REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Akli Mohand Oulhadj de Bouira

Faculté des Sciences et des Sciences Appliquées

Département de Génie Electrique

Mémoire

MASTER ACADÉMIQUE

Domaine : Sciences et Technologie

Filière : *Génie Biomédical*

Spécialité : *Instrumentation Biomédicale*

THÈME

Réalisation d'un Système de Reconnaissance Biométrique Multimodal

Réalisé par :

IDRIGUEN Sonia ***BAHLOUL Wissam***

Soutenu publiquement le : 29/09/2018

Devant le Jury composé de:

M. BENZIANE	Mourad	M.A.A	Président	UAMOB Bouira
M. BENZAOUI	Amir	M.C.A	Encadreur	UAMOB Bouira
M. MOUDACHE	Said	M.A.A	Examinateur	UAMOB Bouira

Année Universitaire : 2017/2018

Remerciement

Ce travail est l'aboutissement d'un long cheminement au cours duquel nous avons bénéficié de l'encadrement, des encouragements et du soutien de plusieurs personnes à qui nous tenons à dire profondément et sincèrement merci.

Tout d'abord, nous tenons à remercier le bon dieu le tout puissant de nous avoir donné la force et le courage de mener à bien ce modeste travail, également nous remercions nos parents pour leur encouragement et leur patience.

Tous nos infinis remerciements à notre encadreur Mr : ***Amir BENZAOUI*** *pour son aide, sa patience, ses conseils et ses remarques qui nous ont permis de présenter notre travail dans sa meilleure forme.*

Nos vifs remerciements vont également aux membres du jury pour l'intérêt qu'ils ont porté à notre recherche en acceptant d'examiner notre travail de l'enrichir par leurs propositions.

Nous tenons à exprimer nos sincères remerciements à tous les enseignants du département génie électrique qui nous ont enseigné et qui par leurs compétences nous ont soutenu dans la poursuite de nos études.

Enfin nous remercions tous nos proches, nos amis et tous ceux qui ont contribué de prés ou de loin à l'élaboration de notre travail trouvant ici l'expression de notre profonde gratitude et profonds respects.

Merci à tous et à toutes.

Dédicace

Je dédie ce modeste travail
A mes très chers parents pour leur soutient et encouragement durant toutes mes années d'études et sans lesquels je n'aurais jamais réussi.
A mes très chers frères et ma chère sœur.
A tous mes ami(e)s ainsi qu'à toutes les personnes que j'ai connues, qui m'ont aidées, soutenues et encouragées.
A tous mes enseignants durant mes années d'études avec lesquels j'ai beaucoup appris.

Sonia

Dédicace

Je dédie ce travail

A la mémoire de mon père, que dieu lui accorde sa miséricorde et l'accueille dans son vaste paradis et le préserve du châtiment de la tombe et du châtiment de l'enfer. Repose en paix n'challah.

A ma mère ***Sabah*** *qui a toujours su m'écouter et pris le temps de m'entendre, sa tendresse et sa volanté ont toujours mérité mon plus profond respect.*

A mon cousin ***Samir*** *qui était à la place de mon père qui ne cesse jamais de m'offrir son amour et son soutien.*

A mes deux frères ***Salah*** *et* ***Yakoub*** *que je ne pourrais jamais exprimer le respect et l'amour que j'ai pour vous.*

A toute ma famille, mes grands-parents, mes cousins, mes cousines, mes tantes, mes oncles.

A mes ami(e)s, tout particulièrement ma chère binôme ***Sonia*** *qui m'on toujours poussé et m'encouragé.*

A tous mes enseignants du département génie électrique pour leurs soutiens et encouragements.

Wissam

Table des matières

Chapitre 01 : Généralité sur la Biométrie et les Systèmes biométriques

Chapitre 02 : La Biométrie Multimodale et la Reconnaissance des Formes

Chapitre 03 : Etude Expérimentale & Résultats

Abréviation

ADN: Acide **D**ésoxyribose **N**ucléique.

EER: Equal **E**rror **R**ate.

FRR: False **R**ejection **R**ate.

FAR: False **A**cceptance **R**ate.

ROC: Receiver **O**perating **C**haracteristic.

IR: Identification **R**ate.

CI: Correctement **I**dentifiée.

CMC: Cumulative **M**atch **C**urve.

RdF: Reconnaissance **d**es **F**ormes.

IRM: Imagerie par **R**ésonnance **M**agnétique.

LG-PCA: Log **G**abor-**P**rincipal **C**omponent **A**nalysis.

LBP: Local **B**inary **P**attern.

LPQ: Local **P**hase **Q**uantization.

AAM: Active **A**pparence **M**odel.

BIC: Bayesian **I**nformation **C**riterion.

SVM: Support **V**ector **M**achines.

K-PCA: Kernel **P**rincipal **C**omponent **A**nalysis.

K-LDA: Kernel **L**inear **D**iscriminants **A**nalysis.

ICA: Independent **C**omponent **A**nalysis.

LDA: Linear **D**iscriminants **A**nalysis.

PCA: Principal **C**omponent **A**nalysis.

EBGM: Elastic **B**unch **G**raph **M**atching.

HMM: Hidden **M**arkov **M**odels

EO: Eigen **O**bjects

K-NN: K-Nearest **N**eighbors.

K-PPV: K-Plus **P**roches **V**oisins.

ORL: Olivetti **R**esearch **L**aboratory.

MCYT: Ministerio de **C**iencia **Y T**ecnologia (en Espagnol).

MB-LBP: Multi **B**lock **L**ocal **B**inary **P**attern.

ML-LBP: Multi **L**evel **L**ocal **B**inary **P**attern.

Liste des figures

Chapitre 01 : Généralité sur la Biométrie et les Systèmes biométriques

Chapitre 02 : La Biométrie Multimodale et la Reconnaissance des Formes

Chapitre 03 : Étude Expérimentale & Résultats

Liste des tableaux

Chapitre 01 : Généralité sur la Biométrie et les Systèmes biométriques

Chapitre 03 : Etude Expérimentale & Résultats

INTRODUCTION GÉNÉRALE

Introduction Générale

Savoir déterminer l'identité d'une personne d'une façon automatique reste un dilemme d'actualité. Dans un monde qui devient de plus en plus interconnecté, il est nécessaire de reconnaitre les utilisateurs afin de leur donner accès à un immeuble ou les procurer des autorisations d'utiliser de ressources spécifiques. Il s'avère donc plus que nécessaire de développer des systèmes d'authentification automatique capables de lutter contre les fraudes et d'assurer la sécurité dans différents domaines comme le passage dans les postes frontaliers internationaux au moins ardu comme l'accès aux informations personnelles [1].

En revanche, les techniques d'authentification utilisées comme les mots de passe et les cartes d'identité ne sont pas à la hauteur des exigences de sécurité. En effet, les utilisateurs peuvent facilement être privés d'utiliser un service en prétendant que leurs mots de passe ont été volés, devinés ou même oubliés. Pour pallier à ces différents problèmes de non sécurité et d'inefficacité, la biométrie semble être une solution évidente et pratique dont le coût en effort et en argent est en constante diminution.

La biométrie est une technique globale visant à établir l'identité d'une personne en mesurant l'une de ses caractéristiques physiques ou comportementales telles que le visage, l'empreinte digitale, la signature électronique, la voix, l'iris…etc.

Bien que les techniques biométriques montrent leurs puissances, ils ne peuvent pas garantir actuellement un taux de reconnaissance de 100 % avec les systèmes biométriques basés sur une seule donnée biométrique ou une signature unique [2]. En outre, ces systèmes sont souvent affectés par les problèmes suivants : non universalité, manque d'individualité, le bruit généré par le capteur, sensibilité aux attaques…etc.

Pour remédier à ces inconvénients, la solution est d'utiliser plusieurs modalités biométriques au sein du même système, ce qu'on appelle un ***système biométrique multimodal***.

Il existe cinq types des systèmes multimodaux [1] : multi-capteur, multi-instance, multi-algorithme, multi-échantillon et multi_biométries. Ces différents types de systèmes multi-modaux pourraient réduire plusieurs problèmes rencontrés dans les systèmes unimodaux.

L'objectif principal de notre travail est la réalisation d'un système d'identification biométrique multimodal basé sur la combinaison de deux modalités biométriques : ***le visage et la signature électronique***.

Notre mémoire sera structuré comme suit :

Le premier chapitre est consacré à des généralités sur la biométrie ainsi que le concept des systèmes biométriques et leurs performances.

Le deuxième chapitre contient deux parties. Dans la première partie l'accent est mis sur une présentation de la biométrie multimodale en se basant sur les niveaux de fusion ainsi que l'architecture des systèmes biométriques correspondants à chaque niveau. Dans la deuxième partie nous allons présenter le concept de la reconnaissance des formes par la présentation de son processus en détails.

Dans le dernier chapitre nous allons implémenter le système biométrique multimodal (fusion de la modalité du visage avec celle de la signature électronique) et la mise en évidence de ce système. Puis nous allons présenter les résultats expérimentaux obtenus par chaque méthode par l'analyse de leurs performances avec une discussion et une interprétation sur les résultats obtenus.

A la fin nous terminerons notre travail par une conclusion générale.

Chapitre 01

Généralités sur la Biométrie et les Systèmes Biométriques

Chapitre 01 : Généralités sur la Biométrie et les Systèmes Biométriques

1.1. Introduction

Dans le contexte actuel et devant la croissance exponentielle des communications, tant physiques que virtuelles qui présentent des risques sur la sécurité des individus. Il est nécessaire de contrôler l'identité de ces individus et leurs échanges que ce soit pour garantir leurs sécurités dans les lieux publics ou pour éviter le détournement et le vol d'information sensible. Ces échanges comme l'achat en ligne et transactions bancaires, exigent l'authentification des personnes avec deux manières classiques [3] : la première repose sur la connaissance à priori (mot de passe et le code d'activation) et la seconde est basée sur la possession d'un objet (la pièce d'identité, un badge ou clef). Cependant, ces deux méthodes présentent quelques inconvénients. En effet, le mot de passe peut être oublié où espionné et la pièce d'identité risque d'être volée ou perdue. Afin de remédier aux problèmes des méthodes précédentes, ***la biométrie*** semble être une solution pratique [1].

Dans ce premier chapitre, nous allons définir des généralités sur ***la biométrie*** dans l'état de l'art, en commençant par un bref historique puis nous définirons la biométrie, ensuite nous citrons ses domaines d'applications, les systèmes biométriques, nous présenterons quelques techniques de reconnaissances par biométrie et nous établirons un tableau général (comparatif) des techniques les plus utilisés sur le terrain. Enfin nous terminerons notre chapitre par la motivation de notre choix de la biométrie multimodale.

1.2. La biométrie :

1.2.1. Historique :

L'homme a toujours essayé de trouver les différences existantes entre lui-même et son entourage et les exploiter dans ses besoins quotidiens.

- Les chinois ont été les premiers à utiliser, il y a 1000 ans, les empreintes digitales à des fins de signatures de documents. Après, c'était le tour de l'anatomiste *MARCELLO MALPIGHI* (1628-1694) qui les a étudié avec un nouvel instrument nommé microscope. Puis le physiologique tchèque *JAN EVANGELISTA PURKINGE* (1787-1859) a essayé de les catégoriser selon certaines caractéristiques [4].

- Vers la fin du XIX siècle, le *DR HENRY FAULDS* (1843-1930), chirurgien à Tokyo, a marqué le premier pas vers l'élaboration d'un système d'identification d'individus en se basant sur des méthodes statistiques pour la classification des empreintes [4].
- En ce moment, un de ses contemporains, le français *ALPHONSE BERTILLON* (1853-1914), était entrain de tester une méthode d'identification des prisonniers nommée anthropométrie judiciaire. *BERTILLON* procédait à la prise de photographies de sujets humains, mesurait certaines parties de leurs corps (tête, membres, etc.) et notait les dimensions sur les photos et sur des fiches à des fins d'identification ultérieure. C'était la naissance de la première base de données contenant des informations des individus. Et depuis, ces systèmes de reconnaissance ne cessent de se développer et de devenir plus performants [4].

1.2.2. Définition de la biométrie :

La biométrie est un terme d'origine grec, qui se compose en deux parties : « bios » qui veut dire « la vie » et « métron » qui se traduit par « la mesure » [5], autrement dit c'est la mesure du vivant. Donc, la biométrie est une technique naissante visant à la reconnaissance et l'identification des individus en utilisant des informations étroitement liés à leurs caractéristiques. Les méthodes biométriques reposent sur l'utilisation des empreintes digitales, du visage, de la voix, de l'iris ou de l'ADN… [6].

1.3. Les champs d'application de la biométrie :

Les techniques biométriques sont présentées dans les domaines de la sécurité où il est nécessaire de connaitre l'identité des personnes. On peut diviser ses applications en trois groupes principaux qui sont [7]:

1.3.1. Applications gouvernementales : comme le contrôle des passeports, la sécurité sociale, permis de conduire, carte d'identité, etc.

1.3.2. Applications commerciales : telle que l'accès d'internet, le téléphone cellulaire, utilisation des cartes de crédit bancaire, l'étude à distance, la gestion des registres médicaux, l'accès à un réseau ordinateur, etc.

1.3.3. Application médico-légales : telle que la recherche criminelle, l'identification de cadavre, la détermination parentèle, l'identification du corps humain, etc.

1.4. Les systèmes biométriques :

1.4.1. Définition d'un système biométrique:

Un système biométrique est défini comme un système automatique de reconnaissance des formes d'individus [8]. Il permet de capter l'information biométrique (image ou signal), ensuite il va extraire des éléments caractéristiques pour les comparer avec d'autres données déjà mémorisées dans la base de données et à la fin une décision est prise à partir du résultat de comparaison [9].

1.4.2. Modes de fonctionnement d'un système biométrique :

Généralement les systèmes biométriques fonctionnent selon trois modes principaux (**figure 1.1**) : l'enrôlement, la vérification d'identité et l'identification [10]. On présente dans ce qui suit l'ensemble du processus pour plus de détails :

1.4.2.1. Enrôlement :

Elle est considérée comme la première phase de tout système biométrique qui sert à créer une base de données de référence. Pendant cette phase, l'utilisateur est enregistré pour la première fois dans le système par la capture d'un échantillon biométrique puis l'extraction des données caractéristiques de cet échantillon pour les enregistrer dans une base de données.

1.4.2.2. Vérification ou authentification :

C'est une étape qui permet de vérifier l'authenticité d'une personne. En effet le système consiste à contrôler l'identité d'un individu en effectuant une comparaison entre les données biométriques acquises avec le modèle biométrique propre stocké dans la base de données, c'est une comparaison de type « un contre un ». Un système biométrique en mode de vérification doit répondre à la question « suis-je réellement moi ? ». Ce mode est utilisé pour but d'empêcher l'utilisation de la même identité par plusieurs personnes.

1.4.2.3. Identification :

C'est un mode de reconnaissance des individus. Le système biométrique va comparer l'identité d'une personne inconnue avec les modèles de toutes les personnes enregistrées dans la base de données donc on parle d'une correspondance 1 : N en répondant à la question « suis-je bien connu du système ? ». Typiquement, la personne sera rejetée si son identité ne correspond pas aux modèles d'identités de la base de données ce qui signifie que l'utilisateur n'était pas parmi les personnes enrôlées par le système. Dans le cas contraire, la personne sera acceptée.

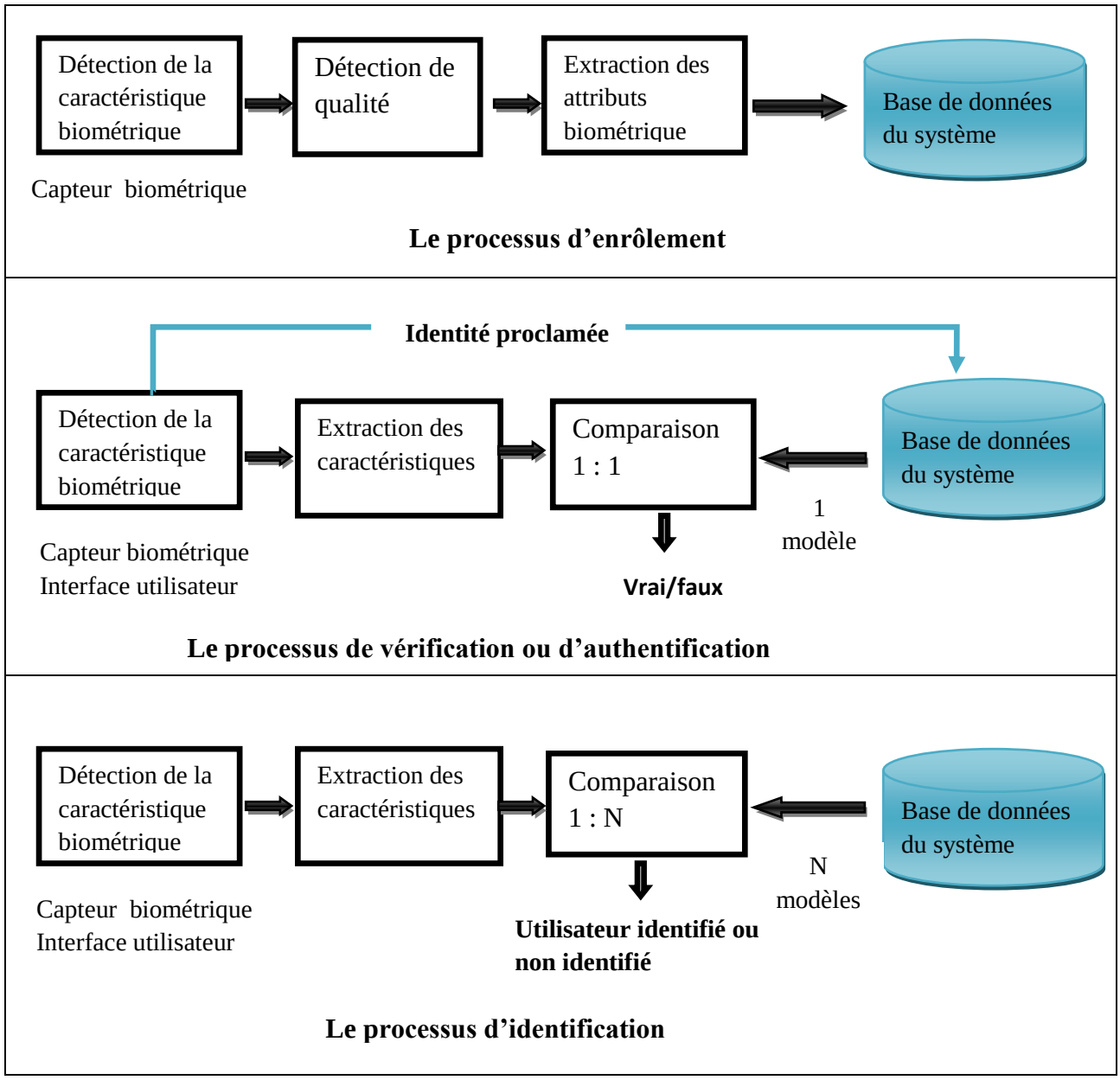

Figure 1.1 : Les modes de fonctionnement d'un système biométrique [3].

1.4.3. Structure interne d'un système biométrique :

L'architecture d'un système biométrique est composée de cinq modules principaux. Pour avoir plus de détails, nous allons expliquer le fonctionnement de chaque module comme suit [11] :

1.4.3.1. Module de capteur biométrique : il est défini comme une interface d'interaction entre l'homme et la machine, il permet la lecture ou l'acquisition de certains caractéristiques biométriques d'un individu à l'aide d'un capteur (appareil photo, un microphone, un lecteur d'empreintes digitale, etc.).

1.4.3.2. Module d'extraction des données : son principe est basé sur l'évaluation des données biométriques acquises par le capteur biométrique pour extraire les informations pertinentes. Pour améliorer la qualité des données acquises, il faut les passées par un algorithme de restauration.

1.4.3.3. Module de création de signature (stockage) : consiste à créer un modèle numérique pour représenter les données biométriques acquises. Ce modèle sera sauvegardé sur un support portable (puce) ou bien dans une base de données.

1.4.3.4. Module de comparaison (correspondance) : il effectue une comparaison entre les caractéristiques biométriques extraites d'un individu avec les modèles stockés dans la base de données. Ce module peut fonctionner soit en mode d'authentification pour déterminer une identité proclamée, soit en mode d'identification pour déterminer une identité recherchée.

1.4.3.5. Module de la base de données : c'est l'enregistrement et le stockage des modèles biométriques des personnes enrôlées dans une base de données de référence.

1.5. Les différents types de reconnaissance par biométrie :

Il existe plusieurs modalités qui ont été utilisées dans divers systèmes biométriques. Nous pouvons distinguer trois grandes catégories de ces modalités qui sont [6] :

1.5.1. Analyse des traces biologiques :

Cette analyse est basée sur les propriétés biologiques des individus comme les tests portants sur le sang, l'ADN, l'urine, la salive, etc. Ce type de biométrie est utilisé que dans des cas d'extrême nécessite (test de paternité, enquête criminel, etc.).

