REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEURE ET DE LA RECHERCHE SCIENTIFIQUE

Faculté des Nouvelles technologies de l'information et de la communication
Département D'électronique

MEMOIRE MASTER ACADEMIQUE

Domaine : Sciences et Techniques.
Filière : Électronique.
Spécialité : Automatique.

Présenté par :

Ahmed Oussama LAZOUL
Islam CHETIOUI

THEME

Identification Des Personnes Par Utilisant Un Descripteur De Texture

Soutenu publiquement
Le : 25/05/2017

Devant le jury :

Mr.	Abdelghani MONCER	MAA	Président	UKM Ouargla
Mr.	Fatah HAMMOUCHI	MAA	Examinateur	UKM Ouargla
Mr.	Abdallah MERAOUMIA	MCA	Encadreur	U.TEBESSA
Mr.	Maarouf KORICHI	Doctorant	Co-Encadreur	UKM Ouargla

Année Universitaire : 2016/2017

Remerciements

Nous tenons tout d'abord à remercier ALLAH le tout puissant et miséricordieux, qui nous a donné la force et la patience d'accomplir ce modeste travail.

Tous nos infinis remerciements à notre encadreurs ***Mr : Abdallah MERAOUMIA*** *pour leurs aide, conseils et leurs remarques qui nous ont permis de présenter notre travail dans sa meilleure forme*

Nos remerciements s'étendent également à tous le personnel du centre de recherche. ET particulièrement ***Mr : Maarouf KORICHI*** *et* ***Khaled BENSID*** *pour ses bonnes explications, Qui nous ont éclairé le chemin de la recherche et sa collaboration avec nous dans L'accomplissement de Ce modeste travail.*

Nous tenons à exprimer nos sincères remerciements à tous les professeurs qui nous ont Enseigné et qui par leurs compétences nous ont soutenu dans la poursuite de nos études.

Nos gratitudes s'expriment à tous les consultants et internautes rencontrés lors des Recherches effectuées et qui ont accepté de répondre à nos questions aves gentillesse.

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 et de l'enrichir par Leurs propositions.

Enfin nous remercions tous ceux qui ont contribués de près ou de loin à l'élaboration de Ce modeste travail, trouvant ici l'expression de notre profonde gratitude et profonds respects.

Merci à tous et à toutes.

OUSSAMA ET ISLAM

Dédicace

Je dédie ce mémoire à mes chers parents pour leur patience, leur amour, leur soutien et leurs encouragements

À mes frères Abderahmen, Yasmine et Amani

A mes amis Sayah, Lakhdar, Adel. Nour elhouda, Belkhir, mamma et marwa

Tous mes professeurs et A tous qui Compulse ce modeste travaille.

Oussama.

Dédicace

Je dédie ce mémoire à mes chers parents pour leur patience, leur amour, leur soutien et leurs encouragements

À mes frères et Mes sœurs

A mes amis Daho, Mamma, Elhadj, Imane, Nour elhouda, tifo et Khaled

Tous mes professeurs et A tous qui Compulse ce modeste travaille.

Islam.

Table des matières

Page

CHAPITRE II : MULTIMODALITÉ ET FUSION DES DONNÉES

CHAPITRE III : SYSTÈME BIOMÉTRIQUE BASÉ SUR FKP UTILISANT UNE NOUVELLE MÉTHODE DE MOTIFE BINAIRE LOCAL (BLBP)

CHAPITRE IV : RÉSULTATS EXPÉRIMENTAUX

Liste des figures

Liste des tableaux

Glossaire

AND : **A**cide **D**ésoxyribo **N**ucléique

CCD : **C**harged **C**oupled **D**evice

CMC : **C**umulative **M**atch **C**urve

DB : **D**ata **B**ase

EER : **E**qual **E**rror **R**ate

FAR: **F**alse **A**cceptance **R**ate

FRR : **F**alse **R**ejection **R**ate

FKP : **F**inger **K**nuckle **P**rint

GAR : **G**enuine **A**cceptance **R**ate

IBG : **I**nternational **B**iometric **G**roup

ICA : **I**ndependent **C**omponent **A**nalysis

LBP : **l**ocal **B**inary **P**attern

LED : **l**ight-**E**mitting **D**iode

LIF : **L**eft **I**ndex **F**ingers

LMF: **L**eft **M**iddle **F**ingers

LPQ : **l**ocal **P**hase **Q**uantization

PIN : **P**ersonal **I**dentification **N**umber

RIF : **R**ight **I**ndex **F**ingers

RMF: **R**ight **M**iddle **F**ingers

ROC : **R**eceiver **O**perating **C**urve

ROI: **R**egion **O**f **I**nterest

ROR: **R**ank **O**ne **R**ecognition

RPR : **R**ank of **P**erfect **R**ecognition

Introduction générale

Introduction générale

Le développement international des communications, autant en volume qu'en diversité (déplacements des individus, transactions financières, accès aux services...), d'autre part l'augmentation du taux de criminalité, le piratage…etc. Ce qui nécessite le besoin de s'assurer de l'identité des individus, les systèmes traditionnels de sécurité sont basés sur une connaissance à priori des mots de passe traditionnels en code PIN ou sur une possession d'un objet comme clef, pièce d'identité et badge…etc. Mais ces systèmes sont moins fiables pour beaucoup d'environnements, à cause de leur inhabilité commune à distinguer un individu réellement autorisé d'un fraudeur. L'identification de l'individu est devenue essentielle pour assurer la sécurité des systèmes et des organisations face à cette sollicitation grandissante, plusieurs méthodes de reconnaissances biométriques ont été proposées : reconnaissance faciale, reconnaissance du locuteur, empreinte digitale, reconnaissance de l'iris, de la forme de la main, de la rétine.

La biométrie est un terme dont on entend de plus en plus parler dans la vie de tous les jours. Les systèmes de reconnaissance biométrique utilisés de plus en plus autant dans le domaine privé que public, comportent de nombreux avantages pour les personnes qui les introduisent et les personnes concernées. Si de nombreuses applications utilisent aujourd'hui la biométrie, celle qui correspond au plus grand déploiement est la mise en place, prévue pour 2009 des passeports biométriques utilisant le visage et l'empreinte digitale pour la délivrance et le contrôle de l'identité. Cependant, la biométrie n'est pas vraiment récente. Toutefois, l'utilisation de données biométriques pour l'identification ou la vérification d'une identité prétendue comporte également des risques quant au respect des droits et des libertés fondamentales. De nombreux travaux ont été réalisés sur l'optimisation séparée des modalités biométriques, et ont proposé une approche d'intégration de plusieurs modalités biométriques (en l'occurrence deux modalités) afin de pallier aux problèmes de la vérification biométrique unimodale.

Dans cette perspective, un de ces systèmes a été choisi d'être étudié, c'est le système qui utilise l'empreinte des articulations des doigts FKP (Finger-Knuckle-Print) comme caractéristique biométrique de reconnaissance par image. Cette modalité a été choisie selon ses nombreux avantages remarquables, à savoir c'est une technique acceptable par les individus, simple et facile à utiliser. Finalement, la combinaison de tous les doigts (dix doigts dans les deux mains) peut être utilisée afin d'établir un système biométrique robuste et précis. Nous

allons focaliser dans ce travail sur l'étude d'un système complet d'identification par FKP comme trait biométrique. Le but est de développer une extraction d'un vecteur caractéristique robuste par l'utilisation de la méthode LBP et BLBP. Par celui-ci, ces deux algorithmes sont très utilisés pour l'analyse de texture pour choisir le meilleur résultat après la comparaison de ces modèles.

Notre mémoire est scindé en **quatre chapitres** :

Dans **le premier,** nous définirons la biométrie ainsi que les différentes techniques biométriques utilisées. Ce chapitre sera finalisé par un aperçu sur les domaines principaux d'application de la biométrie ainsi que leur contribution dans le marché mondial.

Dans **le deuxième** chapitre, nous introduirons quelques notions dans la biométrie multimodale et traiterons la question de la fusion et ses différents niveaux, ainsi que les méthodes principales de normalisation des scores.

Dans **le troisième** chapitre, nous allons présenter des généralités sur les méthodes d'extraction des caractéristiques, et allons développer l'utilisation du descripteur de texture. Notre contribution à l'extraction de caractéristiques sera également aussi présentée. Dans cette contribution, des notions sur les deux techniques BLBP et LBP, ainsi que la façon de les appliquer pour extraire les caractéristiques discriminantes seront présentés.

Le quatrième chapitre présentera les résultats des tests effectués avec les méthodes LBP et BLBP sur la base des données FKP (notre base des données contient quatre doigts pour chaque personne). Cette dernière sera subdivisée à deux sections. Dans la première section de ce chapitre, nous allons mettre en œuvre un système d'identification uni-modale basé à chaque fois sur l'un des doigts. Une description détaillée des résultats obtenus, par les méthodes **BLBP** et du **LBP**, sera présentée dans cette section. La deuxième section de ce chapitre discutera les résultats expérimentaux obtenus pour les systèmes biométriques multimodaux. Trois scenarios de fusion, à savoir le système multi-traits, le système multi-algorithmique et le système hybride seront être évalués. Afin de sélectionner le meilleur système, qui présente la plus faible erreur d'identification, une comparaison entre les différents systèmes sera exécutée dans cette section. Enfin, nous allons terminer notre mémoire avec une conclusion et quelques perspectives visées.

CHAPITRE I

GÉNÉRALITÉ A LA BIOMÉTRIE

I.1. Préambule

Au niveau international, la sécurité est devenue une préoccupation majeure depuis plusieurs années. Certaines technologies, qui étaient à l'époque encore marginales, ont alors pris un essor considérable. Les futurs passeports et cartes d'identité envisagent actuellement des nombreux systèmes informatiques, aussi bien que pour de nombreux autres usages en lien avec la sécurité. C'est dans ce contexte que des efforts importants sont fournis (domaine de la recherche en biométrie) afin de concevoir un système d'authentification de personnes. Trois types de méthodes sont distingués, afin d'authentifier une personne. Les deux méthodes les plus utilisées sont basées sur ce que connaît la personne, comme un mot de passe, ou sur ce que possède une personne comme un badge ou une carte d'identité. Un troisième type de méthodes qui la plus original et qui se base sur ce que l'on est ; comme exemple : les empreintes digitales ou la forme de la main, ou bien sur ce que l'on sait faire comme la signature manuscrite ou la dynamique de frappe au clavier. Désormais et en pleur développement, cette troisième approche repose sur les caractéristiques de l'individu lui-même, on parle alors de biométrie [1].

Dans ce chapitre, nous se présentons notamment les concepts d'utilisation de la biométrie. Pui nous passons à dresser un panorama des différentes techniques biométrique présentées dans la littérature.

I.2. Un bref historique de la biométrie

Dans la Chine des dynasties, les documents étaient signés à l'aide d'empreintes digitales. Selon le rapport de l'explorateur Joao de Barros. Il a écrit que les marchands chinois relevaient les empreintes des mains et des pieds des enfants de jeune âge sur du papier en utilisant de l'encre afin de les distinguer les uns des autres. C'est une des méthodes les plus anciennes de la biométrie en pratique et elle est toujours utilisée de nos jours. Dans les échanges commerciaux de Babylone, 3000 ans avant-J.-C., le même système était utilisé. En Amérique précolombienne, nombre d'architectes laissèrent également la trace de leurs mains colorées sur les parois de grottes aménagées [2].

Mais ce n'est qu'au début du XVIIIème siècle que le Docteur Henri Faulds développe l'utilisation de traces de doigt pour l'identification des personnes. A la même époque, l'anglais Francis Galton réalise des travaux de mesures de corps humains et crée une table de statistiques basée sur les tailles et les poids des personnes. Il met au point la méthode "Fingerprints" qui établit l'unicité et la permanence des figures cutanées. En 1881, le médecin italien Cesare

Lombroso tente de prouver que l'humain criminel présente des caractéristiques repérables et stables. Ainsi, le poids du cerveau des honnêtes gens pèserait entre 1475 et 1550 grammes tandis que celui des criminels serait d'à peu près 1455 grammes. Ces théories, non fondées scientifiquement, sont vite abandonnées. En 1885, Alphonse Bertillon ne laisse cependant pas de côté cette hypothèse, responsable de l'identité judiciaire en France, il construit "le Bertillonnage" qui s'appuie sur les mensurations des criminels. Le principe connaît un vif succès jusqu'au jour où une erreur judiciaire grave vient détruire le rêve de ségrégation.

Après l'échec du Bertillonnage, la police a commencé à utiliser la technique des empreintes digitales, qui a été développée par Richard Edward Henry de Scotland Yard, ressemblant essentiellement aux mêmes méthodes employées par les Chinois durant des années. Au XIXème siècle, la police criminelle fait considérablement avancer la recherche du fait de la multiplication des Analyses d'Indices Biologiques (ADN) [3].

Dans les trois dernières décennies, la biométrie a évolué d'une seule méthode simple (empreintes digitales) vers plus de dix méthodes discrètes. Les sociétés de biométrie comptent des centaines de nouvelles méthodes appliquées et continuent à améliorer leurs méthodes de sécurité tant que la technologie répond à leurs exigences. Les prix du hardware requis continuent à baisser rendant des systèmes faisables pour de faibles et moyens budgets. Cependant le développement de l'industrie, fait ainsi le souci du public concernant les libertés et l'intimité. Des lois et des règlements continuent à être rédigés et des normes commencent à être mises en place. Tandis qu'aucune autre technique biométrique n'a encore atteint le succès de l'utilisation de l'empreinte digitale, certaines commencent à être employées dans des secteurs d'activité judiciaire et commerciale.

Aujourd'hui, la biométrie est une technologie à part entière qui utilise des critères permanents, uniques et infalsifiables. Elle permet de garantir la sécurité des accès aux environnements physiques et numériques et révolutionne du même coup le ebusiness et le e-commerce.

I.3. Pourquoi utilise-t-elle ?

La biométrie est un domaine émergeant où la technologie améliore notre capacité à identifier une personne. La protection des consommateurs contre la fraude ou le vol est un des buts de la biométrie. L'avantage de la reconnaissance biométrique est que chaque individu a ses propres caractéristiques physiques qui ne peuvent être changées, perdues ou volées [4]. La

méthode de reconnaissance biométrique peut aussi être utilisée en complément ou remplacement de mots de passe. Plusieurs raisons peuvent motiver l'usage de la biométrie :

I.3.1. Confort

En remplaçant juste le mot de passe, exemple pour l'ouverture d'un système d'exploitation, la biométrie permet de respecter les règles de base de la sécurité (ne pas inscrire son mot de passe à côté du PC, ne pas désactiver l'écran de veille pour éviter des saisies de mots de passe fréquentes). Et quand ces règles sont respectées, la biométrie évite aux administrateurs de réseaux d'avoir à répondre aux nombreux appels pour perte de mot de passe (que l'on donne parfois au téléphone, donc sans sécurité) [4].

