REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

UNIVERSITE KASDI MERBAH OUARGLA

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

MEMOIRE MASTER ACADEMIQUE

Domaine : Électronique
Spécialité : Automatique

Présenté par :

BENAGGA Abderahmane TELIB Lina

Thème

Reconnaissance des personnes basée sur l'empreinte de l'articulation de doigt

Soutenu publiquement
le : 01/06/2016

Devant le jury :

Mr	Samai Djamal	MCB	Président	UKM Ouargla
Mr	Meraoumia Abdallah	MCB	Encadreur	UKM Ouargla
Mr	Korichi maarouf	Doctorant	Co-Encadreur	UKM Ouargla
Mme	Cherif fella	MCB	Examinatrice	UKM Ouargla
Mme	Ben krinah sabra	MAA	Examinatrice	UKM Ouargla

Année Universitaire : 2015 /2016

Remerciements

J’ai l’honneur d’être dirigé par mon Professeur **Dr.** ***A·Meraoumia***, et **Mr.** ***maarouf korichi*** dans la présente recherche.

Je vous remercie énormément mon professeur pour avoir encadré et suivi ce travail.

Merci beaucoup pour votre disponibilité, pour les nombreuses et intéressantes discussions scientifiques, pour les remarques et orientations constructives, pour les nombreux conseils avisés, pour vos encouragements quotidiens, pour ne pas avoir cessé, pour le soutien permanent, pour votre compréhension, pour la confiance que vous avez accordée et qu’il a toujours témoignée à mon égard, pour votre écoute et tout simplement pour votre gentillesse.

Sans oublier ***Mr· bensid khaled*** , merci beaucoup pour que vous êtes encouragés et vous êtes aidés.

Je tiens à exprimer tout au fond de mon cœur mes reconnaissances à département d’électronique et télécommunication pour toutes les années de spécialité et ce que je pris de la science et de la connaissance.

Remercie également monsieur le directeur du centre de recherche ***Mr.*** ***Ghilani Nacer***, ce qui nous a donné l’occasion à la recherche et l’accomplir de ce travail .

Dédicaces Lina

Je dédie ce modeste travail à celle qui m'a donné la vie, le symbole de tendresse, qui s'est sacrifiée pour mon bonheur et ma réussite, à ***ma mère*** *·A* ***mon père,*** *école de mon enfance, qui a été mon ombre durant toutes les années des études, et qui a veillé tout au long de ma vie à m'encourager, à me donner l'aide et à me protéger·*

Que dieu les gardes et les protège ;

Je dédie toutes la famille ***TELIB*** *;*

*A mes adorables sœurs (****fadila****) ;*

A mes frères ;

*A mes amis (****abdeldjalil tarmoune****) ;*

A tous ceux qui me sont chères ;

A tous ceux qui m'aiment ;

A tous ceux que j'aime ;

Je dédie ce travail ;

Dédicaces Abderrahmane

Louange à ''الله'' qui m'a aidé sur ce travail.

Je dédie ce travail, à toute ma famille

et à tous mes amis.

Et à tous ceux qui ont m'aidé à la réalisation de ce

travail.

Table de Matières

Table de Matières……...……I
Liste des Figures……...…III
Liste de Tableaux……...V
Abréviation……...……VI
Introduction générale……01
Chapitre I : Sécurité et biométrie
I.1 Introduction……...……..03
I.2 Biométrie……..…..03
I.2.1 Caractéristiques biométriques……04
I.2.2 Modalités biométriques……04
I.3 Architecture d'un Système Biométrique……...……...……..12
I.3.1 Fonctionnement…….……12
I.3.2 Principaux Modules……...……13
I.4 Système en Ligne et Système Hors Ligne ……..14
I.4.1 Système en ligne……...14
I.4.2 Système hors ligne……14
I.5 Évaluation d'une Performance……14
I.5.1 Evaluation de la vérification……14
I.5.2 Evaluation de l'identification……16
I.6 Domaine d'Applications…….….16
I.7 Marché de la Biométrie……...…17
I.8 Conclusion……..……..18
Chapitre II : Biométrie multimodale
II.1 Introduction……19
II.2 Système Unimodal……...…..19
II.3 Limitations des Systèmes Unimodaux……..……20
II.3.1 Non-Universalité des biométries……..…20
II.3.2 Variabilité lors de la capteur ……...……...…….21
II.3.3 Sensibilité aux attaques……...21
II.3.4 Non-unicité des biométries……...……21
II.4 Système Multimodal……...……...…22
II.4.1 Fusion des données……...…22

II.4.2 Sources des Informations……..23
II.4.3 Niveaux des fusions……..24
II.5 Motivations……...…….27
II.6 Extraction des Caractéristiques……...……...27
II.6.1 Quantification de la phase locale……...……..28
II.6.2 Motifs binaires locaux……...……...…….29
II.7 Mesure des Similarités……...……30
II.8 Décision……..30
II.9 Conclusion……..30
Chapitre III : Résultats Expérimentales
III.1 Introduction……...…….32
III.2 Système de Reconnaissance de FKP……..……..32
III.3 Base de Donné……...……...33
III.4 Résultats Expérimentales……..…...…….34
III.4.1 Protocol de test……34
III.4.2 Système Unimodal……...……...35
III.4.3 Système Multimodal……...……39
III.4.4 Etude comparative……...……...45
III.6 Conclusion……...……....46
Conclusion générale ……....47
Bibliographie……...……...……48
Annexe……...…..52

Liste des Figures

Figure I.1	:	Empreinte digitale……..	5
Figure I.2	:	Visage……	6
Figure I.3	:	Image de l'iris…….	6
Figure I.4	:	Empreinte des articulations des doigts……..	7
Figure I.5	:	Empreinte palmaire……..	8
Figure I.6	:	Signal de voix……	8
Figure I.7	:	Signature manuscrite…….	9
Figure I.8	:	Frappe dynamique sur le clavier……	9
Figure I.9	:	Démarche……..	10
Figure I.10	:	Veines de la main……..	10
Figure I.11	:	Exemple de l'ADN……	11
Figure I.12	:	Thermogramme faciale…….	11
Figure I.13	:	Système biométrique…….	12
Figure I.14	:	Distribution des scores et les taux d'erreurs pour un seuil donné…….	14
Figure I.15	:	Courbe ROC……..	15
Figure I.16	:	Différentes courbes CMC…….	16
Figure I.17	:	Evolution du marché international de la biométrie……..	17
Figure I.18	:	Parts dumarché des différentes méthodes biométriques….....	18
Figure II.1	:	Différents systèmes biométriques multimodaux…….....	23
Figure II.2	:	Fusion au niveau capture……..	25
Figure II.3	:	Fusion au niveau caractéristique……..	25
Figure II.4	:	Fusion au niveau score……..……	26
Figure II.5	:	Fusion au niveau decision……	27
Figure II.6	:	Organigramme de l'ensemble des étapes nécessaire à la génération du vecteur des caractéristiques par la méthode LPQ.	28
Figure II.7	:	Exemple de traitement de l'opérateur LBP……..	29
Figure II.8	:	Organigramme de l'ensemble des étapes nécessaire à la génération du vecteur des caractéristiques par la méthode LBP.	29
Figure III.1	:	Dispositif d'acquisition de FKP développé par Poly U….....	33

Figure III.2	:	Quelques images de la base de données Poly U-FKP…….....	34
Figure III.3.1	:	Schéma de réalisation illustre les étapes du travail…….....	35
Figure III.3.2	:	Performance de système biométrique sous les différents paramètres	36
Figure III.3.3	:	Performance de système unimodal (ensemble ouvert) basé sur l'algorithme LPQ……	37
Figure III.3.4	:	Performance de système unimodal (ensemble fermé) basé sur l'algorithme LPQ……	37
Figure III.3.5	:	Performance de système unimodal (ensemble ouvert) basé sur l'algorithme LBP……	38
Figure III.3.6	:	Performance de système unimodal (ensemble fermé) basé sur l'algorithme LBP……	39
Figure III.3.7	:	Comparaison des performances des systèmes multi-échantillons dans le cas d'identification ensemble ouvert……..	41
Figure III.3.8	:	Comparaison des performances des systèmes multi-échantillons dans le cas d'identification ensemble fermé……...	42
Figure III.3.9	:	Comparaison des performances des systèmes multi-algorithme dans le cas d'identification ensemble ouvert……..	43
Figure III.3.10	:	Comparaison des performances des systèmes multi-algorithme dans le cas d'identification ensemble fermé……...	44
Figure A.1	:	Filtrage et sous-échantillonnage de l'image de doigt……..	51
Figure A.2	:	Détermination de l'axe X…….....	51
Figure A.3	:	Sous-image extraite avant l'extraction de la ROI…….……..	52
Figure A.4	:	Image des contours obtenue……...	52
Figure A.5	:	Courbes sur l'image de doigt……..	52
Figure A.6	:	Image obtenue par l'application de codage de la direction convexe…..	53
Figure A.7	:	Détermination de l'axe Y…….....	53
Figure A.8	:	Localisation de la ROI dans l'image de doigt…….	54
Figure A.9	:	Extraction de la ROI à partir l'image de doigt…….....	54

Liste des Tableaux

Tableau III.1 Sélection des paramètres de l'algorithme LPQ ……..….. 36
Tableau III.2 Performance de système unimodal basé sur l'algorithme LPQ …….. 36
Tableau III.3 Performance de système unimodal basé sur l'algorithme LBP ……...…. 38
Tableau III.4 Performance de système multi-échantillons basé sur l'algorithme LPQ …….. 40
Tableau III.5 Performance de système multi-échantillons basé sur l'algorithme LBP ..…… 41
Tableau III.6 Performance de système multi-algorithmique ……..……... 43
Tableau III.7 Performance de système hybride…….. 44
Tableau III.8 Temps d'exécution pour les différents systèmes…….. 45

Abréviation

ADN	**:**	**Acide Désoxyribo Nucléique**
CCD	**:**	**Charged Coupled Device**
CMC	**:**	**Cumulative Match Curve**
DB	**:**	**Data Base**
EER	**:**	**Equal Error Rate**
FAR	**:**	**False Acceptance Rate**
FRR	**:**	**False Rejection Rate**
FKP	**:**	**Finger Knuckle Print**
GAR	**:**	**Genuine Acceptance Rate**
IBG	**:**	**International Biometric Group**
ICA	**:**	**Independent Component Analysis**
LBP	**:**	**Local Binary Pattern**
LED	**:**	**Light-Emitting Diode**
LIF	**:**	**Left Index Fingers**
LMF	**:**	**Left Middle Fingers**
LPQ	**:**	**Local Phase Quantization**
PIN	**:**	**Personal Identification Number**
RIF	**:**	**Right Index Fingers**
RMF	**:**	**Right Middle Fingers**
ROI	**:**	**Region Of Interest**
ROR	**:**	**Rank One Recognition**
RPR	**:**	**Rank of Perfect Recognition**
ROC	**:**	**Receiver Operating Curve**

Introduction Générale

Introduction Générale

La biométrie est un terme dont on entend de plus en plus parler dans la vie de tous les jours. 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. Son apparition remonte au 19ème siècle, avec les premières études alors appelées anthropométrie. Les empreintes digitales ont ensuite été utilisées pour l'identification des personnes par la police. Cette utilisation policière n'a d'ailleurs jamais été abandonnée, et les empreintes digitales sont toujours utilisées (aujourd'hui de manière automatique avec les traitements informatiques) pour l'identification criminelle. La biométrie souffre d'ailleurs un peu de cette image policière et a du mal à se faire accepter par le grand public pour d'autres types d'applications. Cela dit, aujourd'hui la biométrie n'est plus limitée aux empreintes digitales et à l'identification criminelle. De nombreuses modalités sont aujourd'hui utilisées pour des applications de contrôle d'accès à des locaux ou à des objets personnels. On peut citer le visage, la voix, la signature, l'iris ou la forme de la main, et d'autres encore sont à l'étude comme la démarche, la forme de l'oreille ou la dynamique de frappe au clavier et articulations des doigts.

Dans ce travail, un de ces systèmes a été choisi d'être étudié c'est celui de la reconnaissance des personnes par leurs images des surfaces extérieurs des doigts, ou plus exactement, un système qui utilise l'empreinte des articulations des doigts (Finger Knuckle

Print (FKP)). Cette modalité a été choisie selon leur nombreux avantages remarquables, à savoir c'est une technique acceptable par les individus, simple et facile à utilisée. Finalement, la combinaison de tous les doigts (dix doigts dans les deux mains) peut être utiliser afin d'établir un système biométrique robuste et précis.

Dans le cadre de ce travail, dans la première série des expériences, nous avons concevoir un système mono-biométrique, c.-à-d. un système qu'utilise une seule modalité biométrique. Pour cela, deux algorithmes, LPQ et LBP, ont été utilisés pour la phase la plus importante, à savoir la phase d'extraction des caractéristiques. Ces deux algorithmes sont très utilisés pour l'analyse de texture. Dans la deuxième série des expériences, la fusion multimodale est examinée afin d'obtenir un système biométrique performant, c.-à-d. un système qui peut être fonctionné avec une très petite erreur d'identification, cette erreur rend le système apte pour l'utiliser dans des applications de très hautes sécurisées.

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

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

Le **deuxième chapitre** est consacré à la fusion multimodale. Dans ce chapitre plusieurs notions sur la façon d'utiliser et de combiner plusieurs modalités ont été abordées. Notre contribution à l'extraction de caractéristiques est également présentée dans ce chapitre. Dans cette contribution, des notions sur les deux techniques LPQ et LBP, ainsi que la façon de les appliqués pour extraire les caractéristiques discriminants sont présentés.

Finalement, **le troisième chapitre** est consacré pour les résultats expérimentaux. Dans la première section de ce chapitre, nous avons mis en œuvre un système d'identification uni-modale basé à chaque fois sur l'un de doigt (notre base des données contient quatre doigts pour chaque personne). Une description détaillée des résultats obtenus, par les algorithmes **LPQ** et du **LBP**, est présentée dans cette section. La deuxième section de ce chapitre discute 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 ont été évalués. Afin de sélectionner le meilleur système, qui présente la plus faible erreur d'identification, une comparaison entre les différents systèmes est exécutée dans cette section. Enfin, nous avons terminé notre mémoire avec une conclusion et quelques perspectives visées.

CHAPITRE I

Sécurité & Biométrie

Sécurité et Biométrie

I.1. Introduction

Dans ces jours les méthodes de sécurité classique ou traditionnelle des systèmes d'informations ne sont pas acceptables tellement elles sont utilisée par quelqu'un, il existe deux manières de cette sécurité : La première repose sur la connaissance de la personne comme un mot de passe ou un code PIN. La seconde est basée sur ce que possède la personne comme un badge ou une carte à puce. Dans le premier cas, le mot de passe peut être oublié par son utilisateur ou bien deviné par une autre personne. Dans le second cas, le badge (ou la pièce d'identité ou la clef) peut être perdu ou volé. Pour contourner cette limitation ou cette faiblesse, un autre moyen de la sécurité a été développé qui permet d'utiliser, non pas l'information qu'un individu possède ou connait, mais une information intrinsèque à cette personne. Cette nouvelle façon d'identification des individus est la biométrie [1].