1.5.2. Analyse des traits physiologique ou morphologique :

Cette catégorie se base sur la mesure de l'une des caractéristiques physiques d'un individu et qui est unique et permanente pour toutes les personnes (exemple : les empreintes digitales, géométrie de la main, le visage, iris, etc.).

1.5.3. L'analyse comportementale :

Cette analyse s'appuie sur l'étude de la manière de faire des individus autrement dit c'est l'étude de l'activité ou le comportement d'un l'individu. Ces modalités peuvent changer au cours du temps comme exemple on peut citer : la dynamique de frappe au clavier, la façon de marcher, la voix, etc.

1.6. Les techniques biométriques :

Actuellement les techniques biométriques sont utilisées dans le domaine de sécurité. Elles se divisent en deux groupes [12] :

1.6.1. Techniques intrusives : elles sont généralement mal acceptées car elles nécessitent un contact physique avec l'individu, afin de l'identifier à titre d'exemples : l'iris, la rétine et les empreintes digitales, etc.

1.6.2. Techniques non intrusives : elles peuvent effectuer à distance par l'utilisation des capteurs qui ne nécessitent pas un contact direct avec l'utilisateur (façon de marcher, signature, frappe de clavier, etc.).

1.7. Caractéristiques biométriques :

La reconnaissance biométrique fait référence à l'utilisation de différentes caractéristiques d'un être humain. En effet, pour qu'un système biométrique puisse fonctionner en environnement réel, les caractéristiques physiologiques ou comportementales doivent satisfaire les conditions suivantes [7,13] :

- ***Universalité*** **:** veut dire que chaque individu doit posséder cette caractéristique (existe chez tous les individus).
- ***Unicité*** **:** c'est une caractéristique qui permet de distinguer la différence d'un individu par rapport à un autre.
- ***Stabilité*** **:** signifie que le trait biométrique d'un individu doit être invariant au cours du temps (permanente).
- ***Acceptabilité*** **:** indique la mesure dans laquelle les gens sont prêts à accepter l'utilisation d'une caractéristique biométrique dans leurs vies quotidiennes.
- ***Performance*** **:** elle dépend de la précision de la reconnaissance et la vitesse d'exécution face aux variations des caractéristiques biométriques, aux bruits et aux déformations des appareils de capteurs.
- ***Enregistrable*** **:** c'est la capacité d'acquérir les caractéristiques d'un individu à l'aide d'un dispositif approprié.
- ***Infalsifiable*** **:** c'est la difficulté de falsifier une caractéristique biométrique d'une personne (ex., les faux doigts dans le cas de trait physique).

Malheureusement, dans la pratique, on ne trouve pas toutes ces caractéristiques dans une modalité. Donc chaque modalité possède ses caractéristiques biométriques propres mais avec

des degrés différents. Le tableau 1.1 compare certaines modalités biométriques en fonction de leurs propriétés.

Tableau 1.1 : Comparaison de quelques modalités biométriques [8].

Modalité	Universalité	Unicité	Permanence	Mesurabilité	Acceptabilité	Performance	Circonvention
Visage	Haute	Faible	Moyenne	Haute	Haute	Faible	Haute
Empreinte Digitale	Moyenne	Haute	Haute	Moyenne	Moyenne	Haute	Moyenne
Iris	Haute	Haute	Haute	Moyenne	Faible	Haute	Faible
ADN	Haute	Haute	Haute	Faible	Faible	Haute	Faible
Signature	Faible	Haute	Moyenne	Haute	Haute	Moyenne	Haute
Voix	Moyenne	Faible	Faible	Moyenne	Haute	Moyenne	Haute
Démarche	Moyenne	Faible	Faible	Haute	Haute	Faible	Moyenne
Rétine	Haute	Haute	Moyenne	Faible	Faible	Haute	Faible
Frappe sur clavier	Faible	Faible	Faible	Moyenne	Moyenne	Faible	Moyenne
Géométrie de la main	Moyenne	Moyenne	Moyenne	Haute	Moyenne	Moyenne	Moyenne
Thermo-gamme faciale	Haute	Haute	Faible	Haute	Haute	Moyenne	Faible
Oreille	Moyenne	Haute	Haute	Haute	Haute	Haute	Moyenne

Le **Tableau 1.1.** montre qu'il n'existe pas de modalité parfaite ou idéale ou moins adaptée à des applications malgré l'existence de plusieurs modalités biométriques.

Donc, le choix de la modalité biométrique dépend essentiellement des exigences et des besoins de chaque application.

1.8. Performances des systèmes biométriques :

Pour le choix d'un système biométrique il faut prendre en considération sa performance qui joue un rôle très important.

D'une part, durant le processus d'évaluation elle permet de tester et évaluer le comportement des utilisateurs. D'autre part, elle permet d'identifier pour chaque système, les applications industrielles.

Pour définir les performances d'un système biométrique, il faut tester les deux modes opératoires : la vérification et l'identification [14] :

1.8.1. Test de vérification :

Lorsqu'un système biométrique fonctionne en mode vérification, l'utilisateur va demander de vérifier son identité par le système, à titre d'exemple il va proclamer « je suis Moussa », pour savoir si l'identité proclamée par l'utilisateur est acceptée ou bien rejetée. Pour cela deux taux sont calculés comme suit [15] :

- **Le taux des faux rejets (TFR) ou False Rejection Rate (FRR) :** qui représente le pourcentage de personnes qui sont rejetés par le système alors qu'ils devraient être reconnues. Ce taux est calculé par le rapport entre le nombre de personnes rejetées (FR) sur le nombre total de personnes légitimes. Sa formule est [16] :

$$\boldsymbol{Taux\ des\ Faux\ Rejets\ (TFR) = \frac{nombres\ des\ personnes\ rejetés(FR)}{nombre\ total\ d'accès\ de\ prsonnes}}$$

- **Le taux de fausse acceptation ou False Acceptation Rate (FAR) :** il représente le pourcentage de personnes censées à ne pas être reconnues mais elles sont acceptées par le système. C'est le rapport entre le nombre de personnes acceptées (FA) sur le nombre de personnes totales non autorisées qui ont tenté de se faire acceptées. Ce taux peut être formulé comme suit [16] :

$$\boldsymbol{Taux\ des\ Fausses\ Acceptations\ (TF) = \frac{nombres\ des\ personnes\ acceptés\ (FA)}{nombre\ total\ d'accès\ d'imposteurs}}$$

On peut définir le test de vérification par la relation suivante :

$$(I, X_Q) = \begin{cases} W_1 & si\ S\ (X_Q, X_t) \geq \theta \\ W_2 & sinon \end{cases}$$

Avec :

$\boldsymbol{X_Q}$: C'est le vecteur de caractéristiques de la personne proclamée.

$\boldsymbol{X_t}$: C'est le vecteur de la personne I enregistrée dans la base de données.

$\boldsymbol{S(X_Q, X_t)}$: C'est une fonction de similarité entre X_Q et X_t, cette fonction S permet d'évaluer le résultat de similarité entre les mesures biométriques de la personne proclamée et la personne de la base de données.

$\boldsymbol{W_1}$: indique l'acceptation de la personne proclamée.

$\boldsymbol{W_2}$: indique que la personne est un imposteur (rejetée).

$\boldsymbol{\theta}$: C'est le seuil de similarité. Son choix est très important car il influe sur les performances du système.

En effet, si θ est très petite cela peut engendrer un grand nombre de faux de rejets, tandis que, si θ est très grande, cela engendre un taux important de fausses acceptations.

Dans le contexte de vérification, la statistique qui permet de mesurer la performance d'un algorithme est de calculer le point d'équivalence des erreurs (''Equal Error Rate'' ou EER). Ce dernier est déterminé par le point d'intersection entre la courbe de FRR et la courbe de FAR, ce point correspond à l'endroit où FRR=FAR.

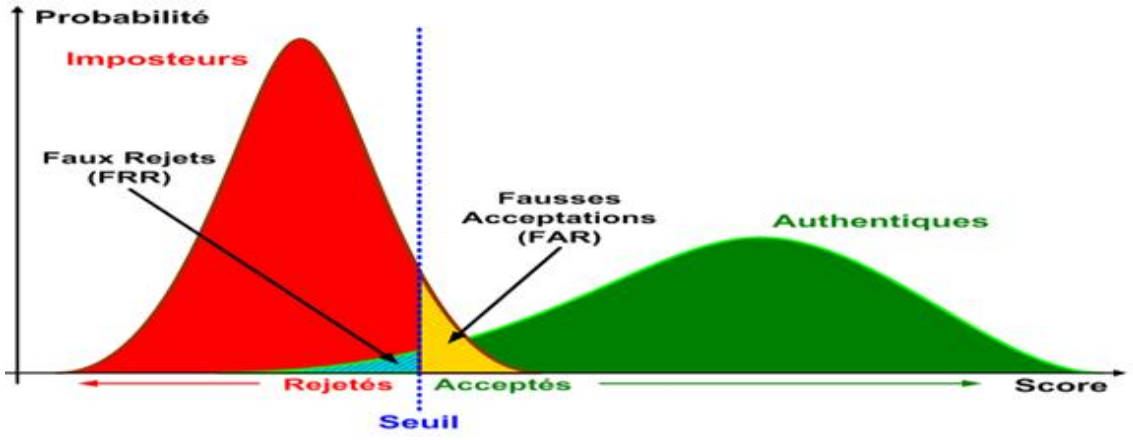

Figure 1.2 : Courbe de la distribution de FRR et FAR [12].

Durant le mode d'authentification, on utilise la courbe ROC « Receiver Operating Characteristic » qui trace le taux de faux rejets (FRR) en fonction du taux de fausses acceptations comme elle est montrée dans la **figure 1.3.**

Figure 1.3 : La courbe de ROC [17].

1.8.2. Test d'identification :

Dans le cas d'un système utilisé en mode identification, une comparaison est effectuée entre les données biométriques en entrée avec les données stockées dans la base de données pour identifier l'identité d'un individu.

On peut formuler le test d'identification mathématiquement de la manière suivante :

On considère que X_Q c'est le vecteur de caractéristiques, pour identifier l'identité I_K avec $k \in \{1,2, \dots \dots, N, N+1\}$, donc la fonction (I, X_Q) est définie comme suit :

$$(I, X_Q) = \begin{cases} I_k & si\ max_k \left\{S(X_Q, X_{I_k})\right\} \geq \theta, k = 1, \dots, N \\ I_{N+1} & sinon \end{cases}$$

D'où :

$I_1, \dots, I_N$: sont les identités des utilisateurs enrôlées dans le système.

I_{N+1} : une identité rejetée.

X_{I_k}: le modèle biométrique qui correspond à I_k.

S : la fonction de similarité.

θ: c'est le seuil de décision.

Le taux d'identification (''Identification Rate'' ou IR) c'est le pourcentage des personnes correctement identifiées (CI) par rapport au nombre total de personnes testées (N), ce taux est formulé par :

$$IR(\theta) = \frac{CI(\theta)\times 100}{N}$$

Ce test d'identification n'est pas toujours suffisant. En effet en cas d'erreur, il peut être utile de savoir si le bon choix se trouve parmi le N premières réponses du système. Alors dans ce mode on utilise ce qu'on appelle une courbe CMC « Cumulative Match Charactéristic, en anglais » [18] (voire la figure 1.4) qui donne le pourcentage de personnes reconnues en fonction d'une variable appelée rang. Par exemple on peut dire qu'un système reconnait au rang 1 lorsqu'il choisit la plus proche image comme résultat de reconnaissance. Et qu'un système reconnait au rang 2, s'il choisit parmi 2 images celle qui correspond mieux à l'image d'entrée, etc. Donc si le rang augmente signifie que le taux de reconnaissance est lié à un niveau de sécurité faible.

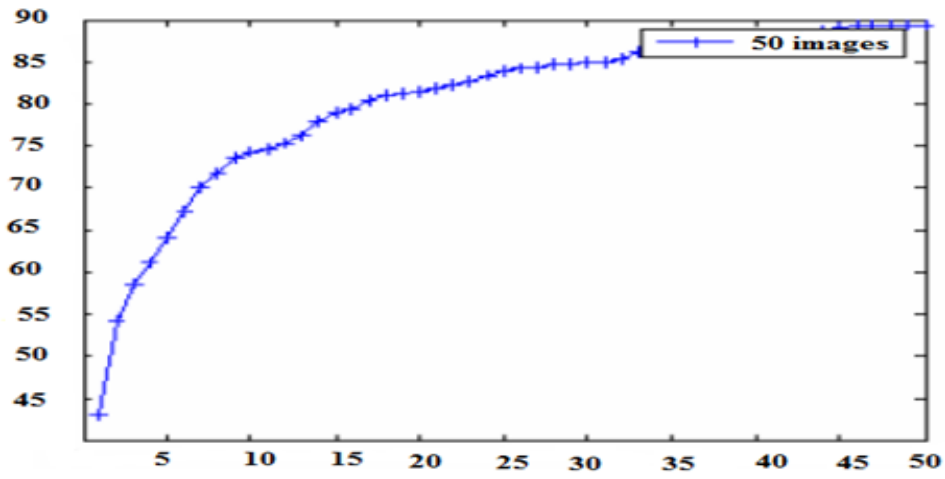

Figure 1.4 : La courbe CMC [18].

1.9. Avantages et inconvénients de quelques modalités biométriques :

1.9.1. Modalités morphologiques :

L'empreinte digitale : c'est une technique biométrique ancienne qui est généralement très connue par la plupart des gens [17]. Elle peut être définie comme une impression produite par la transpiration, la graisse, ou l'encre qui sont présentés dans la partie supérieure de chaque doigt de la main d'un être humain. Ces empreintes sont uniques pour chaque individu.

Elles sont utilisées sur des microordinateurs ou téléphones portables pour la sécurité de leurs utilisations [1].

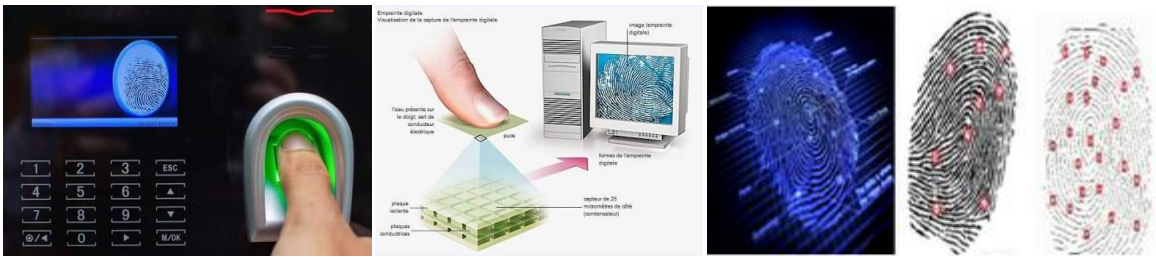

Figure 1.5 : Système biométrique de l'empreinte digitale.

Avantages et inconvénients de la reconnaissance de l'empreinte digitale [19]**:**

Avantages :

- Facile à utiliser.
- La technologie la plus connue et éprouvée par le public.
- Faible coût.
- Traitement rapide.
- Petite taille de lecteur.
- Un bon compromis entre le taux de faux rejet et le taux de fausse acceptation.

Inconvénients :

- Acceptabilité moyenne.
- Possibilité d'attaque.
- Certains systèmes peuvent accepter un moulage de doigts ou un doigt coupé.

Géométrie de la main : chaque personne possède une forme propre de sa main. C'est une technique biométrique basée sur la mesure de la position et la taille des doigts placés sur une surface plane [20]. L'acquisition d'une image de la main est obtenue à l'aide d'un scanner spécialisé.

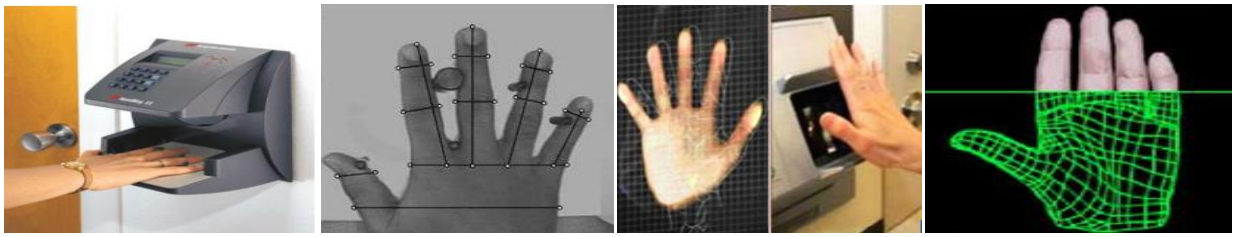

Figure 1.6 : Géométrie de la main.

Avantages et inconvénients de l'identification de la géométrie de la main [19]**:**

Avantages :

- Utilisation simple.
- Bonne acceptabilité par les individus.
- Moins coûteuse que les empreintes digitales.
- Pas d'effet en cas d'humidité des doigts.

Inconvénients :

- Risque de fausse acceptation pour des jumeaux ou des membres de la même famille.
- Trop encombrant pour un usage sur le bureau ou un téléphone.
- Modification de la forme des doigts avec le vieillissement.

Le visage : la reconnaissance biométrique du visage est effectuée d'une façon spontanée dans la vie des individus. C'est la technique la plus populaire et commune car elle correspond à ce qu'on utilise naturellement pour reconnaitre une personne [21]. Les propriétés qui permettent de reconnaitre le visage sont la bouche, les yeux et la forme du visage (son contour), etc. Cette technologie permet le contrôle d'accès aux distributeurs automatiques de billets, et le contrôle d'accès logique à la surveillance [22].

Figure 1.7 : Système de reconnaissance du visage.

Avantages et inconvénients de reconnaissance de visage [19] **:**

Avantages :

- Peu encombrant.
- Utilisation simple.
- Bonne acceptabilité.
- Peu coûteuse.

Inconvénients :

- Problème de distinguer les vrais jumeaux.
- Peu d'efficacité.
- Sensibilité à la variation de l'éclairage et au changement de la position du visage.

La géométrie de l'oreille : l'oreille humaine a été utilisée comme un moyen de reconnaissance en médecine légale, et son morphologique extérieur est relativement stable durant une période de temps qui est acceptable pour les applications biométriques. Les approches de reconnaissance d'oreille sont basées sur la correspondance de la distance entre les différents points de référence de l'oreille [9]. L'oreille humaine possède une richesse d'information qui se situe sur une surface 3D incurvée, cette richesse d'information a attiré l'attention des scientifiques légaux [23].

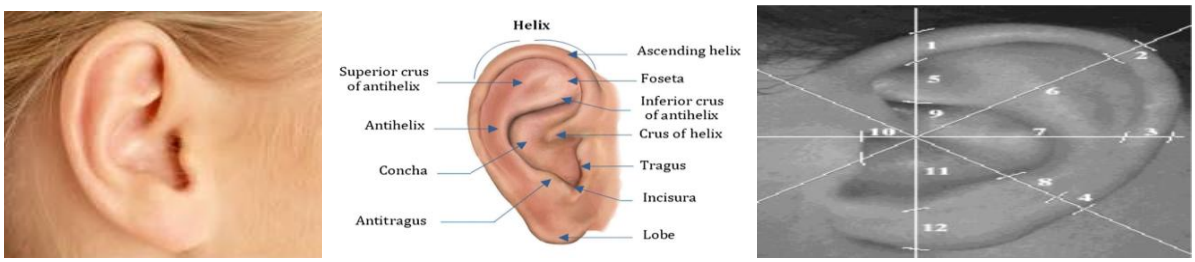

Figure 1.8 : Système de reconnaissance biométrique de l'oreille.

Avantages et inconvénients de la reconnaissance biométrique de l'oreille [12]**:**

Avantages :

- Une technique efficace, car il n'existe pas deux formes d'oreilles identiques.
- Très acceptable.

Inconvénients :

- Il n'existe encore aucune application commerciale [12].

L'iris : c'est un voile très fin formé de lamelles pigmentaires qui donnent la couleur des yeux. L'identification par l'iris utilise plus de paramètres par rapport aux autres méthodes d'identification [6]. Cette technique biométrique est employée dans le secteur financière, dans les hôpitaux et les grands aéroports [1].

Figure 1.9 : Système biométrique basée sur l'iris.

Avantages et inconvénients de la reconnaissance par iris [19] **:**

Avantages :

- Distinguer les vrais jumeaux.
- Grande quantité d'information contenue dans l'iris.
- Fiabilité et durabilité.

Inconvénients :

- Aspect psychologiquement invasif de la méthode.
- Coûteuse.
- Contraintes d'acquisition.
- Faible acceptabilité.

La rétine : c'est la couche sensorielle de l'œil qui permet la vision. La détermination des caractéristiques de la rétine consiste à extraire la distribution géographique des vaisseaux sanguins [24]. Cette technologie est adapté aux applications de haute sécurité (salles de coffres forts, sites militaires, etc.) [12].

