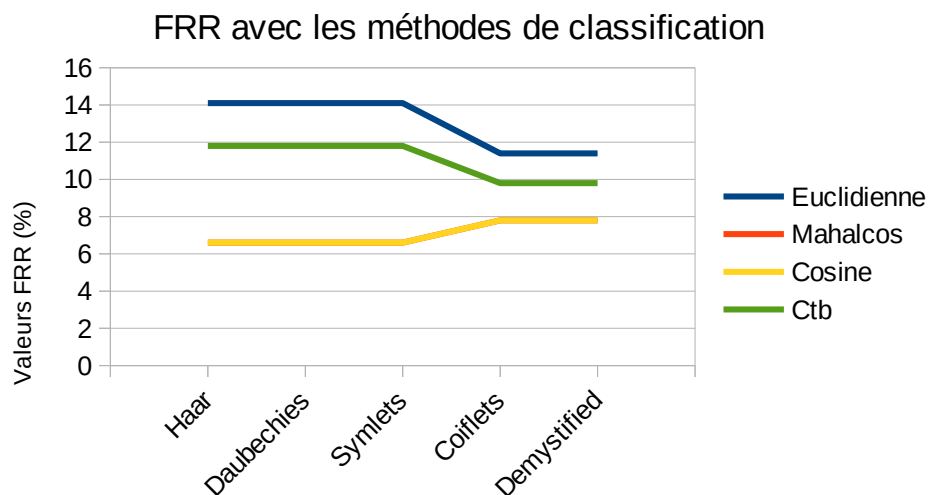


Figure VI.7 FRR en fonction du type d'ondelette et de la distance

	Haar	Daubechies	Symlets	Coiflets	Demystified
Euc	14,1	14,1	14,1	11,4	11,4
Mahalcos	6,6	6,6	6,6	7,8	7,8
Cosine	6,6	6,6	6,6	7,8	7,8
Ctb	11,8	11,8	11,8	9,8	9,8

Tableau VI.2 FRR en fonction du type d'ondelette et de la distance

en ce qui concerne le FRR on remarque dans la figure et le tableau ci-dessus qu'on atteint le Taux de faux rejet (FRR) le plus bas avec les distances « Cosine » et « Mahalcos » et les ondelettes de « Haar », « Daubechies » et « Symlets ».

Dans un système biométrique de reconnaissance, on préfère un FAR plus bas qu'un FRR, en d'autres termes il vaut mieux rejeter un client qu'accepter un imposteur. Ainsi, pour notre sous-système de reconnaissance de visages final, nous avons opté sur l'utilisation des ondelettes de « Haar » et avec comme distance, la norme « Ctb » pour le mode « Authentification », vu que le système converge à **11,53** et **11.80** pour le **FAR** et **FRR** respectivement.

B. Mode identification (TID) :

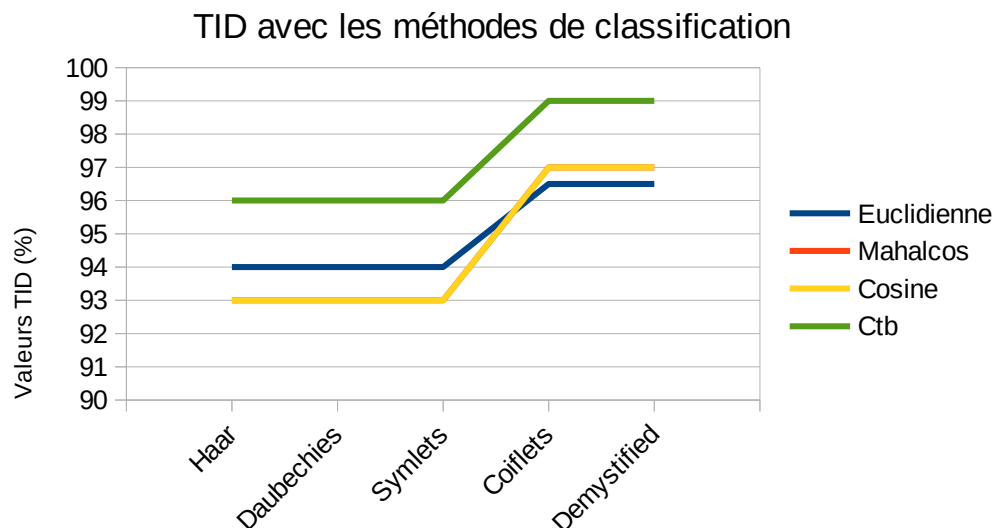


Figure VI.8 TID en fonction du type d'ondelette et de la distance

	Haar	Daubechies	Symlets	Coiflets	Demystified
Euc	94	94	94	96,5	96,5
Mahalcos	93	93	93	97	97
Cosine	93	93	93	97	97
Ctb	96	96	96	99	99