I.2. Biométrie

La biométrie est une alternative aux deux précédents modes d'identification. Elle consiste à identifier une personne à partir de ses caractéristiques physiques comme les

visages, les empreintes digitales, l'iris... etc. ou comportementales par exemple la voix, l'écriture, le rythme de frappe sur un clavier...etc. en plus les caractéristiques biologiques comme l'ADN, les veines et le thermogramme faciale. Ces caractéristiques qu'elles soient innées comme les empreintes digitales ou bien acquises comme la signature, sont attachées à chaque individu et ne souffrent donc pas des faiblesses des méthodes basées sur une connaissance ou une possession. En effet, un attribut physique ou comportemental ne peut être oublié, perdu ou volé [2].

I.2.1 Caractéristiques biométriques

Les caractéristiques biométriques par lesquelles il est possible de vérifier l'identité d'un individu sont appelées modalités biométriques. Ces modalités sont basées sur l'analyse des données liées à l'individu et sont généralement classées en trois catégories : biométrie biologique, comportementale et morphologique. Pratiquement, n'importe quelle caractéristique morphologique ou comportementale peut être considérée comme une caractéristique biométrique, dans la mesure ou elle satisfait les propriétés suivantes :

- ***Universalité* :** toutes les personnes à identifier doivent la posséder.
- ***Unicité* :** l'information doit être aussi dissimilaire que possible entre les déférentes personnes.
- ***Collectabilité* :** l'information doit être collectable et mesurable afin d'être utilisée pour les comparaisons.
- ***Permanence* :** l'information collectée doit être présente pendant toute la vie d'un individu**.**
- ***Acceptabilité* :** le système doit respecter certains critères (facilité d'acquisition, rapidité…etc.) afin d'être employés.

I.2.2 Modalités biométriques

Aucune biométrie unique ne pouvant répondre efficacement aux besoins de toutes les applications d'identification. Un certain nombre de techniques biométriques ont été proposées, analysées, et évaluées, chaque biométrie à ses forces et ses limites et ses conséquences, chaque biométrie est utilisée dans une application particulière. La biométrie biologique se base sur l'analyse des données biologiques liées à l'individu (salive, ADN, etc.). La biométrie comportementale se base sur l'analyse des comportements d'un individu (manière de marcher, dynamique de frappe au clavier, etc.)[3]. La biométrie

morphologique se base sur les traits physiques particuliers qui, pour toute les personne, sont permanents et uniques (empreinte digitale, visage, etc.).

1) Biométrie physique

✍ **Empreint digitale :** La reconnaissance des empreintes digitales est la technique biométrique la plus utilisée. Les empreintes digitales sont composées de lignes localement parallèles présentant des points singuliers et constituent un motif unique, universel et permanant. Les lecteurs d'empreintes digitales scannent puis relèvent des éléments permettant de différencier les empreintes. Ces éléments sont appelés minuties. Il existe plusieurs types de minuties : lac, bifurcation, delta ou impasse…etc. Ce type de technique biométrique est utilisé par les institutions financières pour leurs clients et se trouve en même temps dans les hôpitaux, les écoles, les aéroports…etc.

Fig. I.1 : Empreinte digitale

Avantages

- Prix faible
- Taille du lecteur biométrique n'est pas volumineuse
- Système reste très simple à mettre en place
- Utilisation facile

Inconvénients

- L'inscription est par toutes les parties concernées ce qui peut poser un problème dans le cas où la maladie soit physique ou psychologique**.**

✍ **Visage :** Nos visages sont des objets complexes avec des traits qui peuvent varier dans le temps. Cependant, les humains ont une capacité naturelle à reconnaitre les visages et d'identifier les personnes dans un coup d'œil. Bien sûr, notre capacité de reconnaissance naturelle n'étend au-delà de la reconnaissance du visage, où nous somme également en mesure de repérer rapidement des objets, des sons ou des odeurs. Malheureusement, cette aptitude naturelle n'existe pas dans les ordinateurs, c'est ainsi qu'est né le besoin de simuler artificiellement la reconnaissance afin de créer des systèmes intelligents autonomes simuler notre capacité naturellement. La reconnaissance des visages dans les machines est une tâche difficile mais pas impossible. Tout au long de notre vie, de nombreux visages

sont vus et conservés naturellement dans nos mémoires formant une sorte de base de données. La reconnaissance du visage est utilisée comme un système de surveillance ou d'identification par les autorités ou les corps policiers principalement dans les lieux publics. Elle est parmi les techniques les plus acceptables, mais elle nécessite un arrière-plan simple et fixe pour que le résultat soit précis [4].

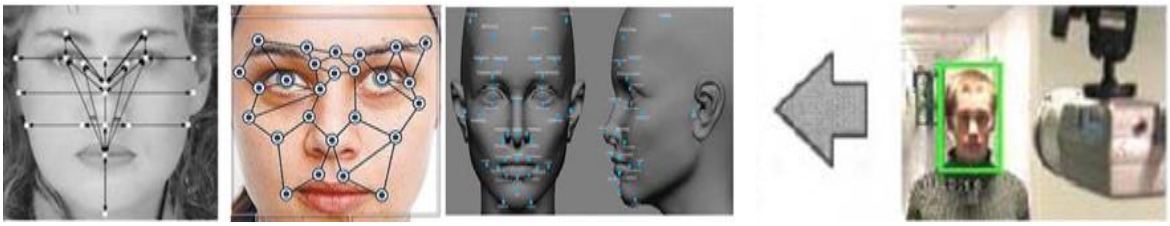


Fig. I.2 : Visage

Avantages

- Technique acceptable par le public.
- Fonctionnement simple et capable.
- Technique peu coûteuse et peut s'appuyer sur l'équipement d'acquisition des images actuel.

Inconvénients

- Les vrais jumeaux ne sont pas différenciés.
- Les changements physiques peuvent tromper le système.
- La technique est trop sensible au changement d'éclairage ou l'angle de l'appareil-photos…etc.

Iris : L'iris est la région, sous forme d'anneau, située entre la pupille et le blanc de l'œil, il est unique.L'iris a une structure extraordinaire et offre de nombreuses caractéristiques de texture qui sont uniques pour chaque individu. La reconnaissance de l'iris est développée dans les années 80 c'est pour cela elle est une technologie plus récente .l'image de l'iris est capturée par un appareil qui contient une caméra infrarouge, lorsque la personne se place à une courte distance de l'appareil.

Fig. I.3 : Image de l'iris

Avantages

- Les vrais jumeaux sont non confondus
- Les structures de l'iris restent stables durant toute la vie
- Grande quantité d'informations contenue dans l'iris

Inconvénients

- L'acquisition des images exige une certaine formation et de la pratique
- La fiabilité diminue proportionnellement à la distance entre l'œil et la camera.
- les gens ont du mal à accepter cette biométrie.

✍ **Empreintes des articulations des doigts (FKP) :** C' est la technologie biométrique basée sur la surface arrière de doigt , elle contient des caractéristiques distinctives, telles que les lignes principales, les lignes secondaires et les crêtes, qui peuvent être extraites à partir des images à basse résolution. La main contient plusieurs doigts, pour cela, il faut conserver les informations à chaque doigt pour une reconnaissance précise dans le domaine d'identification [5].

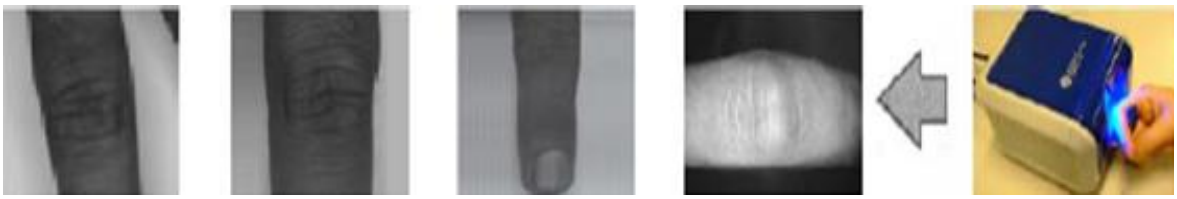


Fig. I.4 : Empreinte des articulations des doigts

Avantages

- Technique acceptable.
- Utilisation simple.
- En combinant tous les doigts de la main, il est possible d'établir un système biométrique robuste et précise.

Inconvénients

- Très similaire pour les jumeaux.
- Problème dans le cas de couper un doigt.
- Pose incorrecte de doigt sur le lecteur provoque une grande erreur.

✍ **Empreinte palmaire :** Cette technique utilise la surface intérieure de la paume pour l'identification et/ou la vérification des personnes. Elle est bien adaptée pour les systèmes de moyenne sécurité telle que le contrôle d'accès physique ou logique [5].

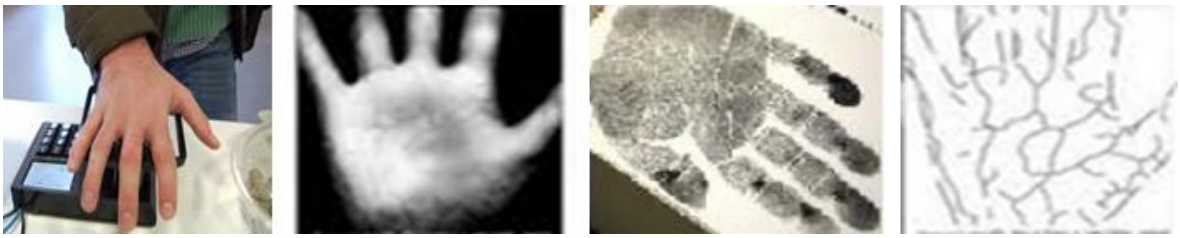


Fig. I.5 : Empreinte palmaire

Avantages

- Facile à utiliser, Il a une grande acceptation.
- Après l'utilisation, la main resté propre et ne laisser aucune trace.
- Presque disponible par tous les individus.

Inconvénients

- Pourrait être similaire dans des jumeaux ou des membres de la famille.
- Il n'est pas permanent en termes de changements tels que le vieillissement.

2) Biométrie comportementale

Voix : La voix humaine varie d'une personne à l'autre et peut se constituer de composantes physiologiques et comportementales. L'identification par la voix basée sur la forme et la taille des appendices (bouche, cavités nasales et les lèvres) utilisées dans la synthèse du son [2]. La reconnaissance des locuteurs est plis utilisé par les téléphones, les corps policiers, les hôpitaux…etc.

Fig. I.6 : Signal de voix

Avantages

- Très bien acceptée parce que la voix est un signal naturel à produire
- Dynamique des ondes produites sont uniques

Inconvénients

- Biométrie moins permanant.
- Caractéristiques comportementales changent avec le temps.
- Possibilité de fraude par enregistrement.
- Sensibilité aux bruits lors d'acquisition.

✍ **Signature manuscrite :** C'est une écriture personnelle d'un individu, la vérification de la signature est basée sur deux modes :

Mode statique : la vérification de la signature statique met l'accent sur les formes géométriques de la signature, dans ce mode en générale la signature est normalisée à une taille connue ensuite décomposer en élément simple.

Mode dynamique : il utilise les caractéristiques dynamiques telles que l'accélération, la vitesse et les profils de trajectoire de la signature[5].

Fig. I.7 : Signature manuscrite.

Avantage

- Très acceptable par l'utilisateur.
- Peut protéger l'ensemble de vos fichiers personnels.

Inconvénients

- Grande variabilité durant le temps (vous ne pouvez pas maintenir la même forme de la signature pour toute la vie).
- Grande possibilité de fraude.

✍ **Frappe dynamique sur le clavier :** C'est un système de reconnaissance d'un individu basé sur la manière de ses écritures par un dispositif logicielle qui calcule la vitesse de frappe, la suite des lettres, le temps de frappe et la pause entre chaque mot [5].

Fig. I.8 : Frappe dynamique sur le clavier

Avantage

- Acceptation forte par l'utilisateur.
- Sécurité bien précise.

Inconvénients

- N'est pas plus pratique.
- N'est pas permanent durant toute la vie (âge, émotion, fatigue).

✍ **Démarche :** Chaque personne a une façon particulière de marche, nous pouvons identifier les individus de la nature du mouvement des jambes, des bras et des articulations ou le mouvement spéciale obtenus par un caméra vidéo afin de l'envoyer à un ordinateur pour l'analyse afin de déterminer la vitesse et l'accélération de chaque individu [5].

Fig. I.9 : Démarche

Avantage

- Très acceptable par les individus.

Inconvénients

- N'est pas permanant (âge, fatigue, maladie)

2) Biométrie biologique

✍ **Veines de la main :** Les veines de la main sont du réseau varient de personne à l'autre. L'analyse de cette différence permet de maintenir des points pour différencié une personne à l'autre.

Fig. I.10 : Veines de la main

Avantage

- Ne nécessite pas de contact.
- Difficile à falsifier.

Inconvénients

- Très cher.

✍ **Analyse de l'ADN :** Il est la façon la plus précise pour déterminer l'identité de la personne. Il est impossible de trouver deux personnes qui ont le même ADN. Cette modalité possède l'avantage d'être unique et permanant durant toute la durée de vie [5].

Fig. I.11 : Exemple de l'ADN

Avantage

- Distinguer les individus avec une grande précision
- Il facilite la détection des délinquants

Inconvénients

- Lente pour obtenir les résultats
- Avoir un coût élevé

✍ **Thermogramme faciale :** 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. contrairement à la reconnaissance de visage, la chirurgie plastique n'a que peu d'influence sur les thermogrammes faciaux. Pour capturer l'image, il est possible d'utiliser un appareil photo ou une caméra numérique dans le domaine de l'infrarouge. La capture peut se faire dans n'importe quelle condition d'éclairage et même dans le noir complet ce qui est un avantage supplémentaire sur la reconnaissance de visage classique [5].

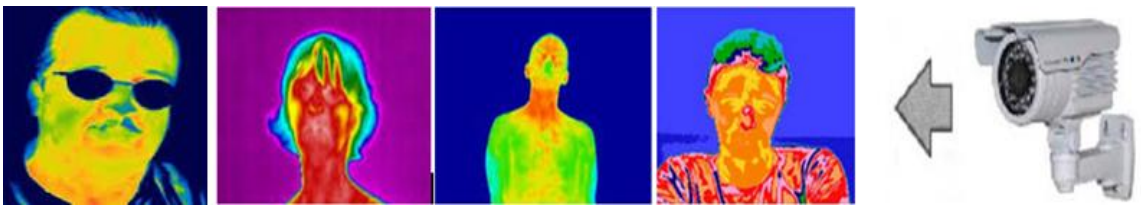


Fig. I.12 : Thermogramme faciale

Avantage

- Pouvez reconnaître les visages, même dans l'obscurité
- Pouvez distinguer des jumeaux

Inconvénients

- Influencée par des facteurs tels que la température du corps et l'état émotionnel

I.3 Architecture d'un système biométrique

Dans ces jours les systèmes biométriques sont de plus en plus utilisés aux dernières années. En général, un système de reconnaissance des personnes basé sur leurs descripteurs biométriques peut se décomposer en deux phases, phase d'enrôlement (création de la base de données) et phase de reconnaissance [5] (voir Fig. I.13).