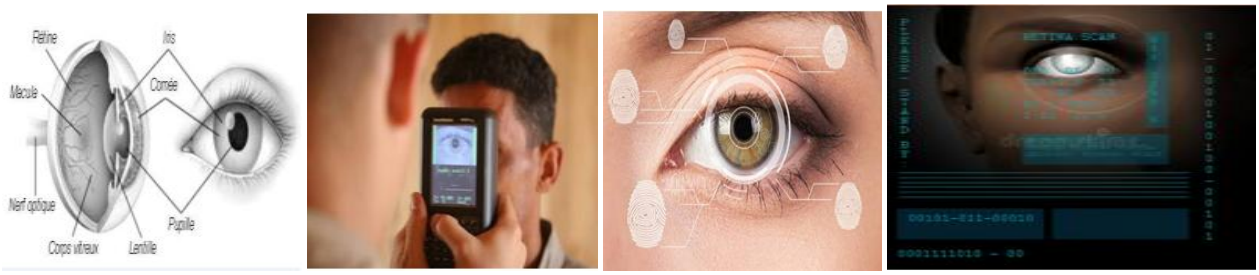

Figure 1.10 : Identification par rétine.

Avantages et inconvénients d'identification par rétine [19] **:**

Avantages :

- La rétine est stable durant la vie d'un individu.

- Très efficace.
- La rétine est différente chez les vrais jumeaux.
- Haute sécurité.

Inconvénients :

- Système intrusif car il faut placer l'œil prés du capteur.
- Mal acceptée par le public.
- Un coût important.

1.9.2. Les modalités comportementales :

La dynamique de frappe au clavier : c'est une propriété comportementale propre à chaque individu. Il s'agit d'une graphologie des temps modernes car on écrit plus souvent avec un clavier qu'avec un stylo. Les éléments principaux analysés par cette modalité sont : la vitesse de frappe, la suite de lettre, le temps de frappe, les pauses, etc. [9].

Figure 1.11 : La reconnaissance biométrique basée sur la dynamique de frappe au clavier.

Avantages et inconvénients de reconnaissance basée sur dynamique de frappe au clavier [19] **:**

Avantages :

- Identification d'une personne à distance à partir de son ordinateur.
- Mise en œuvre rapide pour un grand nombre d'utilisation.
- Non intrusif, geste naturel pour une personne.

Inconvénients :

- Dépend de l'état physique, émotion, fatigue, etc.
- Sensibilité à la différence entre les claviers.

La signature électronique : chaque personne est caractérisée par sa façon d'écriture unique. A partir de sa signature on peut définir un modèle qui pourra être utilisé pour l'identification des personnes [25].

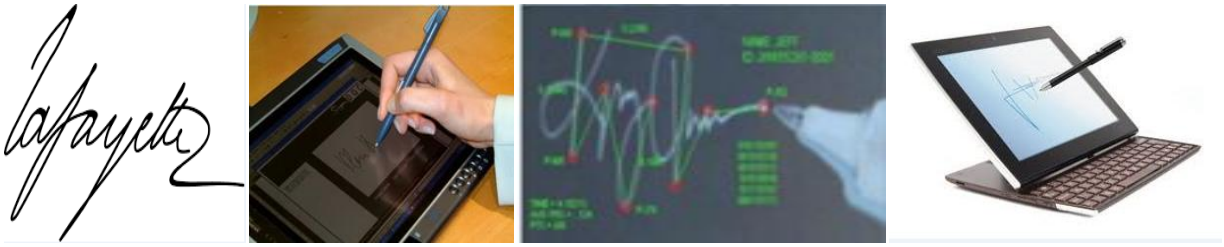

Figure 1.12 : La signature électronique.

Avantages et inconvénients d'identification basée sur la signature électronique [19] **:**

Avantages :

- Bonne acceptabilité.
- La signature peut être conservée.
- Facile à utiliser.
- Elle implique la responsabilité de l'individu.

Inconvénients :

- Sensibilité aux émotions de la personne.
- Besoin d'une tablette graphique.
- Non utilisable pour le contrôle d'accès en extérieur.

Analyse de la démarche : c'est une technique de reconnaissance biométrique utilisée à distance pour identifier et distinguer une personne grâce à sa manière de marcher et de bouger. En fait, chaque personne montre plusieurs traits tout en marchant tel que le maintien du corps, la position des genoux et les chevilles, la distance entre les deux pieds ce qui permet de l'identifier [25,26].

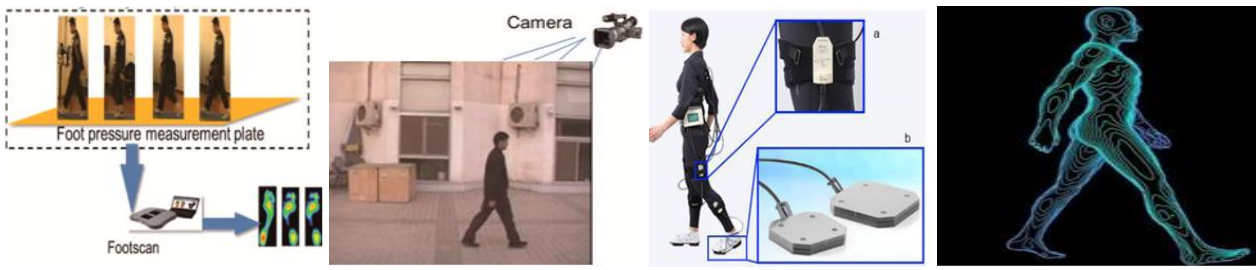

Figure 1.13 : Analyse de la démarche.

Avantages et inconvénients de l'analyse de la démarche [19]**:**

Avantages :

- Possibilité de suivre un individu pendant une longue durée.

Inconvénients :

- Faible acceptabilité par les gens.
- Elle dépend du choix des chaussures et la nature d'habillement.

La voix : la voix d'une personne peut être considérée comme la combinaison des caractéristiques morphologiques et comportementales. La voix est caractérisée par une intensité, une fréquence et une tonalité que l'on peut analyser par un microphone et à l'aide d'un traitement informatique. On peut isoler deux voix qui semblent être identiques pour l'oreille. L'aspect comportemental de la parole peut changer au cours du temps à cause de l'âge, l'état de santé et les émotions [27].

Figure 1.14 : Identification vocale.

Avantages et inconvénients d'identification vocale [19] :

Avantages :

- Non intrusive.
- Facilité de protéger le lecteur.
- Seule information utilisable via le téléphone.
- Impossible d'imiter la voix.
- Sécurité d'une conversation téléphonique.

Inconvénients :

- Taux élevé de faux de rejets et de fausses acceptations.
- Sensibilité aux bruits ambiants.

- La voix n'est pas un attribut permanent (elle change au cours du temps).
- Technologie biométrique vulnérable aux attaques.

1.9.3. Modalité biologiques :

Analyse de l'ADN : ADN (acide désoxyribonucléide) présent dans les cellules du corps, il est spécifique pour chaque individu. C'est une analyse du patrimoine génétique qui permet une identification à partir des cheveux, fragment de peau, d'une trace de sang et d'une goute de salive. De plus l'ADN contient plus d'information sur l'identité des personnes [12].

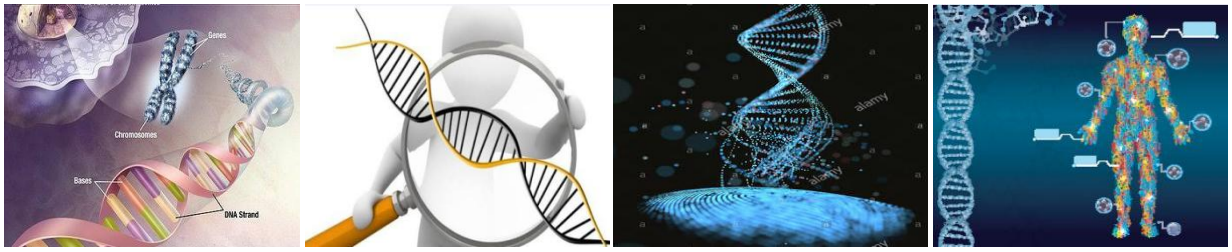

Figure 1.15 : Système de reconnaissance basé sur l'ADN.

Avantages et inconvénients de système de la reconnaissance d'ADN [19]:

Avantages :

- Unique et permanant.
- Possibilité de différencier les individus à haute précision.
- Facile à obtenir.

Inconvénients :

- Coûteux.
- Pour avoir les résultats, il faut attendre une longue durée.
- Facile à être volé.

La reconnaissance de thermographie faciale : une caméra infrarouge capte la quantité de chaleur émise par les différentes parties du visage qui caractérise chaque personne. Contrairement à la biométrie faciale, la capture peut se faire dans des états d'éclairages différents. Donc on peut l'utiliser dans l'obscurité ou de mauvaises conditions de visibilité [12,17].

Figure 1.16 : Thermo-gamme faciale.

Avantages et inconvénients de la thermo-gamme faciale [19] **:**

Avantages :

- Faire une différence entre les vrais jumeaux.

Inconvénients :

- Sensibilité aux émotions et à la température corporelle.
- Coûteuse.

1.10. Motivation 1 : pourquoi nous avons choisi la biométrie multimodale ?

Les systèmes biométriques uni-modaux ont des limitations dans la performance car ils sont basés sur le degré de correspondance entre les données biométriques comparées, qui ne permet pas une reconnaissance exacte d'un individu.

En effet, les systèmes biométriques sont souvent affectés par des problèmes comme le bruit du capteur, non universalité, manque d'individualité et la sensibilité aux attaques. Ainsi à causes de ces limitations, les taux d'erreurs associés aux systèmes biométriques uni-modaux sont élevés, ce qui les rend inacceptable dans un déploiement d'applications critiques de sécurité. Pour pallier à ces problèmes, les chercheurs ont essayé toujours de voir d'autres façons pour améliorer la rentabilité des systèmes biométriques par l'utilisation de plusieurs modalités biométriques dans le même système, on parle alors de la biométrie ***multimodale*** [28].

La biométrie multimodale consiste à combiner plusieurs systèmes biométriques. En effet, l'utilisation de plusieurs systèmes biométriques a pour but d'améliorer les performances de reconnaissance et de réduire certaines limitations des systèmes biométriques uni-modaux, comme l'impossibilité d'acquérir les données de certaines personnes ou la fraude

intentionnelle. Ces avantages apportés par la multimodalité aux systèmes biométriques « monomodaux » sont obtenus en fusionnant plusieurs systèmes biométriques [28].

1.11. Motivation 2 : pourquoi nous avons choisi de combiner la reconnaissance du visage avec la reconnaissance de la signature électronique parmi les autres modalités biométriques ?

Nous avons essayé de simuler le système biométrique utilisé pour le passeport algérien qui utilise : le visage, la signature et les empreintes des doigts. C'est pour cette raison, notre choix a été fait sur la combinaison de la modalité morphologique (visage) avec la modalité comportementale (signature électronique). Ce choix des deux modalités (visage et signature) n'est pas pris au hasard, mais dû à certains critères qui caractérisent ces deux modalités.

Tout d'abord, la modalité du visage est une technique plus commune et populaire. Elle reste la plus acceptable puisqu'elle correspond à ce que les humains utilisent dans l'interaction visuelle. La reconnaissance faciale est plus avantageuse par rapport aux autres méthodes, d'une part c'est une méthode non-intrusive c'est-à-dire elle n'exige pas la coopération du sujet (observation des individus à distance), et d'une autre part la disponibilité des équipements d'acquisition, leurs simplicités et leurs coût faibles (une simple caméra) [29].

Toutefois, l'authentification par le visage présente des limitations d'usage dues à plusieurs facteurs (changement d'éclairage, le vieillissement, les conditions de prise de vue, les variations des expressions faciales, …etc.) qui peuvent influencer sur les performances d'un système de reconnaissance faciale [30]. C'est pour cette raison on a ajouté une autre modalité biométrique (signature électronique) pour rendre le système plus performant en précision et en reconnaissance.

La reconnaissance de signature électronique est l'une des modalités biométriques les plus personnelles et les plus uniques (c.-à-d. que chaque personne a un style d'écriture unique). De plus, cette technique biométrique comportementale est depuis longtemps le moyen le plus utilisé dans les services postaux, pour authentifier les documents, les transactions financières et bancaires, et identifier des personnes [1]. La signature électronique est une méthode peu intrusive et bien acceptée par le public car elle est un geste commun pour tout le monde. L'avantage le plus important de la reconnaissance de signature est qu'elle est très résistante aux imposteurs [22].

La signature électronique peut aussi être utilisée comme une caractéristique complémentaire du visage dans un système biométrique multimodal afin d'améliorer d'une manière significative la précision de la reconnaissance.

1.12. Conclusion :

Dans ce chapitre, nous avons défini la biométrie et ses applications. Puis, nous avons décrit l'architecture et le principe de fonctionnement d'un système biométrique ainsi que les techniques de mesure de leurs performances. Par la suite, nous avons défini quelques modalités avec leurs avantages et leurs inconvénients.

Enfin, face aux nombreuses limitations des systèmes biométriques uni-modaux, on a trouvé que la fusion de plusieurs modalités biométriques dans un seul système est l'une des solutions pour améliorer la fiabilité de ces systèmes.

Dans le chapitre prochain, nous détaillons le principe de biométrie multimodale ainsi que la reconnaissance des formes.

Chapitre 02

La Biométrie Multimodale et la Reconnaissance des Formes

Chapitre 02 : la Biométrie Multimodale et la Reconnaissance des Formes

2.1. Introduction :

Nous allons décomposer ce chapitre en deux parties. Nous introduirons dans la première partie la biométrie multimodale qui utilise la combinaison de plusieurs systèmes biométriques ; dans notre cas, on a choisi de combiner la modalité du visage avec celle de la signature électronique. Ensuite, nous allons déterminer les différentes formes de la multimodalité, ainsi que les architectures qui peuvent être utilisées. Enfin, nous allons étudier la fusion des données avec ses divers niveaux.

Dans la deuxième partie, nous allons étudier la reconnaissance des formes, son concept, et nous présenterons brièvement le domaine de RdF et leurs centres d'intérêts. Ensuite nous donnerons un aperçu sur le processus d'un système de reconnaissance des formes et leurs approches.

L'objectif de ce chapitre est de proposer un système biométrique multimodal plus performant. Dans notre cas, on s'intéresse à la combinaison de la modalité du visage et celle de la signature électronique; la reconnaissance du visage et de la signature électronique relèvent du domaine de la reconnaissance des formes.

2.2. La biométrie multimodale :

Actuellement en biométrie, l'ajout d'une modalité à un système biométrique uni-modal, c'est l'ajout d'une nouvelle source d'information. Pour cette raison, les systèmes biométriques multimodaux permettent d'avoir une meilleure performance par rapport aux systèmes uni-modaux [1].

2.2.1. Définition de la biométrie multimodale :

La multimodalité est l'utilisation de plusieurs systèmes biométriques, par exemple l'utilisation de la biométrie de la signature avec la biométrie du visage. Elle consiste à combiner des données issues de plusieurs sources biométriques afin d'obtenir une décision meilleure que celle obtenue à partir de chacune des sources prises isolément. La combinaison de plusieurs systèmes biométriques a pour objectif d'en réduire certaines limitations des systèmes basés sur une seule modalité (systèmes uni-modaux) tout en améliorant la quantité

d'informations discriminantes de chaque personne et réduisant ainsi le risque d'impossibilité d'acquérir les données de certaines personnes, et obtenant un système robuste aux fraudes [28].

2.2.2. Types de fusion :

Il existe cinq types de fusion de traits biométriques qui dépendent du type de sources et de caractéristiques utilisées (voir **figure 2.1**) [31]:

a. **Systèmes multi-capteurs :** ce système correspond à l'utilisation de plusieurs capteurs pour acquérir une seule modalité biométrique. A titre d'exemple, l'acquisition d'une image 2D du visage s'effectue à l'aide d'une caméra classique, et la même acquisition en 3D en utilisant une caméra plus sophistiquée. Ou aussi l'utilisation d'un capteur optique et un capteur thermique pour la reconnaissance de l'empreinte digitale.
b. **Systèmes multi-instances ou multi-unités :** c'est une classe qui désigne l'acquisition de la même modalité biométrique par plusieurs unités ou instances. Par exemple, un système qui utilise l'oreille droite et l'oreille gauche, l'acquisition de plusieurs images de visage avec des changements de pose, d'expression ou d'illumination.
c. **Systèmes multi-algorithmes ou multi-classifieurs :** c'est le type le plus classique des autres types. Dans ce cas l'utilisation d'un seul capteur est suffisante pour l'extraction des caractéristiques biométriques par différentes algorithmes. Par exemple pour traiter la même image d'empreinte digitale on utilise deux algorithmes, l'un pour analyser la texture du doigt et l'autre pour l'extraction des minuties.
d. **Systèmes multi-échantillons :** dans ce type, un même capteur est utilisé pour obtenir plusieurs représentations complémentaires d'une seule modalité biométrique, c'est le cas de la reconnaissance faciale en se basant sur les images du visage de face et selon les profils droit et gauche pour tenir compte des variations de la pose faciale.
e. **Systèmes multimodaux ou multi-caractères :** c'est la combinaison de plusieurs modalités biométriques d'une même personne pour améliorer la performance d'un système. Ces types de système nécessitent différents capteurs ainsi que différents algorithmes dédiés à chaque modalité biométrique. Le coût de la réalisation de ces systèmes est généralement élevé.

Toutes les formes de systèmes multimodales présentent l'avantage de traiter plusieurs informations biométriques et peuvent ainsi réduire le problème de la non-universalité et le problème de la résistance aux fraudes. Les quatre premiers systèmes (multi-capteurs, multi-

instances, multi-algorithmes et multi-échantillons) combinent des informations issues d'une seule et même modalité biométrique ce qui ne permet pas de tenir compte de toutes les limitations des systèmes biométriques uni-modaux, contrairement aux systèmes multimodaux.

En effet, les cinq types de la multimodalité peuvent être aussi combinés entre eux. Par exemple, une reconnaissance de l'identité par le visage et l'oreille peut être effectuée avec différents algorithmes, de même une acquisition multi-capteurs peut être opérée sur le visage et l'oreille [32].

Systèmes multi-instances

Visage

Système multi-caractères

Signature électronique

Systèmes biométriques multimodaux

Systèmes multi-échantillons

Oreille droite

Oreille gauche

Systèmes multi-capteurs

Capteur d'empreinte digitale optique

Capteur d'empreinte digitale thermique

Systèmes multi-algorithmes

Plusieurs algorithmes d'extraction de caractéristiques sont utilisés pour la même donnée biométrique (exemple : algorithme d'analyse de texture et de minuties).

Figure 2.1 : Les différents types de fusion des traits biométriques.

2.2.3. Architectures d'un système biométrique multimodal :

Les systèmes biométriques multimodaux ont besoin d'effectuer l'acquisition et le traitement de plusieurs données selon deux architectures différentes l'une en série et l'autre en parallèle. Dans ce qui suit nous allons expliquer brièvement les deux architectures [1]:

a. **Architecture en parallèle :** c'est la plus utilisée car elle permet l'acquisition et le traitement des données en même temps (simultanément) (voir **figure 2.2**).

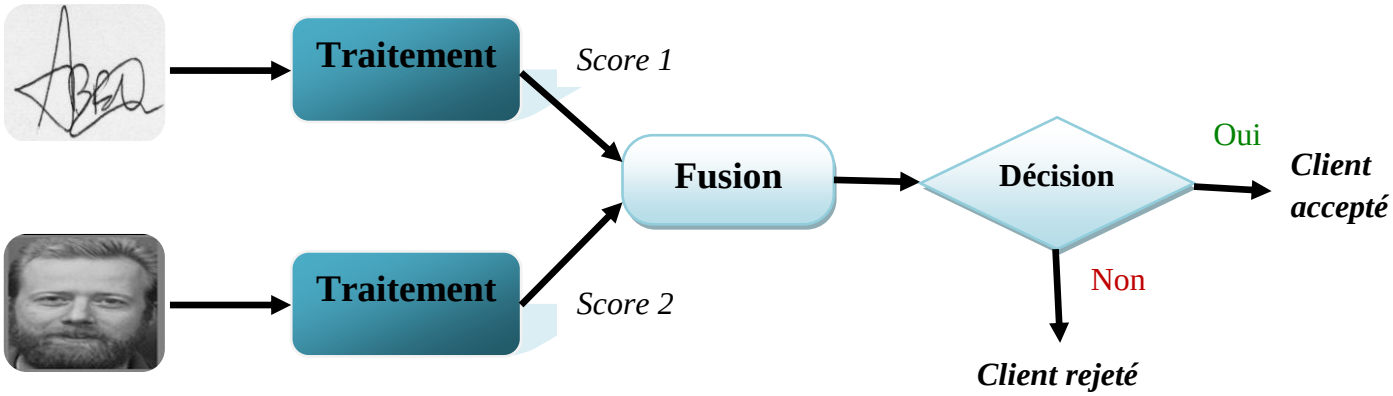

Figure 2.2 : Architecture de fusion en parallèle.

b. **Architecture en série (séquentielle) :** c'est l'acquisition et le traitement des données d'une façon successive (voir **figure 2.3**).