Tableau VI.3 TID en fonction du type d'ondelette et de la distance

Dans le mode identification on voit sur les figures (Tableau VI.3 et Figure VI.8) ci-dessus que notre système atteint le meilleur taux d'identification (TID) en ondelettes « Coiflets », « Demystified » et la distance «Ctb» .

C. Synthèse pour le sous-système de reconnaissance du visage :

Après plusieurs tests en variant le type d'ondelette et les distances les meilleurs résultats obtenus sont : **FAR=11.53** , **FRR=11.8** pour le mode authentification avec les paramètres suivants type d'ondelette « Haar » et « Ctb » comme distance et un **TID = 99** pour le mode identification avec « Coiflets » comme ondelette et « Ctb » comme distance.

Les résultats reste assez satisfaisant avec un **TID** proche de 100 pour l'identification et un **FAR** et **FRR** qui convergent pour le mode authentification .

VI.3 Le Sous-système de reconnaissance des empreintes digitales :

VI.3.1 La base de données FVC2002 DB2 :

La base DB2 est une base de données d'empreintes digitales utilisée dans la compétition Fingerprint Verification Competition (FVC2002). Elle est composée de 100 personnes (8 images par personne). Les images sont de résolution 560×296 pixels. La figure 8 illustre un exemple des images de cette base.



Figure VI.9 Exemple d'empreintes digitales de la base FVC2002 DB2

VI.3.2 Evaluation du sous-système :

Dans cette section nous allons présenter les performances du sous-système dans ses deux modes (identification & authentification).

Le système a été soumis à une série de tests en ses deux modes (identification et vérification) avec l'approche d'extraction de minuties comme paramètres, ceci avec l'utilisation de l'appareillement basé sur les minuties pour l'étape de la classification.

VI.2.2.1 Résultats des tests :

Afin de faire des tests sur ce sous-système, nous avons divisé la base de données FVC2002 DB2 comme suit :

- 160 images pour l'apprentissage , on prend les 4 premières images des 40 premières personnes de la base de données.
- 160 images pour les tests, on prend les 4 dernières images des 40 premières personnes de la base de données.

A. Mode authentification (FAR & FRR) : Valeur du FAR et FRR en variant le Seuil

SEUIL	FAR (%)	FRR (%)
0.40	0.12	14.06
0.35	1.4	9.06
0.30	7.5	5
0.325	3.33	7.03
0.312	5.38	6.4
0.3035	5.78	6.66

Tableau VI.4 FAR et FRR du sous-système de reconnaissance des empreintes digitales

A partir de ce tableau (VI.4) on constate que le système converge vers un FAR proche du FRR à mesure que le seuil converge vers 0.3035.

B. Mode identification (TID) :

	TID (%)
Système basé minuties	93,125

Tableau VI.5 TID du sous-système de reconnaissance des empreintes digitales

Dans ce mode on voit que notre système atteint le meilleur taux d'identification (TID) avec 93,125 %

C. Synthèse pour le sous-système de reconnaissance des empreintes digitales :

Après plusieurs tests en variant le seuil, les meilleurs résultats obtenus sont : **FAR= 5,78** , **FRR= 6,66** et un **TID = 93,125** avec un seuil qui égale à 0,3035.

Les résultats reste assez satisfaisant avec un **TID** proche de 100 pour l'identification et un **FAR** et **FRR** qui convergent pour le mode authentification.

VI.4 Le Système de reconnaissance multimodal :

VI.4.1 Évaluation du système :

Dans cette section nous allons présenter les performances de notre système multimodal dans ses deux modes (identification & authentification).

Le système a été soumis à une série de tests en ses deux modes (identification et vérification) avec une approches de normalisation des scores « Min-Max », et plusieurs approches de fusion comme : La règle somme , produit, maximum, minimum et enfin la règle somme pondérée.

VI.2.2.1 Résultats des tests :

Afin de faire des tests sur notre système, nous avons élaboré à partir des bases de données ORL et FVC2002 DB2 un corpus de 640 images (2 modalités × 40 personnes × 8 images pour chaque personnes). Pour chaque modalité on a pris 160 images d'apprentissage (40 individus avec 4 photos par individus), 160 images de test (40 individus avec 4 photos par individus).