I.3.2. Sécurité / Psychologie

Dans certains cas, particulièrement pour le commerce électronique, l'usager n'a pas confiance. Il est important pour les acteurs de ce marché de convaincre le consommateur de faire des transactions. Un moyen d'authentification connu comme les empreintes digitales pourrait faire changer le comportement des consommateurs [4].

I.4. Définition

Actuellement, Nos sociétés préoccupent d'une façon majeure la sécurité des personnes, des biens ou des informations. L'authentification de l'identité des personnes est l'un des moyens permettant de s'en assurer. La grosse faille qui se marque au niveau des moyens actuels de vérification d'identité apparîat clairement en : l'identité d'une personne est directement liée à ce qu'elle possède comme un passeport, un badge magnétique, etc. et /ou à ce qu'elle sait (un code PIN de carte bancaire, un mot de passe, etc.). Or, Cependant, un badge peut être volé, un mot de passe deviné ou cassé par force algorithmique brute : ceci menant à l'usurpation d'identité. En conséquence, la biométrie permettrait l'indentification d'une personne sur la base de caractères physiques ou de traits comportementales automatiquement reconnaissables et vérifiables. L'avantage d'une telle identification est que chaque individu a ses propres caractéristiques qui ne peuvent être ni changées, ni perdues, ni volées [1].

La biométrie est le domaine technologique traitant de la vérification d'identité et/ou de l'identification de personnes par leurs caractéristiques individuelles, pouvant être physiques ou comportementales. Elle apparaît comme une solution évidente au problème soulevé

précédemment : l'identité d'une personne est liée à ce qu'elle est et non plus à ce qu'elle possède ou sait.

I.5. Classification des modalités biométrique

Il existe deux grandes catégories des modalistes biométriques : les biométries morphologiques et les biométries comportementales.

✓ **Les biométries morphologiques :** sont les biométries utilisant une partie du corps humain. Cette modalité regroupe l'iris de l'œil, le réseau veineux, de la rétine, la forme de la main, les empreintes digitales, les traits du visage, les veines de la main, etc [5].

✓ **Les biométries comportementales :** sont celles utilisant un trait personnel du comportement. Cette modalité regroupe la reconnaissance vocale, la dynamique de frappe au clavier, la dynamique de la signature, l'analyse de la démarche, etc [5].

✓ Il existe également **des biométries biologiques**. Elle regroupe des caractéristiques telles que la thermographie faciale, la forme des veines de la main, le sang, la salive, l'urine, l'odeur, et l'ADN (Acide DésoxyriboNucléique) [5].

Pour être efficaces dans l'exploitation de la biométrie, les caractéristiques utilisées doivent bien entendu posséder certaines qualités intrinsèques pour permettre le développement des systèmes biométriques fiables et robustes. Les qualités indispensables pour chaque caractéristique sont les suivantes : l'universalité, unicité, permanence et mesurabilité. Ces qualités assurent que chaque personne possède la caractéristique considérée (c'est-à-dire commune à tous les individus), qu'elle est unique pour chaque individu (peut différencier deux individus), qu'elle ne change pas ou peu dans le temps (c'est-`a-dire invariantes dans le temps pour chaque individu), qu'il est possible d'en récolter un échantillon et de l'analyser [5].

I.6. Techniques biométriques

Il existe plusieurs techniques biométriques utilisée dans plusieurs application et secteurs ont en commun de viser à établir l'identité d'une personne en analysant ses caractéristiques physiques ou comportementales. Avec l'introduction de la numérisation, ces techniques se sont raffinées, mais leur principe reste le même [6]. Elles se divisent en deux groupes selon la coopération ou non de l'individu :

- **Techniques intrusives :** Ces techniques requièrent un contact physique avec l'individu pour l'identifier, tel que les Empreinte des articulations des doigts, les empreintes digitales, la rétine, l'ris ou la forme de la main. Leur usage est généralement mal accepté [7].
- **Techniques non intrusives :** Ces techniques ne requièrent pas la coopération de l'individu en question. Leur application peut se faire à distance en utilisant des capteurs qui ne nécessitent pas de contact directe avec l'utilisateur (visage, démarche,…) [7].

La biométrie permet l'identification ou l'authentification d'une personne sur les bases de données reconnaissables et vérifiables qui lui sont propres.

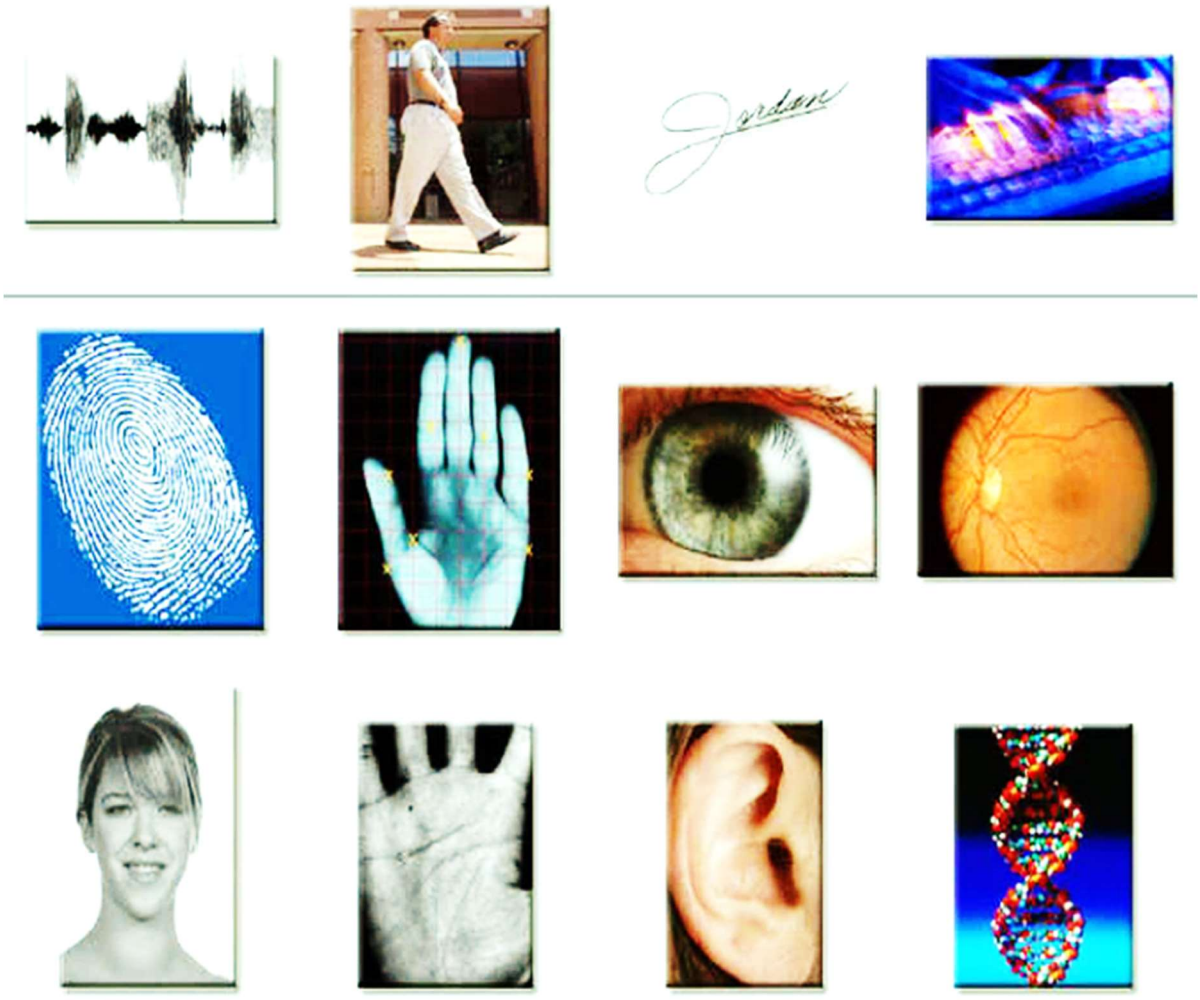

Figure I.01 : *Défirent technique biométrique.*

Parmi les différentes techniques biométriques existantes, on distingue trois grandes catégories par suite :

I.6.1. Biométrie morphologique (physiologique)

Elle est basée sur l'identification de traits physiques particuliers qui, pour toute personne, sont uniques et permanents. Cette catégorie regroupe la reconnaissance de la forme du visage, de la forme de la main, des empreintes digitales, de la rétine et de l'iris de l'œil, les traits du visage, le réseau veineux de la rétine, les veines de la main, etc [1].

➊ **Empreinte des articulations des doigts :** La surface extérieure du doigt contient des caractéristiques distinctives, surtout au voisinage des articulations (Figure I.02), telles que les lignes principales, les lignes secondaires et les crêtes, qui peuvent être extraites à partir des images à basse résolution. Ces dernières années, un nouveau descripteur biométrique (nouvelle technologie biométrique) basé sur la surface extérieure du doigt, appelé empreinte de l'articulation du doigt [6], est exploité. La main contient plusieurs doigts, pour cela, plusieurs travaux montrent que l'empreinte de l'articulation du doigt peut être utilisée dans le domaine d'identification des personnes pour une reconnaissance robuste et précise, si on utilise la combinaison ou la fusion de l'information prise de chaque doigt.

Figure I.02 : *Empreinte des articulations des doigts.*

➋ **Empreinte digitale :** Un système biométrique utilisant l'empreinte digitale comme moyen d'identification ou de vérification ne procède pas de la même façon, ce n'est pas l'image de l'empreinte digitale qui sert de point de comparaison, mais l'ensemble des données biométriques qui est tiré à partir des minuties de l'empreinte digitale. Les minuties représentent les fins de crêtes, les bifurcations, les lacs, les Lots et les points qui composent l'empreinte digitale. La combinaison des minuties est quasi infinie. L'acquisition des données est faite par un capteur électronique de type optique, thermique, capacitif ou à ultrasons. Cette dernière est considérée comme la plus fiable, mais aussi la plus coûteuse (figure I.03) [1].

Le recours à l'empreinte digitale compte pour plus du tiers du marché des procédés biométrique. Elle représente nettement la solution préférée des entreprises œuvrant dans ce domaine. La force de ce procédé tient au fait que l'utilisation de l'empreinte digitale est plus facile à accepter par la communauté et qu'elle est une des plus efficaces et des moins coûteuses.

La qualité d'image de l'empreinte digitale peut varier selon que la peau du doigt est sale, trop humide ou trop sèche, huileuse ou affligée d'une coupure.

Figure I.03 : *Empreinte digitale.*

❸ **Géométrie du la main :** Les données biométriques pouvant être saisies relativement à la main sont les veines, les lignes et la géométrie en 3D (Figure I.04). Plusieurs technologies sont aptes à effectuer la capture de ces trois types de données, combinées ou séparées. Il est à noter que le degré d'unicité de la géométrie de la main serait relativement faible, puisque les similarités entre les mains de différents individus ne sont pas rares. C'est pourquoi il est généralement recommandé de l'utiliser pour l'authentification uniquement. Parmi ses autres faiblesses, la reconnaissance de la main requiert un minimum d'hygiène, afin de ne pas nuire à la captation de l'image. Par contre, ce système résisterait à la fraude car il serait impossible de soumettre une paume de main artificielle [7].

En général, une caméra infrarouge prend l'image de la main sous deux angles différents pour obtenir les trois dimensions. L'image scannée est convertie en modèle numérique et associée à un code. Quand une personne passe son badge devant le lecteur, celle-ci cherche le code dans la base de données et procède à la comparaison [1].

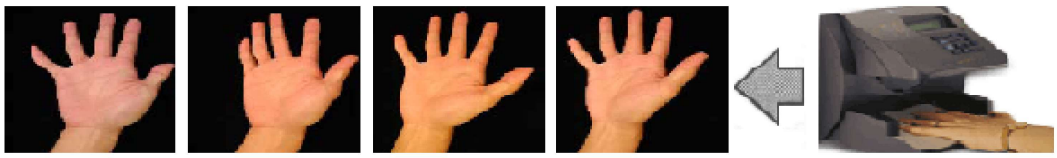

Figure I.04 : *Géométrie de la main.*

❹ **L'iris :** L'iris est le muscle coloré à l'intérieur de l'œil, visible à travers la cornée, placé devant le cristallin et percé en son centre de la pupille. Une caméra parcourt l'œil à l'aide d'une lumière infrarouge et capture une image, afin de mesurer plusieurs caractéristiques telles que le relief, les anneaux, les sillons et la texture de l'iris. Étant donné son caractère stable et très unique, la reconnaissance de l'iris est reconnue pour sa fiabilité très élevée. Le système est d'ailleurs à l'épreuve des lunettes, des verres de contacts et des fluctuations de la taille de la pupille et peut observer près de 200 points de comparaison. Sa fiabilité est due en partie à la

quasi-impossibilité de le reproduire artificiellement. Toutefois, le succès du système dépendra de la qualité de l'image saisie par la caméra digitale, de la même manière que pour la rétine (figure I.05)[1].

On peut distinguer jusqu'à 244 points de comparaison, et le taux d'erreur des produits disponibles sur le marché est quasi nul (la probabilité de trouver 2 iris identiques serait de 1 sur 10^{72}). D'autant plus que qu'on peut faire doubler la simple photographie de certaines caractéristiques dynamiques de l'œil : réactivité de la pupille (dilatation/rétraction) par rapport à la quantité de lumière, étude de l'iris dans l'infrarouge et l'ultraviolet, …etc...

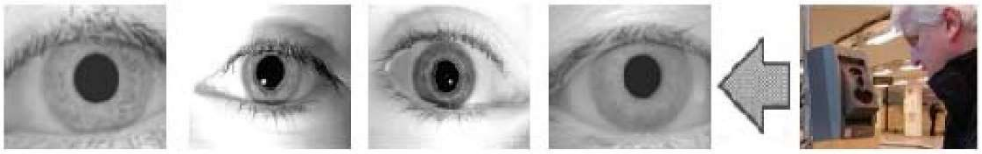

Figure I.05 : *Iris.*

❺ **Le visage :** Plusieurs parties du visage (Figure I.06) (joues, yeux, nez, bouche…) sont extraites d'une photo ou d'une vidéo et analysées géométriquement (distance entre différents points, positions, formes…). Le problème de cette méthode vient des possibles perturbations pouvant transformer le visage (maquillage, faible luminosité, présence d'une barbe ou d'une lunette, expression facial inhabituelle, changement avec l'âge, …etc [1].

Il s'agit ici de faire une photographie plus ou moins évoluée pour en extraire un ensemble de facteurs qui se veulent propres à chaque individu. Ces facteurs sont choisis pour leur forte invariabilité et concernent des zones du visage tel que le haut des joues, les coins de la bouche, …etc. Il existe plusieurs variantes de la technologie de reconnaissance du visage. La première technologie de reconnaissance du visage développée est nommée "Eigenface". Elle consiste à décomposer le visage en plusieurs images faites de nuances de gris, chacune mettant en évidence une caractéristique particulière [1].