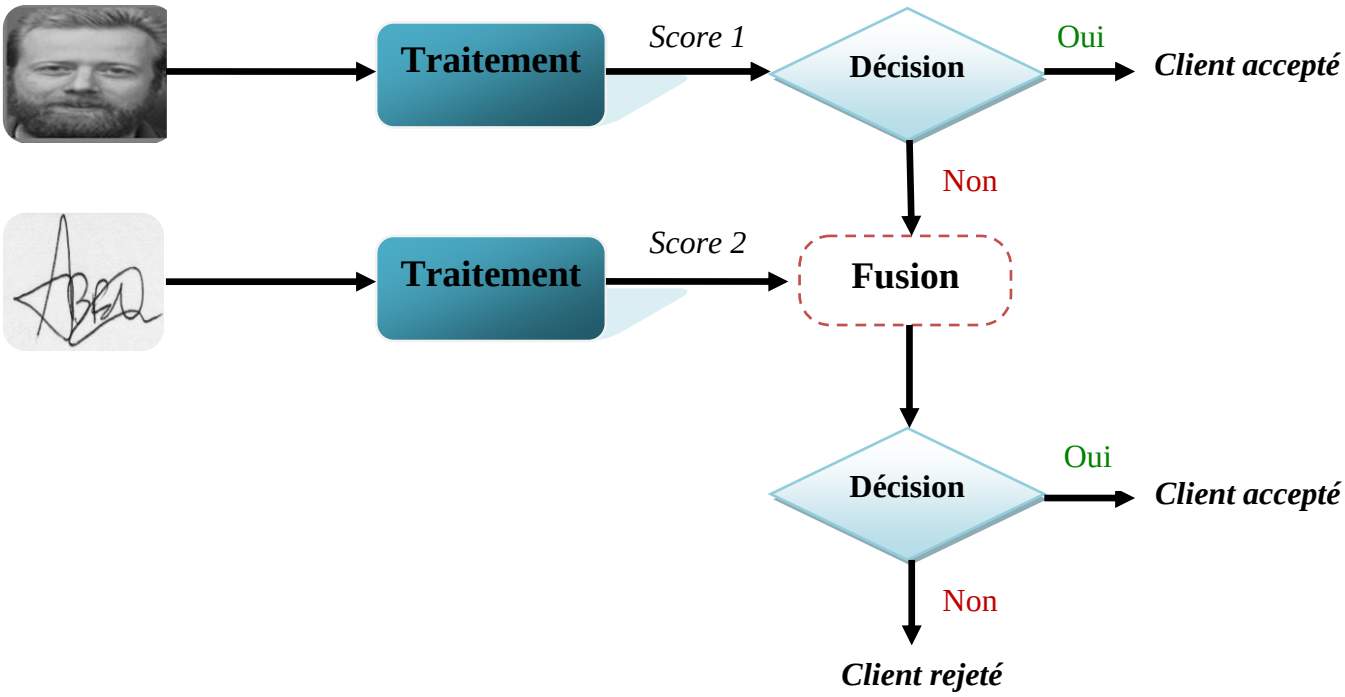

Figure 2.3 : Architecture de fusion en série.

La différence entre un système multimodal en parallèle et autre en série réside dans le fait qu'à l'issue de premier c'est un système qui procède à l'ensemble des acquisitions avant de prendre une décision tandis que dans le deuxième système on obtient un score de similarité de chaque acquisition.

2.2.4. Les niveaux de fusion :

La combinaison de plusieurs systèmes biométriques peut se faire à quatre niveaux différents (voir **figure 2.4**) [33]: au niveau des données, au niveau des caractéristiques extraites, au niveau des scores de comparaison ou au niveau des décisions.

On peut classer ces quatre niveaux de fusion en deux grandes familles qui sont :

2.2.4.1. La fusion pré-classification (avant comparaison) :

Ce type de fusion correspond à la fusion des informations issues de plusieurs données biométriques au niveau du capteur et au niveau des caractéristiques extraites par le module d'extraction de caractéristiques.

a. **Fusion au niveau du capteur :** la fusion au niveau du capteur peut se faire uniquement si les diverses captures sont des instances du même trait biométrique obtenu à partir de plusieurs capteurs compatibles entres eux ou plusieurs instances du même trait biométrique obtenu d'un seul capteur.
b. **La fusion au niveau des caractéristiques :** ce type de fusion concerne la combinaison de différents vecteurs de caractéristiques extraites après diverses phases de traitement et l'analyse des mesures.

Les méthodes de fusion pré-classification sont assez peu utilisées, car elles posent un certain nombre de contraintes qui ne peuvent être remplies que dans certaines applications très spécifiques.

2.2.4.2. La fusion post-classification (après la comparaison) :

Cette fusion peut se faire au niveau des scores obtenus à partir des modules de comparaison ou au niveau des décisions.

a. **La fusion au niveau des scores :** c'est un type de fusion largement utilisé car elle peut être appliquée à tous les types de systèmes multimodaux. Dans ce type on effectue une combinaison des scores obtenus par les différents systèmes. La fusion de scores consiste à la classification : ***oui*** ou ***non*** pour la décision finale d'un vecteur de nombres réels dont la dimension est égale au nombre des sous-systèmes.
   Généralement, il existe plusieurs méthodes de normalisation de score qui sont nécessaire pour rendre les scores dans le même intervalle avant de les combiner.

   Les méthodes de combinaisons des scores sont des méthodes très simples dont l'objectif est d'obtenir un score final $\boldsymbol{S}$ à partir des $\boldsymbol{N}$ scores disponibles si pour $\boldsymbol{i=1}$ à $\boldsymbol{N}$ issus de $\boldsymbol{N}$ systèmes. Les méthodes les plus utilisées sont la moyenne, le produit, le minimum, le maximum ou la médiane [34].
   La moyenne : combiner les scores par la moyenne se fait par la relation suivante :

$$\boldsymbol{S = \frac{1}{N} \sum_{i=1}^{N} Si \, , i = 1 \ldots N}$$

Le produit : combiner les scores par le produit consiste à multiplier tous les scores tel que :

$$\boldsymbol{S = \prod_{i=1}^{N} Si}$$

Le maximum des scores : la combinaison des scores par la règle de maximum se fait par la façon suivante :

$$\boldsymbol{S = max(Si)}$$

Le minimum des scores : combiner les scores par le minimum se fait par la relation suivante :

$$\boldsymbol{S = min(Si)}$$

La médiane : la médiane est définie par la relation suivante :

$$\boldsymbol{S = med(Si)}$$

Toutes ces méthodes sont des méthodes simples. Il existe également des méthodes un peu plus évoluées de combinaison qui nécessitent le réglage de paramètres comme **la somme pondérée** qui est définie par la relation mathématique suivante :

$$\boldsymbol{S = \sum_{i=1}^{N} \omega_i S_i}$$

La somme pondérée permet de donner des poids différents $\boldsymbol{\omega_i}$ à chacun des systèmes en fonction de leur performance individuelle dans le système multimodal.

Cependant, toutes ces méthodes ne peuvent pas être utilisées que si tous les scores issus des sous-systèmes sont cohérents entre eux (homogènes). Pour cela l'étape de normalisation des scores est nécessaire avant de les combiner.

b. La fusion au niveau des décisions : cette fusion est souvent utilisée en raison de sa simplicité. En effet, chaque système biométrique fournit une décision binaire sous forme ***oui*** ou ***non*** que l'on peut représenter par **0** et **1**, le système de fusion des décisions va prendre une décision finale en fonction de **0** et **1**.

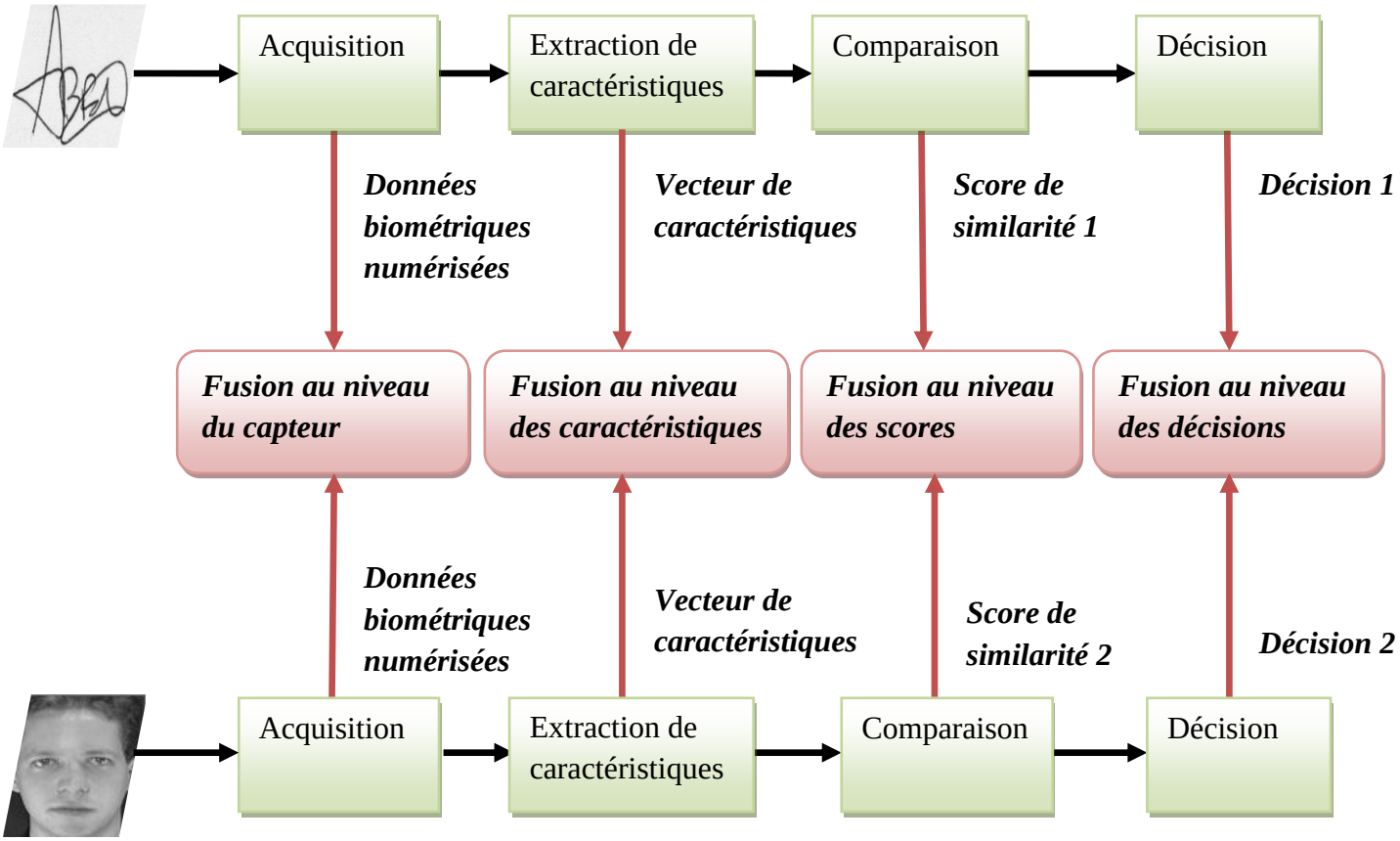

Figure 2.4 : Les différents niveaux de fusion d'un système biométrique.

Un système biométrique est essentiellement un système de reconnaissance des formes qui utilise les données biométriques d'un individu. Dans ce qui suit nous allons détailler le principe et le processus de la reconnaissance des formes.

2.3. La reconnaissance des formes :

2.3.1. Définition de la reconnaissance des formes (RdF):

La reconnaissance des formes (RdF) est une discipline entre les mathématiques et l'informatique, elle désigne un ensemble de techniques et méthodes qui servent à identifier des motifs à partir des données brutes afin de prendre une décision qui dépend de la catégorie attribuée à ce motif. Elle est considérée comme une branche de l'intelligence artificielle qui fait largement appel aux techniques d'apprentissage automatique et aux statistiques [35].

Les formes à reconnaitre sont souvent des formes géométriques ou descriptibles par des formules mathématiques, telles que les cercles, les courbes,…etc. Elles peuvent aussi de nature plus complexe comme les chiffres et les lettres [36]. Comme elles peuvent être de contenu visuel (visage, oreille, empreinte digitale,…) ou sonore (reconnaissance de parole), d'images médicale (rayon X, IRM) ou multi spectrales (images satellitaires).

2.3.2. Champs d'applications de RdF :

Les applications de la reconnaissance des formes sont nombreuses et couvrent un champ d'activité large. Dans ce qui suit nous énumérons quelques domaines d'applications :

- **Finances :** les systèmes de reconnaissance des formes sont utilisés pour la détection de transactions bancaires frauduleuses. Elle est aussi utilisée pour classer les consommateurs selon les produits qu'ils sont susceptible d'acheter [37].
- **Usinage :** les systèmes de reconnaissance des formes sont utilisés pour classer les paramètres selon la qualité des produits qu'ils sont susceptibles de générer [38].
- **Energie :** les systèmes de RdF sont utilisés pour prévoir la consommation électrique (réduite, normale, élevée) permettant ainsi aux clients de réduire leur consommation si nécessaire [39].
- **Biométrie :** la reconnaissance vocale et rétinienne sont des exemples d'applications typiques de la reconnaissance des formes pour l'authentification. La vérification des signatures est aussi très populaire.
- **Médical :** les systèmes de reconnaissance des formes permettent le repérage des cellules ou d'événement anormaux (tumeurs) dans les images et les signaux médicaux et elle est aussi utilisée pour le diagnostic médical.

2.3.3. Principe de la RdF :

Son principe est basé généralement sur la classification de nouvelles formes par l'utilisation d'un classifieur qui permet de générer une fonction d'appartenance pour chaque classe. Ainsi la classification d'un nouveau point peut se faire en fonction de la valeur d'appartenance qu'il obtient par rapport à chaque classe [40].

On considère $\boldsymbol{M}$ formes, chacune définie par un ensemble de $\boldsymbol{P}$ paramètres regroupés dans un vecteur de forme $\boldsymbol{Y}$ avec un espace de représentation $\boldsymbol{R^P}$ (voir **figure 2.5**). Les formes-types constituent des points représentatifs de l'espace de représentation. Chaque forme-type est représentée par une zone géométrique qui s'appelle « classe » en RdF. Le principe général

est d'observer des formes de M classes différentes. L'ensemble **Ω** définit l'espace de décision avec : **Ω= {wi, i=1…N}.** Le but est de construire des frontières réalisant une partition de façon à affecter un nouveau vecteur forme à l'une des classes $w_1 \ldots w_N$. Cette association désigne l'opération de classement ou discrimination [41].

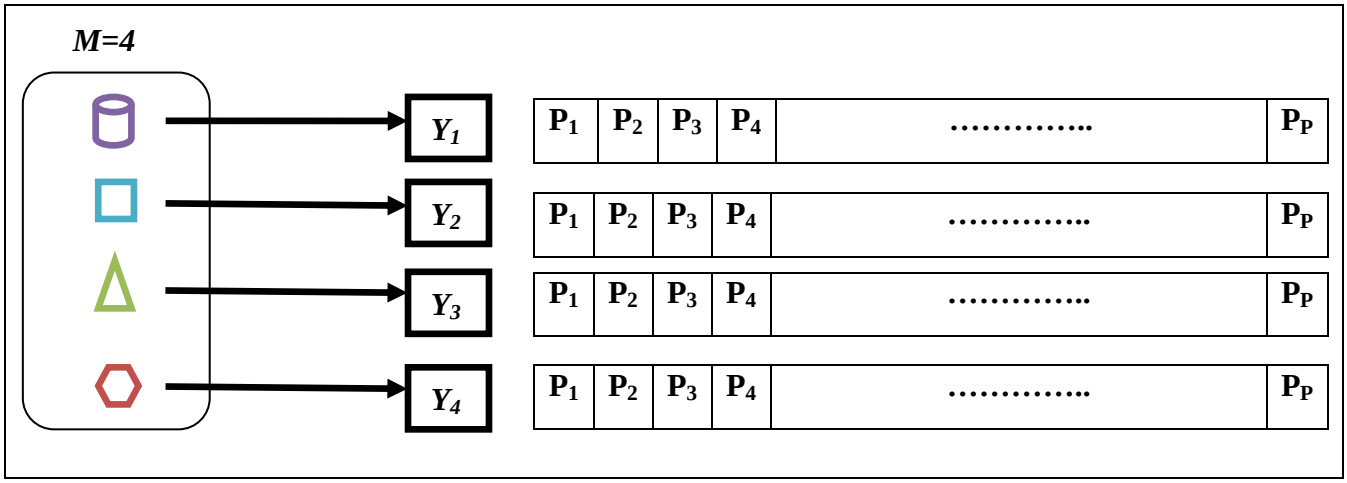

Figure 2.5 : Exemple d'un espace de représentation des formes.

2.3.4. Les méthodes de RdF :

Il est généralement admis de classer les méthodes de reconnaissances des formes en deux méthodes suivantes [40]:

a. **Les méthodes paramétriques :** qui considèrent l'ensemble d'apprentissage comme des données indépendantes, toutes distribuées selon la même loi de probabilité, comme le fait le classifieur Bayésien. Cette hypothèse n'est pas souvent valide dans le cas d'applications réelles.
b. **Méthodes non paramétriques :** qui génèrent les fonctions d'appartenance des classifieurs soit en estimant la fonction de densité de probabilité conditionnelle pour chaque classe comme les méthodes de K-plus proches voisins et soit en construisant par apprentissage, les régions de décision comme les réseaux de neurones et les fonctions potentielles.

2.3.5. Construction d'un système de reconnaissance des formes :

Un système de RdF se décompose généralement en cinq étapes séquentielles [41] (voir **Figure 2.6**). Le but de ces étapes est de réduire la quantité de données à manipuler, partant de l'information originale qui fait partie du monde réel jusqu'à arriver à sa description symbolique dans l'espace d'interprétation en passant par l'espace de représentation ou on extrait les primitives pertinentes.

Chaque étape du processus de RdF dépend des étapes précédentes. Dans ce qui suit nous allons détailler ce processus :

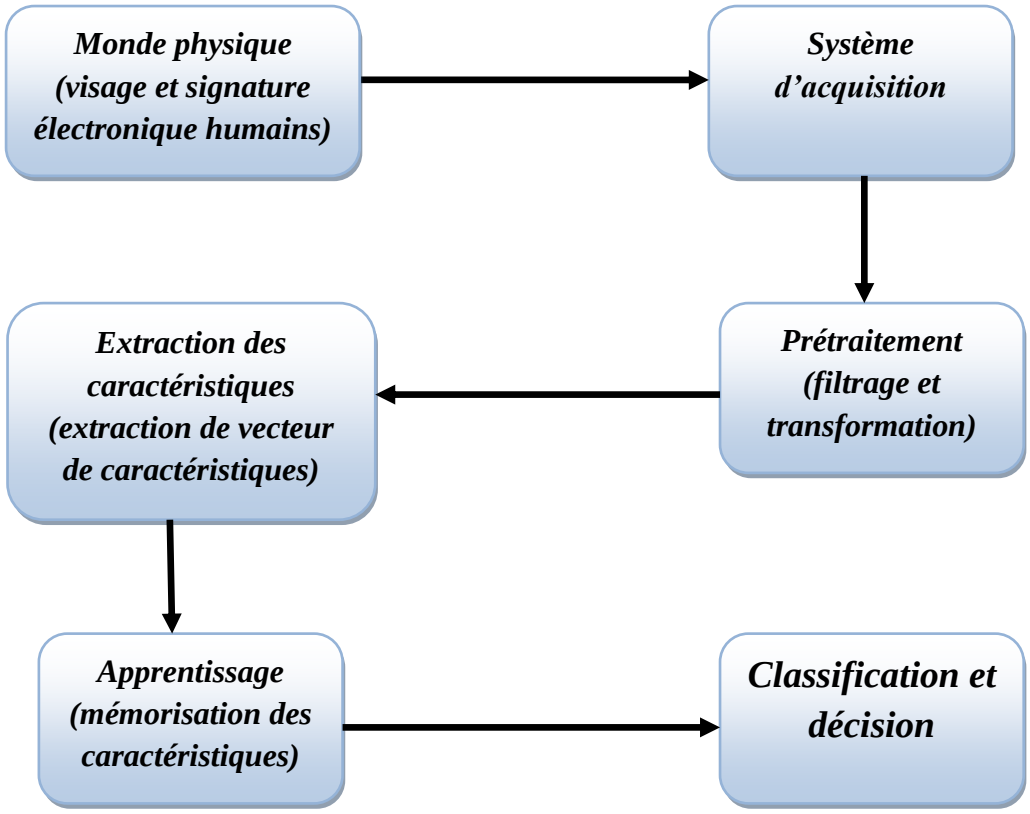

Figure 2.6 : Schéma des étapes principales d'un système de reconnaissance des formes.