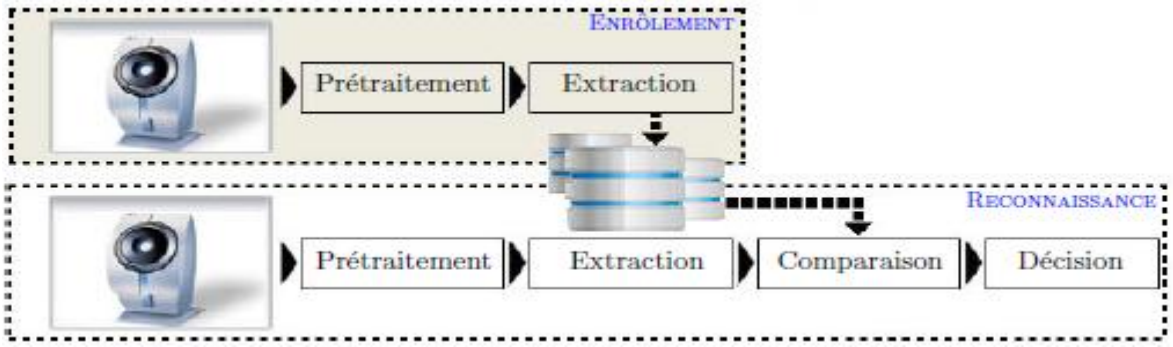


Fig. I.13 : Système biométrique

I.3.1 Fonctionnement

Chaque système biométrique comprend deux phases distinctes :

1) **Phase d'enrôlement :** La phase d'enrôlement est définie par le procédé de la collection de traits biométriques d'un individu et le convertir en référence biométrique (Template, vecteur de caractéristique), et à la stocker dans une base de données pour une comparaison ultérieure.

2) **Phase de reconnaissance :** Au cours de la reconnaissance, la modalité biométrique est mesurée et un ensemble des caractéristiques distinctives (Template) est extrait comme lors de l'enrôlement [1]. Cette phase peut être décomposée en deux modes :

- ***Mode vérification*** : le système doit répondre à une question de type : «Suis-je bien la personne que je prétends être ?».L'utilisateur propose une identité au système et le système doit vérifier que l'identité de l'individu est bien celle proposée. Il suffit donc de comparer le signal avec un seul des modèles présents dans la base de données (type ***1:1***). En mode vérification, on parle de problème ouvert puisque l'on suppose qu'un individu qui n'a pas de modèle dans la base de données (imposteur) peut chercher à être reconnu.

- ***Mode identification***, le système doit deviner l'identité de la personne. Il répond donc à une question de type : «Qui suis-je ?». Dans ce mode, le système compare le signal mesuré avec les différents modèles contenus dans la base de données (type ***1 : N***). En général, lorsque l'on parle d'identification, on suppose que le problème est fermé, c'est-à-dire que toute personne qui utilise le système [1] possède un modèle dans la base de données.

i) ***Identification en mode ensemble fermé :*** Par exemple on utilise.ce type d'identification afin d'enregistrer la présence de personnes dans certaine entreprise. Si l'échantillon possède un certain degré de similitude avec les échantillons dans le système, la personne sera acceptée.

ii) ***Identisation en mode ensemble ouvert*** : S'il y a une grande similitude entre l'échantillon biométrique testé et tous les modèles préenregistrés et si cette similitude est inférieure (ou supérieure) au seuil de sécurité, cette personne est rejetée. Cela signifie que la personne ne fait pas partie de celles enregistrées par le système. Sinon le système est l'acceptée.

I.3.2. Principaux Modules

Le système biométrique est un système pour identifier les tendances et le stockage des données à sauvegarder ou de les identifier dans la forme de matrices. Ensuite, le système est prêt à identifier les intrus. Ce système se compose de quatre unités : l'acquisition, l'extraction des caractéristiques, la comparaison (mesure de similarité) et la décision. L'inscription ou l'enrôlement est utilisé pour une future comparaison tandis que la décision est de reconnaître la personne ou non[5].

- **Acquisition des données :** Cette phase collecte les données biométriques des personnes clients. Plusieurs processus industriels peuvent être utilisés pour l'acquisition telle qu'un appareil photo, un lecteur d'empreintes digitales, etc.

- **Extraction des caractéristiques :** Les images sont traitées pour en extraire des caractéristiques du procédé. Ce processus sert à éviter les informations inutiles qui existent. Donc, ce module sert à traiter l'image afin d'extraire uniquement les caractéristiques biométriques, sous forme d'un vecteur ou Template, qui ensuite peuvent être utilisées pour reconnaitre les personnes. Ces caractéristiques sont uniques à chaque personne et stable.

- **Comparaison :** Dans ce module, les caractéristiques biométriques extraites sont comparées avec un vecteur précédemment stocké dans la base de données et en marquant le degré de similitude (différence ou distance).

- **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) vecteur(s) stocké(s).

I.4 Système en ligne et système hors ligne

Les systèmes de reconnaissance biométriques sont classifiés en deux catégories : reconnaissance en ligne et reconnaissance hors ligne.

I.4.1 Système en ligne : Dans ce type des systèmes, les images de modalité sont capturées par un dispositif de capture spécifique et les images numériques acquises sont traitées en temps réel.

I.4.2 Système hors ligne : Ce type des systèmes traite les images de chaque modalité capturées précédemment par un scanner numérique. Ces approches fournissent des images à haut résolution, mais ne sont pas convenables aux systèmes de sécurité en temps réel.

I.5 Évaluation d'une performance

La performance d'un système d'identification biométrique peut se mesurer principalement à l'aide de trois critères : sa précision, son efficacité (vitesse d'exécution) et le volume de données qui doit être stocké pour chaque personne. Nous nous concentrerons dans cette section sur le premier aspect. Comme nous l'avons vu précédemment, l'identification et la vérification sont des modes opératoires différents. Elles nécessitent donc des mesures de précision différentes que nous étudierons dans les deux sous-sections suivantes.

I.5.1 Evaluation de la vérification

❒ **Taux d'erreurs :** Lorsqu'un système en mode de vérification ou identification ensemble ouvert, il existe deux types d'erreur qui peuvent être utilisés pour évaluer leur performance. La première erreur mesure le taux de faux rejet (False Rejection Rate ou FRR) et la deuxième erreur mesure le taux d'acceptation des imposteurs, on parle alors à la fausse acceptation (False Acceptance Rate ou FAR) [3].

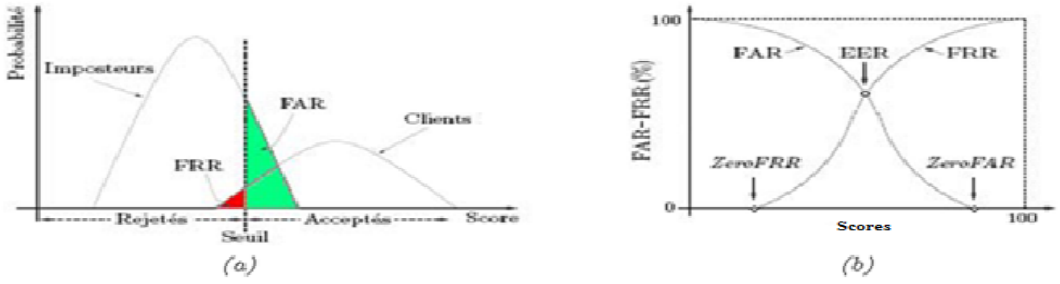


Fig. I.14. Distribution des scores et les taux d'erreurs pour un seuil donné. *(a)* Distributions des Scores client et des scores imposteur et *(b)* Variation des FRR et des FAR en fonction du seuil.

FAR : C'est le pourcentage d'individus reconnus par le système biométrique, ce système clase alors deux caractéristiques provenant de deux personnes différentes

$$\text{FAR} = \frac{\text{nombre des imposteurs acceptés}}{\text{nombre totale d'accès imposteurs}}$$

FRR : Ce taux représente le pourcentage d'individus censés être reconnus par le système mais qui sont rejetés, le système indique la probabilité qu'un utilisateur connu soit rejeté.

$$\text{FRR} = \frac{\text{nombre des clients rejetés}}{\text{nombre total d'accés clients}}$$

Le taux le plus simple pour mesurer la performance d'un algorithme dans le contexte de la vérification est de calculer le point d'équivalence des erreurs (Equal Error Rate ou EER).

EER : Ce taux est calculé à partir de FAR et FRR et constitue un point de mesure de performance courant, c.-à-d. **EER=FRR=FAR**.

$$\text{EER} = \frac{\text{nombre de fausses acceptations} + \text{nombre de faux rejets}}{\text{nombre totale d'accès}}$$

❒ **Courbe caractéristiques :** Les performances d'un système biométrique peuvent être présentées graphiquement à l'aide de la courbe ROC (Receiver Operating Characteristic) [4]. Cette courbe représente les valeurs de FRR en termes de FAR. Ceci est obtenu en calculant le couple (FAR, FRR) ou chaque valeur du seuil de décision. Celui-ci diffère de la plus petite valeur obtenue à une valeur supérieure. Cette courbe peut être décomposée en trois zones : zone de haute sécurité, zone de compromis et zone de basse sécurité [2].

Fig. I.15 : courbe ROC

I.5.2 Evaluation de l'identification

Le taux d'identification (ensemble fermé) est la mesure la plus couramment utilisée mais il n'est pas toujours suffisant. En effet, en cas d'erreur, il peut être utile de savoir si le bon choix se trouve dans les N premiers. On trace alors le score cumulé (cumulative match score) qui représente la probabilité que le bon choix se trouve parmi les N premiers [4]. Dans le cas où il existe plusieurs modèles pour chaque individu dans la base de données, les mesures classiques des systèmes de recherche dans une base de données peuvent être utilisées.

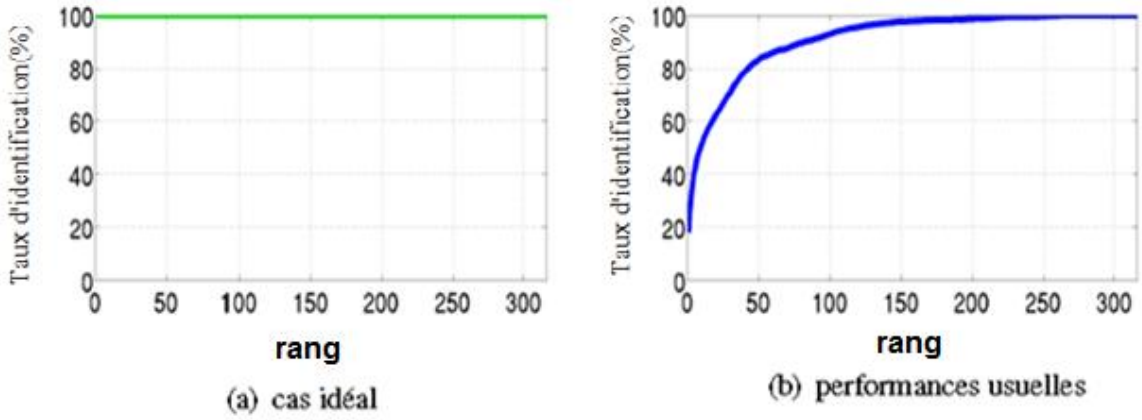


Fig. I.16 : Différentes courbes CMC. *(a)* 100% des paires sont correctement associées au premier essai et *(b)* 16% au rang 1 et il faut attendre le rang 270 (sur 316) pour atteindre 100%.

I.6 Domaine d'applications

La biométrie répond aux exigences de sécurité par les secteurs particuliers et les entreprises dans tous les pays. La sécurité biométrique couvre presque tous les domaines. Aujourd'hui, La sécurité biométrique est utilisée dans l'accès aux réseaux et aux systèmes d'information, paiement électronique et cryptage des données. Généralement, les applications de la sécurité biométrique peuvent être classées en quatre sections principales [2].

I.6.1 Service public

- ✓ Le contrôle et la sécurité des bâtiments gouvernementaux frontière.
- ✓ Contrôle les immigrants qui entrent et sortent du pays.
- ✓ Utilisés dans les aéroports et la santé.
- ✓ Aidant à passer de la carte d'assurance sociale

I.6.2 Pouvoir judiciaire

- ✓ L'utilisation des empreintes digitales pour prouver certains faits concernant les infractions pénales.
- ✓ L'utilisation de l'ADN extrait du sang ou des cheveux dans la scène du crime pour obtenir le criminel.

I.6.3 Secteurs des banques

- ✓ Les transactions bancaires (retraits en espèces, les cartes bancaires, paiement par le téléphone et Internet).
- ✓ La réduction de la proportion de la fraude grâce à l'intégration des cartes à puce avec reconnaissance des empreintes digitales.

I.6.4 Accès physique et logique

Ceci se rapporte au contrôle d'accès physique comme la sécurisation des lieux (bâtiment ou une pièce) ou le contrôle d'accès logique comme la sécurisation d'une session informatique (ordinateur ou base de données).

I.7 Marché de la biométrie

Régulièrement, un rapport sur le marché mondial de la biométrie est édité par IBG (International Biometric Group). Cette étude est une analyse complète des chiffres d'affaires, des tendances de croissance, et des développements industriels pour le marché de la biométrie actuel et futur.

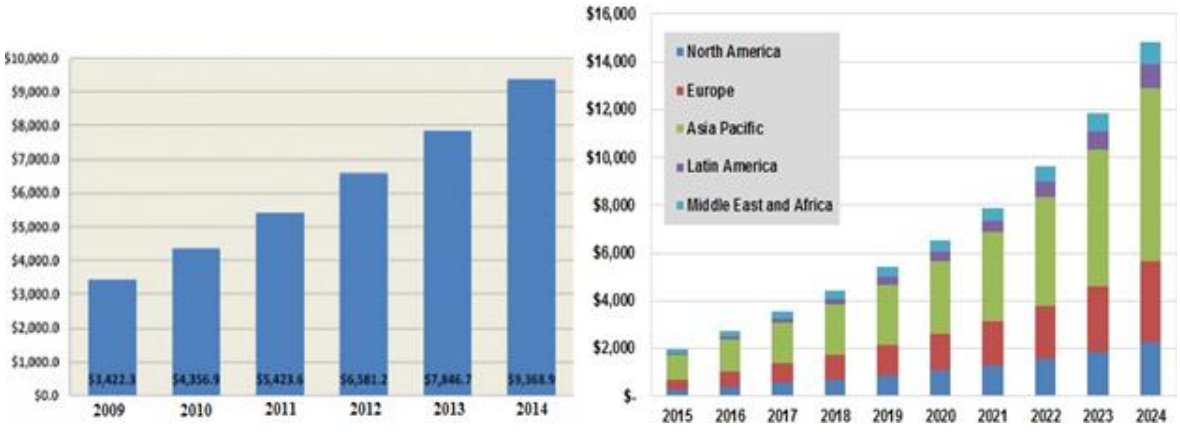


Fig. I.17 : Evolution du marché international de la biométrie

La lecture de ce rapport est essentielle pour des établissements déployant la technologie biométrique, les investissements dans les entreprises biométriques, ou les développeurs de solutions biométriques. Le chiffre d'affaires de l'industrie biométrique incluant les applications judiciaires et celles du secteur public, se développe rapidement. Une grande partie de la croissance sera attribuable au contrôle d'accès aux systèmes d'information (ordinateur/réseau) et au commerce électronique, bien que les applications du secteur public continuent à être une partie essentielle de l'industrie. On prévoit que le chiffre d'affaires des marchés émergents (accès aux systèmes d'information, commerce électronique et téléphonie, accès physiques et surveillance) dépasse le chiffre d'affaires des secteurs plus matures (identification criminelle et identification des citoyens) [2]. Les empreintes digitales continuent à être la principale technologie biométrique en termes de part de marché, près de 50% du chiffre d'affaires total (hors applications judiciaires), dépasse la reconnaissance de la main, qui avait avant la deuxième place en termes de sources de revenus après les empreintes digitales [2].