Figure I.06 : *Visage.*

❻ **La rétine :** La rétine (Figure I.07) est la paroi interne et opposée de l'œil sur laquelle se projettent les images que nous voyons. Cette paroi est tapissée par un réseau de vaisseaux

sanguins, qui forment un motif unique pour chaque individu. L'identification consiste à éclairer le fond de l'œil par un faisceau lumineux de faible intensité [1].

Cette reconnaissance basée sur le fait que le schéma et le dessin formé par les vaisseaux sanguins de la rétine est unique pour chaque individu, différent entre jumeaux et assez stable durant la vie de la personne. Cette mesure biométrique peut ainsi fournir jusqu'à 400 points caractéristiques du la personne. Elle a été moins bien acceptée par le public et les utilisateurs, sans doute à cause de son caractère trop contraignant : la mesure doit en effet s'effectuer à très faible distance du capteur (quelques centimètres) pour que le balayage soit réussi [1].

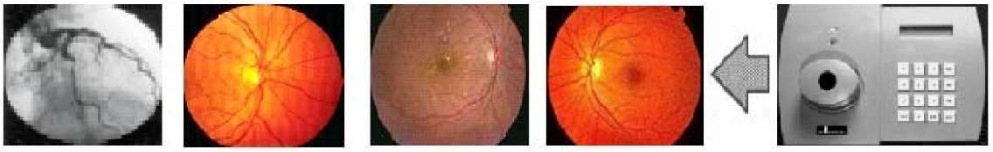

Figure I.07 : *Rétine.*

❼ **Les veines de la main :** Il s'agit ici d'analyser le dessin formé par le réseau des veines sur une partie du corps d'un individu (la main) pour en garder quelques points caractéristiques. L'utilisateur place sa main dans une chambre ou un gabarit de lecture. Les caractéristiques des veines sont lues par une caméra infrarouge qui en tire une image en deux dimensions. Cette image est ensuite digitalisée et enregistrée pour comparaison future [1].

Figure I.08 : *Les veines de la main.*

❽ **La géométrie de l'oreille :** La forme de l'oreille externe (Figure I.09), des lobes et la structure du cartilage représentent un champ moins connu de la biométrie physiologique (figure I.9). Apparemment la police est capable de relever les empreintes des oreilles laissées par les criminels lorsqu'ils écoutent aux portes et aux fenêtres [4].

Figure I.09 : *Oreille.*

I.6.2. Biométrie comportementale

Elle se base sur l'analyse de certains comportements d'une personne comme le tracé de sa signature, l'empreinte de sa voix, sa démarche et sa façon de taper sur le clavier., …etc.

❶ **La voix :** La reconnaissance reposant sur la tonalité de la voix de la personne contrôlée (Figure I.10), la fréquence vocale et la distance entre la formation des lettres. Elle peut distinguer un homme d'une femme mais reste très dépendante de la qualité de l'enregistrement et du type de message. Elle représente à l'heure actuelle 11% du marché. Cette technique appelée analyse du locuteur s'applique avec succès là où les autres technologies sont difficiles à employer. Elle est utilisée dans des secteurs comme les centres d'appel, les opérations bancaires, l'accès à des comptes, sur PC domestiques, pour l'accès à un réseau [1].

Figure I.10 : *la voix.*

❷ **La signature manuscrite :** Chaque personne possède une signature (Figure I.11) qui lui est propre et qui peut donc servir à l'identifier. Il existe deux modes de reconnaissance : le mode statique et le mode dynamique. Le mode statique n'utilise que l'information géométrique de la signature. Le mode dynamique utilise à la fois l'information géométrique et dynamique, c'est- à-dire les mesures de la vitesse, la pression et les accélérations et le temps total de la signature [1].

Figure I.11 : *Signature manuscrite.*

❸ **L'analyse de la démarche :** Il s'agit de reconnaître un individu par sa façon de marcher (Figure I.12) et de bouger (vitesse, accélération, mouvements du corps…etc.), en analysant des séquences d'images. La démarche serait en effet étroitement associée à la musculature naturelle et donc très personnelle. Son inconvénient majeur est qu'elle est sensible aux changements

d'habits, chaussures et surface. Ceci rend cette approche limitée au monde de la recherche seulement[1].

Figure I.12 : *La démarche.*

❹ **La frappe dynamique sur le clavier :** La dynamique de la frappe est propre à chaque individu. Un système basé sur la dynamique de frappe au clavier (Figure I.13) ne nécessite aucun équipement particulier, chaque ordinateur disposant d'un clavier. Il s'agit d'un dispositif logiciel qui calcule le temps où un doigt effectue une pression sur une touche et le temps où un doigt est dans les airs (entre les frappes). Cette mesure est capturée environ mille fois par seconde. La séquence de frappe est prédéterminée sous la forme d'un mot de passe [1].

Figure I.13 : *Frappe sur le clavier.*

I.6.3. Biométrie biologique

Une autre catégorie qui est l'étude des traces biologiques. Elle regroupe des caractéristiques telles que l'odeur, le sang, la salive, cheveu ou bien l'ADN et thermographie facial et la forme des veines de la main, …etc.

❶ **L'analyse de l'ADN :** La génétique a permis de démontrer que l'ADN (acide désoxyribonucléique) est la particularité la plus fiable pour identifier une personne (figure I.14). Cette technique est assez contraignante pour l'utilisateur (prélèvement sanguin ou capillaire) et nécessite beaucoup de temps, d'où sa non utilisation pour des applications temps réel. L'analyse des empreintes génétiques est une méthode extrêmement précise d'identification, issue directement de l'évolution de la biologie moléculaire [1].

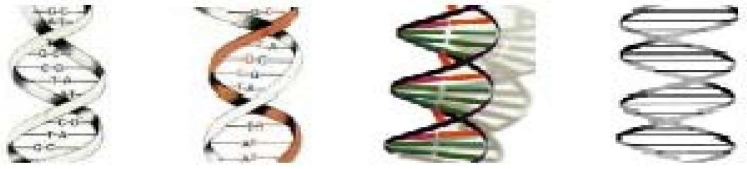

Figure I.14 : *Analyse de l'ADN.*

❷ **Les ongles :** La technique est basée sur les stries longitudinales des ongles, qui dépendent de la structure de l'épiderme sous-jacent. On peut révéler le relief de l'ongle grâce à un interféromètre, et le cartographier [1].

❸ **Thermo-gramme facial :** La quantité de chaleur émise par les différentes parties du visage caractérise chaque individu. Elle dépend de la localisation des veines mais aussi de l'épaisseur du squelette, La quantité de tissus, de muscles, de graisses, …etc. Une caméra thermique est utilisée pour réaliser un cliché infrarouge du visage. Cela permet de faire apparaître une répartition de la chaleur unique à chaque individu, voire de cartographier le réseau veineux du visage invisible à l'œil nu [1].

❹ **Odeur de corps :** La biométrie d'odeur de corps est basée sur le fait que pratiquement chaque humaine est son odeur unique. Elle est capturée par les sondes qui sont capables pour obtenir l'odeur de parties non-intrusives du corps telles que le dos de la main. L'odeur humaine se compose des produits chimiques connus sous le nom de volatiles ils sont extraits par le système et converti dans un calibre [1].

Toutefois, dans un système biométrique pratique (à savoir, un système qui utilise la biométrie à des fins personnelles de reconnaissance), il y a un certain nombre d'autres questions qui devraient être considérées, y compris :

- **La performance,** qui se réfère à la précision de la reconnaissance et de la vitesse possible ainsi que les ressources nécessaires pour obtenir cette précision de la reconnaissance et de la vitesse désirées. La performance se réfère également au fonctionnement et aux facteurs environnementaux qui influent sur la précision et la vitesse.
- **L'Acceptabilité,** qui indique la mesure dans laquelle les gens sont prêts à accepter l'utilisation notamment d'un identifiant biométrique (caractéristique) dans leur vie quotidienne.
- **Le contournement,** ce qui reflète la façon dont le système peut facilement être dupe en utilisant des méthodes frauduleuses.

I.7. Système biométrique et mode de fonctionnement

I.7.1. Caractérisation d'un système biométrique

En général un système biométrique est un système automatique de mesure basé sur la reconnaissance de caractéristiques propres à un individu : physique ou comportementale. Il est basé sur l'analyse de données liées à l'individu qui peuvent être classées en trois grandes catégories : analyse basée sur la morphologie, analyse de traces biologiques, l'analyse comportementale [3]. Il peut être représenté par quatre modules principaux :

✓ **Le module de capture** est responsable de l'acquisition des données biométriques d'un individu (cela peut être un appareil photo, un lecteur d'empreintes digitales, une caméra de sécurité, etc.

✓ **Le module d'extraction de caractéristiques** prend en entrée les données biométriques acquises par le module de capture et extrait seulement l'information pertinente afin de former une nouvelle représentation des données. Idéalement, cette nouvelle représentation est censée être unique pour chaque personne et relativement invariante aux variations intra-classe.

✓ **Le module de correspondance** compare l'ensemble des caractéristiques extraites avec le modèle enregistré dans la base de données du système et détermine le degré de similitude (ou de divergence) entre les deux.

✓ **Le module de décision** vérifie l'identité affirmée par un utilisateur ou détermine l'identité d'une personne basée sur le degré de similitude entre les caractéristiques extraites et le(s) modèle(s) stocké(s).

I.7.2. Mode de fonctionnement d'un système biométrique

L'étude du fonctionnement d'un système biométrique, que nous conduisons ici, permet de mettre en évidence quelques points essentiels de la mise en place d'un système biométrique. Quel que soit le système biométrique mis en place, celui-ci comporte toujours deux briques principales: le module d'enregistrement ou d'enrôlement et le module de reconnaissance [4].

➢ **Phase d'enregistrement/enrôlement :** La phase d'enregistrement (l'enrôlement) (Figure I.15) est la première phase de tout système biométrique, il s'agit de l'étape pendant laquelle un utilisateur est enregistré dans le système pour la première fois et où une ou plusieurs modalités biométriques sont capturées et enregistrées dans une base de données. Cet

enregistrement peut s'accompagner par l'ajout d'information biographique dans la base de données [4].

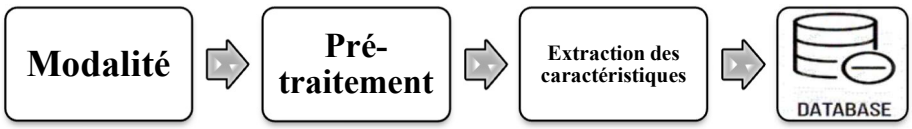

Figure I.15 : *Module d'enregistrement classique d'un système biométrique.*

➢ **Phase de reconnaissance :** Ce second module du système biométrique permet d'effectuer la reconnaissance des individus. C'est au cours de cette phase qu'une décision sera prise concernant l'identité de l'utilisateur. Cette phase diffère en fonction de l'objectif recherché : Veut-on vérifier ou identifier un utilisateur ? [4].

▪ **Processus identification :** Dans un système biométrique opérant en mode identification (Figure I.16), l'utilisateur ne dévoile pas explicitement son identité. Cependant, l'affirmation implicite faite par l'utilisateur est qu'elle est une des personnes déjà enrôlées par le système [4]. Ainsi, l'échantillon biométrique de l'individu est comparé avec les modèles de toutes les personnes de la base de données. On parle alors de correspondance 1 : N.

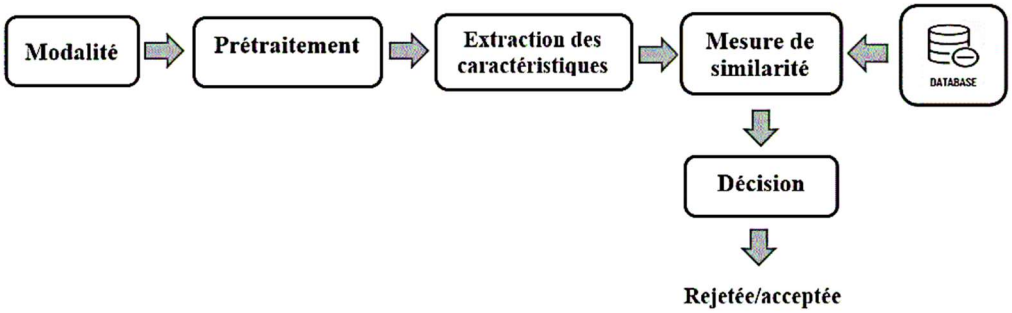

Figure I.16 : *Processus d'identification.*

L'identification peut décomposer en deux modes opératoires (ensemble ouvert et ensemble fermé) [4].

L'identification en mode ensemble fermé : La sortie du système biométrique est constituée par l'identité de la personne dont le modèle possède le degré de similitude le plus élevé avec l'échantillon biométrique présenté en entrée.

L'identification en mode ensemble ouvert : Si la plus grande (petite) similarité entre l'échantillon et tous les modèles est inférieure à un seuil de sécurité minimum fixé, la personne

est rejetée, ce qui implique que l'utilisateur n'était pas une des personnes enrôlées par le système. Dans le cas contraire, la personne est acceptée.

▪ **Processus de vérification :** Lorsqu'un système biométrique opère en **mode vérification** (Figure I.17), l'utilisateur affirme son identité et le système vérifie si cette affirmation est valide ou non [4].

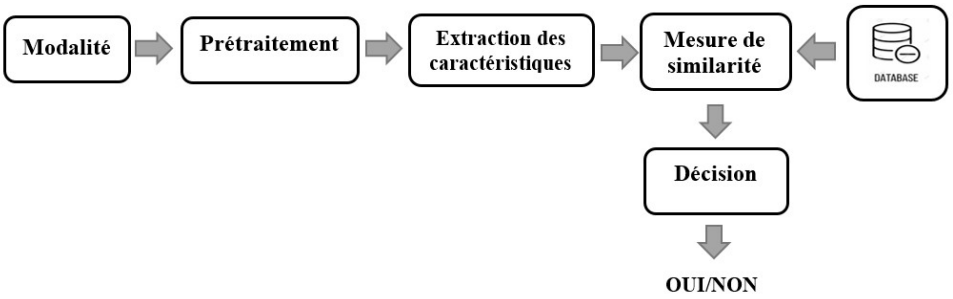

Figure I.17 : *Processus de vérification.*

Chacune des étapes peut être sujette à des erreurs ou attaques, qu'elles soient volontaires ou non de la part des utilisateurs. Il faut donc travailler et évaluer chacune si l'on veut garantir les performances d'un système biométrique.