2.3.5.1. Monde physique (extérieur) :

Il est considéré comme une étape préparatoire de tout processus de reconnaissance des formes. C'est un espace analogique de dimension infinie appelée espace des formes. Les objets dans cet espace, sont décrits de différentes façons avec plusieurs propriétés. La loi de

passage au monde discret nécessite une sélection et par conséquent une certaine simplification. Cette étape dépend de trois paramètres essentiels : l'éclairage, la variation de posture et l'échelle [42].

2.3.5.2. Système d'acquisition :

La capture de données (signature, visage, empreintes,…etc.) est la première étape dans le processus de RdF. Il faut tout d'abord acquérir l'information originale (la forme à reconnaitre) en utilisant des capteurs spécifiques (appareil photo pour le visage et le capteur d'oreille), et de la convertir à des grandeurs numériques pour qu'elle soit traitable par l'échantillonnage et quantification.

Dans cette phase l'image est bruitée ce qui nécessite une phase de prétraitement.

2.3.5.3. Prétraitement :

Afin d'optimiser les performances du système de RdF (présence de bruit), le prétraitement semble être une solution concernant le filtrage (filtre médian) et la transformation des données qui permettent d'obtenir des données plus adaptées à la recherche de caractéristiques informatives. Le traitement de l'image s'effectue par la modification de l'histogramme (égalisation et normalisation), l'amélioration des contrastes, extraction de contour et luminosité. Ce prétraitement permet une préparation aux phases suivantes [40].

2.3.5.4. Extraction des caractéristiques :

Cette étape est considérée comme une base de tout système de RdF. A partir d'une représentation physique complexe (signal, image) d'un objet, la phase d'extraction de caractéristiques permet d'obtenir un vecteur caractérisant cet objet. Ce vecteur est couramment obtenu à partir d'opérations de prétraitement puis d'analyses et de mesures.

Cette étape est généralement délicate en RdF car il est nécessaire de sélectionner les différentes opérations qui définissent les différentes composantes du vecteur.

L'introduction d'un étage de caractérisation des formes a donc permis de rendre les systèmes de classification plus efficaces aux transformations et aux dégradations. Il existe deux classifications concernant l'extraction des caractéristiques : les méthodes globales et les méthodes locales [10] (voir **Figure 2.7**):

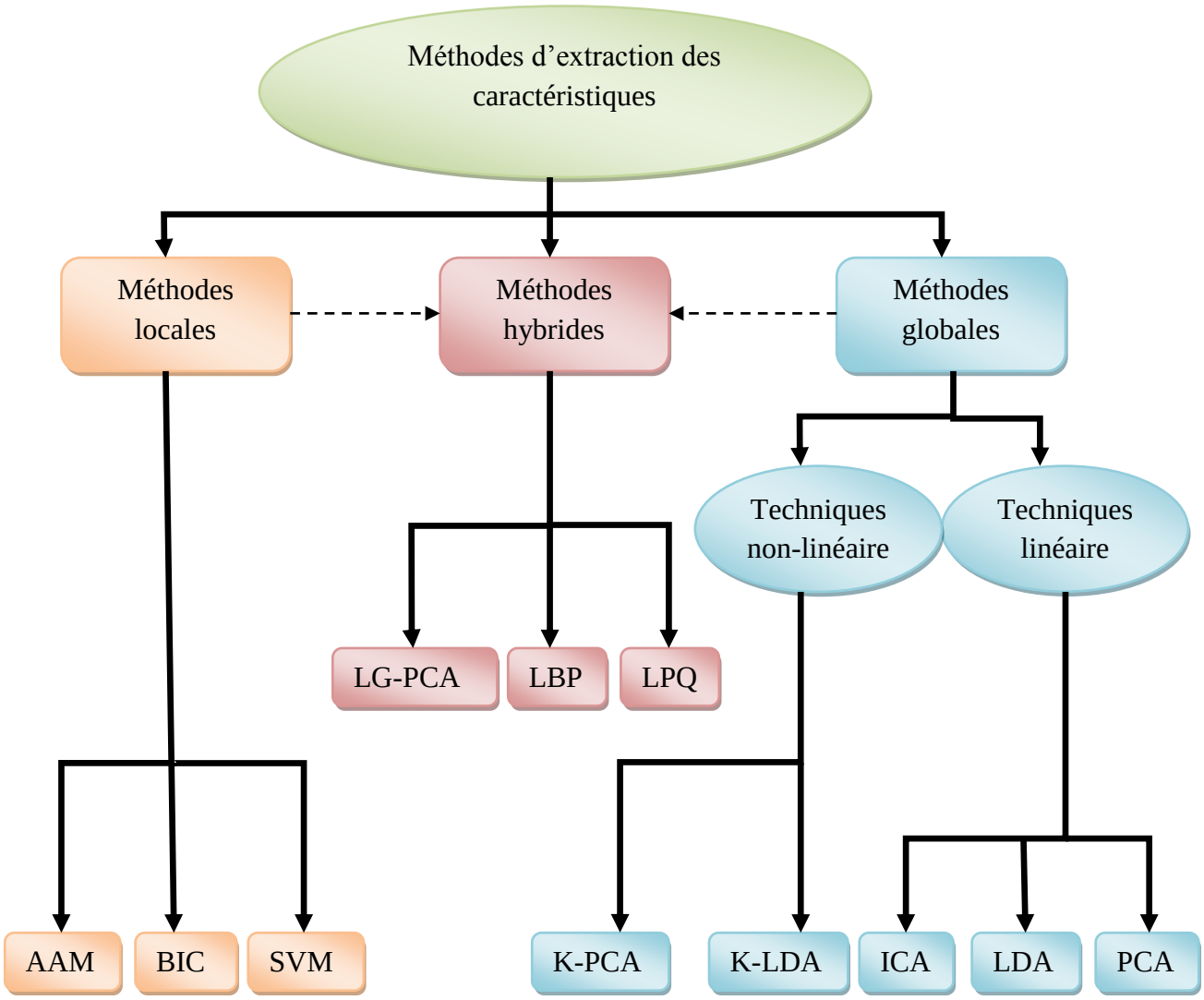

Figure 2.7 : Principales algorithmes utilisés en reconnaissance des formes [10].

a. <u>Méthodes géométriques (locales)</u> :

Cette approche utilise des descripteurs de texture locale. Ce descripteur permet de convertir l'information au niveau du pixel en forme utile qui capture le contenu le plus important avec insensibilité aux variations causées par l'environnement [43].

Ces méthodes locales consistent à appliquer des transformations en des endroits spécifiques de l'image ce qui nécessite donc une connaissance à priori sur les images. Toutes

ces méthodes ont l'avantage de pouvoir modéliser plus facilement les variations de pose, d'éclairage et d'expression [44]. Parmi les opérateurs utilisés dans cette approche on trouve :

- EBGM (Elastic Bunch Graph Matching)
- HMM (Hidden Markov Models)
- Eigen Objects (EO)

b. Méthodes statistiques (globales) :

Les méthodes globales sont basées généralement sur des techniques d'analyse statiques bien connues. Dans ces méthodes les images sont traitées de manière globale et sont transformées en vecteurs plus faciles à manipuler dont la taille de vecteur est représentée par le nombre total des pixels de l'image traitée. L'avantage principal de ces méthodes est qu'elles sont rapides à mettre en œuvre et les calculs de base sont d'une complexité moyenne. Par ailleurs, elles sont très sensibles aux variations de pose, d'éclairement et d'expression faciale puisque un certain nombre de variation des conditions de l'environnement ambiant provoque des changements inévitables dans les valeurs de pixels qui sont traités directement [10].

Les méthodes de cette approche utilisent un autre espace de représentation qui s'appel un sous-espace dans le but de réduire le nombre de pixels par la sélection des informations utiles et l'élimination des redondances. Parmi les méthodes d'extraction employées dans cette approche nous citons [45]:

- Analyse des composantes principales (ACP) (PCA)
- Analyse discriminante linéaire (ADL ou LDA)
- Analyse indépendante des composantes (ICA)

c. Méthodes hybrides :

Ces méthodes concernent la combinaison des caractéristiques globales et locales afin d'améliorer la stabilité de la performance de reconnaissance lors de changement de pose, d'éclairement et d'expression faciale en cas de visage [10]. Parmi les opérateurs hybrides utilisés dans la RdF, on peut citer :

- **Algorithme log Gabor PCA (LG-PCA):** qui effectue une convolution avec des ondelettes de Gabor orientées autour de certaines caractéristiques de la modalité afin de créer des vecteurs contenant la localisation et la valeur d'amplitudes énergétiques locales, ces vecteurs sont ensuite envoyés dans un algorithme PCA afin de réduire la dimension des données [10].
- **Motif binaire local (LBP) :** l'opérateur LBP (en anglais : local binary pattern) est l'un des descripteurs d'analyse de texture les plus performants. Il a été proposé à la fin des années 90 par Ojala et al [46] dans le but de caractériser la texture d'une image. Ses avantages se résument dans son invariance pour les changements monotones de l'intensité (niveaux de gris) et son efficacité de calcul [46].

Principe de LBP :

Son principe de base : le motif LBP est une mesure de texture invariante à l'échelle de gris. Son concept est simple, il propose d'assigner un code binaire à un pixel en fonction de son voisinage. Ce code est calculé par un seuillage d'un voisinage de 3*3 de chaque pixel avec le niveau de gris du pixel central. La **Figure 2.8** présente le processus de calcul du code LBP. Afin de générer un motif binaire, tous les voisins prendront alors une valeur 1 si leur valeur est supérieure ou égale à la valeur du pixel central sinon le résultat est mis à zéro. Le code LBP du pixel central est ensuite obtenu en multipliant les résultats par des poids donnés par les puissances de deux (2^{poids}) et en les résumant ensemble. On obtient alors pour toute l'image, des pixels dont l'intensité se situe entre 0 et 255 comme dans une image à 8 bits ordinaire. On peut choisir comme descripteur de texture un histogramme de dimension 255 [45].

Le calcul des codes LBP peut être facilement effectué en un seul balayage à travers l'image. La valeur du code LBP d'un pixel (X_c, Y_c) est donnée comme suit [43] :

$$\boldsymbol{LBP^{P,R}(X_c, Y_C) = \sum_{n=1}^{P} U(g_i{}^{P,R} - g_c)2^{i-1}}$$

Avec :

$\mathbf{X_c}$ et $\mathbf{Y_c}$: sont les coordonnées du pixel central.

$\boldsymbol{g_i{}^{P,R}}$ Et $\boldsymbol{g_c}$: sont respectivement les niveaux de gris d'un pixel voisin et du pixel central.

U : la fonction de seuillage qui est définie comme suit :

$$U(x) = \begin{cases} \mathbf{1} & \boldsymbol{si\ x \geq 0} \\ \mathbf{0} & \boldsymbol{autrement} \end{cases}$$

Les occurrences des codes LBP dans l'image sont collectées dans un histogramme. La classification est ensuite effectuée en calculant les similitudes d'histogramme.

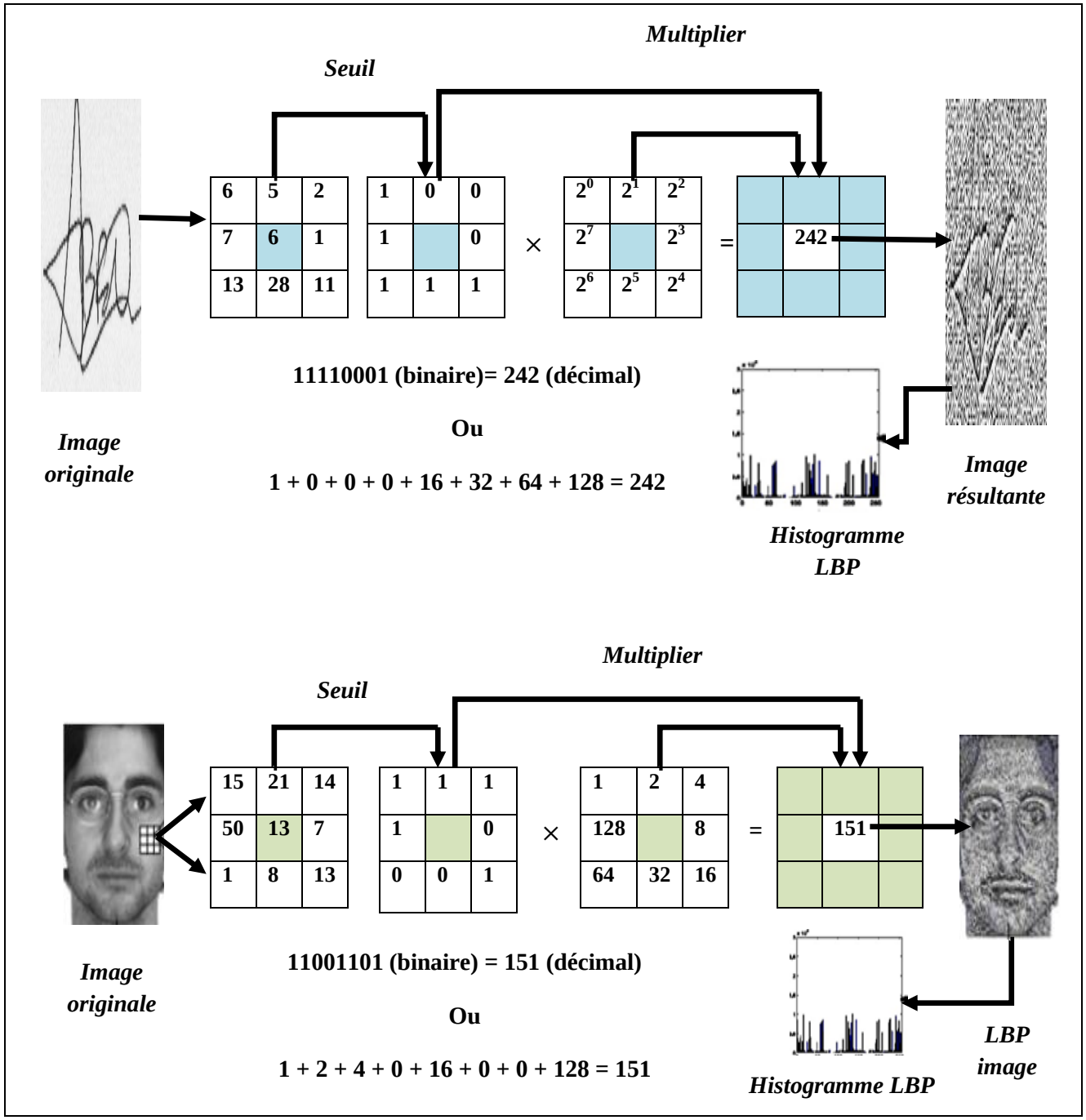

Figure 2.8 : Exemple de calcul de l'opérateur LBP appliqué à une image de signature et du visage.

La notation (P, R) est généralement utilisée pour les voisinages de pixel pour se référer à P points d'échantillonnage sur un cercle de rayon R comme indiqué sur la **Figure 2.9** [43]

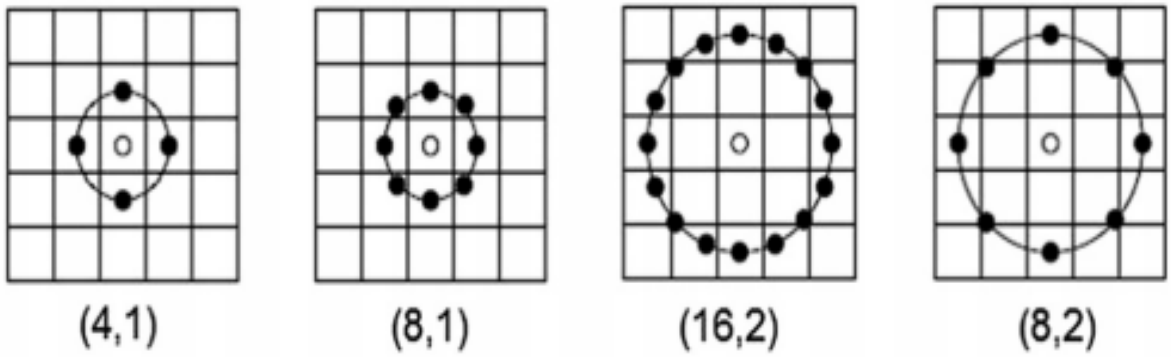

Figure 2.9 : Exemple de traitement de l'opérateur LBP avec des voisinages (P, R) différents.

2.3.5.5. Apprentissage :

C'est une étape où on fait apprendre les individus au système, elle consiste à mémoriser les paramètres après la phase d'extraction de caractéristiques dans une base de données bien ordonnée pour faciliter la phase de reconnaissance et la prise d'une décision. Il existe deux types d'apprentissage qui sont les suivants [40] :

a. **Apprentissage supervisé :** les méthodes supervisées utilisent les formes connues, ça veut dire l'ensemble d'apprentissage pour construire un classifieur qui sépare au mieux les différentes classes connues pour minimiser l'erreur de classification. Le modèle de chaque classe est alors représenté par une fonction d'appartenance qui détermine la valeur d'appartenance d'une forme à une classe.
b. **Apprentissage non supervisé :** il est basé sur des fonctions de similarité. Quand des formes aux caractéristiques similaires apparaissent elles sont classifiées dans la même classe et par ailleurs quand leurs caractéristiques sont différentes une nouvelle classe est crée par le classifieur.

2.3.5.6. La décision :

C'est la dernière phase de tout le système de RdF qui permet de déterminer l'identité d'une personne qui se base sur le degré de correspondance entre les caractéristiques biométriques extraites et les modèles stockés.

La décision repose sur la définition de trois règles essentielles : la classification, les distances et K-plus proches voisins (K-NN)

- **La classification** : cette phase est le noyau de tout système de RdF par l'utilisation des paramètres obtenus lors de l'apprentissage, le classifieur assigne chaque forme inconnue sa ou ses formes les plus probables. Le type d'une méthode de classification se divise généralement en deux familles : le monde supervisé et le monde non supervisé. Si l'on dispose d'un ensemble de points étiquetés on parle d'une classification supervisée. Dans le cas contraire on effectue une classification non supervisée qui s'appelle une classification automatique.

Parmi les méthodes de classification supervisée la plus classique est la plus utilisée c'est l'algorithme des « K-plus proches voisins (KPPV) ou K-NN (K Nearest Neighbors) ».

- **K-plus proche voisins ou (K-NN) (Nearest Neighbors en anglais) :**

  Les méthodes floues basées sur les K plus proches voisins n'imposent pas la forme des classes et sont uniquement fondées sur la distance entre les éléments dans la classe. Elles proposent des fonctions d'appartenance aux classes. Différentes distances peuvent être utilisées dans ces méthodes (euclidienne, city-block…).

  L'optimisation de l'algorithme de recherche des Kppv s'effectue selon deux principes soit par recherche rapide des distances, soit par réduction du nombre de points dans l'ensemble d'apprentissage.

- **Les distances :**

  Lorsqu'on souhaite comparer deux vecteurs de caractéristiques issus du module d'extraction de caractéristiques d'un système biométrique, on peut effectuer soit une mesure de ressemblance, ou bien une mesure de distance (divergence) [10].

  La première catégorie des distances est constituée de distances euclidiennes et sont définies à partir de la distance de Minkowski d'ordre $\boldsymbol{p}$ dans un espace euclidien $\boldsymbol{R^N}$, avec $\boldsymbol{N}$: c'est le déterminant de la dimension de l'espace euclidien [42].

  On considère deux vecteurs : $X = (X_1, X_2, \ldots, X_N)$ et $Y = (Y_1, Y_2, \ldots, Y_N)$

La distance de Minkowski d'ordre **P** notée $\mathbf{L_P}$ est définit par :

$$\boldsymbol{L_P = \left(\sum_{i=1}^{N} |X_i - Y_i|^P \right)^{1/p}}$$

C'est à partir de cette formule on peut calculer la distance dans l'espace original des images comme suit :

c. Distance City-Block : pour **P=1** on obtient la distance City-Block :

$$L_1(X,Y) = \sum_{i=1}^{N} |X_i - Y_i|$$

d. Distance euclidienne : pour **P=2** on obtient la distance euclidienne :

$$L_2(X,Y) = \sqrt{\sum_{i=1}^{N} |X_i - Y_i|^2}$$

2.4. Conclusion :

Nous avons divisé ce chapitre en deux patries. Dans la première partie, nous avons abordé la multimodalité qui fournit une alternative aux systèmes biométriques uni-modaux afin d'améliorer leurs performances mais aussi de limiter certaines contraintes liées à l'utilisation d'une seule modalité biométrique. Ensuite, nous avons déterminé les différentes formes de la multimodalité, ainsi que les architectures qui peuvent être utilisées. Enfin, nous avons étudié la fusion des données avec ses divers niveaux.