A. Mode authentification (FAR & FRR) :

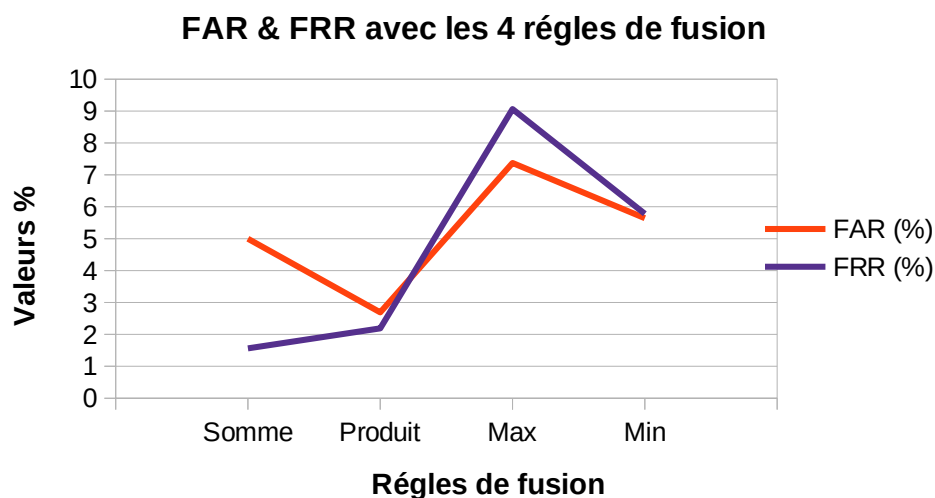


Figure VI.10 Variation du FAR (%) et du FRR (%) en fonction des règles de fusion.

	Somme	Produit	Maximum	Minimum
FAR	5	2,6923	7,3718	5,64103
FRR	1,5625	2,1875	9,0625	5,78125

Tableau VI.6 Résultats du FAR (%) et du FRR (%) de chaque règle de fusion

A travers les résultats des tests voir (tableau VI.6) et la figure ci-dessus on remarque qu'on atteint le Taux de fausse acceptation (FAR) le plus bas avec la règle de fusion « Produit » et le Taux de faux rejet (FRR) le plus bas avec la règle de fusion « somme » juste devant la règle « produit », il est à savoir que dans un système biométrique de reconnaissance plus le FAR est proche de zéro plus les performances est bonnes et vice versa.

B. Mode identification (TID) :

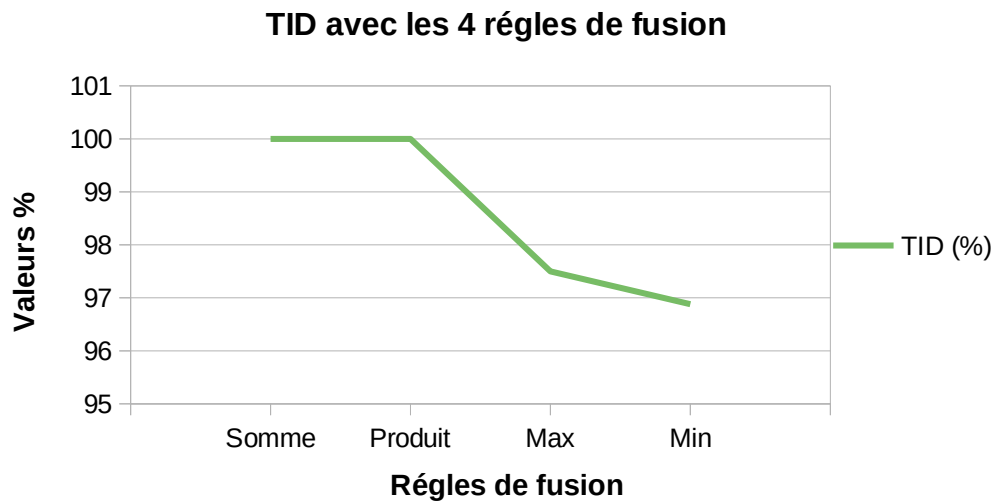


Figure VI.11 Variation du TID (%) en fonction des règles de fusion.