➢ **Phase d'adaptation** : Pendant la phase d'apprentissage, le système biométrique ne capture souvent que quelques instances d'un même attribut afin de limiter la gêne pour l'utilisateur. Il est donc difficile de construire un modèle assez général capable de décrire toutes les variations possibles de cet attribut. De plus, les caractéristiques de cette biométrie ainsi que ses conditions d'acquisition peuvent varier. L'adaptation est donc nécessaire pour maintenir voire amélioré la performance d'un système utilisation après utilisation [4]. L'adaptation peut se faire en mode supervisé ou non-supervisé mais le second mode est de loin le plus utile en pratique. Si un utilisateur est identifié par le module de reconnaissance, les paramètres extraits du signal serviront alors à réestimer son modèle. En général, le taux d'adaptation dépend du degré de confiance du module de reconnaissance dans l'identité de l'utilisateur. Bien entendu, l'adaptation non-supervisée peut poser problème en cas d'erreurs du module de reconnaissance.

I.8. Performance d'un système biométrique

Tout d'abord, afin de comprendre comment déterminer la performance d'un système biométrique, il nous faut définir clairement trois critères principaux (FRR, FAR et EER) :

I.8.1. Taux de faux rejet

("False Reject Rate" ou FRR), Ce taux représente le pourcentage de personnes censées être reconnues mais qui sont rejetées par le système [3].

I.8.2. Taux de fausse acceptation

("False Accept Rate" ou FAR). Ce taux représente le pourcentage de personnes censées ne pas être reconnues mais qui sont tout de même acceptées par le système [3].

I.8.3. Taux d'égale erreur

("Equal Error Rate" ou EER). Ce taux est calculé à partir des deux premiers critères et constitue un point de mesure de performance courant. Ce point correspond à l'endroit où FRR = FAR, c'est-à-dire le meilleur compromis entre les faux rejets et les fausses acceptations [3].

La (figure I.18) illustre le FRR et le FAR à partir de distributions des scores authentiques et imposteurs tandis que l'EER :

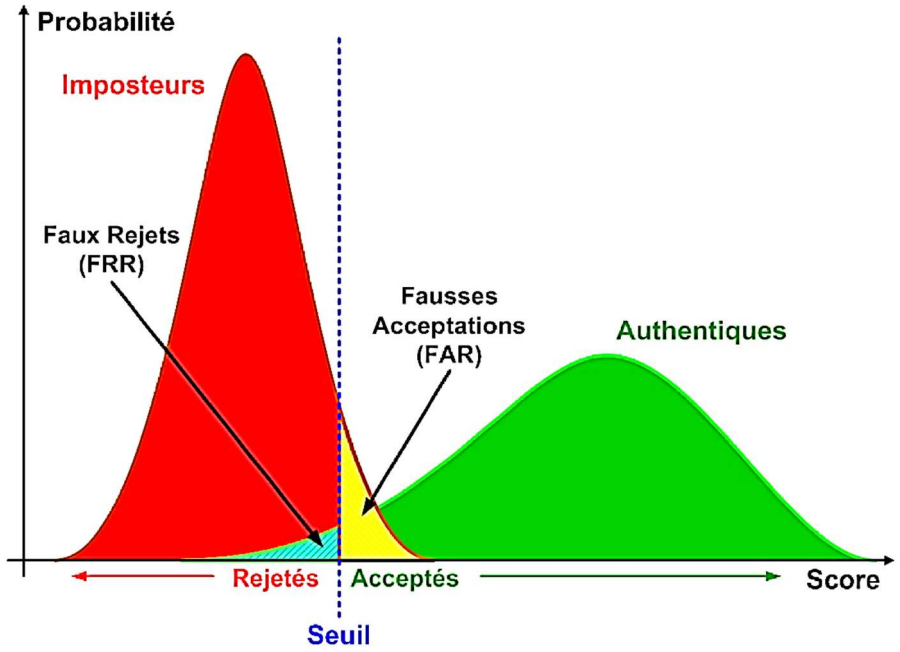

Figure I.18 : *Illustration du FRR et du FAR.*

Selon la nature (authentification ou identification) du système biométrique, il existe deux façons d'en mesurer la performance :

- Lorsque le système opère en mode authentification, on utilise ce que l'on appelle une courbe ROC (pour "Receiver Operating Characteristic" en anglais). La courbe ROC (Figure I.19) trace le taux de faux rejet en fonction du taux de fausse acceptation. Plus cette courbe tend à épouser la forme du repère, plus le système est performant, c'est-à-dire possédant un taux de reconnaissance global élevé [3].

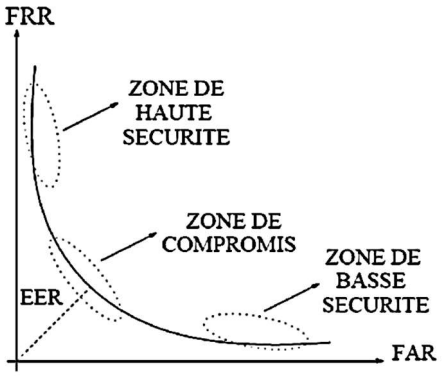

Figure I.19: *Courbe ROC.*

- En revanche, dans le cas d'un système utilisé en mode identification, on utilise ce que l'on appelle une courbe CMC (pour "Cumulative Match Characteristic" en anglais). La courbe CMC (Figure I.20) donne le pourcentage de personnes reconnues en fonction d'une variable que l'on appelle le rang. On dit qu'un système reconnaît au rang 1 lorsqu'il choisit la plus proche image comme résultat de la reconnaissance. On dit qu'un système reconnaît au rang 2, lorsqu'il choisit, parmi deux images, celle qui correspond le mieux à l'image d'entrée, etc. On peut donc dire que plus le rang augmente, plus le taux de reconnaissance correspondant est lié à un niveau de sécurité faible [3].

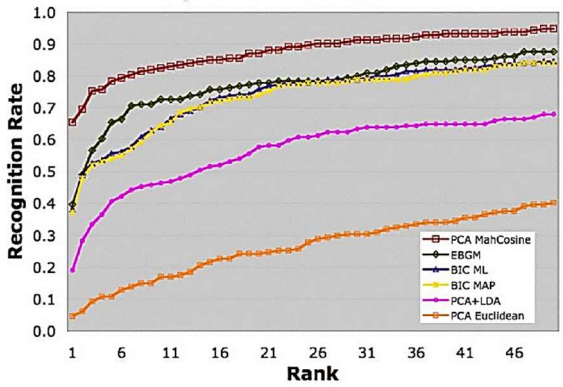

Figure I.20 : *Courbes CMC*

Enfin, il faut savoir que la courbe CMC n'est qu'une autre manière d'afficher la performance d'un système biométrique et peut également être calculée à partir du FAR et du FRR.

I.9. Domaine d'application

Aujourd'hui, les principales applications sont la production de titres d'identité, le contrôle d'accès à des sites sécurisés, le contrôle des frontières, l'accès aux réseaux, systèmes d'information et stations de travail, le paiement électronique, la signature électronique et même le chiffrement de données [4]. Cette liste n'est pas exhaustive, et de nouvelles applications vont très certainement voire rapidement le jour.

Les techniques biométriques sont appliquées dans plusieurs domaines et leur champ d'application couvre potentiellement tous les domaines de la sécurité où il est nécessaire de connaître l'identité des personnes [7]. Les applications peuvent être divisées en quatre groupes principaux :

✓ **Service public :** La biométrie est fréquemment utilisée par les services d'immigration pour contrôler automatiquement l'identité des personnes entrantes ou sortantes d'un territoire, ainsi l'iris, le visage et l'empreinte digitale sont à l'essai dans de nombreux aéroports. De même en santé publique, la biométrie serait utile pour supprimer les cartes d'assurance sociale, ou du moins vérifier l'identité de leur propriétaire [4].

✓ **Application judiciaire :** telles que l'identification de cadavre, la recherche criminelle, l'identification de terroriste, les enfants disparus, etc [7].

✓ **Transaction commerciale et bancaire :** telles que l'accès au réseau informatique, la sécurité de données électroniques, le commerce électronique, l'accès d'internet, l'ATM, la carte de crédit, le contrôle d'accès physique, le téléphone portable, le PDA, la gestion des registres médicales, l'étude de distances, etc.

✓ **Accès physique et logique** : On parle de contrôle d'accès physique lorsqu'on cherche à sécuriser l'accès à un lieu (entrée d'un bâtiment), alors que le contrôle d'accès logique concerne l'accès informatique à un terminal, serveur et réseau informatique ou de télécommunication (ex : ordinateur, téléphone portable, base de données privée). La plus ancienne technologie de contrôle d'accès relève bien sûr de la serrurerie. Celle-ci a plusieurs défauts qui conduisent aujourd'hui à son remplacement progressif [4]. Les hôtels, par exemple, utilisent des clés magnétiques ou optiques qui peuvent être neutralisées et remplacées en un instant si elles sont perdues ou emportées par un hôte distrait. La clé magnétique peut aussi être individualisée,

devenant ainsi une technologie d'identification de son usager. Dans une entreprise où chaque employé détient une carte personnalisée, il devient dès lors facile de savoir qui a ouvert quelle porte à quel moment, et de conserver cette information dans des banques de données pour consultation éventuelle, ou pour en extraire des patterns de comportement. Fonctionnellement, ceci est équivalent à l'assignation d'un code personnel à chaque individu disposant d'un accès dans un lieu. L'avantage est que le code imprimé sur une carte peut être beaucoup plus long que celui que son titulaire doit tenter de mémoriser, et qu'il offre ainsi davantage de combinaisons possibles.

I.10. Marché mondial de la biométrie

Dans son rapport intitulé « Sensors for Biometry and Recognition 2016 », l'Institut d'études **Yole** Développement estime que les technologies d'empreintes digitales dominantes évolueront progressivement vers des solutions multimodales. La conclusion la plus importante souligne que le secteur des applications smartphone constitue le moteur majeur du développement de la biométrie à près de 66% du marché total de la biométrie. La biométrie pour le consommateur bénéficiera sans doute d'une croissance de l'ordre de 10% de 2016 à 2021, selon les analystes de **Yole** [8].

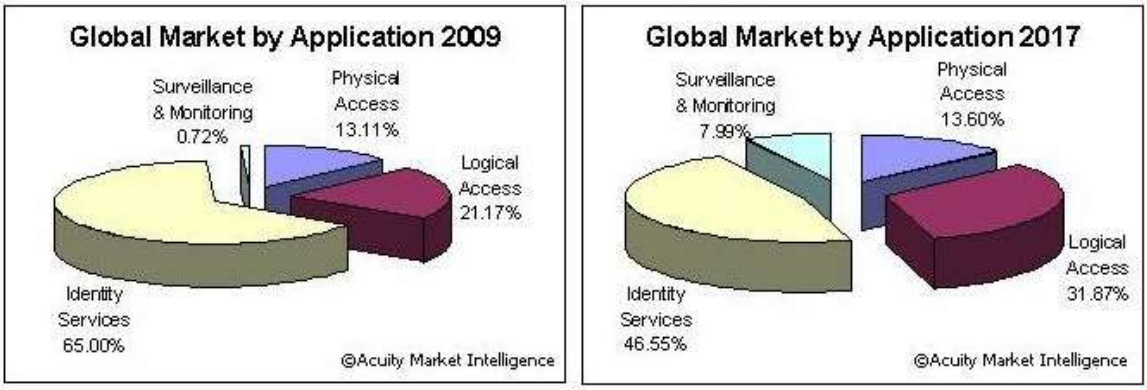

Figure I.21 : *le marché biométrique partager par application.*

Selon **Yole**, 525 millions d'unités de capteurs auraient été vendues en 2015 et ce chiffre devrait atteindre 1.500 millions d'unités d'ici à 2021. A côté de la détection des empreintes digitales pour le déverrouillage et le paiement mobile, il faut compter avec les technologies de reconnaissance visuelle pour la sécurité basée sur les images combinées de l'œil et du visage. En outre, les assistants vocaux développés par Amazon et Google mettent en jeu des modules de reconnaissance vocale enregistrée [8].

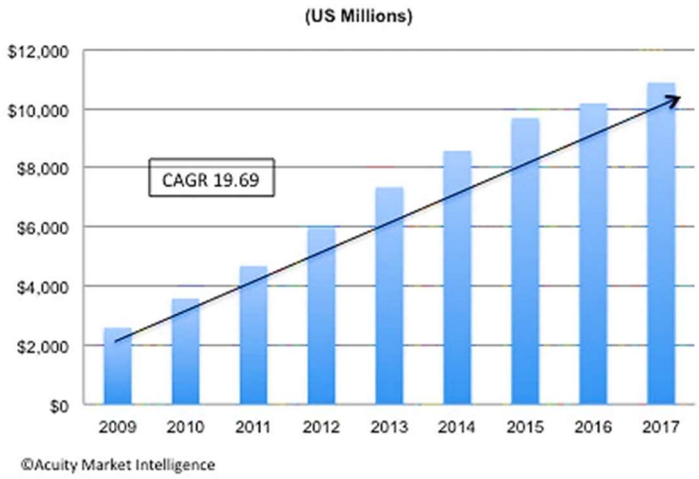

Figure I.22 : *Revenus de l'industrie biométrique*

En ce qui concerne le marché de la sécurité, la Chine, l'Afrique, l'Inde et l'Amérique du Sud sont les nouveaux filons du marché des lecteurs biométriques.

Le marché de la biométrie est en plein boom : selon l'agence **Markets & Markets,** le marché mondial de la biométrie représentera 8,5 milliards d'euros d'ici 2015. Cette expansion se fait particulièrement sentir dans les pays émergents où les états civils, quand ils existent, sont souvent parcellaires [8].

I.11. Conclusion

Aujourd'hui, la biométrie est considérée comme moyen le plus sûr pour la sécurité. Grâce à ses avantages elle est de plus en plus appliquée dans la réalité. Ses applications se catégorisent en : applications de contrôle d'accès, applications dans les téléphone portables, application dans l'e-commerce etc... Néanmoins la biométrie a aussi des limitations ; par exemple la précision des techniques biométriques est faible. Outre on n'a pas encore d'habitude d'utiliser les systèmes biométriques

Dans ce chapitre, nous avons présenté un état de l'art sur les technologies biométriques. Nous avons mis en relief le grand nombre de ces technologies par indiquer quelques points forts et faibles de chaque technologie celles qui mettent en évidence le fait qu'elles ne sont pas toutes de même efficacité.

CHAPITRE II

MULTIMODALITÉ ET FUSION DES DONNÉES

II.1. Préambule

Avec des systèmes biométriques utilisant une seule modalité biométrique (appelés systèmes uni-modaux), on ne peut pas garantir avec certitude une bonne identification. En fait, les taux d'erreur associés à ces systèmes sont relativement élevés, ce qui les rend inacceptables pour des applications critiques de sécurité. Ce problème peut être résolu par la mise en place des systèmes biométriques multimodaux utilisant plusieurs modalités biométriques d'une même personne [6].

Dans le présent chapitre, après avoir dressé un état de l'art sur la biométrie multimodale, nous allons détailler la notion de fusion appliquée à la biométrie et les différents niveaux de fusion possibles. Enfin, nous porterons notre attention sur la notion de normalisation des scores.