Dans la deuxième partie, nous avons étudié la reconnaissance des formes ainsi que son concept et nous avons présenté brièvement le domaine de RdF et leurs centres d'intérêts. Ensuite nous avons détaillé le processus de système de reconnaissance des formes depuis l'acquisition des données jusqu'à la prenne de la décision. Nous avons aussi essayé d'exprimer la relation entre la RdF et la biométrie.

Dans le chapitre prochain, nous allons mettre en œuvre un système de reconnaissance des formes pour notre application qui se base sur la combinaison de deux modalités (visage et la signature électronique) pour identifier des personnes. Ensuite, nous interprétons les résultats de cette application.

Chapitre 03

Etude Expérimentale & Résultats

Chapitre 03 : Etude Expérimentale & Résultats

3.1. Introduction :

Dans le chapitre précédent, nous avons parlé dans la première partie sur la multimodalité avec ses différentes formes et architectures; dans notre cas, nous sommes basés sur la fusion de la modalité du visage et la signature électronique. Ce qui concerne la deuxième partie, nous avons présenté le concept de la reconnaissance des formes avec son processus en détails.

Dans ce dernier chapitre, nous allons implémenter le modèle étudié (fusion de la modalité du visage avec celle de la signature électronique) et la mise en évidence d'un système biométrique multimodal. Puis nous présenterons les résultats obtenus et les outils utilisés en montrant l'efficacité du descripteur de texture local (LBP) que nous avons décrit précédemment.

3.2. Système de reconnaissance biométrique implémenté (visage & signature) :

Notre travail consiste à réaliser un système d'identification biométrique des personnes basé sur la fusion de deux données biométriques (signature électronique et le visage). L'extraction de caractéristiques de ces modalités est basée sur le calcul de la valeur LBP pour réduire la dimension de chaque modalité.

Chaque système de reconnaissance biométrique soit du visage ou de signature électronique doit avoir une étape d'apprentissage durant laquelle nous créons une base de données des personnes connues. Pour ce faire, un système automatique contient deux modes de fonctionnement. Le premier mode c'est l'enrôlement (apprentissage) qui consiste à extraire les éléments caractéristiques pour chaque personne puis les mettre sous forme d'un vecteur de caractéristiques. Ces derniers sont associés par une étiquette d'identité pour être stocker dans une base de données. Le deuxième mode est l'identification qui sert à reconnaitre un individu grâce à sa signature ou son visage, ceux qui veut dire retrouver l'identité associée à l'image.

Le système de reconnaissance que nous avons proposé est montré dans le schéma suivant :

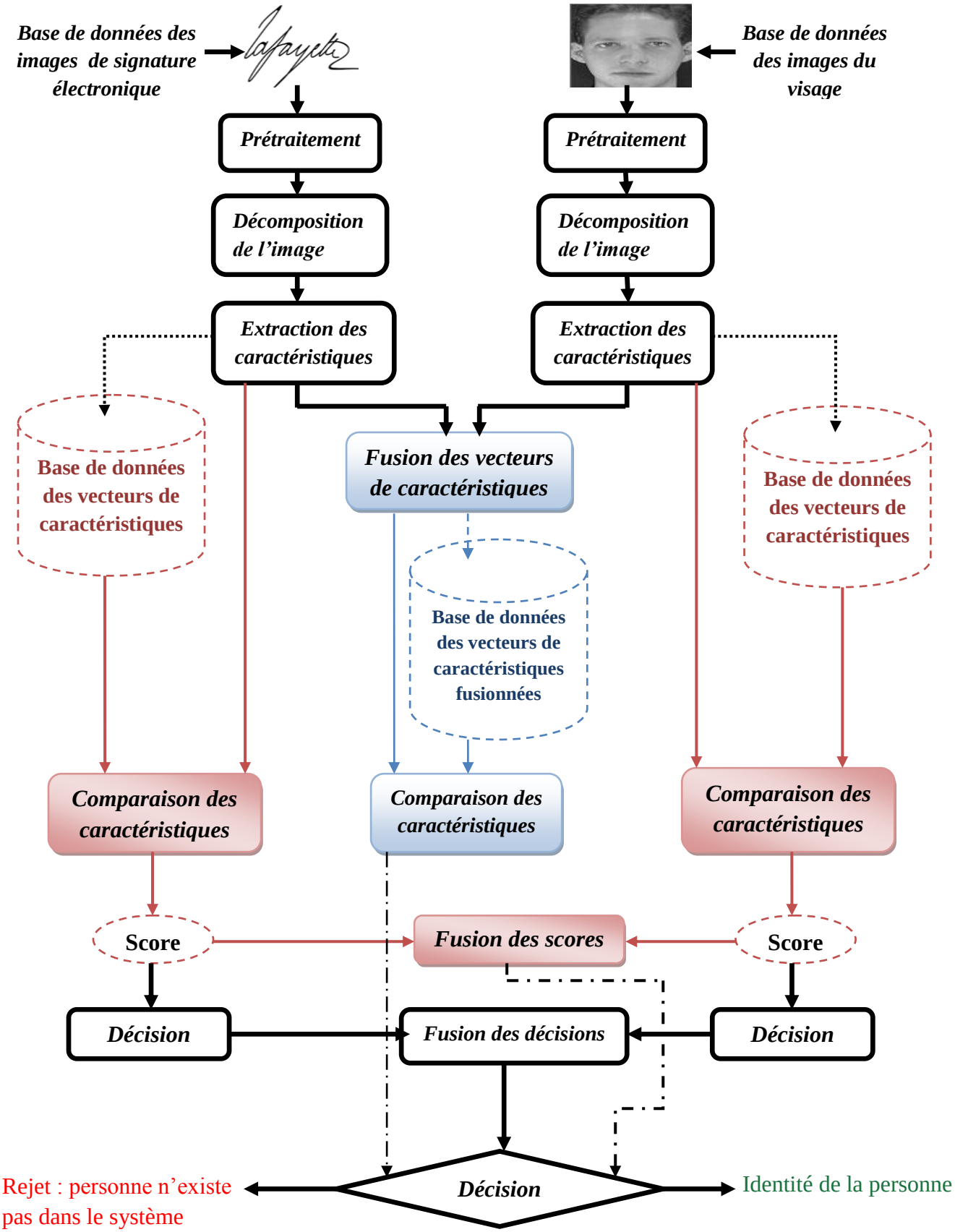

Figure 3.1 : Diagramme conceptuel de reconnaissance de visage et de signature électronique fusionnés au niveau des caractéristiques, au niveau des scores et au niveau des décisions.

Dans le schéma précédant, nous avons présenté les différentes architectures proposées; pour faire apparaitre l'efficacité de la fusion à chaque niveau, nous avons développé un système multimodal au niveau des caractéristiques. D'autres systèmes ont été proposés après la classification en une fusion au niveau des scores et au niveau des décisions, nous avons construit et proposé aussi d'autres architectures pour la fusion multimodale (comme la fusion au niveau des données ou au niveau des images).

Chaque phase du système de reconnaissance biométrique comporte quatre étapes essentielles : (1) Le prétraitement est l'étape qui sert à améliorer la qualité de l'image par le filtrage des bruits et l'amélioration de l'éclairage, (2) la décomposition de l'image consiste à décomposer l'image en sous-blocs (LBP multi-blocs ou LBP multi-échelle), (3) l'extraction des caractéristiques est l'étape qui permet d'extraire un vecteur de caractéristiques de l'image, et (4) l'étape de classification qui effectue une comparaison entre deux vecteurs de caractéristiques.

3.3. Bases d'images utilisées :

Pour faire la fusion multimodale des deux traits biométriques (visage et signature électronique), on a construit une base de données multimodale à partir des bases de données uni-modales existantes. Les personnes dans cas sont nommées : *agents virtuels*, puisque on a pris, par exemple, la première personne de la base du visage et la première personne de la base de signature et on a les considérées comme la même personne. Le choix de travailler avec des agents virtuels a été motivé par la non-disponibilité d'une base d'images multimodale pour visage et signature électronique.

3.3.1. Bases d'images pour la reconnaissance du visage :

Plusieurs bases de données contenant des informations qui permettent d'évaluer les systèmes de reconnaissance de visages sont disponibles pour la recherche et le développement des systèmes biométriques efficaces. Chaque base de visages comporte des conditions de prises de vues différentes.

Dans notre système, nous avons utilisé la base d'images ORL (Olivetti Research Laboratory) [47] pour l'évaluer.

3.3.1.1. La base d'images ORL :

La base ORL (Olivetti Research Laboratory) a été collectée entre avril 1992 et avril 1994 par le laboratoire « **AG&T** » de l'université de Cambridge en Angleterre. Cette base de données est considérée comme une base de données de référence pour les systèmes de reconnaissance automatique des visages. En effet tous les systèmes de reconnaissance de visages trouvés dans la littérature ont été testés par rapport à ORL [47].

Figure 3.2: Base de données d'image « ORL Database of Faces » [47].

3.3.1.2. Description de la base d'images ORL :

La base de données ORL contient des images de 40 personnes différentes, chacune étant enregistrée sous 10 vues différentes, donc il y en a 400 images. Les images sont de taille 112×92 pixels de niveaux de gris à 8 bits. Pour quelques sujets (personnes), les images ont été collectées à des dates différentes, avec des variations dans les conditions d'éclairage, les expressions faciales (expression neutre, sourire et yeux fermés) et des occultations partielles par des lunettes. Toutes les images ont été collectées sur un fond foncé. Les poses de la tête présentent quelques variations ne portent que certaines personnes et ne sont pas systématiques [47].

Nous présenterons dans ce qui suit quelques exemples des images de la base de données **ORL**.

Figure 3.3 : Exemple de 10 vues d'images d'une personne extraites de la base ORL avec des changements de poses, d'expression et d'éclairage.

Figure 3.4 : Exemples de changements en expressions faciales.

Figure 3.5 : Exemples de changements en coiffure et port de barbe.

3.3.2. Base d'images pour la signature électronique :

Il existe plusieurs bases de données pour la reconnaissance de la signature électronique. Dans notre étude nous avons utilisé la base d'images MCYT.

3.3.2.1. Description de la base MCYT

La base de données MCYT englobe des données de signatures en ligne de 330 contributeurs de quatre sites espagnoles différents [48].

Les informations de signatures ont été acquises dans le projet MCYT en utilisant un stylo à encre et modèles de papier sur une tablette (chaque signature est écrite dans un format de 1,75×3,75 cm^2), les images de signatures étaient donc disponibles sur papier. Modèles de papier de 75 signatures ont été choisis au hasard et numérisés avec un scanner à 600 dpi (point par pouce) [48].

La base de données MCYT contient des images de 75 personnes différentes, chacune étant enregistrée sous 30 vues différentes et nous avons choisi des images de 40 personnes avec 10 vues différentes de chaque personne pour avoir un même nombre des images que la base de données du visage. Donc il y en a 400 images. Les images sont de taille 360×850 pixels de niveaux de couleur.

Figure 3.6 : Signature composée de simple épanouissement.

Figure 3.7 : Signature composée en complexe épanouissement.

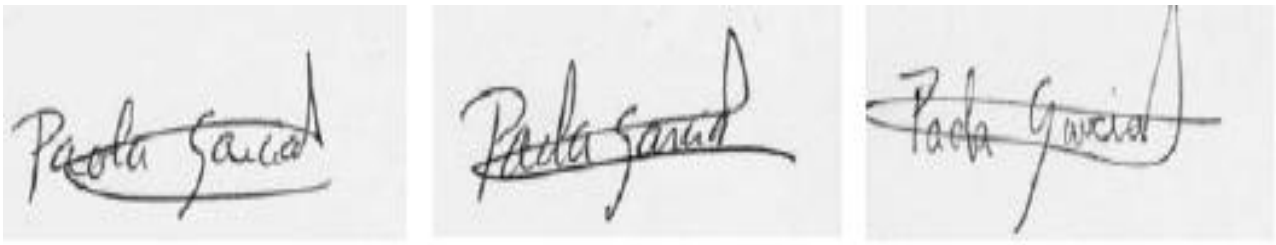

Figure 3.8 : Signature composée en un nom écrit et simple.

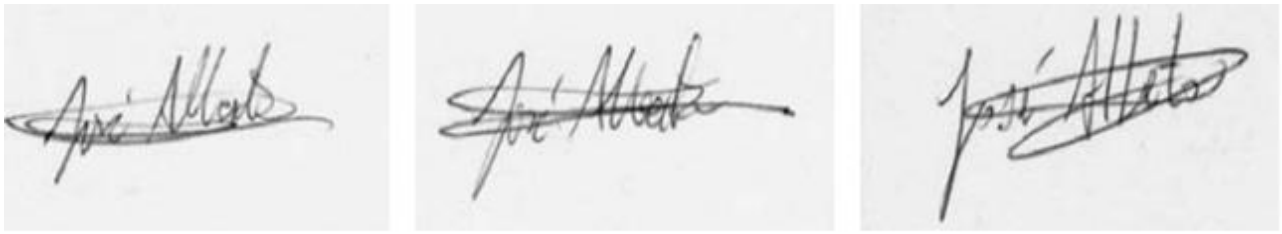

Figure 3.9 : Signature composée d'un nom écrit et complexe.

3.4. Protocole d'évaluation du système implémenté :

Afin de développer une application de reconnaissance multimodale basée sur le visage et signature et pour évaluer sa performances ; pour chaque base de données nous avons pris 40 personnes, chaque personne a 10 images. Nous avons divisé chaque base de données en deux groupes, un groupe pour effectuer l'apprentissage et l'autre pour tester la technique LBP et déterminer leurs performances.

Chaque base de données est subdivisée comme suit :

- **Images d'apprentissages :** les cinq premières images de chaque personne servent pour l'apprentissage, donc on aura 200 images pour cette phase.
- **Images de tests :** les cinq dernières images de chaque personne permettent de réaliser des différents tests, donc on aura aussi 200 images pour cette phase.

Le but est d'évaluer le taux de reconnaissance dont ce taux sera calculé de la façon suivante :

$$\boldsymbol{Taux\ de\ reconnaissance} = \frac{\boldsymbol{nombre\ d'images\ de\ test\ correctement\ reconnues}}{\textbf{nombre total des images de test}}$$

3.5. Expérimentations & Résultats :

3.5.1. Environnement de travail :

Dans cette partie, nous allons présenter les environnements matériels et logiciels utilisés dans notre travail :

a. Environnement matériel :

Afin de développer notre application, nous avons utilisé un ordinateur « Lenovo » dont les caractéristiques sont les suivantes :

- Processeur : Intel ® core™ i3-3110M CPU@ 2.40 GHz.
- RAM : 4.00 Go de RAM.
- Disque Dur : 500 Go.
- Système d'exploitation : Microsoft Windows 7 64bits.

b. Environnement logiciel :

Pour la réalisation de notre système, nous avons utilisé l'environnement de programmation **Matlab R2016a** qui permet de développer des solutions nécessitant une très grande puissance de calcul.

❖ **Matlab R2016a :**

Matlab est un environnement de développement informatique particulièrement dédié aux applications scientifiques. C'est un logiciel qui contient un système interactif et convivial de calcul numérique et de visualisation graphique.

Matlab permet d'effectuer plusieurs tâches comme le traitement d'images, visualisation de données, manipulation des matrices d'une façon simple, et l'extraction de caractéristiques par différents algorithmes; il a un large choix de bibliothèques qui prennent en charge tous les outils mathématiques…etc.

3.5.2. Tests & Résultats :

3.5.2.1. Test avec les paramètres par défauts :

La première expérimentation de notre travail a été réalisée par l'utilisation des paramètres par défauts : aucun prétraitement, LBP (8,1), aucune décomposition de l'image, distance

euclidienne, et fusion au niveau des vecteurs de caractéristiques, celle-ci nécessite certaines compatibilités entre les caractéristiques extraites à partir de différentes modalités et parmi les méthodes que nous avons utilisées : la concaténation des vecteurs de caractéristiques. Les résultats obtenus sont mis dans le tableau suivant :

Tableau 3.1 : Taux de reconnaissance avec les paramètres par défauts (aucun prétraitement, LBP(8,1), aucune décomposition de l'image, distance euclidienne, fusion au niveau des vecteurs de caractéristiques).

Nombre d'images fusionnées d'apprentissages	Nombre d'images fusionnées de tests	Taux de reconnaissance (%)
5	5	**48.5**

D'après le tableau 3.1, nous remarquons que le résultat obtenu pour l'identification est très faible (**48.5 %**). Maintenant, notre but est de chercher une meilleure méthode pour améliorer (maximiser) le taux de reconnaissance en jouant sur les paramètres de : prétraitement, extraction des caractéristiques, et classification.

3.5.2.2. Effet des prétraitements :

Afin d'augmenter le taux de reconnaissance, nous avons utilisé plusieurs prétraitements, à savoir : le filtre médian, l'égalisation d'histogramme et l'ajustement de l'image.

Tout d'abord nous avons appliqué chaque traitement seul, et après nous avons essayé de les utiliser tous à la fois et ensuite deux à deux. Les résultats sont présentés dans le tableau suivant :

Tableau 3.2 : Effet des prétraitements sur le taux de reconnaissance.

Prétraitement	Aucun prétraitement	Filtre médian	Egalisation d'histogramme	Ajustement de l'image	médian+ Egalisation + Ajustement de l'image	**Médian + Egalisation**	Médian + ajustement de l'image	Egalisation + ajustement de l'image
Taux de Reconnaissance (%)	48.5	50.5	50.5	48	52	**53**	52	50

Selon le Tableau 3.2, nous remarquons que l'application de plusieurs techniques de prétraitement sur l'image a un effet important sur l'amélioration du taux de reconnaissance, ce dernier a été amélioré de **48.5 %** à **53 %** dans le cas où nous avons appliqué une égalisation d'histogramme avec le filtre médian.

3.5.2.3. Effet des distances :

A partir de la meilleure configuration obtenue dans les expérimentations précédentes (égalisation d'histogramme avec un filtre médian, LBP (8,1), aucune décomposition, la distance euclidienne, et la fusion au niveau des vecteurs de caractéristiques), nous avons essayé plusieurs types de distances. Les résultats obtenus sont présentés dans le tableau suivant :

Tableau 3.3 : Effet des distances sur le taux de reconnaissance.

Distance	Euclidienne	City-block	Minkowski (P=0.3)
Taux de reconnaissance (%)	53	66.5	**76**

Parmi les trois mesures de distances que nous avons testées, la distance de Minkowski donne une précision supérieure de **23 %** d'après le Tableau 3.3. Donc, le choix de la distance est très important dans un système de reconnaissance biométrique multimodal. Le taux de reconnaissance a été amélioré de **53 %** à **76 %.**

3.5.2.4. Effet de la décomposition de l'image en plusieurs blocs :

- **Taux de reconnaissance avec multi-blocs :**

  Dans cette partie, nous avons divisé l'image en sous-blocs de la même taille et nous avons appliqué le descripteur LBP sur chaque sous-bloc, ensuite tous les vecteurs de caractéristiques extraits de chaque bloc, nous devons les concaténer pour avoir un nouveau vecteur de caractéristiques de l'image entière. Cette méthode est appelée LBP multi-blocs (MB-LBP). (Voir Figure 3.10).

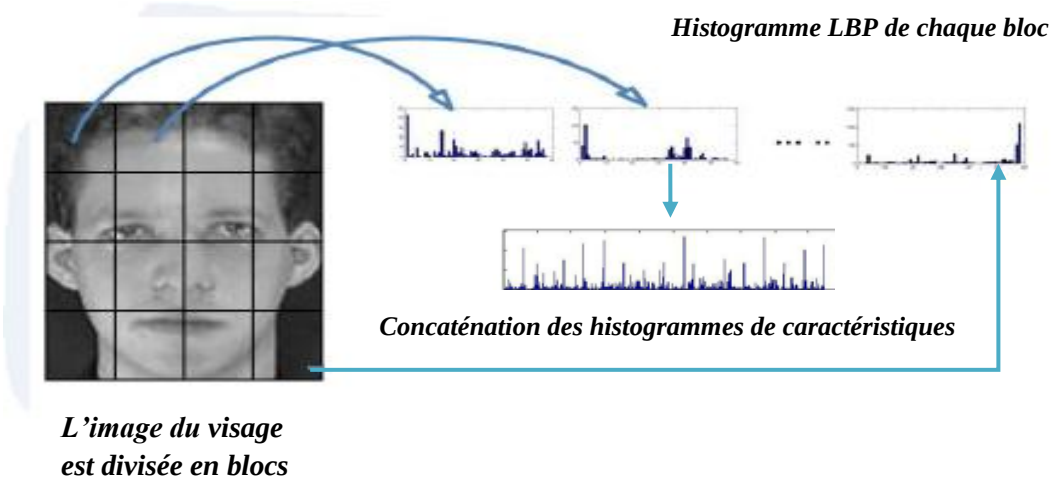

Figure 3.10 : Exemple de décomposition de l'image en 16 blocs.