	Somme	Produit	Maximum	Minimum
TID	100	100	97,50	96,8750

Tableau VI.7 Résultats du TID (%) de chaque règle de fusion

Ces courbes et ce tableau nous montrent que les performances avec l'utilisation des règles de fusion « Produit » et « Somme » sont donne un meilleur TID que les règles Maximum et Minimum.

C. Synthèse pour le système de reconnaissance multimodal :

Après plusieurs tests en variant la règle de fusion (Somme, produit,...etc), les meilleurs résultats obtenus sont : FAR=2,6923 FRR=2,1875 TID = 100 avec la règle de fusion « Produit ».

Les résultats reste assez satisfaisant avec un TID de 100 % pour l'identification et un FAR et FRR qui convergent pour le mode authentification.

VI.5 Conclusion :

Tout au long de ce chapitre, nous avons effectué des tests expérimentaux sur des paramètres constituant notre système et ainsi trouver la meilleure combinaison (ondelette,distance) pour le visage dans ses deux modes de reconnaissance (identification et authentification), le seuil qui donne le meilleur compromis entre le FAR et FRR pour l'empreinte et enfin le meilleur type de fusion pour le système multimodal, en l'occurrence la fusion par règle produit.

Conclusion générale

Dans ce mémoire nous nous sommes intéressés au système biométrique multimodal avec la fusion des deux modalités : visage et empreinte digitale. Celui-ci consiste à vérifier ou à identifier un individu à partir de son image faciale et de son empreinte digitale. Ce genre de systèmes sont utilisés généralement et principalement pour des raisons de sécurité. Notre projet de fin d'étude s'inscrit dans ce contexte.

En effet, nous avons conçu et réalisé notre système de reconnaissance multimodal dans ses deux modes (identification et vérification) en utilisant la transformée en ondelette discrète DWT qui repose sur une décomposition en ondelettes bidimensionnelle à trois niveau pour l'extraction des caractéristiques du visage, et la méthode basée sur l'extraction des minuties pour l'empreinte digitale.

Pour la classification, après avoir présenté un état de l'art sur la multimodalité et les différentes méthodes de fusion, nous avons opté sur l'utilisation d'une classification basé sur les scores. Avant de fusionner ou de combiner les scores de correspondance donnés par les deux sous-systèmes de reconnaissance de visage et celui de l'empreinte, ces même scores doivent être normalisés pour les ramener dans un domaine commun qui permet leur fusion. Pour notre cas nous avons utilisé la normalisation « Min-Max » pour normaliser les scores du visage afin les ramener dans un même intervalle que les empreintes digitales à savoir l'intervalle $[0,1]$.

Dans notre système de reconnaissance, nous avons effectué nos tests dans le but d'améliorer et d'évaluer les performances de notre système dans ces deux modes (identification et vérification) en concluant la TID, FRR et FAR. A cet effet, les tests expérimentaux effectués sur les bases de données ORL pour le sous-système de reconnaissance de visages, sur FVC2002 DB2 pour le sous-système des empreintes digitales et sur les deux bases de données pour le système multimodal, ces tests nous ont permis de constater que la multimodalité donne de meilleurs résultats que l'unimodalité ainsi que dans la multimodalité la fusion avec la règle « Produit » donne des résultats meilleurs que les autres règles utilisées.

A travers ce projet nous avons assimilé plusieurs informations concernant l'architectures des systèmes de reconnaissance biométrique et leur fonctionnement, on a également élargi nos connaissances relatives à l'outil Matlab.

Par ailleurs, et dans le but d'améliorer notre travail nous avons comme perspectives :

- De faire plusieurs tests en utilisant d'autres bases de données virtuelles ou réelles.
- Utiliser d'autres prétraitements dans le but d'améliorer la qualité des images.
- Tester les fusions à d'autres niveaux que le score.
- Utiliser plusieurs méthodes de normalisation.
- Faire varier les seuils pour essayer d'obtenir de meilleurs résultats.