II.2. Multimodalité

Bien que de nos jours il existe des techniques biométriques extrêmement fiables telles que la reconnaissance de la rétine ou de l'iris, elles sont coûteuses et, en général, mal acceptées par le grand public et ne peuvent donc être réservées qu'à des applications de très haute sécurité. Pour les autres applications, des techniques telles que la reconnaissance du visage ou de la voix sont très bien acceptées par les utilisateurs mais ont des performances encore trop peu satisfaisantes pour être déployées dans des conditions réelles [1].

Afin d'améliorer la sécurité des systèmes précédents, une première solution consiste à intégrer plusieurs modalités. Cette méthode permet d'améliorer la sécurité du système. La multi modalité est une alternative qui permet d'améliorer de manière systématique la performance d'un système biométrique. Par performance, nous entendons à la fois la précision du système mais aussi son efficacité. En effet, des classificateurs différents font en général des erreurs différentes, et il est possible de tirer parti de cette complémentarité afin d'améliorer la performance globale du système [1].

II.3. Techniques de multimodalité

La multimodalité est l'utilisation de plusieurs modalités biométriques. La combinaison de plusieurs modalités a pour objectif d'en diminuer les limitations des systèmes uni-modaux. En effet, l'utilisation de plusieurs modalités a pour but premier d'améliorer les performances de reconnaissance. En augmentant la quantité d'informations discriminante de chaque personne, on souhaite augmenter le pouvoir de reconnaissance du système. De plus, le fait d'utiliser

plusieurs modalités biométriques réduit le risque d'impossibilité d'enregistrement ainsi que la robustesse aux fraudes [4].

II.4. Quelques travaux existants

Généralement, le choix et le nombre de modalités biométriques sont largement déterminés par la nature de l'application, les frais consommés par multiples modalités, et la corrélation entre les modalités considérées. Les informations non corrélées sont préférées pour l'amélioration de la performance, par exemple dans un téléphone portable équipé d'une caméra, il pourrait être plus facile de combiner les modalités de visage et de la voix d'un utilisateur. Tandis que dans une application ATM il serait plus facile de combiner les modalités de l'empreinte digitale et du visage de l'utilisateur. Donc, une diversité de systèmes biométriques multimodaux a été proposée dans la littérature utilisant différentes modalités biométriques basées sur différentes approches appropriées à ces données biométriques [9].

George et al. 2008 George a proposé un système de vérification de personnes en se basant sur deux modalités biométriques : l'empreinte digitale et le visage. L'auteur a utilisé le Laplacianface comme extracteur de caractéristiques du visage et l'algorithme de Directionnel Filer Bank pour caractériser l'image d'une empreinte digitale. Donc, Chaque image de visage dans l'espace image est associée à un sous-espace de visage de faible dimension. Ce sous-espace se caractérise par un ensemble de caractéristiques d'images, appelées Laplacianfaces. Alors que pour l'empreinte digitale, l'auteur procède à détecter un point de référence pour localiser une région d'intérêt (ROI). A partir du ROI, il procède ensuite à extraire les caractéristiques de l'empreinte digitale en décomposant l'image en plusieurs sous-bandes directionnelles. De la sous-bande décomposée, des valeurs de l'énergie directionnelle sont calculées pour chaque bloc. Donc, le ROI sera représenté par les énergies directionnelles normalisées pour chaque bloc. Dans cette représentation, seule les énergies directionnelles dominantes sont conservées. Le reste des énergies directionnelles sont remis à zéro, et les traités comme du bruit. Au niveau de la phase de comparaison, l'auteur calcule une distance Euclidienne pour mesurer le degré de vraisemblance entre l'image de référence et celle en question. Pour valider la vérification de la personne en question, l'auteur se base sur MBP-ANN. Donc l'apprentissage de ce classifieur est basé sur les caractéristiques déjà extraites des deux modalités.

Le et al. (2010) ont proposé un système d'identification biométrique multimodale basée sur la géométrie du doigt, l'imprimer jarret et l'empreinte de la paume de la main. Après l'acquisition de l'image de la main, les auteurs procèdent à localiser la paume de la main dans

une image et les doigts dans une autre image. Ils binarisent l'image de la main pour détecter le contour et les points clé qui aident à localiser les deux ROI. Puis, ils passent à extraire les caractéristiques de chaque ROI : les caractéristiques géométriques des 4 doigts, l'imprimer jarret et les points clé de la paume de la main. Les caractéristiques géométriques du doigt se sont déterminées à partir des surfaces de blocs décomposés à partir du doigt.

Khana et al. (2008) ont proposé un système biométrique multimodal basé sur la fusion du visage et de l'empreinte digitale pour l'authentification de personnes. Ce système a été appliqué dans un espace limité de jetons. L'empreinte digitale sera cryptée sur une image d'un visage pour les sauvegarder dans un jeton comme smart cards. L'empreinte digitale est encodée par le filtre de Gabor. En fait, le cryptage et le décryptage du code de l'empreinte digitale sont basés sur la transformée d'ondelette et l'inverse de la transformée d'ondelette. A la suite du décryptage, le visage sera comparé avec l'image de référence ainsi que l'empreinte digitale qui sera comparée avec son gabarit. Donc, deux scores seront générés pour les combiner par une simple équation de somme.

Hassan Soliman (2012) a présenté une étude sur les systèmes biométriques multimodaux basés sur les veines de palmiers et la signature. L'auteur procède à extraire les caractéristiques des deux modalités en se basant sur les opérations morphologiques et l'algorithme invariant d'échelle d'entité Transforme (EIPD). Puis, les deux vecteurs de caractéristiques ont été soumises à la transformée en cosinus discrète (DCT) pour réduire leurs dimensionnalités. Par la suite, le classificateur Vector Linear Quantification (LVQ) est utilisé avec les paramètres modifiés pour classer les différentes personnes dans la base de données. Ainsi, la fusion au niveau des caractéristiques pour les deux utilise une simple règle de somme. Finalement ils en déduisent que l'algorithme SIFT est plus précis et n'a pas besoin de plus d'étapes de prétraitement pour identifier les personnes.

II.5. Nécessités de la multimodalité

Bien que quelques systèmes uni-modaux développés dans la littérature ont permis d'achever des améliorations considérables en termes de fiabilité et de précision, ils souffrent, cependant, de plusieurs problèmes tels que la non universalité des caractéristiques biométriques et l'insuffisance de précision des données qui sont bruitées. Ainsi, les systèmes biométriques uni-modaux ne peuvent pas être en mesure d'atteindre les exigences de performances désirées dans les applications du monde réel. Afin de pallier ces problèmes, les systèmes biométriques multimodaux, qui combinent l'information provenant de multiples modalités, ont été proposés.

Des études ont démontré que les systèmes biométriques multimodaux peuvent obtenir des meilleures performances par rapport aux systèmes biométriques uni-modaux [6].

II.5.1. Problèmes liés aux systèmes uni-modaux

❖ **La non-universalité des biométries :** Les systèmes uni-modaux sont basés sur une seule modalité biométrique. Cependant, cette modalité doit être vérifiée à la condition d'universalité, ce que signifie que chaque personne devrait obligatoirement avoir cette modalité pour un système donné. Ce principe d'universalité constitue une des conditions nécessaires de base pour un système de reconnaissance biométrique. La non-universalité signifie que certaines modalités biométriques ne sont pas possédées par la personne à reconnaitre ou ne sont pas assez riche en information pour permettre la reconnaissance de l'identité de certaines personnes [6]. Par exemple (voir figure II.01), certaines personnes peuvent avoir les empreintes digitales ou palmaires inutilisables à cause d'un accident ou d'un travail manuel prolongé. Une personne muette ne peut utiliser la reconnaissance par la voix ou une personne handicapée ne peut signer. De la même manière, des personnes ayant des maladies oculaires (comme certains glaucomes et cataractes) ne peuvent fournir des images d'iris, ou de rétine, de bonne qualité pour une reconnaissance automatique. Pour toutes ces personnes, certains systèmes biométriques ne sont pas accessibles et ceci risque alors de les exclure de certaines utilisations si aucune alternative ne leur est proposée [6].

Figure II.01 : *malformation des mains, visage et de l'iris.*

❖ **Bruit introduit par le capteur :** Du bruit peut être présent dans les données biométriques acquises, ceci étant principalement dû à un capteur défaillant ou mal entretenu. L'acquisition des biométries peut également être impossible à cause des conditions environnementales lors de l'acquisition. Par exemple il est impossible d'utiliser un système de reconnaissance de la voix dans un endroit très bruité ou de reconnaissance par le visage lorsqu'il fait nuit (si l'on utilise une caméra à lumière visible). Le taux de reconnaissance d'un système biométrique est très sensible à la qualité de l'échantillon biométrique et des données bruitées peuvent sérieusement compromettre la précision du système [4].

❖ **La sensibilité aux attaques :** Une autre limitation des systèmes biométriques est la sensibilité aux attaques en reproduisant certaines modalités biométriques. Ceci est possible pour les modalités biométriques comportementales qui sont plus sensibles à ce genre d'attaque que les modalités biométriques physiologiques. A priori, s'il est relativement simple de reproduire une signature ou imiter la voix d'une personne, il est plus difficile de reproduire, par exemple, l'empreinte digitale. Cependant, certaines études ont montré qu'il était possible de fabriquer des fausses empreintes digitales en gomme et de les utiliser pour contrer un système biométrique [6].

❖ **Manque d'individualité :** Les caractéristiques extraites à partir de données biométriques d'individus différents peuvent être relativement similaires. Par exemple, une certaine partie de la population peut avoir une apparence faciale pratiquement identique due à des facteurs génétiques (père et fils, vrais jumeaux, …etc.) [4].

❖ **Manque de représentation invariante :** Les données biométriques acquises à partir d'un utilisateur lors de la phase de reconnaissance ne sont pas identiques aux données qui ont été utilisées pour générer le modèle de ce même utilisateur lors de la phase d'enrôlement. Ces variations peuvent être dues à une mauvaise interaction de l'utilisateur avec le capteur, à l'utilisation de capteurs différents lors de l'enrôlement et de la reconnaissance et à des changements de conditions de l'environnement ambiant.

A cause de tous ces problèmes pratiques, les taux d'erreur associés à des systèmes biométriques uni-modaux sont relativement élevés, ce qui les rend inacceptables pour un déploiement d'applications critiques de sécurité [4].

II.5.2. Avantages des systèmes multimodaux

La reconnaissance biométrique multimodale constitue un enjeu important pour les prochaines années. L'intérêt croissant pour la multimodalité tient à plusieurs facteurs. Premièrement, la combinaison naturelle de différentes sources d'informations permet d'augmenter les performances de reconnaissance. Ensuite, la disponibilité d'une biométrie parmi d'autres est accrue, *i.e.* le système peut changer de modalité dès lors qu'une modalité donnée devient indisponible [6].

De plus, la multimodalité permet de diminuer les contraintes utilisateurs liées au processus de reconnaissance [4]. L'acquisition de l'image d'une iris, par exemple, est souvent très contraignante. La voix peut être plus aisément acquise par des microphones. Finalement, pour des systèmes réels sous certaines conditions d'utilisation, il a été remarqué que le contrôle

d'accès couplé à l'utilisation de l'iris (une biométrie très performante) est mal perçu par les personnes utilisant le système (problème d'acceptabilité de la modalité biométrique). Il y a donc un compromis à gérer entre les taux d'erreurs présentés pour une modalité et son taux d'acceptabilité. La voix et le visage sont des modalités dont les taux d'erreurs sont beaucoup plus élevés que l'iris, mais qui sont en revanche très bien acceptées par les utilisateurs.

II.6. Types de Multimodalités

Les systèmes biométriques multimodaux diminuent les contraintes des systèmes biométriques uni-modaux en combinant plusieurs systèmes. On peut différencier 5 types de systèmes multimodaux selon les systèmes qu'ils combinent [7] (Figure II.02).

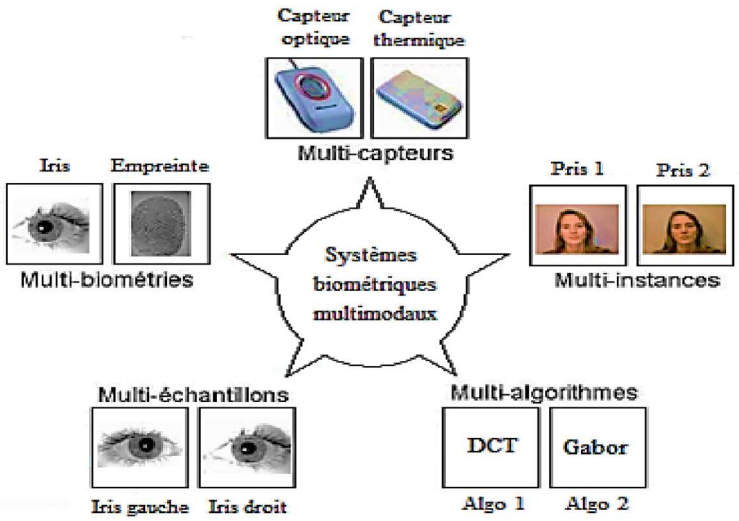

Figure II.02 : *Différents systèmes multimodaux.*

✓ **Multi-capteurs :** lorsqu'ils associent plusieurs capteurs pour acquérir la même modalité, par exemple un capteur optique et un capteur capacitif pour l'acquisition de l'empreinte digitale.

✓ **Multi-instances** : lorsqu'ils associent plusieurs instances de la même biométrie, par exemple l'acquisition de plusieurs images de visage avec des changements de pose, d'expression ou d'illumination.

✓ **Multi-algorithmes :** lorsque plusieurs algorithmes traitent la même image acquise, cette multiplicité des algorithmes peut intervenir dans le module d'extraction en considérant plusieurs ensembles de caractéristiques et/ou dans le module de comparaison en utilisant plusieurs algorithmes de comparaison.

✓ **Multi-échantillons :** lorsqu'ils associent plusieurs échantillons différents de la même modalité, par exemple deux empreintes digitales de doigts différents ou les deux iris. Dans ce

cas les données sont traitées par le même algorithme mais nécessitent des références différentes à l'enregistrement contrairement aux systèmes multi-instances qui ne nécessitent qu'une seule référence.

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

Tous ces types de systèmes peuvent pallier à des problèmes différents et ont chacun leurs avantages et inconvénients. Les quatre premiers systèmes combinent des informations issues d'une seule et même modalité ce qui ne permet pas de traiter le problème de la non-universalité de certaines biométries ainsi que la résistance aux fraudes, contrairement aux systèmes "multi-biométries".

En effet, les systèmes combinant plusieurs informations issues de la même biométrie permettent d'améliorer les performances en reconnaissance en réduisant l'effet de la variabilité intra-classe. Mais ils ne permettent pas de traiter efficacement tous les problèmes des systèmes monomodaux. C'est pour cette raison que les systèmes multi-biométries ont reçu beaucoup d'attention de la part des chercheurs [7].