Pour diviser l'image en blocs, on utilise la commande « ***blkproc*** » sur Matlab, et dans cette expérimentation nous avons essayé plusieurs tests de division de l'image en blocs :

- Le premier test consiste à prendre l'image telle qu'elle est, le deuxième consiste à diviser l'image en 4 blocs et le dernier test consiste à diviser l'image en 16 blocs.

Les résultats sont rassemblés dans le **Tableau 3.4**.

Tableau 3.4 : Effet de la décomposition de l'image en plusieurs blocs (MB-LBP) sur le taux de reconnaissance.

	LBP multi-blocs		
Nombre de blocs	**1 bloc**	**4 blocs**	**16 blocs**
Taux de reconnaissance (%)	76	92.5	**95.5**

D'après les résultats obtenus, nous avons remarqué que la décomposition de l'image en 16 blocs donne un meilleur résultat par rapport aux autres niveaux de décomposition. Ceci implique que le LBP multi-blocs influence sur le taux de reconnaissance. En effet, le taux de reconnaissance a été amélioré de **76 %** à **95.5%.**

- **Taux de reconnaissance avec multi-level :**

  Après avoir extraire les vecteurs de caractéristiques de l'image divisée en plusieurs blocs, nous devons les concaténer pour former un histogramme final ML-LBP. Cette

approche est appelée LBP multi-level, son principe de fonctionnement est illustré dans la **Figure 3.11**.

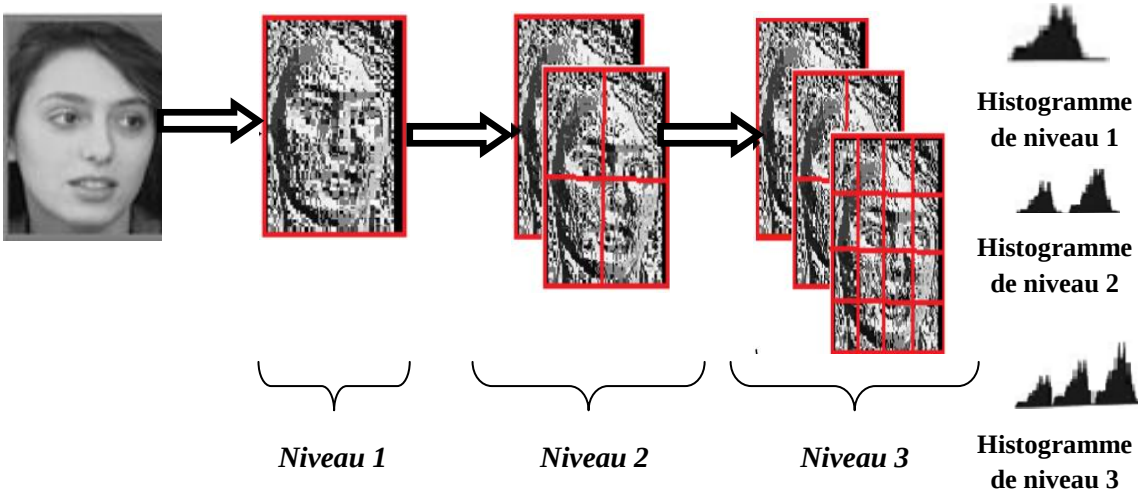

Figure 3.11 : Exemple de la méthode LBP multi-level (ML-LBP).

A partir des meilleures expérimentations précédentes (la division de l'image en 16 blocs, la distance de Minkowski, l'égalisation d'histogramme avec filtre médian, et la fusion au niveau des vecteurs de caractéristiques), nous avons appliqué la méthode ML-LBP et les résultats obtenus sont affichés dans le tableau ci-dessous :

Tableau 3.5 : Effet de la décomposition de l'image en plusieurs blocs (ML-LBP) sur le taux de reconnaissance.

ML-LBP	1&16	4&16
Taux de reconnaissance (%)	95.5	**96**

Nous remarquons que la combinaison des vecteurs de caractéristiques des blocs (4&16) donne le meilleur résultat obtenu où le taux de reconnaissance arrive jusqu'à **96%**.

3.5.2.5. Effet du descripteur LBP :

Dans cette expérimentation, nous avons testé plusieurs types du descripteur LBP, le tableau suivant illustre les résultats obtenus :

Tableau 3.6 : Effet du descripteur LBP utilisé sur le taux de reconnaissance.

LBP	LBP (8,1)	LBP (8,2)	LBP (16.2)	LBP (8,3)
Taux de reconnaissance (%)	96	96.5	97.5	**99**

Le Tableau 3.6 montre que le descripteur LBP (8,3) donne un meilleur taux de reconnaissance qui arrive à **99 %**.

3.5.2.6. Effet de fusion des images :

Pour la fusion au niveau des images, il faut que ces images soient homogènes (ayant la même taille). Pour cette raison, on a utilisé la commande Matlab « ***imresize*** » pour changer la taille d'images de la base de données de signature et les rendre de la même taille avec les images de la base de données du visage. On a utilisé une simple addition des pixels pour la fusion d'images. Le **Tableau 3.7** illustre les résultats obtenus.

Tableau 3.7 : Effet de fusion d'images sur le taux de reconnaissance.

LBP	LBP (8,3)
Taux de reconnaissance (%)	**86.5**

D'après le tableau 3.7, on remarque que les résultats obtenus par la fusion au niveau d'images (capteur) ne sont pas assez parfaits (86.5 %) comme les résultats obtenus par la combinaison des caractéristiques.

3.5.2.7. Effet de la fusion post-classification sur le taux de reconnaissance:

a. Effet de fusion au niveau des scores :

Après avoir subi les différents traitements (prétraitement et l'extraction des caractéristiques), les scores de chaque système uni-modal sont d'abord normalisés avant d'aborder l'étape de fusion. On a essayé la méthode de normalisation Min-Max des scores. Une fois les scores sont normalisés, ils sont prêts pour être fusionnés. On a utilisé la méthode Somme pour la fusion.

Le **Tableau 3.8** récapitule nos résultats obtenus après avoir effectué la fusion au niveau des scores.

Tableau 3.8 : Effet de la fusion des scores sur le taux de reconnaissance.

Méthode de normalisation / Méthode de Combinaison	Taux de reconnaissance (%)	
	Sans normalisation	**Normalisation Min-Max**
La Somme	94.5	**98.5**

D'après les résultats obtenus, nous constatons que la normalisation des scores a des effets sur l'augmentation du taux de reconnaissance.

b. Effet de la fusion au niveau des décisions :

Dans ce cas, chaque système uni-modal est traité séparément et fournit à la fin une décision. Le système de fusion des décisions consiste à prendre une décision finale à partir des méthodes de fusion « AND » et « OR » qu'on a utilisé dans cette expérimentation. Le tableau suivant illustre les résultats que nous avons obtenus à partir de cette fusion.

Tableau 3.9 : Effet de la fusion des décisions sur le taux de reconnaissance.

La méthode de fusion	**AND**	OR
Taux de reconnaissance (%)	**88.5**	99.5

Le taux d'identification qu'on a obtenu à partir de la méthode « AND » est le plus fiable / logique par rapport à la méthode « OR ».

Les résultats obtenus dans chaque niveau de fusion ont montré que la fusion dans le niveau avant la correspondance (au niveau des caractéristiques) a donné de bons résultats en les comparants avec les autres niveaux.

Les résultats trouvés au niveau des fusions des images, scores et décisions ont été satisfaisants par des méthodes de fusion simple, mais pas assez pour les résultats trouvés par la fusion au niveau des caractéristiques. Le tableau suivant résume tous les résultats obtenus dans chaque fusion.

Tableau 3.10 : Les résultats obtenus dans chaque fusion.

Système biométrique fusionnée		Taux de reconnaissance (%)
La fusion pré-classification	**La fusion au niveau des caractéristiques**	**99**
	La fusion au niveau des images	86.5
La fusion post-classification	La fusion au niveau des scores	98.5
	La fusion au niveau des décisions	88.5

3.5.2.8. Effet du nombre d'images d'apprentissage et de test sur le taux de reconnaissance :

Dans cette dernière expérimentation, nous avons changé le nombre d'images d'apprentissage et de test au même temps. Le **Tableau 3.11** résume nos résultats.

Tableau 3.11 : Effet du nombre d'images d'apprentissage et de test sur le taux de reconnaissance.

Images d'apprentissage	Images de test	Taux de reconnaissance (%)
		LPB (8,3)
1	9	87.5
2	8	95.31
3	7	97.14
4	6	97.91
5	5	99
6	4	**100**
7	3	**100**
8	2	**100**
9	1	**100**

D'après les résultats obtenus dans le tableau ci-dessus, nous remarquons que le taux de reconnaissance est positivement proportionnel au nombre d'images d'apprentissage (c'est-à-dire que le taux de reconnaissance augmente avec l'augmentation de nombre d'images d'apprentissage) jusqu'à atteindre un maximum (le taux converge à partir de 6 images en apprentissage). Cette augmentation a été représentée par l'allure de la courbe de la **Figure 3.12**.

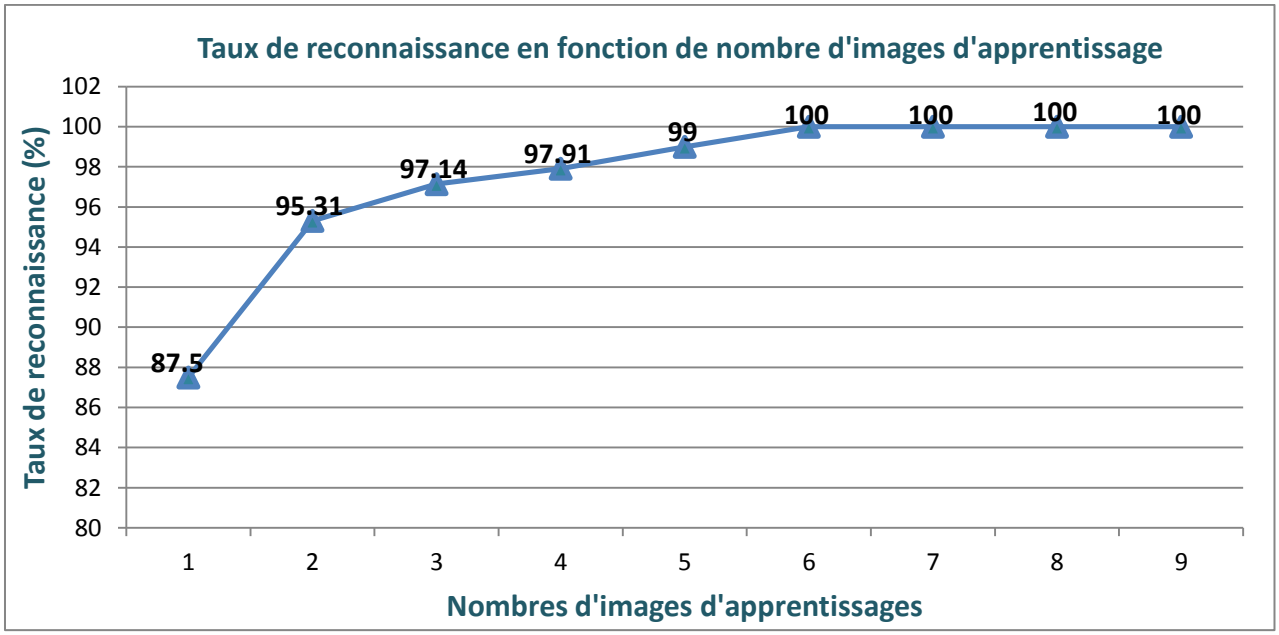

Figure 3.12 : Effet du nombre d'images d'apprentissage sur le taux de reconnaissance.

3.5.2.9. Effet de l'ordre d'images destinées à l'apprentissage et au test :

- Les cinq premières images pour l'apprentissage et les cinq dernières pour le test :

Tableau 3.12 : Taux de reconnaissance avec les 05 premières d'images destinées pour l'apprentissage et les 05 dernières d'images pour le test.

LBP	LBP (8,3)
Taux de reconnaissance (%)	99

- Les cinq premières images pour le test et les cinq dernières pour l'apprentissage.

Tableau 3.13 : Taux de reconnaissance avec les 05 dernières d'images destinées pour l'apprentissage et les 05 premières d'images pour le test.

LBP	LBP (8,3)
Taux de reconnaissance (%)	**100**

- Les images paires pour l'apprentissage et les images impaires pour le test.

Tableau 3.14 : Effet d'images paires pour l'apprentissage et les images impaires pour le test sur le taux de reconnaissance.

LBP	LBP (8,3)
Taux de reconnaissance (%)	**100**

- Les images impaires pour l'apprentissage et les images paires pour le test.

Tableau 3.15 : Effet d'images impaires pour l'apprentissage et les images paires pour le test sur le taux de reconnaissance.

LBP	LBP (8,3)
Taux de reconnaissance (%)	99

D'après les résultats obtenus, nous constatons que la meilleure configuration est lorsque les cinq premières images destinées pour le test et les cinq dernières images pour l'apprentissage et les images paires pour l'apprentissage et les images impaires pour le test, où le taux de reconnaissance a atteint 100%.

3.6. Conclusion :

Dans ce dernier chapitre, nous avons implémenté un modèle d'étude de notre système d'identification biométrique multimodal basé sur la combinaison des deux modalités (visage et signature électronique) en évaluant l'efficacité de la méthode LBP utilisée pour l'extraction des caractéristiques. La fusion de ces deux modalités a été utilisée dans différents niveau, nommés : la fusion au niveau des caractéristiques basées sur la concaténation, la fusion au

niveau d'images, la fusion des scores ainsi que la fusion au niveau des décisions ont été également présentées. Plusieurs tests et expérimentations ont été effectués pour valider notre système jusqu'à ce qu'est arrivé aux résultats prévus. Notre système a été validé par l'utilisation des deux basses de données standards : « ORL » qui présente les différentes images du visage et « MCYT » celle de la signature électronique.

CONCLUSION GÉNÉRALE & PERSPECTIVES

Conclusion Générale & Perspectives

La biométrie est un domaine en expansion dont le nombre de recherches est en croissance continue dont le but est d'aboutir à un moyen efficace, fiable et rapide pour identifier les personnes.

Bien que les techniques de reconnaissance biométrique promettent d'être très performantes, on ne peut pas garantir actuellement un excellent taux de reconnaissance avec les systèmes biométriques unimodaux basés sur une seule modalité. C'est pour cette raison que les systèmes multimodaux ont gagné une place importante dans différents domaines.

Le but de notre mémoire est la réalisation d'un système de reconnaissance biométrique multimodal basé sur la fusion de la modalité du visage avec celle de la signature électronique par l'extraction de caractéristiques de chacune en utilisant le motif local binaire (LBP) puis les fusionnés pour avoir un meilleur taux de reconnaissance.

Pour arriver à notre but nous avons procédé de la manière suivante :

Dans le premier chapitre, nous avons décrit la biométrie ainsi les différentes modalités biométriques tout en soulignant les avantages et les inconvénients de chacune puis nous avons parlé sur les systèmes biométriques et leurs performances.

Dans le deuxième chapitre, nous avons présenté la multimodalité et les différents types de combinaison de modalités possibles mais aussi les architectures et les différents niveaux de fusion. Puis comme une autre partie nous avons parlé sur le concept de la reconnaissance des formes et son processus en détails.

Dans le dernier chapitre, nous avons implémenté notre système multimodal et nous avons évalué ses performances en utilisant le LBP pour l'extraction de caractéristiques. Nous avons utilisé deux bases de données « ORL » pour le visage et « MCYT » pour la signature électronique.

Pour les futurs travaux, nous visons :

- Ajouter une troisième modalité qui est l'empreinte des doigts pour avoir compléter notre travail qu'on a fais pour la réalisation d'un passeport ou la carte d'identité algérienne.

- L’utilisation des autres descripteurs de caractéristiques tels que le PCA, LPQ.
- L’utilisation des autres méthodes de classification comme le SVM.
- Nous envisageons d’utiliser des bases de données réelles et assez grande pour confirmer l’approche de la multimodalité.

Annexe

Généralités sur le traitement d'image

1. Définition de l'image [49]:

Une image est plutôt difficile à décrire d'une façon générale. Une image est une représentation du monde en traitement d'image, la majorité du temps, on considère qu'elle s'agit d'une fonction mathématique de R*R dans R ou le couplet d'entrée est considéré comme une position spatiale, le singleton de sortie comme l'intensité (couleur ou niveau de gris) du phénomène physique. Il arrive cependant que l'image soit ''3D''donc la fonction est de R*R*R dans R. Les images couleurs peuvent être représentées soit par trois images représentant les trois couleurs fondamentales, soit par une image de R*R dans R*R*R.

L'image numérique est l'image dont la surface est divisée en éléments de tailles fixes appelés cellule ou pixel, ayant chacun comme caractéristique un niveau de gris ou de couleurs prélevé à l'emplacement correspondant dans l'image réelle ou calculé à partir d'une description interne de la scène à représenter

2. Caractéristiques d'une image [49]:

L'image est un ensemble structuré d'informations caractérisé par les paramètres suivants :

Dimension : C'est la taille de l'image qui est présentée sous forme de matrice dont les éléments sont des valeurs numériques représentative des intensités lumineux (pixels). Le nombre de lignes de cette matrice multiplie par le nombre de colonnes donne le nombre total de pixels dans une image.

Pixel : C'est le plus petit élément constitutif d'une image numérique. L'ensemble de ces pixels est contenu dans un tableau à deux dimensions constituant l'image finalement obtenu. Chaque pixel à sa valeur numérique qui représente le niveau de gris a de couleur selon la nature de l'image.

Résolution : C'est la clarté ou la finesse de détails atteinte par un moniteur ou une imprimante dans la production d'images. Sur les moniteurs d'ordinateurs, la résolution est exprimée en nombre de pixels de mesure (pouce ou centimètre). On utilise aussi le mot résolution pour désigner le nombre total de pixels affichables horizontalement ou verticalement sur un moniteur plus grand est ce nombre, meilleure est la résolution.

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

Histogramme d'une image : il représente la répartition des pixels en fonction de leur niveau de gris. Il permet de donner un grand nombre d'information sur la distribution des niveaux de gris et de voir entre quelles bornes est repartie la majorité des niveaux de gris dans le cas d'une image trop claire ou trop foncée. Pour tracer l'histogramme d'une image sous Matlab, on utilise la commande « ***imhist*** ».

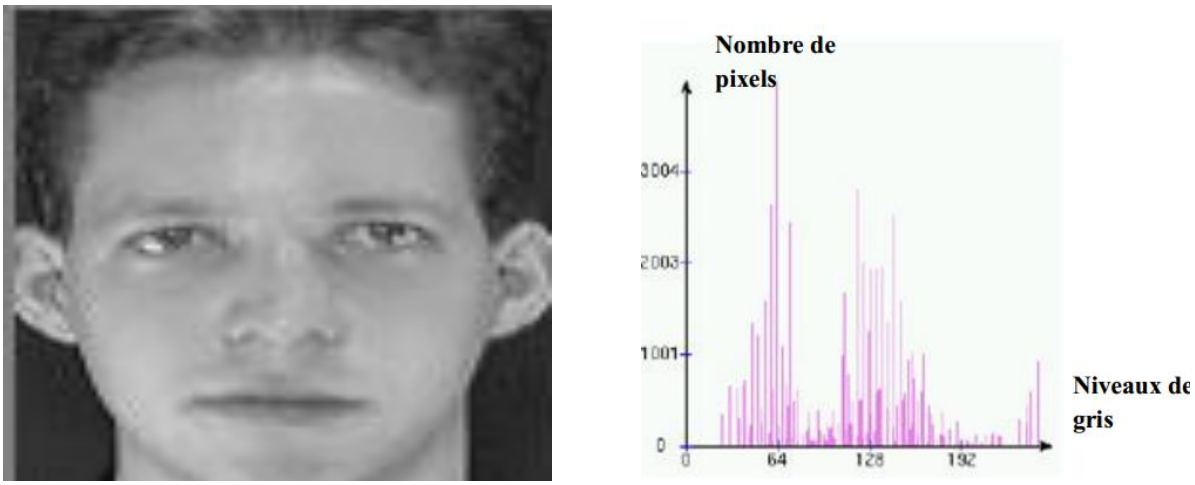

Figure 1 : Exemple d'histogramme d'une image.

Luminance : C'est le degré de luminosité des points de l'image. Elle est définie aussi comme étant le quotient de l'intensité lumineux d'une surface par l'aire apparente de cette surface.

Contraste : C'est l'opposition marquée entre deux régions d'une image plus précisément entre les régions claires de cette image.