Références :

Références bibliographiques :

- [2] : FRÉDÉRIC MASSICOTTE, LA BIOMÉTRIE, SA FIABILITÉ ET SES IMPACTS SUR LA PRATIQUE DE LA DÉMOCRATIE LIBÉRALE ; le lien : <http://archipel.uqam.ca/791/1/M10088.pdf>
- [3] : Clémence Carron, « Les vrais jumeaux ont-ils les mêmes empreintes digitales ? », *Pour la science*, ° 396,.
- [4] : P. Meenen, R. Adhami, "Fingerprinting for Security", IEEE potentials, vol. 20, n°3, p. 33-38, 2001.
- [5] : G.Nedjma S.Karima, Développement d'un système biométrique pour la reconnaissance de visages, basé sur les ondelettes et les réseaux de neurones, Mémoire de Fin d'Etudes De MASTER ACADEMIQUE, UNIVERSITE MOULOUD MAMMERI DE TIZI-OUZOU
- [6] : Bruce E. Koenig "Spectrographic voice identification: A forensic survey", FBI, Engineering section, Technical Service Division, 1986.
- [10] : M. Hashiyada. Development of biometric dna ink for authentication security. Tohoku Journal of Experimental Medicine, pages 109–117, 2004.
- [11] : K. Phua, J. Chen, T. H. Dat, and L. Shue. Heart sound as a biometric. Pattern Recognition, 41 :906–919, 2008.
- [12] Mémoire online, lien : http://www.memoireonline.com/02/13/6979/m_Reconnaissance-de-visages-par-Analyse-Discriminante-LineaireLDA-4.html
- [14] : L. Hong, A. Jain, S. Pankanti, « Can Multibiometrics Improve Performance ? », Proceedings AutoID'99, Summit, NJ, p.59-64, Oct 1999.
- [15] : J. Kittler, M. Hatef, R. Duin, J. Matas, « On Combining Classifiers », IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 20, n°3, p. 226-239, 1998.
- [16] : A. Ross, K. Nandakumar, A.K. Jain. Handbook of Multibiometrics. 1sted. International series on biometrics, 2006
- [17] : M. Mohamad El Abed , Evaluation de systèmes biométriques, lien : <https://www.greyc.fr/sites/default/files/secretariat/theses-soutenues-2011/These-Mohamad-ElAbed-2011.pdf>
- [20] : Anil K. Jain, P. Flynn, A. Ross, "Handbook of biometrics", Springer, 2007.
- [21] : Pierre Buyssens, Fusion de différents modes de capture pour la reconnaissance du visage appliquée aux e-transactions (Thèse de Doctorat), le lien : <https://hal.archives-ouvertes.fr/tel-01079134/document>
- [22] : BENCHENNANE Ibtissam, Etude et mise au point d'un procédé biométrique multimodale pour la reconnaissance des individus (Thèse de Doctorat), le lien : www.univ-usto.dz/images/coursenligne/These_BENCHENNANE_I.pdf
- [24] : R. Jain and A. Ross. Multibiometric systems. Communications of the ACM, 47:34–40, 2004.

- [25] : NOUAR Larbi, Identification Biométrique par Fusion Multimodale, UNIVERSITE DJILLALI LIABES DE SIDI BEL ABBES lien:
http://rdoc.univ-sba.dz/bitstream/123456789/2418/1/D_ELN_NOUAR_Larbi.pdf
- [26] : NICOLAS MORIZET, Reconnaissance Biométrique par Fusion Multimodale du Visage et de l'Iris (Thèse de Doctorat), lien : <https://tel.archives-ouvertes.fr/pastel-00005811/document>
- [27] : R. Beveridge, M. Kirby, Biometrics and Face Recognition, IS&T Colloquium, p.25, 2005.
- [28] : BELLILI Manel ,FARSI Meriem, Application de la DCT modifiée et GMM Orthogonale pour la Vérification du visage, ECOLE NATIONALE SUPERIEURE D'INFORMATIQUE
- [29] : Mohamed YOUNSI, Younes MEDJTOUH, Développement d'un système biométrique pour la reconnaissance de visages, basé sur les ondelettes, Mémoire de Fin d'Etudes De MASTER ACADEMIQUE, UNIVERSITE MOULOUD MAMMERI DE TIZI-OUZOU
- [31] : MEBARKA BELAHCENE, Système de Reconnaissance de Visage ; le lien :
[https://scholar.google.fr/citations?user=sC2F4DYAAAAJ&hl=fr\\$](https://scholar.google.fr/citations?user=sC2F4DYAAAAJ&hl=fr$)
- [32] : M. A. Turk and A. P. Pentland, "Face recognition using Eigenfaces", IEEE Conference on Computer Vision and Pattern Recognition, p. 586-590, Hawaii, 1992.
- [33] : M. Kirby, L. Sirovich, "Application of the karhunen-loeve procedure for the characterization of human faces", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 12, n o . 1, p. 103-108, 1990
- [34] : A. M. Martínez, A. C. Kak, "PCA versus LDA". IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 23, n o . 2, p. 228-233, 2001.
- [35] : D. J. Kriegman, J. P. Hespanha, P. N. Belhumeur, "Eigenfaces vs. Fisherfaces : Recognition using class-specific linear projection", European Conference on Computer Vision, p. 43-58, 1996.
- [36] : G. Bahtiyar, "Holistic Face Recognition by Dimension Reduction", Master's thesis, Department of Electrical and Electronics Engineering, Graduate School of Natural and Applied Sciences of the Middle East Technical University, 2003.
- [37] : M. S. Bartlett, J. R. Movellan, T. J. Sejnowski, "Face recognition by independent component analysis", Transactions on Neural Networks, 2002.
- [38] : I. Buciu, I. Pitas, "Application of non-negative and local non negative matrix factorization to facial expression recognition", International Conference on Pattern Recognition, p. 288-291, 2004.
- [39] : Y. Wang, Y. Jia, C. Hu, M. Turk, "Non-negative matrix factorization framework for face recognition", International Journal of Pattern Recognition and Artificial Intelligence, vol.19, n o . 4, p. 495-511, 2005.
- [40] : M. Visani, C. Garcia, J. M. Jolion, "Normalized radial basis function networks and bilinear discriminant analysis for face recognition", IEEE Conference on Advanced Video and Signal Based Surveillance, p. 342-347, 2005.
- [41] : H. Cevikalp, M. Neamtu, M. Wilkes, A. Barkana, "Discriminative common vectors for face recognition", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 27, n o . 1, p. 4-13, 2005.
- [42] : B. Schölkopf, A. Smola, K.-R. Müller, "Nonlinear component analysis as a kernel eigenvalue problem", Neural Computation, vol. 10, n o . 5, p. 1299-1319, 1998.