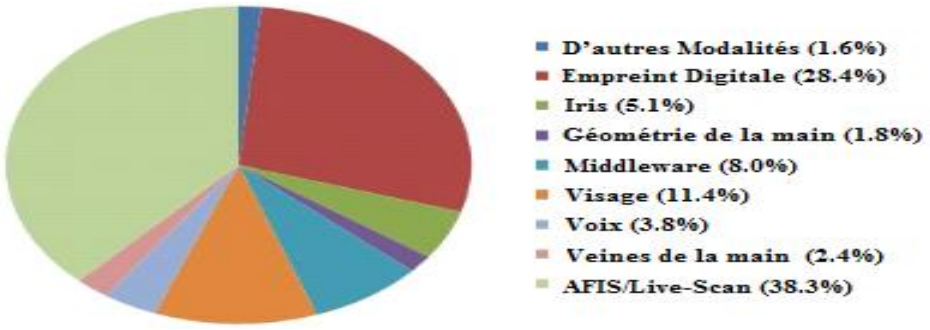


Fig. I.18 : Parts de marché des différentes méthodes biométriques

I.8 Conclusion

De nos jours la biométrie est considéré comme le moyen le plus sûr pour la sécurité. Elle est de plus en plus appliquée dans la réalité grâce à ses avantages. Dans ce chapitre, nous avons présenté un état de l'art sur les technologies biométriques et mis l'accent sur le grand nombre de ces technologies. Nous avons aussi indiqué quelques points forts et points faibles de chaque technologie qui mettent en évidence le fait qu'elles ne sont pas toutes de le même efficacité. Comme nous avons introduit la notion de vérification de l'identité du modèle et de la structure globale et les applications analytiques ou magazines sur l'utilisation du système de la technologie biométrique. Dans ce dernier chapitre a expliqué le marché de la biométrie dans le monde.

CHAPITRE II

Systèmes multimodaux

Systèmes Multimodaux

II.1 Introduction

La biométrie est généralement utilisée alternativement pour décrire les caractéristiques d'une personne. Cette caractéristiques définit un physiologique mesurable (visage, FKP, palmaires, géométrie de la main, l'oreille) et comportementaux (discours, démarche, course clé, signature)...etc. Ces éléments sont essentiels pour identifier une personne. Un système biométrique est un système de reconnaissance de motif, qui acquise des données requises, extrait l'ensemble des fonctionnalités celui-ci, et comparer avec le jeu de modèle stocké dans la base des données. Dans ce chapitre, nous allons parler sur les limitations du système unimodal ; qui utilise une seule modalité biométriques d'un individu et il soufre pour identifier une personne avec une grande précision. Pour remédier cet inconvénient, on utilise un système biométrique multimodal. Dans ce procédé, deux ou plusieurs modalités biométriques sont utilisés pour identifier la personne, nous parlerons aussi sur différents niveaux de fusion possibles. Enfin, nous présenterons nos méthodes proposées.

II.2 Système unimodal

Le système unimodal, c'est un système plus simple qui utilise une seule modalité biométrique, par exemple l'utilisation d'un seul doigt ou un seul algorithme pour identifier les personnes. Ce type des systèmes possède généralement un taux d'erreur très élevé.

Ainsi, ce type des systèmes à plusieurs limitations qui peuvent être rend la sécurisation biométrique inapplicable pour des entreprises ou des personnes particulières.

II.3 Limitations des systèmes unimodaux

L'évaluation des performances d'un système biométrique est une phase importante dans le processus de sa conception et de sa mise en œuvre dans la mesure où elle permet de savoir si le système est suffisamment performant pour l'application visée. Cependant, les critères de performance d'un système biométrique ne sont pas les seuls à prendre en compte mais aussi les critères de coûts et d'acceptation par le public. Ainsi, selon les situations d'usage et les buts recherchés, chaque technologie biométrique (modalité) a ses points forts et ses inconvénients. Par conséquent, on ne peut garantir un excellent système de reconnaissance (un excellent taux de reconnaissance) avec l'utilisation d'une seule modalité biométrique. Malgré les avantages des systèmes biométriques unimodaux par rapport aux systèmes traditionnels, leur utilisation souffre de plusieurs limitations qui peuvent dégrader considérablement leur intérêt. En effet, ces systèmes sont souvent affectés par les problèmes suivants :

II.3.1 La non-universalité des biométries

Les systèmes unimodaux 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 reconnaître ou ne sont pas assez riche en information pour permettre la reconnaissance de l'identité de certaines personnes. Certaines personnes peuvent avoir les articulations des doigts 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.

II.3.2 La variabilité lors de la capture

Ce type de variabilité n'est pas intrinsèquement lié à la modalité mais à l'acquisition de celle-ci. Il peut être introduit à plusieurs phénomènes. Le premier phénomène est la déformation physique lors de la capture (variabilité du capteur), c.-à-d. que 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 (par exemple, changements de pose et d'expression faciale lorsque l'utilisateur se tient devant une caméra), à l'utilisation de capteurs différents lors de l'enrôlement et de la vérification, à des changements de conditions de l'environnement ambiant (par exemple, changements en éclairement pour un système de reconnaissance faciale) ou encore à des changements inhérents à la modalité biométrique (par exemple, apparition de rides dues à la vieillesse, présence de cheveux dans l'image du visage, présence de cicatrices dans une empreinte digitale, etc.) [5].

II.3.3 La sensibilité aux attaques

Une autre limitation des systèmes biométriques est la sensibilité aux attaques (possibilité de fraude). Il est toutefois possible de reproduire certaines modalités biométriques. A priori s'il est relativement simple de reproduire une signature ou imiter la voix d'une personne (les modalités biométriques comportementales sont plus sensibles à ce genre d'attaque que les modalités biométriques physiologiques), il est plus difficile de reproduire, par exemple l'empreinte digitale, mais cela est possible. En effet, certaines études ont montré qu'il était possible de fabriquer de fausses empreintes digitales en gomme et de les utiliser pour contrer un système biométrique [5].

II.3.4 La non-unicité des biométries

C'est la variabilité entre les modalités de plusieurs Individus. Cependant, 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 (ex : père et fils, vrais jumeaux). Ce manque d'unicité augmente le taux d'erreur d'un système biométrique (accepter des personnes non enregistrées dans la base des données) [5].

Comme il a été annoncé précédemment concernant les systèmes unimodaux (c’est à dire utilisant une seule modalité), nombreuses limitations imposées par l’utilisation des

systèmes biométriques unimodaux inclus les taux d'erreurs associés à ces systèmes biométriques qui sont restés relativement élevés. Ce qui les rend inacceptables pour un déploiement d'applications critiques de sécurité. Donc, chaque système en ne peut pas, toujours, être utilisé de manière fiable pour effectuer la reconnaissance. Cependant, la consolidation d'informations présentées par les différentes modalités peut permettre une authentification précise de l'identité. Ces dernières années, on a vu l'émergence d'une approche innovante qui est l'utilisation de plusieurs modalités biométriques au sein d'un même système. On parle alors de système biométrique multimodal qui va être étudié dans le reste de notre mémoire.

II.4 Système multimodal

Les humaines se reconnaissent entre eux à partir de plusieurs modalités biométriques physiques ou comportementales. Chaque modalité en soi ne peut pas toujours être utilisée de manière fiable pour effectuer la reconnaissance [6]. Cependant, la consolidation d'information présentées par les déférentes modalités peut paramètre une reconnaissance précise de l'identité. Cette stratégie peut être utilisée pour réduire quelques problèmes et limitations, liées aux systèmes multimodaux. En effet, la combinaison de plusieurs modalités à pour but d'améliorer les performances se reconnaissance .En augmentant la quantité d'information discriminantes de chaque personne, on souhaite augmenter le pouvoir de reconnaissance du système (vérification ou l'identification) [7] .

II.4.1 Fusion des données

La fusion des données est une technique utilisée en traitement d'informations issues des sources multiples [8]. Elle consiste à combiner des données issues de plusieurs sources afin d'obtenir une décision meilleure que celle obtenue à partir de chacune des sources prise isolément. La fusion de données a été initialement développée surtout dans un contexte militaire pour des objectifs tels que la localisation des cibles ennemies et la fusion d'images radar [9]. Les systèmes employés ont recours à des techniques diverses issues de domaines variés tels le traitement du signal, l'intelligence artificielle, la reconnaissance des formes, la classification, etc... De façon générale, la fusion de données est une opération d'intégration de plusieurs données en vue d'en extraire une nouvelle information plus représentative de l'ensemble des données. Actuellement, la fusion des données prend une place de plus en plus importante dans de nombreux domaines. Elle permet d'aider efficacement les scientifiques à extraire des informations de plus en plus pertinentes et

précises. La fusion de données a d'abord visé d'améliorer la qualité des réponses aux problèmes posés par les militaires mais aujourd'hui elle touche énormément de domaines telles que [10] : la télédétection, la prévision météorologique, la biométrie multimodale, l'application médicale et la robotique.

II.4.2 Sources des informations

Le problème général de la fusion est la synthèse d'un ensemble d'informations obtenues à partir de la mise en commun d'informations provenant des sources différentes. Cependant, il existe, de nombreux scénarios possibles pour les sources d'information qui peuvent être considérées dans un système biométrique multimodal [11].

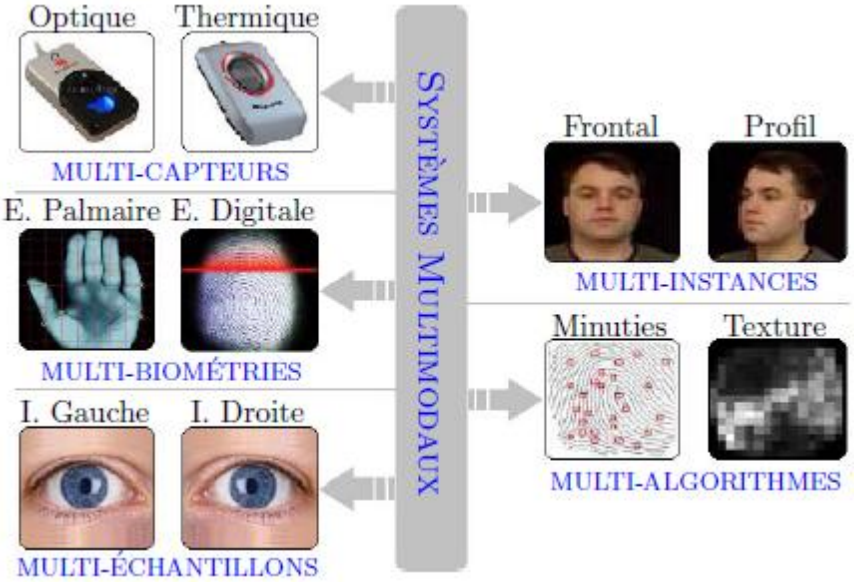


Fig. II.1 : Différents systèmes biométriques multimodaux

1) **Systèmes multi-algorithmes :** Dans ces systèmes, les mêmes données biométriques sont traitées à travers plusieurs algorithmes. Par exemple, des algorithmes d'analyse de texture et de minuties peuvent être associés pour traiter la même image d'empreinte digitale afin d'extraire diverses caractéristiques qui peuvent améliorer la performance du système [12]. Ainsi, ce genre de système ne nécessite pas de capteurs supplémentaires et n'oblige pas l'utilisateur à interagir avec de multiples capteurs, d'où l'amélioration de la commodité d'utilisation.

2) **Systèmes multi-instances :** Un unique capteur peut être utilisé pour acquérir plusieurs instances de la même modalité biométrique dans le but de prendre en compte les variations qui peuvent se produire au sein de cette modalité. Par exemple, un système de reconnaissance faciale peut capturer plusieurs images du visage avec des

changements de pose (profil frontal, profils gauches et droits), d'expression ou d'illumination de tenir compte des variations de la pose faciale [5].

3) **Systèmes multi-capteurs :** Correspondant à l'utilisation de plusieurs capteurs pour l'acquisition d'une seule modalité biométrique. Pour la reconnaissance de l'image, par exemple, il est possible d'utiliser plusieurs caméras 2D, des capteurs 3D ainsi que des capteurs infrarouges. L'utilisation de plusieurs capteurs permet d'acquérir des informations complémentaires pour accroître les performances des systèmes unimodaux [13].

4) **Systèmes Multi-biométries :** Dans ces systèmes, différentes modalités biométriques sont combinées afin d'établir l'identité d'un individu. Par exemple, les caractéristiques du l'empreinte palmaire et l'empreinte digitale. Cette stratégie de fusion consiste à exploiter les avantages de chaque système biométrique tout en évitant leurs inconvénients. En fait, 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 [5].

5) **Systèmes 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 [14].

II.4.3 Niveaux des fusions

Dans un système biométrique multimodal, la fusion peut se faire en utilisant l'information disponible dans n'importe quel ces modules. La combinaison de plusieurs systèmes biométriques peut se faire à quatre niveaux différents [15] : 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. Ces quatre niveaux de fusion peuvent être classés en deux sous-ensembles : La fusion pré-classification (avant comparaison) et la fusion post-classification (après la comparaison).

1) Fusion au niveau du capteur : Elle est une combinaison de données ou d'informations provenant de plusieurs capteurs. Elle est relativement peu utilisée car elle nécessite une homogénéité entre les données. Par exemple il est possible de combiner plusieurs images de visages dans des canaux de couleurs différents ou en visible et en infrarouge s'ils correspondent à la même scène. Il est également possible de faire une mosaïque à partir d'images prises de différents points de vue [14].

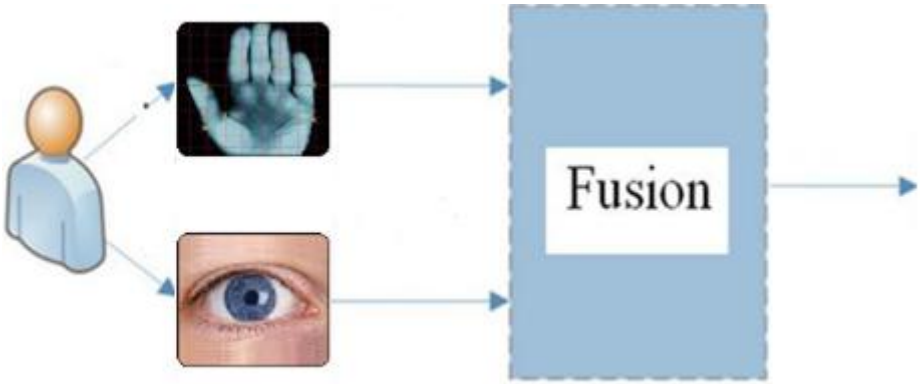


Fig. II.2 : Fusion au niveau capture

2) Fusion au niveau des caractéristiques : Elle désigne la combinaison des vecteurs de caractéristiques obtenus par les différentes sources suivantes : plusieurs capteurs, plusieurs instances ou unités d'une même modalité biométrique, plusieurs modalités biométriques. Lorsque les vecteurs de caractéristiques sont homogènes (plusieurs prises d'une empreinte d'un individu), il résulte un seul vecteur de caractéristiques qui représente la moyenne des poids des vecteurs individuels. Dans le cas contraire (des vecteurs de caractéristiques de différentes biométries telles que : le visage et la signature), une concaténation de ces derniers est possible afin de former un seul vecteur de caractéristiques. La concaténation n'est pas possible dans le cas où les caractéristiques ne sont pas compatibles (c'est le cas pour les minuties des empreintes et les coefficients de visage propre, par exemple) [13].