II.7. Architectures

Les systèmes multimodaux associent plusieurs systèmes biométriques et nécessitent donc l'acquisition et le traitement de plusieurs données. L'acquisition et le traitement peuvent se faire successivement, on parle alors d'architecture en série, ou simultanément, on parle alors d'architecture en parallèle.

L'architecture est en réalité surtout liée au traitement. En effet, l'acquisition des données biométriques est en général séquentielle pour des raisons pratiques. Il est difficile d'acquérir en même temps une empreinte digitale et une image d'iris dans de bonnes conditions. Il existe cependant certains cas où les acquisitions peuvent être faites simultanément lorsque les différentes données utilisent le même capteur par exemple les capteurs d'empreintes multi-doigts qui permettent d'acquérir plusieurs doigts simultanément ou même les empreintes palmaires [5].

L'architecture est donc en général liée au traitement et en particulier à la décision. En effet la différence entre un système multimodal en série et un système multimodal en parallèle réside dans le fait d'obtenir un score de similarité à l'issue de chaque acquisition (fusion en

série) ou de procéder à l'ensemble des acquisitions avant de prendre une décision (fusion en parallèle).

II.7.1. Architecture en parallèle

C'est la plus utilisée car elle permet d'utiliser toutes les informations disponibles et donc d'améliorer les performances du système. En revanche, l'acquisition et le traitement d'un grand nombre de données biométriques est coûteux en temps et en matériel, et réduit le confort d'utilisation [7].

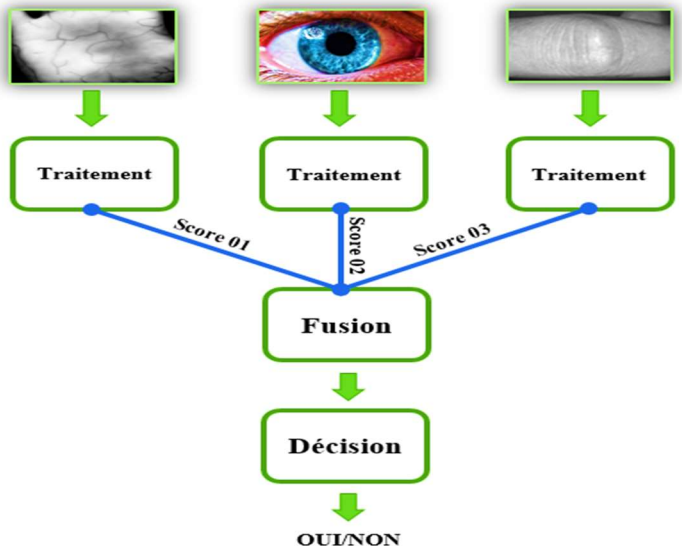

Figure II.02 : *Architecture de fusion en parallèle.*

II.7.2. Architecture en série

Elle Peut être privilégiée dans certaines applications ; par exemple si la multimodalité est utilisée pour donner une alternative pour les personnes ne pouvant pas utiliser l'empreinte digitale. Pour la majorité des individus seule l'empreinte est acquise et traitée mais pour ceux qui ne peuvent pas être ainsi authentifiés on utilise un système à base d'iris alternativement [5].

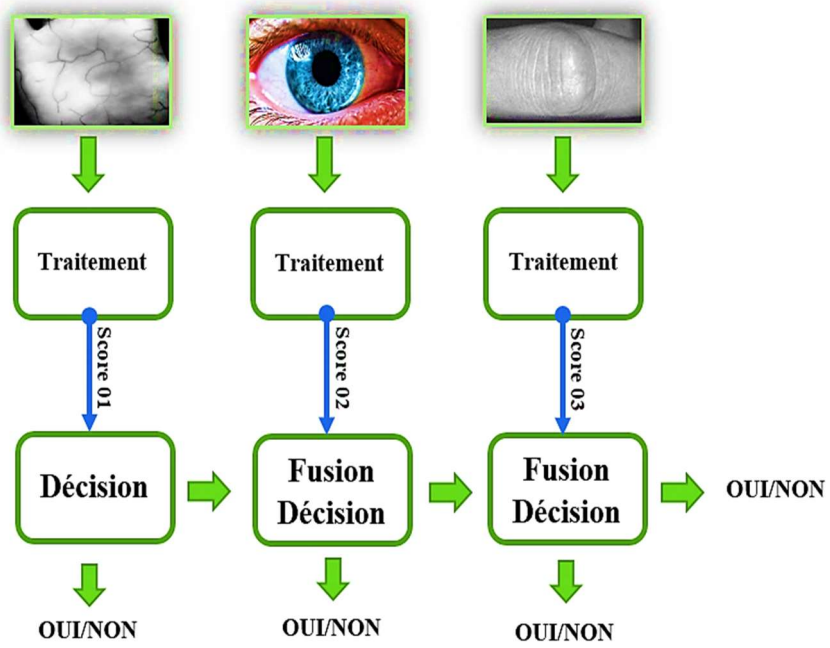

Figure II.03 : *Architecture de fusion en série.*

II.8. Fusion des données

Les humains se reconnaissent entre eux à partir de plusieurs caractéristiques biométriques (physiques ou comportementales) associées à de nombreux détails contextuels de l'environnement. Comme il a été annoncé dans l'introduction concernant les systèmes uni-modaux, chaque modalité en soi ne peut pas toujours être utilisée de manière fiable pour effectuer la reconnaissance. Cependant, la consolidation d'informations présentées par les différentes modalités peut permettre une authentification (ou vérification) précise de l'identité.

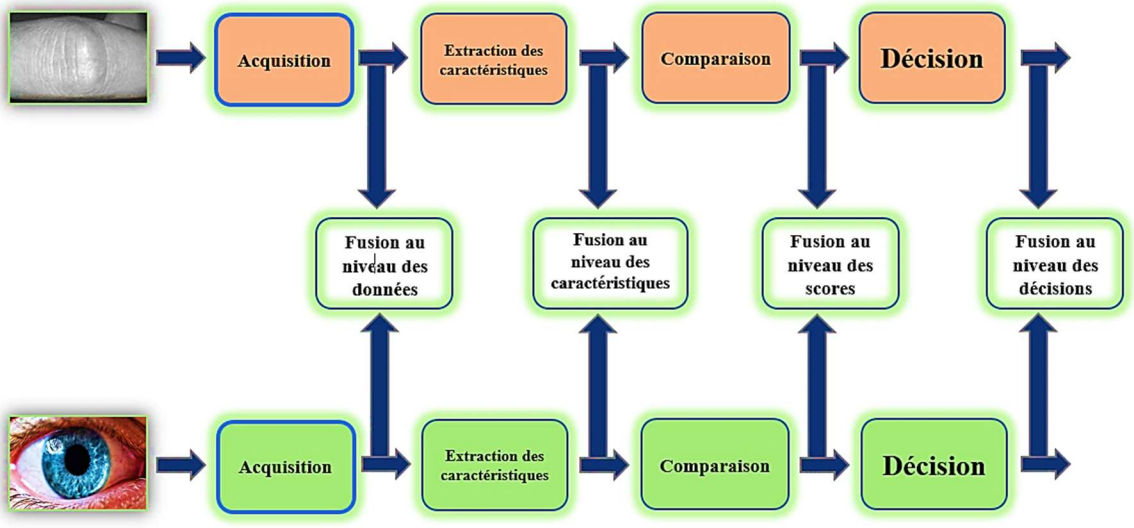

Figure II.04 : *les différents niveaux de fusion.*

On peut donc s'attendre à ce que les systèmes biométriques multimodaux soient plus performants et ceci grâce à la présence de multiples éléments de preuve [10].

II.9. Niveau de fusion

La fusion biométrique multimodale combine des mesures de différents traits biométriques pour renforcer les points forts et réduire les points faibles des différents processus biométriques fusionnés. La combinaison de plusieurs systèmes biométriques peut se faire à quatre niveaux différents : au niveau des données, au niveau des caractéristiques extraites, au niveau des scores issus du module de comparaison ou au niveau des décisions du module de décision [5].

Nous allons maintenant détailler ces niveaux de fusion que l'on peut répartir en deux grandes-ensembles, la fusion avant la correspondance ou pré-classification ("matching") et la fusion après la correspondance ou post-classification.

II.9.1. Fusion pré-classification

Ce genre de fusion correspond à la fusion des informations issues de plusieurs données biométriques au niveau du capteur (images brutes) ou au niveau des caractéristiques extraites par le module d'extraction de caractéristiques. La fusion à ces deux niveaux est limitée car elle nécessite une homogénéité entre les données [7].

✓ **Niveau de capteur :** Les données brutes provenant des capteurs sont combinées par fusion au niveau capteur [11]. La fusion au niveau capteur peut se faire uniquement si les diverses captures sont des instances du même trait biométrique obtenu à partir de plusieurs capteurs compatibles entre eux ou plusieurs instances du même trait biométrique obtenu à partir d'un seul capteur. De plus, les captures doivent être compatibles entre elles et la correspondance entre les points dans les données brutes doit être connue par avance. Par exemple, les images de visage obtenues à partir de plusieurs caméras peuvent être combinées pour former un modèle 3D du visage. Un autre exemple de fusion au niveau capteur consiste à mettre en mosaïque plusieurs images d'empreintes digitales afin de former une image d'empreinte digitale finale plus complexe [12]. La fusion au niveau capteur n'est généralement pas possible si les instances des données sont incompatibles (par exemple, il est peut-être difficile de fusionner des images de visages provenant de caméras ayant des résolutions différentes) [3].

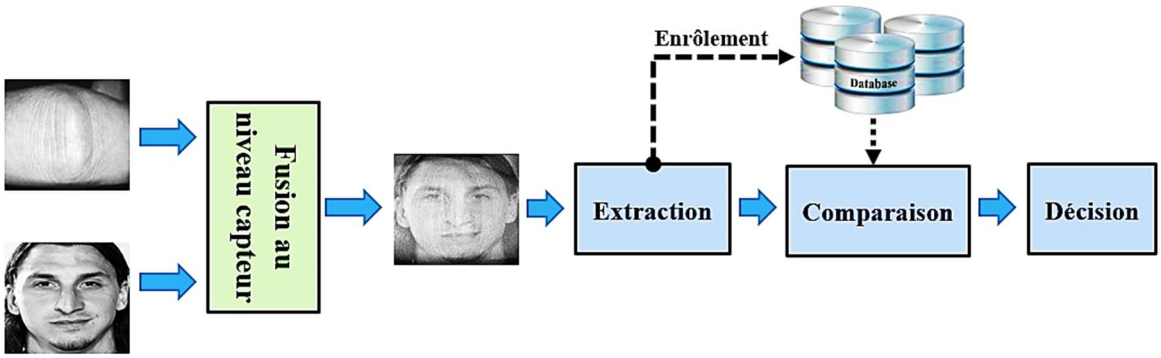

Figure II.05 : *système multimodal basé sur la fusion au niveau de capteur*

✓ **Niveau des caractéristiques :** La fusion au niveau des caractéristiques est moins limitée par la nature des données biométriques. Cependant une certaine homogénéité est nécessaire pour la plupart des méthodes de fusion au niveau des caractéristiques comme par exemple la moyenne de plusieurs "Template" d'empreintes ou de visage. Un exemple de fusion au niveau des caractéristiques qui ne nécessitent pas vraiment d'homogénéité est la concaténation de plusieurs vecteurs de caractéristiques avant le traitement par l'algorithme de comparaison[5]. La raison est que la fusion au niveau caractéristique est plus riche en informations sur les données biométriques brut. Cependant, un tel type de fusion n'est pas toujours possible Par exemple, dans de nombreux cas, les caractéristiques pourraient ne pas être compatibles en raison de la différence dans la nature des modalités. Aussi tel enchaînement peut conduire à un vecteur de caractéristiques avec une très grande dimension. Cela augmente la charge de calcul. Il est rapporté qu'une conception complexe de classificateur pourrait être nécessaire pour opérer sur l'espace des caractéristiques à concaténer [9].

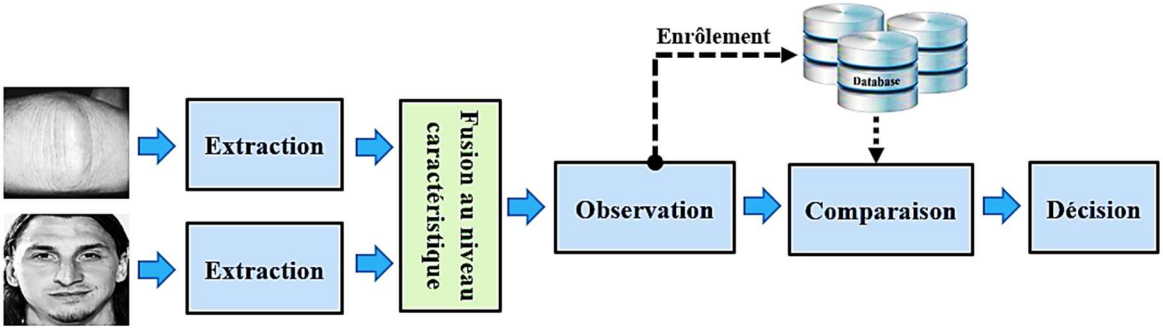

Figure II.06 : *système multimodal basé sur la fusion au niveau de caractéristique*

II.9.2. Fusion post-classification

Elle est très étudiée par les chercheurs. Cette fusion peut se faire au niveau des scores issus des modules de comparaison, au niveau des décisions. La fusion au niveau des décisions

est souvent utilisée pour sa simplicité. Dans les deux cas, la fusion est en fait un problème bien connu de la littérature sous le nom de "Multiple Classifier systems" [7].

✓ **Niveau de décision :** Chaque modalité est d'abord identifiée de façon indépendante. Puis, la décision finale est prise en se basant sur la fusion des décisions des différents processus biométriques. L'intégration d'information au niveau abstrait ou au niveau décision peut être mis en place lorsque chaque matcher biométrique décide individuellement de la meilleure correspondance possible selon l'entrée qui lui est présentée. Les méthodes les plus utilisées sont des méthodes à base de votes telles que le OR (si un système a décidé 1 alors OUI), le AND (si tous les systèmes ont décidé 1 alors OUI) ou le vote à la majorité (si la majorité des systèmes ont décidé 1 alors OUI) [5]. On outre peut également utiliser des méthodes plus complexes qui pondèrent les décisions de chaque sous-système tels que BKS (*Behaviour Knowledge Space*) et le (*weighted voting*) basé sur la théorie "*Dempster-Shafer*" peuvent utilisées afin d'arriver à la décision finale. La fusion au niveau décision est considérée, donc, comme rigide en raison de la disponibilité des informations limitées [9].