- [43] : S. Mika, G. Ratsch, J. Weston, B. Schölkopf, K.-R. Müller. "Fisher Discriminant Analysis With Kernels", Neural Networks for Signal Processing IX, p. 41-48, 1999.
- [44] : H. Kim, H. Park, H. Zha, "Distance preserving dimension reduction for manifold learning", International Conference on Data Mining, 2007.
- [45] : S. Biswas, K. W. Bowyer, Patrick J. Flynn, "Multidimensional scaling for matching low-resolution facial images", Biometrics : Theory, Applications and Systems, 2010.
- [46] : M. N. Teli, "Dimensionality reduction using neural networks", Technical report, 02 2008.
- [47] : M. K. Fleming, G. W. Cottrell, "Categorization of faces using unsupervised feature extraction", IEEE International Joint Conference on Neural Networks, vol. 2, p. 65-70, San Diego, 1990.
- [48] : M. H. Yang, "Face recognition using extended isomap", International Conference on Image Processing, p. 117-120, 2002.
- [49] : G. Hagen, T. Smith, A. Banasuk, R.R. Coifman, I. Mezic, "Validation of low-dimensional models using diffusion maps and harmonic averaging", IEEE Conference on Decision and Control, 2007.
- [50] : Muzhir Shaban Al-Ani¹ and Alaa Sulaiman Al-waisy², FACE RECOGNITION A PROACH BASED ON WAVELET - CURVELET TECHNIQUE, Department of Computer Science, College of Computer, Al-Anbar University, Iraq.
- [51] : Mohamed ADJOUT et Abdelhak BENAÏSSA, «Fusion de la DCT-PCA et la DCT-LDA Appliquée à la reconnaissance de visages ».Institut National de formation en Informatique (I.N.I), Alger, 2007.
- [52] : Toufik AMELLAL, Kamel BENAKLI, « Système de reconnaissance de visage basé sur les GMM ». Institut National de formation en Informatique (I.N.I), Alger, 2007.
- [54] : V. Perlibakas. Face recognition using principal component analysis and log-gabor filters. CoRR, abs/cs/0605025, 2006.
- [55] : A. Pentland, B. Moghaddam, and T. Starner. View-based and modular eigenspaces for face recognition. In IEEE Conference on Computer Vision and Pattern Recognition, 1994.
- [56] : P. Meenen, R. Adhami, "Fingerprinting for Security", IEEE potentials, vol. 20, n°3, p.33-38, 2001.
- [58] : Ben Hamed Amina, Medjadji Omar, Mémoire de fin d'études, Reconnaissance des Empreintes Digitales, Université Abou Berk Belkaid de TLEMCEM
- [59] : L.Saliha, H.Lila, Mémoire de fin d'études, Conception et réalisation d'une authentification par FingerHashing sur carte à puce, Ecole nationale Supérieure d'Informatique (ESI) Oued-Smar, Alger
- [60] : Francis Galton, Fingerprint, McMillan, London, 1892.
- [62] : Maltoni Davide, Dario Maio, Anil K. Jain, Salil Prabhakar, Handbook of fingerprint recognition, Springer, New York, 2003.
- [65] : B. Rima, B. Houada, Mémoire de fin d'étude, Reconnaissance d'empreintes digitales en utilisant les moments de Hu, Université Mouloud Mammeri de TIZI OUZOU
- [66] : Souheila Benkhaira, Mémoire de fin d'études, Systèmes multimodaux pour l'identification et l'authentification biométrique, Université 20 Août 1955 SKIKDA