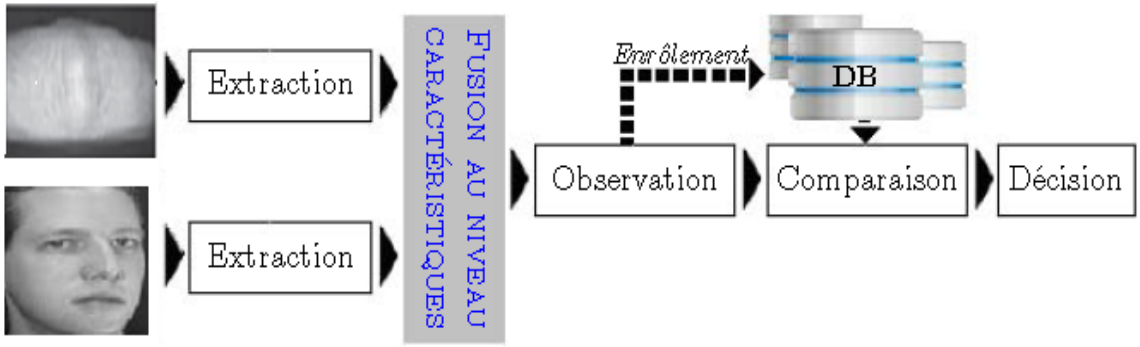


Fig. II.3 : Fusion au niveau caractéristiques

3) Fusion au niveau de score : La fusion au niveau de score c'est la fusion la plus utilisé par ce qu'elle est appliquée tous les types des systèmes avec des méthodes simples est bien précise. Cette fusion est combinée les scores individuels de manière à former un score unique qui est ensuite utilisée pour prendre la décision finale.

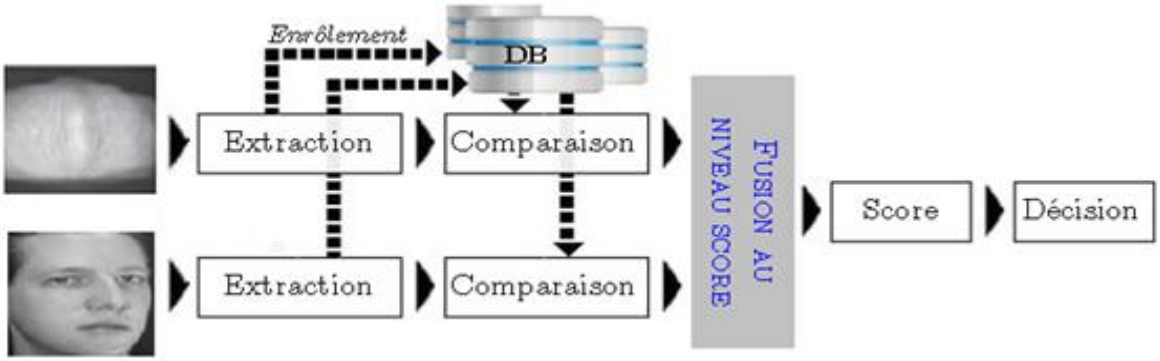


Fig. II.4 : Fusion au niveau score

Les méthodes de combinaisons de scores sont des méthodes très simples dont l'objectif est d'obtenir un score final **S** à partir des **N** scores disponibles si pour i = 1 à N issus de N systèmes. Les méthodes les plus utilisées sont la moyenne, le produit, le minimum, le maximum ou la médiane [14].

- **Somme des scores** : combiner les scores par la moyenne consiste à calculer **S** tel que

$$\mathbf{S} = \frac{\mathbf{1}}{\boldsymbol{N}} \sum_{\boldsymbol{i=1}}^{\boldsymbol{N}} \boldsymbol{s_i} \qquad \textbf{(II.1)}$$

- **Combiner les scores par le produit** : consiste à multiplier tous les scores tel que :

$$\mathbf{S} = \frac{\mathbf{1}}{\boldsymbol{N}} \prod_{\boldsymbol{i=1}}^{\boldsymbol{N}} \boldsymbol{s_i} \qquad \textbf{(II.2)}$$

- **Minimum des scores** : Dans cette technique, on assigne au score final (fusionné) le meilleur (Minimum) score calculé par les différents systèmes. Le minimum est alors défini par :

$$\mathbf{S = min\ (}\boldsymbol{s_i}\mathbf{)} \qquad \textbf{(II.3)}$$

- **Maximum des scores :** la règle maximum est obtenue en assignant la valeur maximum des scores au score final (fusionné) de la façon suivante :

$$\mathbf{S = max\ (}\boldsymbol{s_i}\mathbf{)} \qquad \textbf{(II.4)}$$

4) Fusion au niveau décision : La fusion au niveau des décisions est souvent utilisée pour sa simplicité. En effet, chaque système fournit une décision binaire sous la forme OUI ou NON que l'on peut représenter par 0 et 1, et le système de fusion de décision consiste à

prendre une décision finale en fonction de cette série de 0 et de 1. 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) [14].

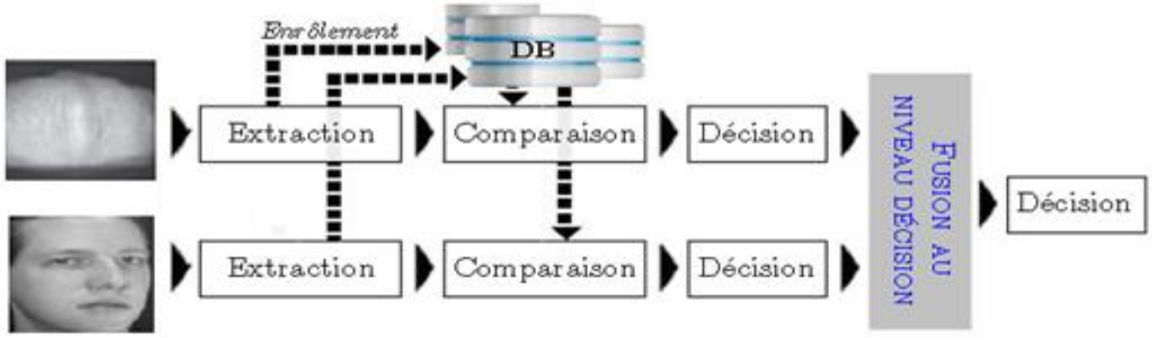


Fig. II.5 : Fusion au niveau décision

II.5 Motivations

La technologie d'identification par leurs FKP reconnaît les individus à travers les articulations des doigts. Cette modalité représente la surface extérieure du doigt qui contient des caractéristiques bien distinctives, surtout au voisinage des articulations, 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, ce nouveau descripteur biométrique basé sur cette surface, appelé empreinte de l'articulation du doigt [16], est commencé à utiliser comme une nouvelle technologie biométrique. Cependant, la main contient plusieurs doigts, pour cela, plusieurs travaux montrent que l'empreinte de l'articulation du doigt (FKP) 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 [5].

II.6 Extraction des caractéristiques

L'extraction des caractéristiques à partir de l'image de modalité (dans notre cas c'est FKP) représente une phase très importante pour concevoir un système d'identification efficace. Cependant, le choix de la méthode d'extraction des caractéristiques est basé sur trois informations essentielles à savoir la texture, les lignes et l'apparence de l'empreinte. La majorité des travaux montrent que l'information la plus distinctive de l'empreinte réside dans la texture, pour cela, nous avons choisis des algorithmes (quantification de la phase

local (LPQ) et motifs binaires locaux (LBP)) très utilisés et donnent des bon résultats remarquables surtout dans la reconnaissance faciale.

II.6.1 Quantification de la phase locale

La quantification de la phase locale (en anglai Local Phase Quantization (LPQ)) est un algorithme très utilisé pour l'extraction de caractéristiques dans plusieurs technologies biométrique telle que le visage, l'empreinte palmaire et l'iris. Cette méthode a été introduite pour la première fois par *Ojansivu et al* [17], ils divisent l'image en petites zones égales N×N, dans chaque zone, les informations locales et utiles de l'image sont extraites. LPQ extrait l'information par l'utilisation de la transformée en Fourier discrète de chaque pixel x, illustré dans l'équation **(**II.7**)** [18].

$$F_u(x) = \sum_{m \epsilon Nx} h(m - x) f(m)\, e^{-2j\pi u^T m} = E_u^T f_x \qquad \textbf{(II.7)}$$

Où *Eu*, de taille = 1 ×M^2, est un vecteur de base de 2DWFT avec la fréquence *u*, et *fx*, taille = M^2× *N*, est un vecteur contenant les valeurs des pixels d'image dans *Nx* à chaque position *x*. La fonction fenêtre, *h* (*x*) est une fonction rectangulaire.

La méthode *LPQ* peut être résumée en quatre étapes distinctes [20]. Dans un premier temps, l'opérateur (*LPQ)* est appliqué sur l'image d'entrée pour obtenir l'image labélisée. Ensuite, l'image obtenue est divisée en petites régions. Pour chacune d'entre elles, un histogramme des étiquettes est construit afin d'obtenir des vecteurs des caractéristiques (Templates) locaux de articulation de doigt (FKP). La représentation globale (vecteur des caractéristiques global qui représente l'image entière) de l'articulation de doigt (FKP) est obtenue par combinaison de tous les vecteurs. La partie (c) de la **Fig. II.6** résume l'ensemble des étapes nécessaires à la génération de ce vecteur [21].

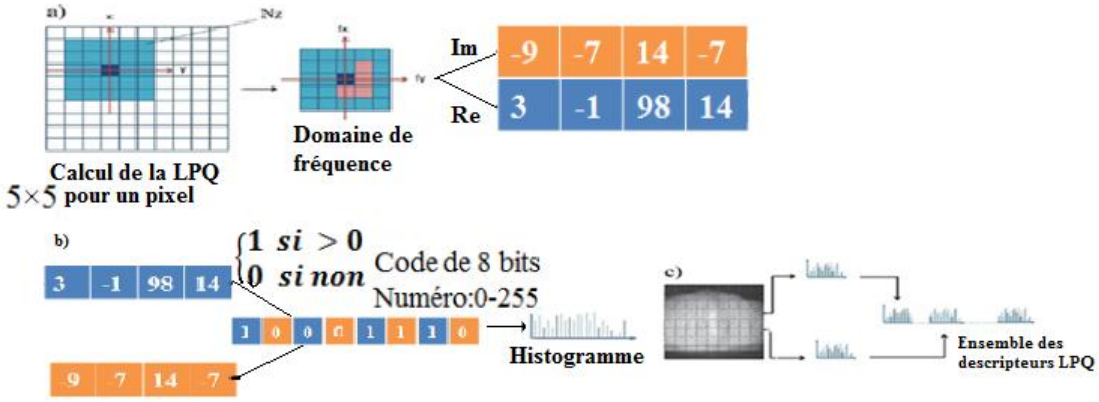


Fig. II.6 : Organigramme de l'ensemble des étapes nécessaire à la génération du vecteur des caractéristiques par la méthode LPQ.

II.6.2 Motifs binaires locaux

Le motif binaire local ((en anglais Local Binary Patterns (LBP)) a été proposé à la fin des années 90 par *Ojala et al* [22]. L'idée de cet opérateur de texture est de donner à chaque pixel un code dépendant des niveaux de gris de son voisinage. Le niveau de gris du pixel central (i_c) est comparé à ceux de ses voisins (i_n) suivant la formule suivante :

$$\text{LBP}\,(x_c\,, y_c) = \sum_{n=0}^{p} s(i_n - i_c)\; 2^n \qquad \textbf{(II.8)}$$

$$s(x) = \begin{cases} 0 & x < 0 \\ 1 & x \geq 0 \end{cases} \qquad \textbf{(II.9)}$$

Le code LBP du pixel courant est alors produit en concaténant ces 8 valeurs pour former un code binaire. La **fig. II.7** donne un exemple de traitement de l'opérateur LBP. On obtient donc, comme pour une image en niveaux de gris, une matrice des valeurs LBP contenant des valeurs d'intensité comprises entre 0 et 255 [19].

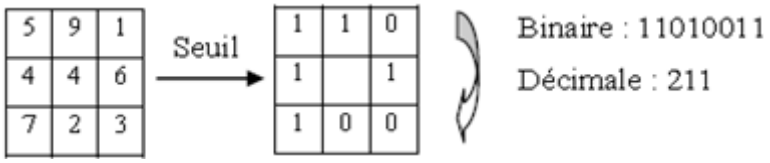


Fig. II.7 : Exemple de traitement de l'opérateur LBP

Afin de représenté les caractéristique de l'empreinte par la méthode LBP et dans un premier temps on considère un voisinage carré, la valeur de niveau de gris du pixel central sert de seuil aux 8 pixels voisins. Après balayage des touts les pixels de l'image, un histogramme de l'image produite est calculé, cet histogramme représente le vecteur des caractéristiques de l'image [22]. Il est à noter, qu'il existe plusieurs variantes de cette méthode. La méthode utilisée dans notre travail est la variante de base (le cas le plus simple).

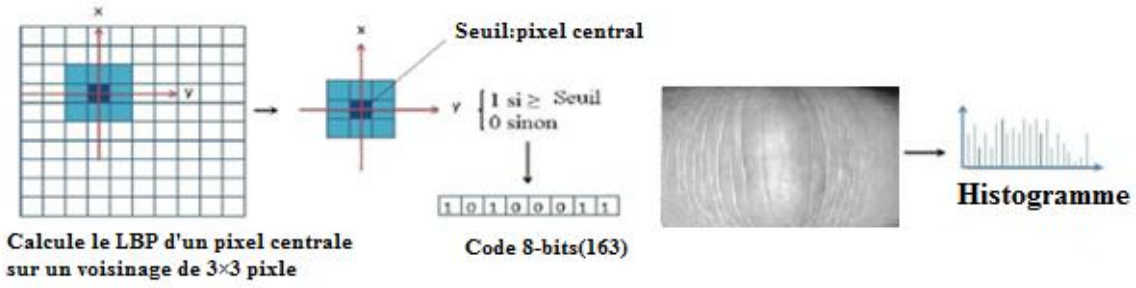


Fig. II.8 : Organigramme de l'ensemble des étapes nécessaire à la génération du vecteur des caractéristiques par la méthode LBP.