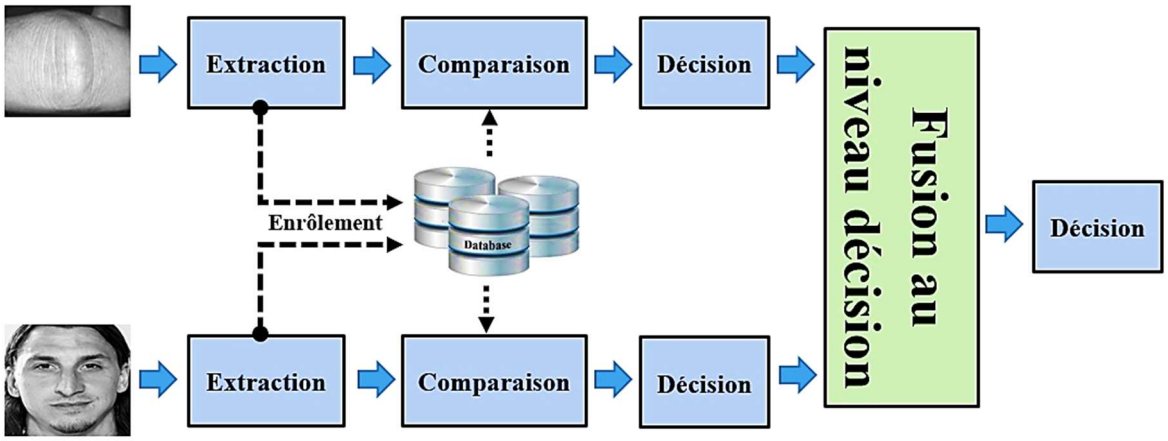

Figure II.07 : *système multimodal basé sur la fusion au niveau de décision*

✓ **Niveau de score :** En fonction de la précision de chaque processus biométrique, nous pouvons fusionner les scores d'appariement résultants de ces processus biométriques pour trouver un appariement composite qui sera envoyé au module de décision. Le niveau des scores est le type de fusion le plus utilisé car elle peut être appliquée à tous les types de systèmes (contrairement à la fusionpré-classification), dans un espace de dimension limité (un vecteur de scores dont la dimension est égale au nombre de sous-systèmes), avec des méthodes relativement simples et efficaces mais traitant plus d'information que la fusion de décisions. La fusion de scores consiste donc à la classification : OUI ou NON pour la décision finale, d'un

vecteur de nombres réels dont la dimension est égale au nombre de sous-systèmes[5]. Aussi, il est relativement facile d'accéder et de combiner les scores générés par les différents matchers. En conséquence, l'intégration d'information au niveau score est l'approche la plus courante dans les systèmes biométriques multimodaux. Nous allons expliquer plus en détail ce niveau de fusion[3].

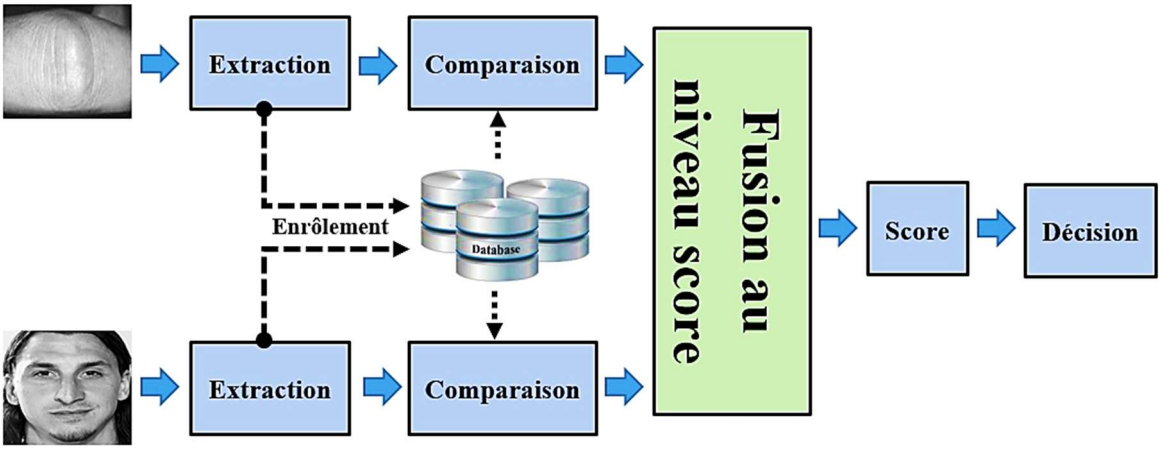

Figure II.08 : *système multimodal basé sur la fusion au niveau de score*

II.10. Fusion au niveau des scores

Il existe deux approches pour combiner les scores obtenus par différents matchers. La première approche est de voir cela comme un problème de classification, tandis que l'autre approche est de traiter le sujet comme un problème de combinaison. Il est important de noter que Jain et al. Ont montré que les approches par combinaison sont plus performantes que la plupart des méthodes de classification [13].

Dans l'approche par classification, un vecteur de caractéristiques est construit en utilisant les scores de correspondance donnés en sortie par les matchers individuels ; ce vecteur est ensuite attribué à une des deux classes : "accepté" (utilisateur authentique ou "genuine user") ou "rejeté" (utilisateur imposteur ou "impostor user"). En général, le classifieur utilisé pour cette opération est capable d'apprendre la frontière de décision sans tenir compte de la manière dont le vecteur de caractéristiques a été généré. Ainsi, les scores en sortie de différentes modalités peuvent être non-homogènes (mesure de distance ou de similarité, différents intervalles de valeurs prises, etc.) et aucun traitement n'est requis avant de les envoyer dans le classifieur [3].

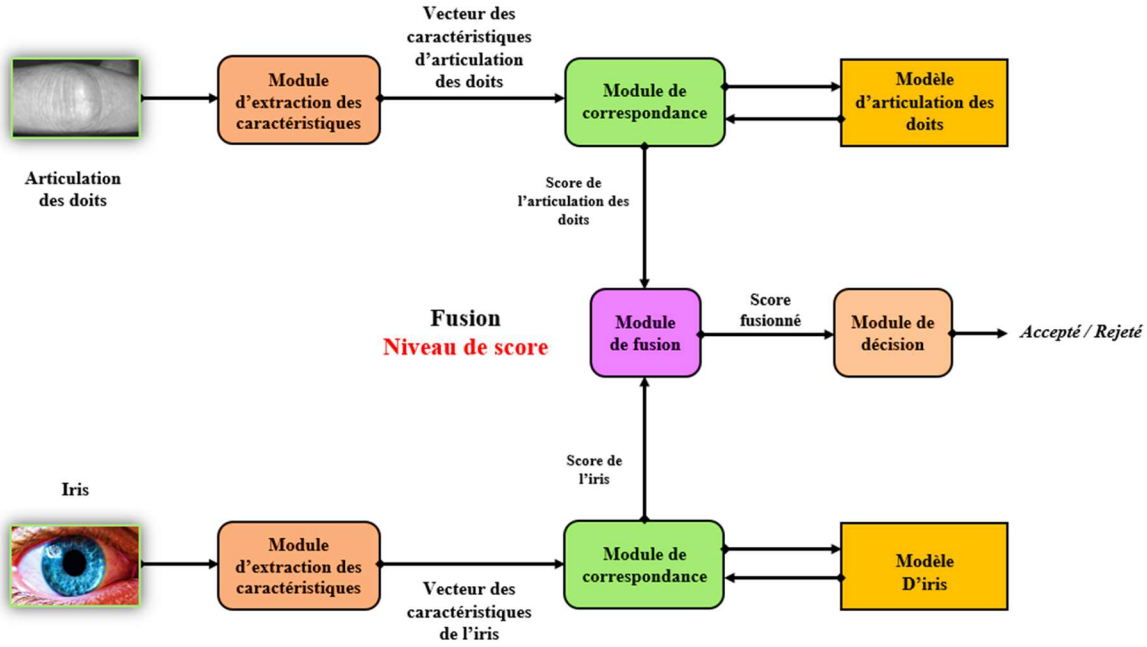

Figure II.09 : *Fusion au niveau score dans un système biométrique multimodal.*

Dans l'approche par combinaison, les scores de correspondance individuels sont combinés de manière à former un unique score qui est ensuite utilisé pour prendre la décision finale. Afin de s'assurer que la combinaison de scores provenant de différentes modalités soit cohérente, les scores doivent d'abord être transformés dans un domaine commun : on parle alors de normalisation de score.

II.11. Normalisation de score

Considérons un système de vérification biométrique multimodale qui adopte une approche de fusion par combinaison, au niveau score [3]. Une étape de normalisation est généralement nécessaire avant que les scores bruts provenant de différents classificateurs peuvent être combinés dans l'étape de fusion. La normalisation aborde le problème des scores incomparables représentant les sorties des différents classificateurs biométriques [9]. Les méthodes de normalisation des scores les plus connus est :

- La méthode Min-Max.
- La méthode Z-score.
- La méthode TanH.

Ont pour objectif de transformer individuellement chacun des scores issus des sous-systèmes pour les rendre homogènes avant de les combiner [6].

II.11.1. Pourquoi normaliser les scores ?

Trois problèmes importants ont besoin d'être considérés avant même de combiner les scores de correspondance en un seul et unique score [3].

- ✓ Les scores de correspondance au niveau des sorties des matchers individuels peuvent ne pas être homogènes. Par exemple, un matcher peut donner en sortie une mesure de distance (dissimilarité) pendant qu'une autre donne en sortie une mesure de proximité (similarité).
- ✓ Les sorties des matchers individuels ne sont pas nécessairement inclus dans le même intervalle.
- ✓ Les scores de correspondance en sortie des matchers peuvent suivre différentes distributions statistiques.

A cause de ces raisons, la normalisation de score est essentielle pour transformer les scores des matchers individuels dans un domaine commun avant de les combiner. La normalisation de score est une étape critique dans la conception d'un schéma de combinaison pour la fusion au niveau score.

II.11.2. Quelques méthodes de normalisation des scores

➢ **Min-Max (MM) :**

Elle est la plus adaptée dans le cas où les bornes (valeurs minimales et maximales) des scores produits par un matchers sont connues. Dans ce cas, on peut facilement translater les scores minimums et maximums respectivement vers 0 et 1 [3]. Cependant, même si les scores de correspondance ne sont pas bornés, on peut estimer les valeurs minimales et maximales pour un jeu de scores de correspondance donné et appliquer ensuite la normalisation Min-Max.

$$n = (s - min(S)) / (max(S) - min(S)) \qquad (II.1)$$

max (S) et *min (S)* définissent les points d'extrémité du domaine de définition des scores[9].

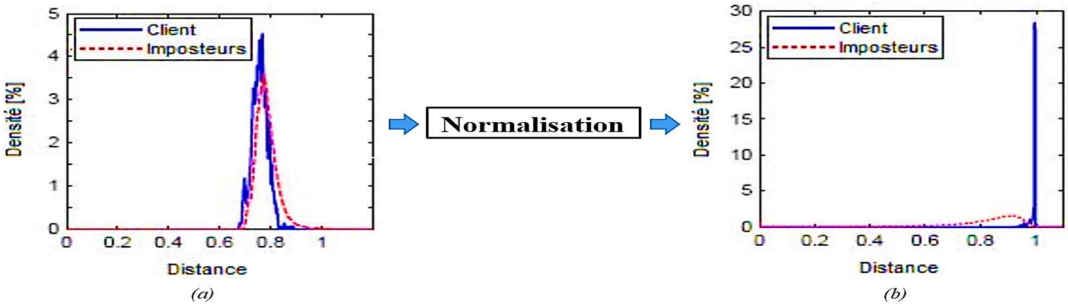

Figure II.10 : *Normalisation des scores par la méthode du Min-Max.*

➢ **Z-score (ZS) :**

La technique de normalisation de score la plus employée qui utilise la moyenne arithmétique et l'écart-type des données. On peut s'attendre à ce que cette méthode fonctionne bien si on a une connaissance a priori du score moyen et des variations de score d'un matcher [3]. Cette méthode transforme les scores à une distribution avec une moyenne égale 0 et un écart type égale 1.

$$n = (s - moyenne\ (S)\ /\ (std\ (S)) \qquad (II.2)$$

moyenne (S) et *std (S)* désignent respectivement la moyenne et le standard de déviation des scores [9].

➢ **Tanh (TH) :**

Sont robustes et très efficaces, Cette méthode est parmi les techniques statistiques les plus solides. Elle trace les scores de la gamme (0, 1) [9].

$$n = 0{,}5\ [tanh\ (0.01\ (s - moyenne\ (S))\ /\ (std\ (S))) + 1] \qquad (II.3)$$

moyenne (S) et *std (S)* désignent respectivement la moyenne et le standard de déviation des scores.

II.11.3. Combinaison des scores

Pour combiner les informations d'identification obtenues à partir de plusieurs modules de recherche en utilisant des schémas tels que la règle somme ("*sum rule*"), la règle maximum ("*max rule*"), la règle somme pondérée ("*weighted sum rule*") et la règle minimum ("*minimum rule*"). Afin d'employer ces schémas, les scores doivent normalisés [4].

Considérons les sorties des modules de recherche individuels $d_1, d_2, d_3, \ldots d_M$ (M sous-systèmes). Les règles suivantes peuvent alors être utilisées pour estimer D_{fusion} [1] :

✓ Règle somme :

$$\boldsymbol{D}_{fusion} = \sum_{i=1}^{M} d_i \qquad (II.4)$$

✓ Règle maximum :

$$\boldsymbol{D}_{fusion} = max_i\ (d_1, d_2, d_3, \ldots, d_M) \qquad (II.5)$$

✓ Règle minimum :

$$\boldsymbol{D}_{fusion} = min_i\ (d_1,\ d_2,\ d_3,\ \ldots,\ d_M) \qquad (II.6)$$

✓ Règle somme pondérée :

$$\boldsymbol{D}_{fusion} = \sum_{i=1}^{M} w_i\, d_i \qquad (II.7)$$

La somme pondérée permet de donner des poids différents w_i à chacun des sous-systèmes en fonction de leur performance individuelle ou de leur intérêt dans le système multimodal [4]. Avec $\sum_{i=1}^{M} w_i = 1$, et :

$$w_i = \frac{1}{\sum_{i=1}^{M} \frac{1}{Ej}} * \frac{1}{Ej} \qquad (II.8)$$

Avec E_j l'erreur associée au i^{eme} sous-système.

II.12. Les stratégies d'intégration

La stratégie adoptée pour l'intégration dépend du niveau au cours duquel la fusion est réalisée. La fusion au niveau de caractéristiques peut être accomplie par la concaténation de deux ensembles de caractéristiques compatibles. La fusion au niveau score a été bien étudié dans la littérature. Les techniques de normalisation robustes et efficaces sont nécessaires pour transformer les résultats de plusieurs vérifications dans un domaine commun avant de les consolider. Dans le cadre de la vérification, deux stratégies distinctes existent pour la fusion à ce niveau. Dans la première approche de la fusion est considérée comme un problème de classification où un vecteur de caractéristiques est constitué en utilisant la sortie correspondante à des scores par les vérifications individuelles. Ce vecteur de caractéristiques est ensuite classé dans l'une des deux classes : Accepter ou rejeter. Dans la seconde approche de la fusion est considérée comme un problème de combinaison où les résultats correspondants sont rassemblés pour générer un score unique scalaire qui est ensuite utilisé pour générer la décision finale. Les stratégies générales pour la combinaison de multiples classificateurs ont montré que la règle de la somme est simple suffisante pour obtenir une amélioration significative de la performance de l'appariement d'un système biométrique multimodal. Ils suggèrent également une technique pour incorporer les poids d'utilisateurs spécifiques afin d'améliorer encore les performances du système. Aussi, les stratégies de fusion au niveau de la décision peuvent inclure le vote majoritaire, la méthode de l'espace de connaissance comportementaux, une vote pondérée basée sur la théorie de l'évidence de Dempster-Shafer**,** règles ET / OU, etc [9].