- [69] : Lamraoui Rawia, Benhmidcha Hanan, La reconnaissance biométrique multimodale, Université Larbi Ben M'hidi OUM EL BOUAGHI
- [70] : S.Kim, D.Lee, J. Kim, "Algorithm for Detection and Elimination of False Minutiae in Fingerprint Image", Lecture Notes in Computer Science, Springer Verlag, vol. 2091, p.235-240, 2001.
- [71] : Z.Bian, D.Zhang, W.Shu, "Knowledge-Based Fingerprint Post-Processing", International Journal of Pattern Recognition and artificial Intelligence, vol. 16, n o .1,p. 53-67, 2002.
- [72] : D. Maio, D. Maltoni, "Direct Gray-Scale Minutiae Detection In Fingerprints", IEEE Transaction on Pattern Analysis and Machine Intelligence, vol. 19, n o . 1, p. 27-39, 1997.
- [73] : Francesco Turrone, "Fingerprint Recognition: Enhancement, Feature Extraction and Automatic Evaluation of Algorithms", dottorato di ricerca in Informatica Ciclo XXIV Università di Bologna , 2012
- [74] : A.K. Jain, S. Prabhakar, L. Hong, S. Pankanti, "Filterbank-based fingerprint matching", IEEE Trans. Image Process, Vol 5, pp. 846–859, 2000.
- [76] : L . M.Munoz-Serrano, "Sistema automatico de reconocimiento de huella dactilar basado en informacin de textura", master's thesis, ETSIT, université Politecnica de Madrid, 2004.
- [77] : L. Hong, A. Jain, and S. Pankanti. Can multibiometrics improve performance?" In: Proceedings of the IEEE Workshop on Automatic Identification Advanced Technologies, 59–64, 1999.
- [78] : K. Nandakumar. Integration of Multiple Cues in Biometric Systems. Master's thesis, Michigan State University, May 2005.
- [79] : S. Oviatt. "Advances in Robust Multimodal Interface Design". IEEE Computer Graphics and Applications, Vol. 23, No. 5, pp. 62–68, 2003.
- [80] : Pierre Bonazza. Système de sécurité biométrique multimodal par imagerie, dédié au contrôle d'accès. Intelligence artificielle [cs.AI]. Université de Bourgogne Franche-Comté, 2019. Français. <https://hal.archives-ouvertes.fr/tel-02180903>
- [81] : Y. Chen, S. Dass, and A. Jain. Fingerprint Quality Indices for Predicting Authentication Performance. In: Proceedings of Fifth International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA), New York, NY, USA, 160–170, July 2005.
- [82] : C. Sanderson and K. K. Paliwal. Information Fusion and Person Verification Using Speech and Face Information. Technical Report IDIAP-RR 02-33, IDIAP, September 2002.
- [83] : Xiao-Yuan Jing, Yong-Fang Yao, David Zhang, Jing-Yu Yang, MiaoLi, "Face and palmprint pixel level fusion and kernel DCV-RBF classifier for small sample biometric recognition", Pattern Recognition, vol. 44, n° 11, p. 3209-3224, 2007.
- [84] : R. O. Duda, P. E. Hart, D. G. Stork, "Pattern Classification", John Wiley & Sons, 2001.
- [85] : K. Woods, W. Kegelmeyer, and K. Bowyer. "Combination of Multiple Classifiers Using Local Accuracy Estimates". IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 19, No. 4, pp. 405–410, 1997.
- [86] : L. Lam and C. Y. Suen, "Application of majority voting to pattern recognition : An analysis of its behavior and performance", IEEE Transactions on Systems, Man, and Cybernetics, vol. 27, 1997.
- [87] : Hao, Anderson, Daugman, "Combining crypto with biometrics efficiently", IEEE Transactions on Computers, vol. 55, 2006.