II.7 Mesures des similarités

Dans l'étape d'identification, une fois le vecteur des caractéristiques sent obtenu par le module de traitement, le système va effectuer un calcul de similarité entre un vecteur enregistré dans la base de données et un vecteur de test. Cette mesure peut être effectuée avec une distance. Nous avons choisi la distance nommée *Chi-squart* (x^2) qui est la plus adaptée pour mesurer la similarité entre deux histogrammes [22].

La distance Chi-Square est utilisée pour calculer la similarité entre les vecteurs. Nous avons utilisé cette distance qui a déjà été employée pour mesurer des similarités entres les images dans le domaine de reconnaissance des actions (*Laptev et al*. 2008, *Kläser et al*. 2008). Elle permet une normalisation implicite des vecteurs. Cependant, la distance Chi-Square (x^2) entre les deux histogrammes H^i et H^jde même dimension *d* est définie comme suit [23] :

$$X^2\left(H^i,\, H^j\right) = \frac{1}{2}\sum_{k=1}^{d} \frac{\left(H_k^i - H_k^j\right)^2}{\left(H_k^i + H_k^j\right)} \qquad \textbf{(}\text{II.10}\textbf{)}$$

II.8 Décision

La dernière étape dans le processus de reconnaissance est d'accepter ou de rejeter la personne en question basé sur un seuil de sécurité, $\boldsymbol{T_0}$. Le choix de ce seuil est basé généralement sur les erreurs produites par le système. Cependant, une simple comparaison entre la distance trouvée et le seuil permet d'accepter ou de rejeter la personne.

$$\begin{cases} D_0 \leq T_0 \Rightarrow Accepté \\ D_0 > T_0 \Rightarrow Rejeté \end{cases} \qquad \textbf{(}\text{II.14}\textbf{)}$$

Dans la majorité des travaux la valeur de seuil est obtenue dans le point de fonctionnement EER = FAR = FRR [25].

II.9 Conclusion

Actuellement, il y'a une nouvelle tendance qui arrive et qui commence à susciter les efforts, c'est le multimodal, dans lequel on combine plusieurs technologies biométriques, ou plusieurs algorithmes de reconnaissance, ou on utilise divers systèmes pondères dans l'optique d'améliorer les performances de reconnaissance. Dans ce contexte, nous avons présenté dans ce chapitre la biométrie multimodale. Après avoir présenté les limitations des systèmes biométriques, lorsqu'ils utilisent une seule modalité biométrique ainsi que les

avantages des systèmes multimodaux, nous avons présenté les différents types de combinaisons des modalités possibles, les architectures et les niveaux de fusion qui peuvent être utilisés dans un système multimodal. Dans la fin de ce chapitre, nous avons présenté les deux méthodes d'extraction des caractéristiques qui ont été utilisées pour représentés les caractéristiques de l'empreinte. Nous avons donné des détails sur l'application de ces méthodes sur l'image de l'empreinte.

CHAPITRE III

Résultats Expérimentaux

Résultats Expérimentaux

III.1 Introduction

Ce chapitre représente les résultats expérimentaux finales de la reconnaissance des images FKP, effectués avec les algorithmes LPQ et LBP sur la base de données qui regroupe plusieurs images de plusieurs personnes. Rappelons que notre travail consiste à concevoir un système d'identification biométrique de personnes par reconnaissance FKP en se basant sur LPQ et LBP qui peuvent être utilisées pour extraire les caractéristiques des images pour chaque modalité (index gauche (LIF), médian gauche (LMF), index droit (RIF), médian droit (RMF)). On a fait la fusion du score de la modalité «LIF-LMF», «LIF-RIF», «RIF-RMF» et «RMF-LMF», la fusion de toutes modalités, et la fusion des algorithmes «LPQ-LBP», pour améliorer les performances du système. Il est à noter que le type de fusion utilisé est la fusion au niveau des scores qui est le type de fusion le plus utilisé.

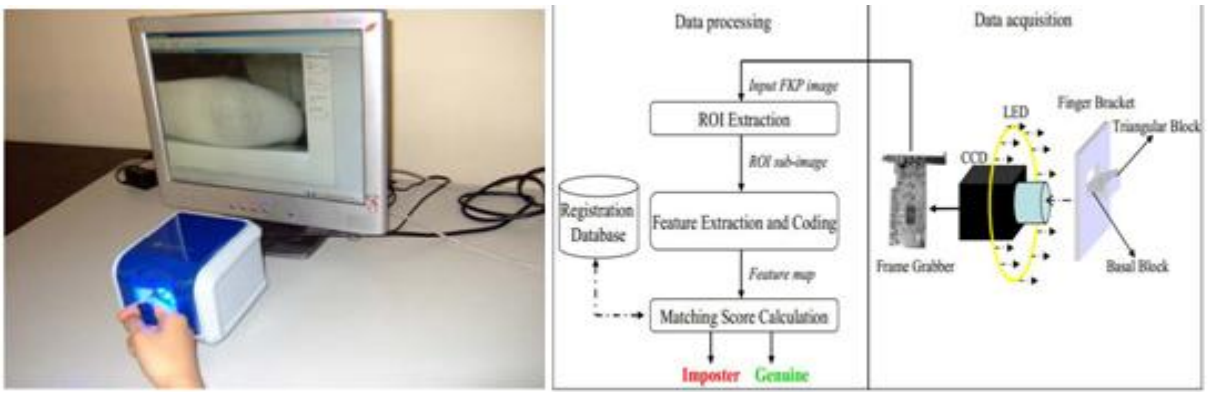
III.2 Système de reconnaissance de FKP

Pour déterminer l'identité de la personne avec la reconnaissance de FKP, il faut nécessairement référencer les images FKP, sous la forme d'une base de données de FKP de toutes les personnes connues par le système. A chaque image est associé un vecteur de

caractéristiques.Ces caractéristiques sont supposées être invariantes pour une même personne, et différentes d'une personne à l'autre. La reconnaissance consiste alors à comparer le vecteur de caractéristiques du FKP à reconnaitre avec celui de chacun des FKP de la base de données.

III.3 Base de données

Le problème critique dans l'acquisition des données est de rendre l'environnement d'acquisition stable le plus possible afin que les variations sur les images collectées, de la même personne, soient réduites. Généralement, un processus d'acquisition stable peut réduire, effacement, la complexité des algorithmes de traitement, ce qui permet d'améliorer les performances de la reconnaissance. Le dispositif d'acquisition des données est composée d'un support de doigt, une source de lumière LED sous forme d'un anneau, une lentille, une caméra CCD et une carte d'acquisition. Le mécanisme d'acquisition des images de cette base de données est illustré par la figure III.1. *(a).* La source de lumière LED et la caméra CCD sont placées dans une boite fermée de sorte que l'éclairage soit constant. La boite contient un support de doigt pour fixer la position de son articulation. Ce support comporte deux blocs, bloc de base et bloc triangulaire, afin de réduire les variations de la position spatiale du doigt dans les déférentes sessions. La taille des images obtenues est de (768×576) pixels avec une résolution ≈ 400 dpi. La figure III.1. *(b)* montre le schéma de principe de ce système (Dispositif d'acquisition de FKP).



(a) *(b)*

Fig. III.1 : Dispositif d'acquisition de FKP développée par Poly U. *(a)* Dispositif d'acquisition et *(b)* Schéma de principe de dispositif.

Les images de cette base de données sont capturées à l'aide du dispositif d'écrit ci-dessus au sein de (Poly U). La base de données PolyU-FKP contient 165 personnes dont 125 personnes sont des masculins. 143 personnes ayant l'âge compris entre 20 et 30 ans et les

autres ayant l'âge entre 30 et 50 ans. Les images de chaque doigt sont capturées en deux sessions avec un intervalle de 25 jours entre les deux sessions. Six images de chaque doigt ont été collectées. Quatre doigts pour chaque personne sont capturés, à savoir, l'index gauche (Left Index Finger-LIF), l'index droit (Right Index Finger-RIF), le milieu gauche (Left Middle Finger-LMF) et le milieu droit (Right Middle Finger-RMF). Par conséquent, 48 images des quatre doigts sont collectées pour chaque personne. La base de données finale rassemble un total de 7920 images en niveaux de gris des doigts, gauches et droits. La figure III.2 illustre quelques exemples d'images de cette base de données.

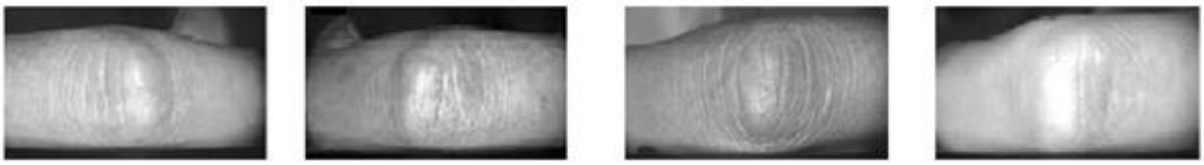


Fig. III.2 : Quelques images de la base de données Poly U-FKP

III.3.1 Séparation de base de données

Les 12 images de l'empreinte (chaque doigt) sont divisées en deux groupes : un groupe pour effectuer l'enrôlement et l'autre pour tester les techniques et déterminer leurs performances. Mais il n'y a pas de règles pour déterminer ce partage de manière quantitative. Il résulte souvent un compromis tenant compte du nombre de données dont on dispose et du temps pour effectuer la reconnaissance. Dans les séries de test que nous avons effectué la base a été scindée de la façon suivante :

✍ **Images d'enrôlement** : La première, la quatrième, la septième et la dixième image de chaque personne servent pour la phase d'apprentissage.

✍ **Images Tests** : Les 8 images restantes de chaque individu nous ont servi pour la réalisation des différents tests.

Le but est d'évaluer le taux de reconnaissance de différents algorithmes présentés, en suivant un protocole de test basé sur la mesure du taux de reconnaissance.

III.4 Résultats Expérimentales

III.4.1.Protocole de test

Pour obtenir les résultats des tests, chaque vecteur de l'image de test a été comparé avec touts les vecteurs dans la base des références. Si les deux vecteurs sont de la même classe (même personne), la mise en correspondance entre eux a été compté comme un client ; sinon

il a été considéré comme un imposteur. Comme nous l'avons énoncé précédemment,les images de chaque personne sont décomposées en deux groupes. Quatre images pour l'enrôlement et huit pour le test. Cependant, 165 × 4 = 660 et 8× (165 × 164/2) = 108240 comparaisons (distances) pour respectivement les distances clients et les distances imposteurs, sont utilisés pour évalué les performances des systèmes et calculé les différents taux et tracé les différents graphes.

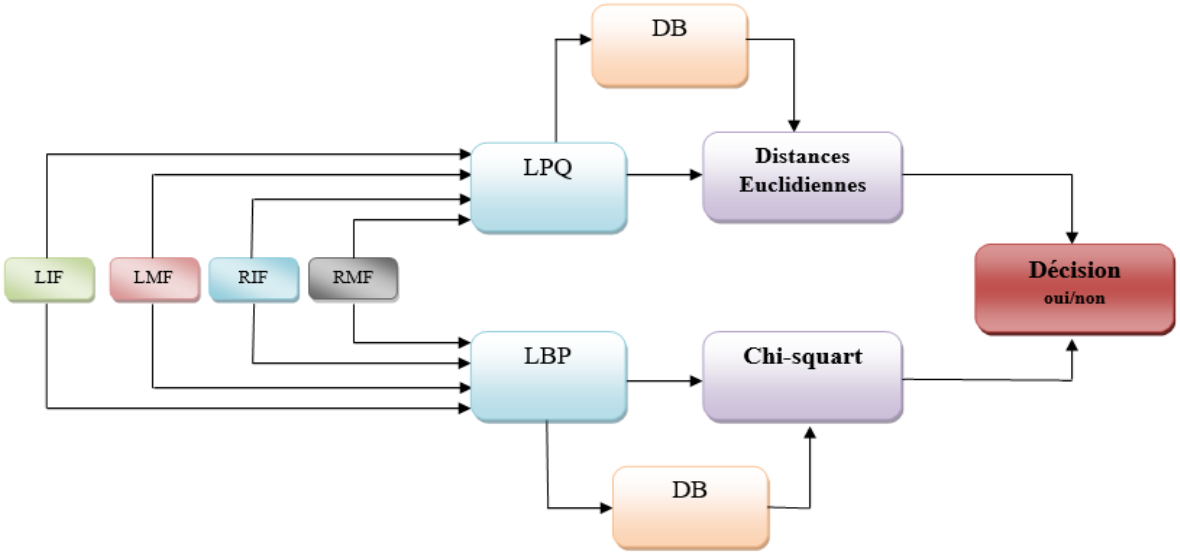


Fig III.4 : Schéma de réalisation illustre les étapes du travail

III.4.2 Système unimodal

Dans cette section, nous nous intéressons tout d'abord à présenter les différents systèmes d'identification biométrique basés sur une seule modalité biométrique (un seul doigt), en utilisant les méthodes décrites dans le chapitre 2.

1) Vecteur basé sur la méthode LPQ

La méthode LPQ est basée sur quatre paramètres essentiels : la taille de fenêtre (windows size), le nombre des blocs et le nombre des filtres. Pour cela, des tests empiriques ont été exécutés afin de sélectionnés les meilleures paramètres de cette méthode. Dans le tableau suivant nous avons présenté les résultats de cette expérience en calculent à chaque fois erreur (EER) de classification.

Tableau III.1 : sélection des paramètres de l'algorithme LPQ

Nbr blocs / Wsize	1	2	4	8
3	3.3008	0.9848	0.3857	0.2985
7	0.9848	0.4412	0.1515	0.3788
11	0.5303	0.2273	0.0884	1.6667
15	0.3485	0.0802	0.1515	-
19	0.2823	0.0549	0.3620	-
23	0.2273	**0.0515**	0.6818	-

Dans ce tableau, nous remarquons qu'un nombre de blocs égal à 2 et une taille de fenêtre égale à 23 donnés un bon résultat. Dans ce cas, le système fonctionne avec une erreur minimale égale à 0.0515%. Noté bien que ces tests sont exécutés sur l'index gauche (LIF).

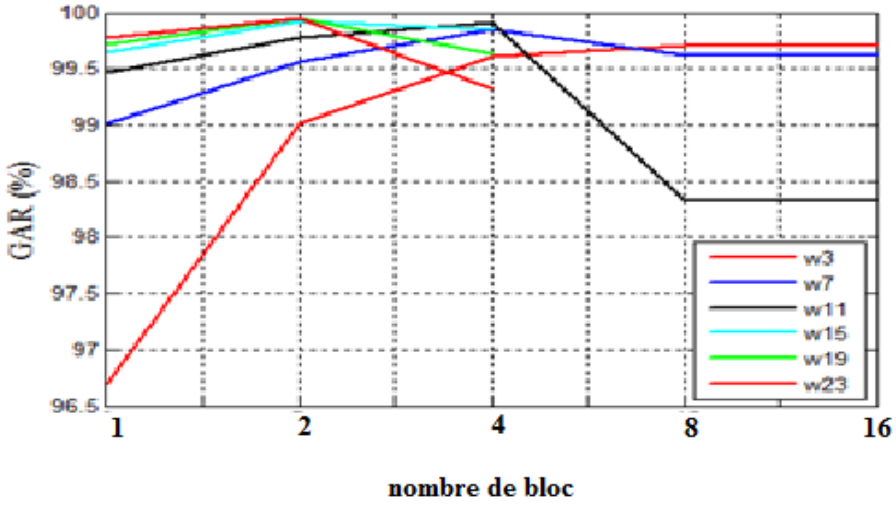


Fig. III.4.2 : Performance de système biométrique sous les différents paramètres

Pour mieux comprendre le comportement de système sous ces paramètres, la courbe ci-dessus, montre le taux des clients acceptés (Genuine Acceptance Rate (GAR)) du système en fonction de différentes valeurs de nombre de bloc. Il est clair qu'une taille de fenêtre égale à 23 (w23) donne la meilleure performance.