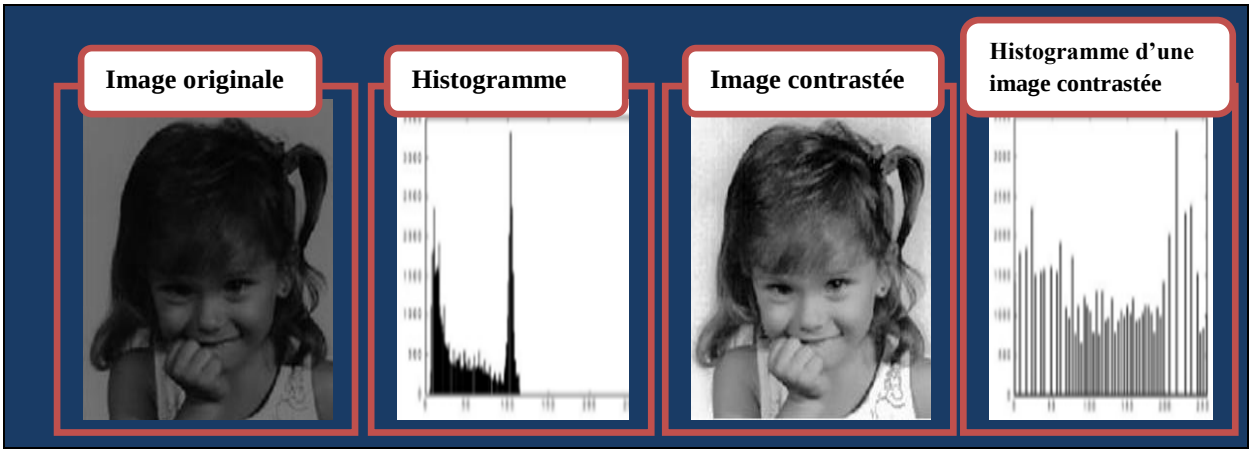

Figure 2 : Exemple d'un histogramme d'une image contrastée.

Image à niveaux de gris : Le niveau de gris est la valeur de l'intensité lumineuse en un point. La couleur du pixel peut prendre des valeurs allant du noir au blanc en passant par un nombre fini de niveau intermédiaires.

Image couleur : C'est une image ou chaque pixel est codé dans l'espace de couleur RGB (rouge, vert, bleu). Donc c'est une représentation dans un espace tridimensionnel de la valeur d'intensité lumineux du pixel.

3. Prétraitement d'images [49]:

Cette phase a lieu juste après l'acquisition des images et a pour objectif d'améliorer la qualité de l'image en vue de sa segmentation.

Les technique de prétraitements les plus courantes qu'on va présenter sont les suivants :

3.1. Egalisation de l'histogramme :

C'est une transformation de l'histogramme qui consiste à rendre le plus plat possible l'histogramme de niveaux de gris de l'image dont le principe est d'équilibrer le mieux possible la distribution des pixels dans la dynamique.

La fonction sous Matlab qui va nous permettre d'effectuer ce traitement est « ***Histeq*** ».

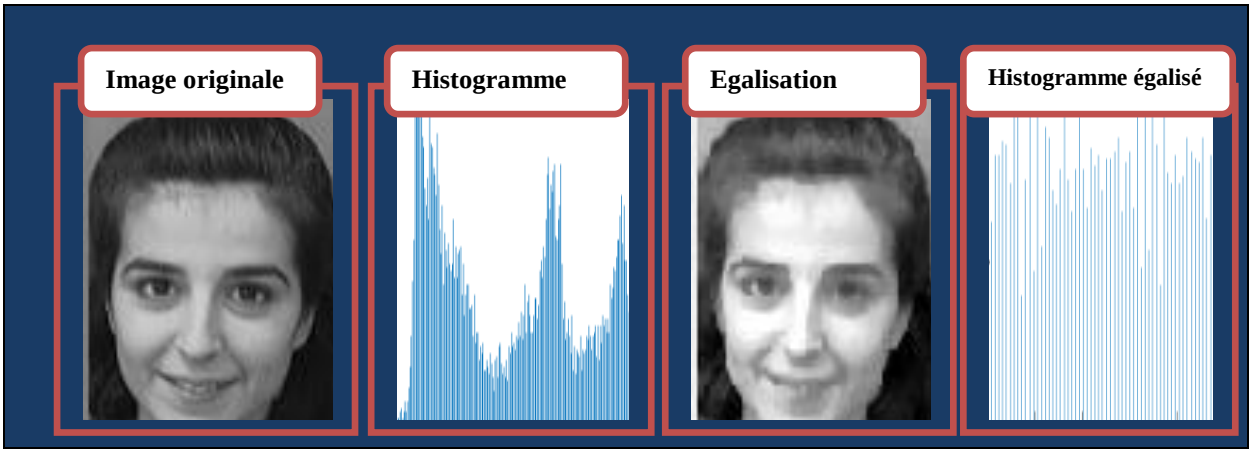

Figure 3 : Exemple d'égalisation d'histogramme.

3.2. Filtrage de l'image :

Le filtrage d'une image consiste à modifier la valeur d'un pixel en lui appliquant une fonction mathématique.

Plusieurs filtres sont utilisés pour la réduction de bruit, ils sont divisés en 2 catégories : filtres linéaires et filtres non linéaires.

Parmi les filtres non linéaires le plus utilisé est le filtre médian.

❖ ***Le filtre médian :***

C'est un filtre non linéaire qui permet d'éliminer certains types de bruit (poivre et sel). Son principe est de remplacer la valeur d'un pixel par la valeur médiane de la suite mathématique constituée de valeurs avoisinantes à ce point.

Ce type de filtres permet la préservation des contours et l'élimination de bruit impulsionnel.

La fonction sous Matlab qui va nous permettre d'effectuer ce traitement est « ***medfilt2*** ».

Figure 4 : Effet d'un filtre médian sur l'image.

3.3. Ajustement d'une image : c'est une fonction qui sert à augmenter le contraste d'une image.

La fonction utilisée sur Matlab est « ***imadjust*** ».

Figure 5 : Exemple d'une image ajustée.

Références Bibliographiques

[1] T. Hafs : « ***Reconnaissance Biométrique Multimodale basée sur la fusion en score de deux modalités biométriques : l'empreinte digitale et la signature manuscrite cursive en ligne*** ».Thèse de doctorat, Université Badji Mokhtar-Annaba (Algérie), 2016.

[2] S. Khellat-Kihel : « ***Identification biométrique par fusion multimodale de l'empreinte d'articulation, l'empreinte digitale et l'empreinte veineuse du doigt*** ». Thèse de doctorat, Université d'Oran Mohamed Boudiaf (Algérie), 2017.

[3] A. Chaari : « ***Nouvelle approche d'identification dans les bases de données biométriques basée sur une classification non supervisée*** ». Thèse de doctorat, Université d'Evry Val d'Essonne (France). Soutenue le 06/10/2009.

[4] M. Chassé, analyste en informatique : « ***La biométrie au Québec : Les enjeux*** ». Document d'analyse de la commission d'accès à l'information (Québec), Juillet 2002.

[5] P. Gregory, M.A. Simon, editors: « ***Biometrics for Dummies*** ». Springer, Canada, 2008. ISBN: 978-0-470-29288-4.

[6] S. Akrouf : « ***Une Approche Multimodale pour l'Identification du Locuteur*** ». Thèse de doctorat, Université de FERHAT ABBAS-Sétif (Algérie). Soutenue le 07/07/2011.

[7] A.K. Jain, A. Ross, and P. Flynn, editors: « ***Handbook of Biometrics*** ». Springer, New York (USA), 2008. ISBN-13:978-0-387-71040-2.

[8] S. Prabhakar, S. Pankanti, and A.K. Jain: « ***Biometric Recognition: Security and Privacy Concerns*** ». IEEE Security & Privacy. Vol.01, No.02, pp.33-42, 2003.

[9] A.K. Jain, A. Ross, S. Prabhakan: « ***An Introduction to Biometric Recognition*** ». IEEE Transactions on Circuits and systems for video technology, Vol. 14, No. 1, pp.04-20, Janvier 2004.

[10] N. Morizet : « ***Reconnaissance Biométrique par Fusion Multimodale du Visage et de l'Iris*** ». Thèse de doctorat, Ecole Nationale des Télécommunications (Paris). Soutenue le 18/03/2009.

[11] M. El Abed : « ***Evaluation de Systèmes Biométriques*** ». Thèse de doctorat, Université de Caen-Basse-Normandie (France). Soutenue le 09/12/2011.

[12] I. Benchennane : « ***Etude et mise au point d'un procédé biométrique multimodale pour la reconnaissance des individus*** ». Thèse de doctorat, Université d'Oran Mohamed Boudiaf (Algérie), 2016.

[13] A.K. Jain, R. Bolle, and S. Pankati, editors: « ***Biometrics: Personal Identification in Network Society*** ». Springer Verlag, New York (USA), 1999.

[14] S.G. Ababsa : « ***Authentification d'individus par reconnaissance de caractéristiques biométriques liées aux visages 2D/3D*** ». Thèse de doctorat, Université d'Evry Val d'Essonne (France). Soutenue le 03/10/2008.

[15] M. Golfarelli, D. Maio, and D.Maltoni: « ***On the Error-Rejet Trade-Off in Biometric Verification Systems*** ». IEEE Transactions on Pattern Analysis and Machine Intelligence (PAMI).Vol.19, No.07, pp.786-796, 1997.

[16] M. Belahcen, M. Benatia: « ***Authentification et Identification de Visage basées sur les Ondelettes et les Réseaux de Neurones*** ». Revue science des matériaux, laboratoire LARHYSS N°02, pp.01-08, septembre 2014.

[17] F. Peronin, J.L. Dugelay: « ***An introduction to biometrics Audio and Video-Based Person Authentification*** ». Revue Traitement du Signal, Vol.19, No.04, 2002.

[18] P. J. Phillips, H. Hyeonjoon, S. Rizvi, P. Rauss: « ***The Feret Evaluation Methodology for Face-Recognition Algorithms*** ». IEEE Transactions on Pattern Analysis and Machine Intelligence, Vo. 22, No.10, Octobre 2000.

[19] T. Autret, R. Bergeron, M. Collignon, M.A. Couwez, A. Denis, J.C. Gandois, G. Khouberman, M. Lecherc, J.Y. Martin: « ***Techniques de contrôle d'accès par biométrie*** ». Dossier Technique de la Commission de Sécurité Physique, Clusif, (France), 2003.

[20] P. Varchol and D. Levicky: «***Using of Hand Geometry in Biometric Security Systems*** ». Radioengineering. Vol.16, No.04, pp.82-87, 2007.

[21] K.B. Raja, R. Raghavendra, and C. Busch: « ***Video Presentation Attack Detection in Visible Spectrum Iris Recognition Using Magnified Phase Information*** ». IEEE Transactions on Information Forensics and Security, Vol.10, No.10, pp.2048-2056, Octobre 2015.

[22] S. Gaur, V.A. Shah, M. Thakker: « ***Biometric Recognition Techniques: A Review*** ». International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering. Vol.1, Issue 4, India, Octobre 2012.

[23] B. Arbab-Zavar and M.S. Nixon: « ***On Guided Model-Based Analysis for Ear Biometrics*** ». Computer Vision and Image Understanding (Elsevier). Vol.115, No.04, pp.487-502, 2011.

[24] D.C. Garcia, R.L. de Queiroz : « ***Face-Spoofing 2D-Detection Based on Moiré-Pattern Analysis*** ». IEEE Transactions on Information Forensics and Security, Vol.10, No.04, pp.778-786, Avril 2015.

[25] R.D. Seely, M. Goffredo, J.N. Carter, and M.S. Nixon: « ***View Invariant Gait Recognition*** ». In M. Tistarelli, S.Z. Li, and R. Chellapa, editors: ‘**’Handbook of Remote Biometrics for Surveillance and Security’’**. Springer Verlag (Advances in Pattern Recognition Series), London (UK), 2009.

[26] G. Kaur, C.K. Verma: « ***Comparative Analysis of Biometric Modalities*** ». International Journal of Advance Research in computer Science and Software Engineering, Vol.4, No.4, April 2014.

[27] S. Chantaf : « ***Biométrie par signaux physiologiques*** ». Thèse de doctorat, Université Paris Est Creteil (France). Soutenue le 02/05/2011.

[28] L. Allano : « ***La Biométrie multimodale : stratégies de fusion de scores et mesures de dépendance appliquées aux bases de personnes virtuelles*** ».Thèse de doctorat, Institut National des Télécommunications (Paris). Soutenue le 21/01/2009.

[29] G. Amirthalingam and G. Radhamani: « ***A Multimodal Approach for Face and Ear Biometric System*** ». International Journal of Computer Science Issues, Vol.10, Issue 5, No.02, September 2013.

[30] A. Benzaoui and A. Boukrouche: « ***Ear Recognition Using Local Color Texture Descriptors From One Sample Image Per Person*** ». International Conference on Control, Decision and Information Technologies (CoDIT’17) / April 5-7, 2017, Barcelona, Spain.

[31] A. Ross, K. Nandakumar and A.K. Jain: « ***Handbook of Multibiometrics*** ». Springer, New York, USA, 1st edition, 2006.

[32] M. Imran, A. Rao, G.H. Kumar: « ***Multibiometric systems: Acomparative study of multi-algorithmic and multimodal approaches*** ». Procedia Computer Science, Vol.2, pp.207-212, 2010.

[33] A. Ross, A.K. Jain: « ***Information Fusion in Biometrics*** ». Pattern Recognition, Vol.24, pp.2115-2125, 2003.

[34] J. Kittler, M. Hatef, R.P.W. Duin, and J. Matas: « ***On Combining Classifiers*** ». IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol.20, No.3, pp.226-239, 1998.

[35] C. Saint-Jean : « ***Classification paramétrique robuste partiellement supervisée en reconnaissance des formes*** ». Thèse de doctorat, Université de La Rochelle (France). Soutenue le 17/12/2011.

[36] S. Nebti : « ***Reconnaissance de Caractères Manuscrits par Intelligence Collective*** ». Thèse de doctorat, Université Ferhat Abass-Sétif (Algérie). Soutenue le 7/3/2013.

[37] I. Kaastra, M. Boyd: « ***Designing a neural network for forecasting financial and economic time series*** ». Neurocomputing. Vol.10, No.3, pp.215-236, 1996.

[38] S.K. Gupta, W.C. Regli, and D.S. Nau: « ***Manufacturing Feature Instances: Which Ones to Recognize?*** ». Symposium on Solid Modeling and Applications, pp.141-152, 1995.

[39] H.S. Hippert, C.E. Pedreira, and R.C. Souza: ***« Neural networks for short-term load forecasting: a review and evaluation*** ». IEEE Transactions on Power Systems, Vol.16, Part 1, pp.44-55, 2001.

[40] L. Hartet : « ***Reconnaissance des formes dans un environnement dynamique appliquée au diagnostic et au suivi des systèmes évolutifs*** ». Thèse de doctorat, Université de Reims Champagne-Ardenne (France). Soutenue le 24/10/2010.

[41] Z.H. Mamar : « ***Analyse Temps-Echelle et Reconnaissance des Formes pour le Diagnostic du Système de Guidage d'un Tramway sur Pneumatiques*** ». Thèse de doctorat, Université de Blaise Pascal-Clermont II (France). Soutenue le 18/7/2008.

[42] M. Senouci, H.A. Baghdadi, livre : « ***Réseaux de Neurones : théorie et pratique*** ». Office des Publications Universitaires (OPU), ISBN : 9961-0-0902-9. Volume (141 pages). décembre 2005.

[43] A. Benzaoui, A. Boukrouche, and A. Hadid: « ***Ear biometric recognition using local texture descriptors*** ». Journal of Electronic Imaging, Vol.23, No.5, 053008 (Sep/Oct 2014).

[44] N. Morizet, T. EA, F. Rossant, F. Amiel, A. Amara : « ***Revue des algorithmes PCA, LDA, EBGM utilisés en reconnaissance 2D du visage pour la biométrie*** ». Revue des algorithmes. Institut Supérieur d'Electronique de paris (ISEP), Département d'Electronique. Paris Cedex 2006.

[45] A. Benzaoui, I. Adjabi, and A. Boukrouche: « ***Experiments and improvements of ear recognition based on local texture descriptors*** ». Optical Engineering, Vol.56, No.4, April 2017.

[46] T. Ojala, M. Pietikäimen, and T. Maenpao: « ***Multiresolution gray-scale and rotation invariant texture classification with local binary patterns*** ». IEEE Transaction Pattern Analysis and Machine Intelligence, Vol.24, No.7, pp.971-987, 2002.

[47] ORL database : https://www.cl.cam.ac.uk/research/dtg/attarchive/facedatabase.html (consulté le 11/09/2018).

[48] J. Ortega-Garcia, J. Fierrez-Aguilar, D. Simon, J. Gonzales, M. Faundez-Zanuy, V. Espinosa, A. Satue, I. Hernaez, J.J. Igarza, C. Vivaracho, D. Escudero and Q.I. Moro : « ***MCYT Baseline corpus : a bimodal biometric database*** ». IEE Proceedings Vision, Image and Signal Processing. Vol.150, No.6, pp.395-401, December 2003.

[49] D. Boukhlouf : « ***Résolution des problèmes par écosystèmes : Application au traitement d'images*** ». Mémoire de Magister, Université Mohamed Khider Biskra (Algérie). Soutenue le 17/11/2005.

Résumé

L'identification de l'individu est devenue essentielle pour assurer la sécurité des systèmes et d'organisations. La biométrie se réfère à la reconnaissance automatique des individus basée sur leurs caractéristiques physiologiques ou comportementales comme la reconnaissance faciale, l'empreinte digitale, la signature électronique, la voix, l'iris…etc.

Les systèmes biométriques unimodaux permettent de reconnaitre une personne en utilisant une seule modalité biométrique, mais ne peuvent pas garantir avec certitude une bonne identification. De plus, ces systèmes sont sensibles aux bruits du capteur, à la non universalité et aux manques d'individualité de la modalité biométrique choisie.

Une des méthodes pour surmonter ces problèmes est d'utiliser des systèmes d'authentification biométriques multimodaux, qui combinent l'information provenue de multiples modalités pour prendre une décision.

L'objectif principal de notre travail est de réaliser un système de reconnaissance biométrique multimodal basé sur la combinaison de deux modalités biométriques, à savoir : le visage et la signature électronique. Nous avons utilisé le motif local binaire (LBP) comme extracteur de caractéristiques afin d'avoir un excellent taux de reconnaissance. Nos résultats expérimentaux sont effectués sur deux bases de données, la base « ORL » pour le visage et la base « MCYT » pour la signature électronique.

Mots clés : Identification, biométrie, système multimodal, LBP, taux de reconnaissance, extracteur de caractéristiques.

Abstract

The identification of individuals has become essential to ensure the security of systems and organizations. Biometrics refers to the automatic recognition of individuals based on their physiological or behavioral characteristics, such as: facial recognition, fingerprint, electronic signature, voice, iris ... etc.

Unimodal biometric systems make it possible to recognize a person by using a single biometric modality, but they cannot guarantee with certainty a good identification. In addition, these systems are sensitive to sensor noise, non-universality and lack of individuality of the selected biometric modality.

One way to overcome these problems is to use multimodal biometric authentication systems, which combine information from multiple modalities to make a good decision.

The main objective of our work is to realize a multimodal biometric recognition system based on the combination of two biometric modalities: the face and the electronic signature. We used the local binary pattern (LBP) as a feature extractor in order to obtain an excellent recognition rate. Our experimental results are performed on two databases, the "ORL" database for the face and the MCYT database for the electronic signature.

Key words: Identification, biometrics, multimodal system, LBP, recognition rate, feature extractor.

ملخص

أصبح التعرف على الفرد ضروريا لضمان أمن الأنظمة و المنظمات.و تشير القياسات الحيوية إلى التعرف التلقائي للأفراد استنادا إلى خصائصها الفسيولوجية و السلوكية مثل التعرف على الوجه, البصمات, و التوقيع الرقمي و القزحية...الخ.

الأنظمة البيومترية الأحادية يمكنها التحقق من هوية شخص باستخدام وضع بيولوجي مفرد, ولكن لا يمكن أن تضمن على وجه اليقين تعريفا جيدا. بالإضافة إلى ذلك, فإن هذه الأنظمة حساسة لضوضاء المستشعرات, وعدم العالمية وعدم وجود شخصية من الطريقة الحيوية المختارة. و تتمثل إحدى طرق التغلب على هذه المشاكل في استخدام أنظمة الاستيقان البيومترية المتعددة الوسائط, التي تجمع المعلومات من طرائق متعددة لاتخاذ قرار.

و الهدف الرئيسي من عملنا هو تحقيق نظام التحقق من الهوية المتعددة الوسائط على أساس مزيج من اثنين من طرائق القياس الحيوي: الوجه و التوقيع الإلكتروني. استخدمنا النمط الثنائي المحلي(LBP) كمستخرج مميز من أجل الحصول على معدل تقدير ممتاز. يتم تنفيذ نتائجنا التجريبية على قاعدتي بيانات, قاعدة بيانات "ORL" للوجه و قاعدة بيانات "MCYT" للتوقيع للإلكتروني.

الكلمات المفتاحية : تحديد الهوية, القياسات الحيوية,نظام متعدد الوسائط,LBP, معدل الاعتراف, مستخرج السمات.