- [88] : L. Lam, C. Y. Suen, "Optimal combinations of pattern classifiers", Pattern Recognition Letters, vol. 16, n° 9, p. 945-954, 1995.
- [89] : L. Xu, A. Krzyzak, C. Y. Suen, "Methods of combining multiple classifiers and their applications to handwriting recognition", IEEE Transactions on Systems, Man, and Cybernetics, vol. 22, n° 3, p. 418-435, 1992.
- [90] : T. Ho, J. Hull, and S. Srihari. "Decision Combination in Multiple Classifier Systems". IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 16, No. 1, pp. 66–75, 1994.
- [91] : F. Hampel, P. Rousseeuw, E. Ronchetti, and W. Stahel. Robust Statistics : The Approach Based on Influence Functions. John Wiley & Sons, 1986.
- [92] : Y.Wang, T. Tan, A. Jain, "Combining face and iris biometrics for identity verification", Proceedings of Fourth International Conference on Audio- and Video-Based Authentication (AVBPA), p. 805-813, Guildford, U.K., 2003.
- [93] : P. Verlinde, P. Druyts, G. Cholet, and M. Acheroy. "Applying Bayes based classifiers for decision fusion in a multi-modal identity verification system". In : Proceedings of International Symposium on Pattern Recognition "In Memoriam Pierre Devijver", Brussels, Belgium, February 1999.
- [94] : V. Chatzis, A. Bors, and I. Pitas. "Multimodal decision-level fusion for person authentication". IEEE Transactions on Systems, Man and Cybernetics, Part A : Systems and Humans, Vol. 29, No. 6, pp. 674–681, November 1999.
- [95] : C. Sanderson and K. Paliwal. "Information fusion and person verification using speech and face information". Tech. Rep. IDIAP-RR 02-33, IDAIP, September 2002.
- [96] : A. Ross and A. Jain. "Information fusion in biometrics". Pattern Recognition Letters, Vol. 24, No. 13, pp. 2115–2125, 2003.
- [97] : J. Kittler, M. Hatef, R. Duin, J. Matas, "On Combining Classifiers", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 20, n o . 3, p. 226-239, 1998.
- [98] : A. Jain, A. Ross, "Learning User-specific Parameters in a Multibiometric System". Proceedings of International Conference on Image Processing (ICIP), p. 57-60, New York, NY, USA, 2002.
- [100] : Maio, D., D. Maltoni, R. Cappelli, J. L. Wayman, et A. K. Jain (2002). Fvc2002 : Second fingerprint verification competition. In International Conference on Pattern Recognition (ICPR'02), Volume 3, pp. 811 – 814.

Références webographiques :

- [1] : <http://biometrie-tpe68.e-monsite.com/pages/introduction/historique.html>
- [7] : <https://justaskthales.com/fr/la-dynamique-de-frappe-au-clavier-une-reference-biometrique/>
- [8] : <https://www.biometrie-online.net/technologies/signature-dynanique>
- [9] : https://fr.wikipedia.org/wiki/Acide_d%C3%A9soxyribonucl%C3%A9ique
- [13] : https://fr.wikipedia.org/wiki/Odeur_corporelle
- [18] : Biometrics market [En ligne]; le lien: <https://www.biometrie-online.net/biometrie/le-marche>
- [19] : Biometrics market [En ligne]. <https://www.tractica.com/newsroom/pressreleases/biometrics-market-revenue-to-total-67-billion-worldwide-over-the-next-10-years/>. Consultée en 14/01/2018.

- [23] : <https://www.globalsign.com/fr/blog/7-avantages-de-la-biometrie-pour-la-securite>
- [30] : https://fr.wikipedia.org/wiki/Syst%C3%A8me_de_reconnaissance_faciale
- [53] : https://fr.wikipedia.org/wiki/R%C3%A9seau_de_neurones_artificiels
- [57] : <http://www.isir.upmc.fr/UserFiles/File/LPrevost/Biometrie%20Empreintes.pdf>
- [61] : International Biometric Group, The Henry Classification, www.biometricgroup.com
- [63] : <https://e-portfolio.uha.fr/artefact/file/download.php?file=83546&view=18927>