Après avoir sélectionné les paramètres optimums de la méthode, les performances des systèmes basés sur les autres doigts ont été évaluées. Le tableau III.2 montre les résultats des tests dans les deux modes d'identification, ensemble ouvert et ensemble fermé.

Tableau III.2 : Performance de système unimodal basé l'algorithme LPQ

Modalité	Ensemble ouvert		Ensemble fermé	
	EER	*To*	*ROR*	*RPR*
LIF	**0.0515**	**0.1520**	99.4697	3
LMF	0.3651	0.0569	**99.9242**	**3**
RIF	0.1620	0.2354	99.5455	45
RMF	0.0996	0.1791	99.5455	36

La figure III.4.3 montre les courbes caractéristiques (Receiver Operating Characteristic (ROC)) du système, dans le mode ensemble ouvert, en utilisant les empreintes des quatre doigts. La méthode d'extraction des caractéristiques basée sur LPQ est utilisée pour touts les doigts. Il est clair, d'après cette figure, que l'index gauche (LIF) offre la meilleure EER (EER = 0.0515%) avec un seuil *To* = 0.1520, en comparaison avec les autres doigts (LMF, RIF et RMF conduisant à un taux d'identification plus grands (GAR = 99.9485%).

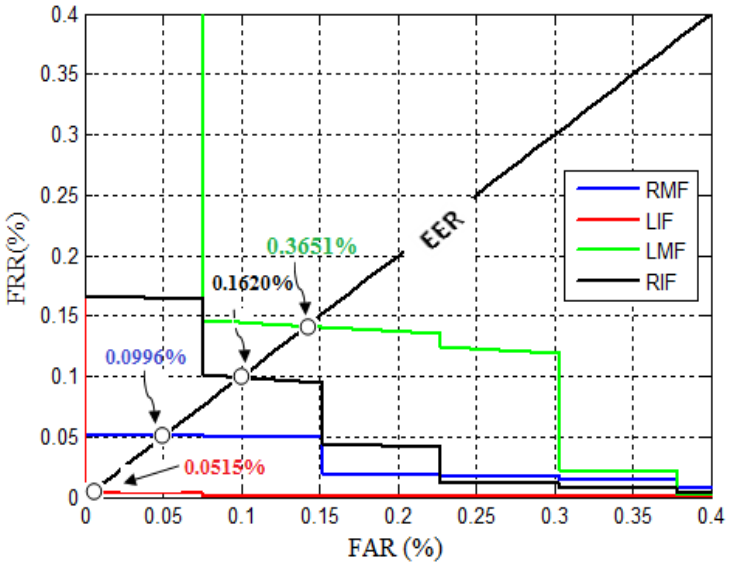


Fig. III.4.3 : Performance de système unimodal (ensemble ouvert) basé l'algorithme LPQ

Nous avons aussi testé les performances de la méthode dans un système identification opérant en mode ensemble fermé. La figure III.4.4, montre la courbe des scores cumulés (Cumulative Match Curve (CMC)) du système basé sur les différents doigts.

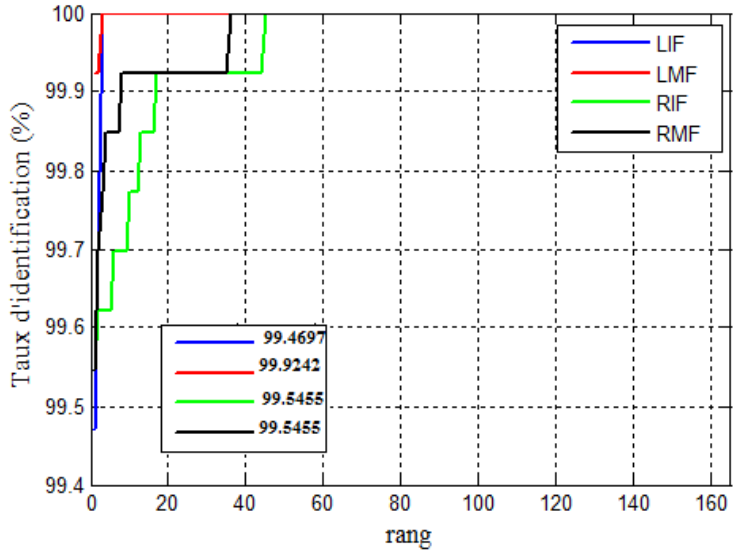


Fig. III.4.4 : Performance de système unimodal (ensemble fermé) basé l'algorithme LPQ

D'après cette figure, ce système fonctionne avec un taux d'identification au rang un (Rank One Recognition (ROR)) égal à 99.9242% et un rang d'identification parfait (Rank of Perfect Recognition-RPR) égal à 3, mais cette fois-ci dans cas de LMF.

Il est à noter, d'après touts les résultats, que la méthode LPQ est des très bon résultats pour touts les doigts dans les deux modes d'identification et elle est comparable et plus efficace que plusieurs travaux dans la littérature.

2) Vecteur basé sur la méthode LBP

D'autres expérimentations, basées sur les images des FKPs, ont été examinées pour l'évaluation du taux d'identification en fonction de la méthode LBP. Le Tableau III.3 nous donne les performances des différentes modalités biométriques (les quatre doigts) en mode d'identification ensemble ouvert et ensemble fermé.

Tableau III.3 : Performance de système unimodal basé l'algorithme LBP

Modalité	Ensemble ouvert		Ensemble fermé	
	EER	*To*	*ROR*	*RPR*
LIF	2.7945	0.0619	84.5455	103
LMF	**2.1631**	**0.0474**	85.8333	65
RIF	2.6342	0.0577	86.5152	110
RMF	2.7147	0.0527	**87.2727**	**67**

Il est clair que l'erreur la plus faible, dans le mode d'identification ensemble ouvert, a été réalisée par le doigt LMF, cette méthode donne an EER égale à 2.1613% avec un seuil To égal à 0.0474. Dans le mode d'identification ensemble fermé, le doigt RMF donne la meilleure performance avec un ROR = 87.2727% et un RPR = 67. Les résultats de comparaison des touts les doigts sont présentés dans les figure III.4.5 et figure III.4.6 pour respectivement le mode d'identification ensemble ouvert et ensemble fermé.

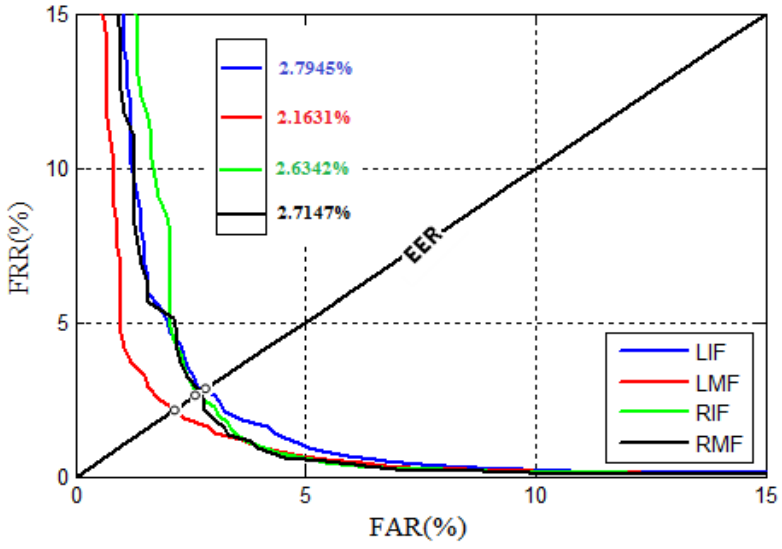


Fig. III.4.5 : Performance de système unimodal (ensemble ouvert) basé l'algorithme LBP

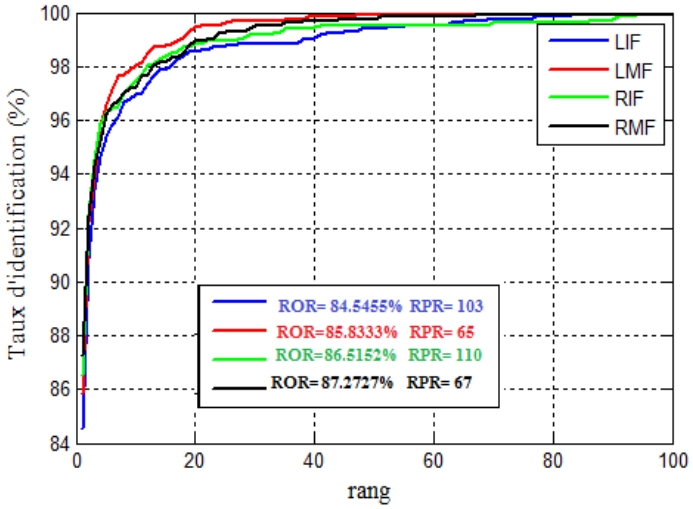


Fig. III.4.6 : Performance de système unimodal (ensemble fermé) basé l'algorithme LBP

L'observation de deux figures nous montre que la méthode basé LBP donne une optimum erreur d'identification ensemble ouvert égale à 2.1631 % et un seuil 0.0474. Ces résultats montrent bien la haute efficacité de la méthode basée sur le LPQ par apport a celle basée sur le LBP, cependant, une grande amélioration égale à 97.620% peut être obtenue par l'utilisation de LPQ au lieu de LBP. Aussi, une grande amélioration (99.404%) dans l'identification ensemble fermé est observée.

III.4.3 Système multimodal

Le but de la multimodalité est d'améliorer le niveau de sécurité du système tel que le taux d'identification des modalités biométriques fusionnées soit supérieur au maximum des taux d'identification des modalités prises séparément. Ainsi, en utilisant les différentes modalités (quatre modalités : quatre doigts pour FKP) ainsi que les deux méthodes d'extraction des caractéristiques (LPQ et LBP), plusieurs systèmes multimodaux peuvent être exploités. Cependant, nous nous limitons, dans ces tests, aux trois scenarios, le multi-algorithmiques, le multi-échantillon et l'hybridation entre les deux scenarios.

1) Systèmes multi-échantillons: Chaque personne dispose quatre doigts (quatre modalités biométriques), par conséquence, la fusion de ces modalités permet d'obtenir un taux d'identification supérieur (au maximum) aux taux d'identification des mêmes modalités prises séparément. Dans notre méthodologie, la fusion au niveau des scores a été testée. Plusieurs combinaisons peuvent être obtenues en utilisant les quatre doigts de chaque personne. Dans notre étude, nous avons utilisé seulement trois combinaisons, à savoir, la combinaison LIF-LMF pour les systèmes qu'utilisent la main gauche pour l'identification, la combinaison RIF-

RMF pour les systèmes qu'utilisent la main droite pour l'identification, et la combinaison TOUT (LIF-LMF-RIF-RMF) pour les systèmes qu'utilisent les deux mains pour l'identification. Le Tableau III.4 montre les performances du système en utilisant les trois combinaisons sous les différentes règles de fusion avec la méthode basée sur LPQ.

Tableau III.4 : Performance de système multi-échantillons basé l'algorithme LPQ

Modalité	FUSION AU NIVEAU SCORE (LPQ)							
	SUM		**MUL**		**MIN**		**MAX**	
	EER	*To*	*EER*	*To*	*EER*	*To*	*EER*	*T0*
LIF-LMF	0	0.159	0	0.147	0	0.159	0.1515	0.2775
RIF-RMF	0	0.066	0	0.069	0	0.087	0.32	0.3023
LIF-RIF	0	0.135	0	0.132	0	0.201	0.3211	0.2753
RMF-LMF	0	0.243	0	0.222	0	0.237	0.0758	0.225
TOUT	0	0.453	0	0.249	0	0.366	0.2273	0.2381
	ROR	*RPR*	*ROR*	*RPR*	*ROR*	*RPR*	*ROR*	*RPR*
LIF-LMF	100	1	100	1	100	1	99.4698	52
RIF-RMF	100	1	100	1	100	1	99.0152	129
LIF-RIF	100	1	100	1	100	1	98.9394	132
LMF-RMF	100	1	100	1	100	1	99.5455	12
TOUT	100	1	100	1	100	1	99.0152	129

D'après ce tableau, il est clair que touts les combinaisons porte des améliorations considérables des performances par comparaison à celle offerte par le system unimodal. Cependant, cette fusion conduit à une erreur nulle (EER = 0.000%) dans le cas des règles SUM, MUL et MIN avec toutes les combinaisons. Ce résultat permet de confirmer l'efficacité de la fusion multimodale dans les systèmes d'identification biométrique.

Nous avons aussi testé les performances de la méthode dans un système d'identification opérant en mode ensemble fermé. Dans le même Tableau sont représentées les performances du système en utilisant les trois combinaisons possibles. On constate sur ce tableau que pour les même combinaisons, le système donne le meilleur résultat avec un ROR égal à 100% et un RPR égale à 1 et ceci avec règles SUM, MUL et MIN.

Dans la deuxième partie de cette section, nous allons exécuter une série des expériences pour examiner la performance de système multi-échantillons basé sur la méthode LBP. Dans le tableau III.5, on remarque une amélioration des résultats obtenus par rapport à ceux des systèmes unimodaux, la diminution d'égalité d'erreur EER avec toutes les règles de la fusion utilisée (SUM, MUL, MIN et MAX) est très observée. A partir des résultats obtenus dans ce tableau on remarque que dans le cas d'identification ensemble ouvert, la fusion de tous les doigts donne une valeur minimal d'erreur (EER) égale à 0.3030% avec la règle de fusion SUM. Dans le cas d'identification ensemble fermé, la meilleure valeur de ROR (99.5455%) est obtenue avec la règle de fusion MUL.