II.13. Conclusion

Ce chapitre a été consacré pour la présentation des généralités sur la biométrie monomodale en plus des généralités sur la biométrique multimodale. C'est un chapitre introductif. Donc, nous avons présenté le jargon de ce domaine biométrique, les avantages et les limitations de la biométrie monomodale ainsi que le contexte général de notre travail en donnant l'avantage d'un système biométrique multimodal par rapport à un système monomodal. Puis, nous avons exposé les différentes formes de la multi modalité, les différents scénarios et niveaux de fusion, les stratégies d'intégration d'un système biométrique multimodal. Dans la dernière section, nous avons donné un aperçu sur l'historique des systèmes

Conclusion Générale

Conclusion générale

Bien que les techniques de la reconnaissance biométrique promettent d'être très performantes, on ne peut pas garantir actuellement un excellent taux de reconnaissance avec des systèmes biométriques unimodaux, basés sur une unique modalité biométrique. C'est pour cette raison que les systèmes multimodaux ont gagné une place importante dans des domaines différents, notamment dans la reconnaissance des individus qui est de plus en plus présente pour accéder à certains endroits privés.

Dans ce mémoire, après avoir dressé un état de l'art en biométrie et la sécurité d'information et les différentes technologies biométriques, nous avons présenté la fusion multimodale où nous avons détaillé les différents niveaux de fusion et de nombreuses techniques de fusion possibles dans un système biométrique multimodal. Nous avons également présenté quelques méthodes d'extraction des caractéristiques basées sur la texture.

Pour le test, nous avons présenté une nouvelle méthode de reconnaissance biométrique de la main basée sur les articulations des doigts (FKP) qui pouvait fournir d'excellents résultats en termes de taux d'égale erreur (EER), de taux de reconnaissance et de séparation globale des distributions des imposteurs et clients. Nous avons utilisé une nouvelle méthode AEBP ou bien LBP par bloc basée sur des blocs pour l'extraction de vecteur de caractéristique.

Les résultats obtenus montrent l'efficacité de la méthode LBP dans l'identification des personnes. L'erreur EER était de moins de 2.626% dans le cas des doigts gauches. Cependant, une nette amélioration a été présentée avec l'application de la méthode AEBP. Ici, la partition de l'image en plusieurs zones a permis de réduire cette erreur à moins de **0.0673%** dans le cas de la taille de bloc est **12x12** et le pourcentage de chevauchement est **75%**. Même que chaque bloc possède son propre vecteur caractéristique, c'est grâce au recouvrement (chevauchement) de ces blocs que le simple assemblage de ces vecteurs produit un vecteur représentatif unique qui identifie mieux la personne. La multimodalité biométrique a été appliquée en fusionnant au niveau des scores les deux modalités doigts gauches et doigts droites avec une mesure de distance par la méthode Min-Max. Une erreur EER nulle a prouvé sa très grande efficacité de ce choix.

D'après l'étude effectuée, on peut conclure que la méthode proposée a donné une performance remarquable dans les deux applications traitées (identification et vérification par la reconnaissance des articulations des doigts).

Notre futur travail sera concentré sur l'évaluation de la performance dans les deux phases (vérification et identification) en utilisant une base de données de grande taille et de l'intégration d'autres traits biométriques pour obtenir les performances du système avec une grande précision.

Bibliographies

Bibliographies

[1] *M. Radia Salhi Mebarka*, “L’identification de l’empreinte palmaire basée sur la fusion des données pour la reconnaissance des personnes”, Mémoire de Fin d’Etude pour l’obtention du diplôme d’ingénieur d’état, 2009.

[2] *Anis CHAARI*, "L' identification dans les bases de données biométriques basée sur une classification non supervisée", Nouvelle approche Pour obtenir le diplôme du doctorat, 2009.

[3] *Nicolas MORIZET*, "Reconnaissance Biométrique par Fusion Multimodale du Visage et de l’Iris", Thèse présentée pour obtenir le grade de Docteur, 2009.

[4] *Laouar radouane et Chelawa rachid*, " Reconnaissance des personnes par leurs empreintes palmaires multi-spectrales basée sur la DCT et le GMM", Mémoire de Fin d’Etude pour l’obtention du diplôme Master académique, 2011.

[5] *Lorène ALLANO*, "La Biométrie multimodale : stratégies de fusion de scores et mesures de dépendance appliquées aux bases de personnes virtuelles", Thèse pour l’obtention du grade de Docteur de l’INSTITUT NATIONAL DES TELECOMMUNICATIONS, 2009.

[6] *Abdallah MERAOUMIA*, “ Modèle de Markov caché appliqué à la multi-biométrie”, THÈSE Présentée pour l’obtention du grade de DOCTEUR, 2014.

[7] *BENCHENNANE Ibtissam*, “ Etude et mise au point d’un procédé biométrique multimodale pour la reconnaissance des individus ”, Thèse pour l’obtention du Diplôme de Doctorat en Sciences, 2016.

[8] www.biometrie-online.net,"http://www.biometrie-online.net/biometrie/le-marche" [Accessed: 01-Jan-2017].

[9] *Hanene Guesmi*, “Identification de personnes par fusion de différentes modalités biométriques”, Thèse de Doctorat Mention, 2014.

[10] *lin hong et al*, “Can multibiometrics improve perfermance”, Dept. of Comp. science and Engg, 1999.

[11] IEEE ENGINEERING IN MEDICINE AND BIOLOGY, “in Distributed” *Education*, pp. 113–115, 1996.

[12] *Tamer Uz et al,* “Minutiae-based template synthesis and matching for fingerprint authentication,” *Comput. Vis. Image Underst.*, vol. 113, no. 9, pp. 979–992, 2009.

[13] Arun a Ross et al, “Score Normalization in Multimodal Biometric Systems Multimodal Biometric Systems,” *Pattern Recognit.*, vol. 38, no. 12, pp. 4–5, 2005.

[14] *D. R. Arun et al*, “Local Binary Patterns and Its Variants for Finger Knuckle Print Recognition in Multi-Resolution Domain,” Scientific Research Publishing Inc, pp. 3142–3149, August 2016.

[15] *A. Kumar et al*, “Personal authentication using finger knuckle surface,” *IEEE Trans. Inf. Forensics Secur.*, vol. 4, no. 1, pp. 98–110, 2009.

[16] *A. Kumar*, "Personal identification using finger knuckles," *SPIE Newsroom*, vol. 45, no. 20, pp. 1–8, 2009.

[17] *BENAGGA Abderahmane et TELIB Lina*, "Reconnaissance des personnes basée sur l'empreinte de l'articulation de doigt", Memoire Master Academique, 2016.

[18] *M. Brahim oussama et A. Mohamed ibrahim*, "Identification des personnes par les articulations des doigts", Memoire Master Academique, 2015.

[19] *Saidat Djemaa et Gueziz Fatiha*, "Identification des personnes par l ' empreinte de l ' articulation des doigts", Memoire Master Academique, 2016.

[20] *Slobodan Ribaric et al*, "An Online Biometric Authentication System Based On Eigenfingers And Finger-Geometry", Faculty of Electrical Engineering and Computing, University of Zagreb Unska 3, 10000, Zagreb, Croatia, April 2015.

[21] *T. Ojala et al*, "A comparative study of texture measures with classification based on feature distributions", *Pattern Recognit.*, vol. 29, no. 1, pp. 51–59, 1996.

[22] *M. Amraoui et al,* "Finger-Knuckle-Print Recognition Based on Local And Global Feature Sets", Journal of Theoretical and Applied Information Technology 15th December 2012. Vol. 46 No.1.

[23] *Salil Kumar Verma et al*, "Finger-Knuckle-Print Based Recognition System using LBP and SURF", International Journal of Computer Science and Information Technologies, Vol. 6 (3) , 2015, 2863-2867.

[24] *K. FAEZ et al*, "Finger-Knuckle-Print Recognition Via Encoding Local-Binary-Pattern", Journal of Circuits, Systems and Computers, vol. 22, issue 06 (2013) p. 1350050.

[25] *Meraoumia Abdallah et al,* "Using of Finger-Knuckle-Print in biometric security systems.", International Conference on Information Technology for Organizations Development, IT4OD 2016 (2016) Published by Institute of Electrical and Electronics Engineers Inc.

[26] *Peng Fei Yu et al,* "Personal Identification Using Finger-Knuckle-Print Based on Local Binary Pattern.", Applied Mechanics and Materials, vol. 441 (2013) pp. 703-706, 2013.

[27] *Udhayakumar.M et al*, "Palmprint Recognition by using Modified Local Binary Pattern", International Journal of Innovative Research in Science, Engineering and Technology (An ISO 3297: 2007 Certified Organization) Vol. 2, Issue 9, September 2013.

[28] *Meraoumia Abdallah*, "Can Finger Knuckle Patterns Help Strengthen the E-banking Security ?", Int. J. of Embedded Systems, Vol. x, No. x, 2016.

[29] *Meraoumia Abdallah et al*, "Oriented Local Binary Pattern : A new scheme for an efficient feature extraction technique," International Journal of Electrical and Computer Engineering (IJECE) Vol. x, No. x, May 2013, pp. 1 – 16.

[30] *Guangwei Gao et al*, "Reconstruction based finger-knuckle-print verification with score level adaptive binary fusion," *IEEE Trans. Image Process.*, vol. 22, no. 12, pp. 5050–5062, 2013.

[31] *Lin Zhang et al*, "Finger-knuckle-print: A new biometric identifier," *Proc. - Int. Conf.*

Image Process. ICIP, pp. 1981–1984, 2009.

[32] *G. S. Badrinath et al*, "An efficient finger-knuckle-print based recognition system fusing SIFT and SURF matching scores", Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics*)*, vol. 7043 LNCS, pp. 374–387, 2011.

Abstract : In the last recent years, automatic personal identification has become an important requirement in variety of applications such as access control, surveillance systems and physical buildings. Biometrics, which deals with identification of individuals based on their physical or behavioral features, has been emerging as an effective automatic identification technology. It offers more properties and several advantages then the traditional security. Finger-Knuckle-Print (FKP) is a very important biometric feature which provides uniqueness, stability and high distinguished ability. The system commitment concept that is associated with the Finger-Knuckle-Print (FKP) is the core of our proposed system. However, such a system will only be efficient if the FKP features are accurately extracted. For this, we have used a new method of feature extraction called Adaptive Extended Binary Pattern (AELBP). The unimodal biometric system has some problem like noisy sensor data, non-universality, lack of individuality, lack of invariant representation and susceptibility to circumvention. So, for overcoming these disadvantages, multimodal biometric system is applied. Our experimental results, using FKP data base (PolyU), demonstrate the higher performance of the proposed FKP based identification system.

Key words: Biometrics, FKP, Feature extraction, Identification, BLBP, LBP, multimodal, fusion.

Résumé : Au cours des dernières années, l'identification personnelle automatique devient une exigence importante en différentes applications telles que le contrôle d'accès, les systèmes de surveillance et les bâtiments physiques. La Biométrie, qui traite l'identification des individus en fonctionnant sur leurs caractéristiques physiques ou comportementales, est apparue comme une technologie d'identification automatique efficace. Elle offre plus de propriétés et plusieurs avantages parrapport à la sécurité traditionnelle. L'empreinte de l'articulation de doigts (FKP) est une caractéristique biométrique importante. Elle fournit l'unicité, la stabilité et la haute distinction de la capacité. Le concept d'engagement du système qui est associé aux articulations des doigts (FKP) est au cœur de notre système proposé. Cependant, un tel système ne sera efficace que les caractéristiques de FKP sont extraites avec précision. Pour cela, nous avons utilisé une nouvelle méthode d'extraction des caractéristiques appelée Adaptive Extended Binary Pattern (AELBP). Le système biométrique uni-modal rencontre des problèmes tels que les données bruyantes du capteur, non-universalité, l'absence de l'individualité, l'absence de représentation invariante et de la sensibilité au contournement. Donc, pour remédier à ces inconvénients, le système biométrique multimodal est appliqué. Nos résultats expérimentaux, en utilisant la base des données FKP (PolyU) démontrent la meilleure performance du système d'identification sur la base FKP proposée.

Mots clés : biométrie, FKP, extraction des caractéristiques, identification, MB-LPQ, LBP, unimodal, multimodale, fusion

ملخص : خلال السنوات الأخيرة، أصبحت الهوية الشخصية مطلب هام وأساسي في عدة تطبيقات مثل الأمن، أنظمة المراقبة والعمارات .... الخ. لذلك تعالج الأنظمة البيومترية هويات الأشخاص بدلالة مميزاتهم الفيزيائية أو المعنوية والتي تبين أنها تقنية فعالة للتعرف التلقائي على الأشخاص. تتيح هذه الأنظمة التعامل بخاصيات كثيرة كما أنها تمتاز بمزايا عدة مقارنة بالأنظمة التقليدية. تعتبر بصمة مفصل الأصبع (FKP) ميزة بيومترية هامة فهي تتميز بالتفرد (فريدة من نوعها) والثبات وقدرة تمييز عالية. وقد تناولنا في عملنا مفهوم عمل نظام بصمة مفصل الأصبع (FKP) والذي يعتبر العنصر الهام في هذا البحث. ومع ذلك، فإن عمل مثل هذا النظام يكون فعالا إلا إذا تم استخراج ميزات بصمة مفصل الأصبع (FKP) بدقة. لهذا، قمنا باستخدام طريقة جديدة لاستخراج هذه الميزات تسمى تكييف النمط الثنائي الموسع (AELBP). يعاني النظام البيومتري الأحادي الوسائط من بعض الإشكالات كبيانات الاستشعار الصاخبة الصوت وعدم توسعه عالميا إضافة إلى عدم إقبال الأفراد عليه وعدم وجود تمثيل ثابت كما أنه قابل لعمليات التحايل. ومن أجل التغلب على هذه العوائق، تم تطبيق نظام التحقق من الهوية المتعدد الوسائط. وقد أظهرت نتائجنا التجريبية، وذلك استنادا لقاعدة بيانات جامعة (PolyU)، أن نظام بصمة مفصل الأصبع (FKP) يتميز بأداء عالي كنظام مقترح.

الكلمات المفتاحية: البيومترية، FKP، استخراج الميزات، الهوية، أحادي الوسائط، متعدد الوسائط، BLBP، LBP، الدمج.