Tableau III.5 : Performance de système multi-échantillons basé sur l'algorithme LBP

Modalité	FUSION AU NIVEAU SCORE (LBP)							
	SUM		MUL		MIN		MAX	
	EER	*To*	*EER*	*To*	*EER*	*To*	*EER*	*To*
LIF-LMF	0.6433	0.0555	0.453	0.0179	0.9848	0.0492	1.5704	0.0589
RIF-RMF	1.2121	0.0654	0.9737	0.0221	0.7379	0.0428	2.1212	0.0651
LIF-RIF	1.2514	0.0682	0.7577	0.0198	0.8333	0.0408	2.3862	0.0765
RMF-LMF	0.8166	0.0467	0.7043	0.0131	1.1819	0.0402	1.5909	0.0568
TOUT	0.3030	0.0636	1.1479	0.0029	0.3788	0.0372	2.3485	0.0872
	ROR	*RPR*	*ROR*	*RPR*	*ROR*	*RPR*	*ROR*	*RPR*
LIF-LMF	96.6667	81	97.2727	81	91.7424	68	93.4091	99
RIF-RMF	96.1364	52	97.0455	23	93.0303	40	93.2576	108
LIF-RIF	96.1364	32	96.9697	9	92.3485	11	93.4091	104
LMF-RMF	97.0455	70	97.7273	51	91.8182	19	93.866	101
TOUT	98.7879	18	99.5455	10	95.7576	10	94.3939	100

Les résultats de comparaison présentés dans la Fig. II.4.7 ont été obtenus sur les doigts LIF et LMF avec une base de données comporte 165 personnes. La figure Fig. III.4.7, pour l'identification ensemble ouvert, doit permettre de comparer les performances de chacun des systèmes multi-échantillons basés sur les méthodes LPQ et LBP. Ces derniers graphiques montre bien la haute performance dans le cas de la méthode basée sur LPQ. Un excellent taux de reconnaissance, égal à 100 % avec une minimum erreur, EER = 0.000% est obtenu.

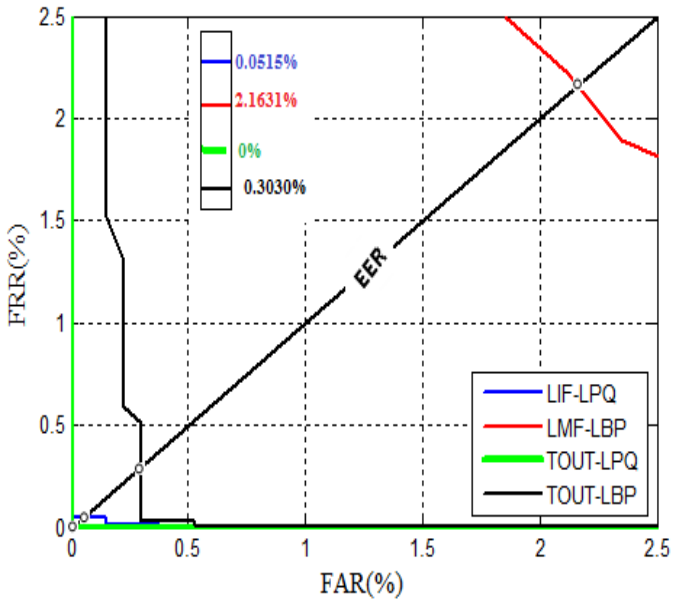


Fig. III.4.7 : Comparaison des performances des systèmes multi-échantillons dans le cas d'identification ensemble ouvert.

Afin de montrer l'efficacité de la fusion multi-échantillons basé sur LPQ ou LBP dans le cas de l'identification ensemble fermé, la figure Fig. III.4.8 présente les résultats de comparaison entre les deux méthodes sous forme des courbes ROCs et CMCs. L'observation de cette figure nous montre que toujours la méthode basée sur LPQ donne un optimum taux d'identification ensemble.

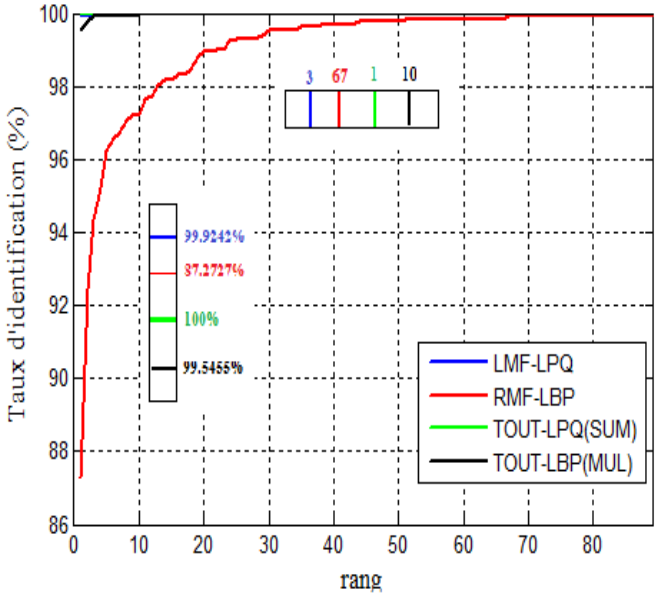


Fig. III.4.8 : Comparaison des performances des systèmes multi-échantillons dans le cas d'identification ensemble fermé.

Cette courbe montre le taux d'identification de chacun du milieu gauche(LPQ), le milieu droite (LBP), la fusion de tous les doigts avec la somme de LPQ et la fusion de tous les doigts avec la multiple de LBP en fonction du rang.

2) Systèmes multi-algorithmes : Dans ce scenario, nous allons mettre en commun les deux méthodes (LPQ et LBP) afin de créer un système multi-algorithmiques, en fusionnant les scores issues du chaque méthode (fusion au niveau scores). Normalement, il est possible d'améliorer l'efficacité et la robustesse des systèmes d'identification de l'empreinte quand la fusion a été réalisée. Dans notre méthodologie, deux représentations différentes de l'empreinte ont été fusionnées au niveau des scores par les quatre règles de fusion (SUM, MAX, MIN et MUL). Cependant, afin d'évaluer la performance du système d'identification multimodal, il faut tout d'abord choisir la règle de fusion des deux scores. Nous avons effectué une étude comparative concernant la performance du système, on change à chaque fois la règle de fusion.

Tableau III.6 : Performance de système multi-algorithmique

Mod	SUM		MUL		MIN		MAX	
	EER	**T0**	**EER**	**T0**	**EER**	**T0**	**EER**	**T0**
LIF	0.0758	0.1597	0.6594	0.0729	2.7945	0.0619	0.0517	0.1520
LMF	0.0018	0.0329	0.303	0.0507	2.1631	0.0474	0.0036	0.0569
RIF	0.1515	0.2375	0.9205	0.0835	2.6342	0.0577	0.1420	0.2357
RMF	0.1061	0.1728	0.5114	0.0637	2.7147	0.0527	0.0996	0.1791
	ROR	**RPR**	**ROR**	**RPR**	**ROR**	**RPR**	**ROR**	**RPR**
LIF	99.3939	11	97.4242	54	84.5455	83	99.4697	3
LMF	99.9242	2	98.7879	10	85.8333	65	99.9242	3
RIF	99.6212	50	97.8788	86	86.5152	110	99.5455	45
RMF	99.6212	49	97.9545	87	87.2727	67	99.5455	36

Les résultats des tests, identification ensemble ouvert et fermé, sont illustrés dans le Tableau III.6. Nous remarquons que pour la modalité LMF, presque toutes les règles de fusion (sauf la règle MIN) donnent un meilleur taux d'identification (GAR et ROR).

Finalement, pour compléter le protocole de test, les figures III.4.9 et III.4.10, montrent une comparaison entre les déférents systèmes dans les deux modes d'identification. D'après ces figures, nous constatons que l'index gauche (LIF) donne le meilleur taux d'identification et il peut atteindre 0.0018% (To = 0.0329) au lieu de 0.3651% dans le cas du LMF. D'autre part, dans l'identification ensemble fermé, ce type de doigt donne toujours le meilleur résultat avec un ROR = 99.9242% et un RPR = 2.

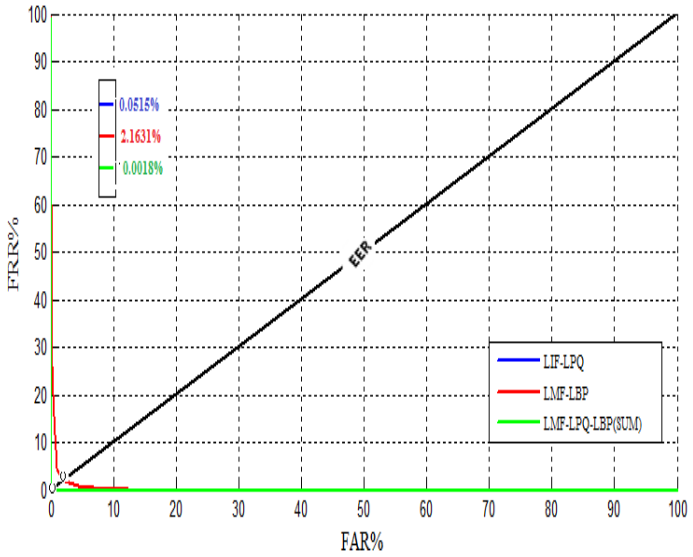


Fig. III.4.9 : Comparaison des performances des systèmes multi-algorithme dans le cas d'identification ensemble ouvert

.

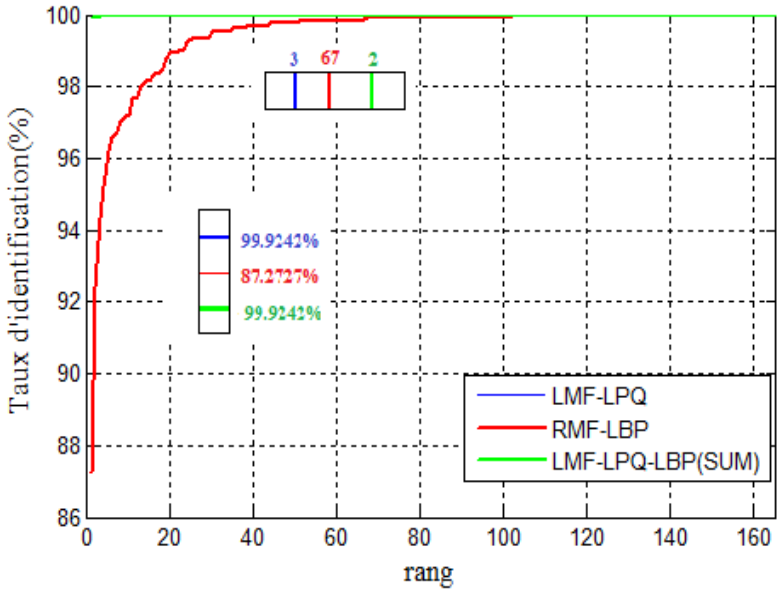


Fig. III.4.10 : Comparaison des performances des systèmes multi-algorithme dans le cas d'identification ensemble fermé

3) Systèmes hybride : Les systèmes hybrides permettent d'associer les performances des différents scenarios en combinant les systèmes multi-échantillon avec les systèmes multi-algorithmiques. Ils permettent d'augmenter les performances de l'identification du point de vue taux d'identification. Dans le mode d'identification ensemble ouvert et fermé ouvert, le Tableau III.7 présente les taux d'identification retenus pour les différents systèmes en respectant les différentes règles de fusion.

Tableau III.7 **:** Performance de système hybride

Mod	SUM		MUL		MIN		MAX	
	EER	T0	EER	T0	EER	T0	EER	T0
LIF-LMF	0	0.0990	0.0758	0.01790	0.9848	0.0492	0.0037	0.0839
RIF-RMF	0	0.0810	0.1515	0.0228	0.7379	0.0428	0.0758	0.183
LIF-RIF	0	0.1319	0.0027	0.0029	0.8333	0.04080	0.0126	0.0925
RMF-LMF	0	0.1500	0.1515	0.0148	1.1819	0.0402	0.0194	0.1282
TOUT	0	0.132	5.8676	0.0835	0.8333	0.0408	0.0126	0.0925
	ROR	RPR	ROR	RPR	ROR	RPR	ROR	RPR
LIF-LMF	100	1	99.9242	6	91.7634	68	99.8493	3
RIF-RMF	100	1	99.6212	13	93.0718	40	99.6249	20
LIF-RIF	100	1	99.8485	2	92.3485	11	99.7727	8
RMF-LMF	100	1	99.8485	27	91.8182	19	99.8485	9
TOUT	100	1	99.8485	2	92.8435	11	99.7727	8

Le tableau III.7 montre que la règle de fusion SUM donne des résultats parfaits, soit avec l'ensemble ouvert (EER = 0%), ou avec l'ensemble fermé (ROR = 100%). Tandis que les autres règles donnent des résultats de EER entre [0.0027%….1.1819%], et ROR entre [91.8182%.....99.9242%].

III.4.4 Etude comparative

Dans cette section, nous avons effectué une étude comparative concernant les différentes méthodes. Les critères de comparaison sont le taux d'identification et le temps de calcul. Le but est de sélectionner la meilleure méthode pour concevoir un système d'identification biométrique. Pour ce faire, nous avons utilisé un ordinateur avec un processeur Intel Dual cadencé à 2.20 Ghz, muni de 2 Go de RAM sous l'environnement Windows 7. Nous avons utilisé le logiciel MATLAB 7.5 pour la mise en œuvre des différentes méthodes. Nous avons retenu les meilleurs résultats obtenus par les différents systèmes pour faire la comparaison.
Les résultats de la comparaison sont donnés sur le Tableau III.8.

Tableau III.8 : Temps d'exécution pour les différents systèmes

Unimodal				Multimodal							
				Echantillons				Algorithme		Hybride	
LMF (LPQ)		RMF (LBP)		LMF-RMF (LPQ)		TOUT (LBP)		LMF (LPQ-LBP)		LIF-RIF (LBP-LPQ)	
EER	$\tau\,(s)$	EER	$\tau\,(s)$	EER	$\tau\,(s)$	EER	$\tau\,(s)$	EER	$\tau\,(s)$	EER	$\tau\,(s)$
0.052	1.3	2.163	0.3	0	2.6	0.3030	1.2	0.0018	1.6	0	3.2

D'après ce tableau, nous remarquons que tous les systèmes multimodaux présentent un temps de calcule considérable (entre 1.2 s et 3.2 s). Le temps de calcule du système basé sur la méthode LPQ, est beaucoup plus grand par rapport aux systèmes basé sur la méthode LBP, malgré LPQ a donné de bon résultat par rapport LBP. Tout dépend de l'application visée, on peut faire un compromis entre ces deux paramètres d'évaluations (taux d'identification et temps de calcule). Cependant, pour une application temps réel, le système basé sur RMF avec la méthode LBP est bien adapté. En contraire, dans les applications de la très haute sécurité, le système hybride est bien adapté.

Finalement, d'après ces résultats, le système d'identification par FKP est un système fiable. Il permet une bonne séparabilité des classes clients et imposteurs. Nous considérons les résultats obtenus comme satisfaisants. De plus, nous avons étudié l'influence de fusion algorithmique (LPQ + LBP) qui nous a donné de bons résultats par rapport au système qui utilise une seule méthode et l'influence de fusion biométrique. L'ensemble des tests effectués a permis de conclure, qu'avec l'utilisation de la fusion de multi-échantillon (quatre doigts) plus la fusion algorithmique, nous avons apporté une amélioration considérable au taux d'identification grâce à ces fusions, ces résultats induisent l'augmentation des performances du système.

III.6 Conclusion

Dans ce chapitre, les travaux biométriques présentés ont conduit à l'élaboration d'un système d'identification des personnes par reconnaissance d'empreintes des articulations des doigts. Pour ce faire, Nous avons proposé plusieurs systèmes biométriques. Outre les systèmes uni-modaux, nous avons exploré quelques systèmes multimodaux. Ces différents systèmes sont testés dans le but d'améliorer le taux d'identification des modalités dans les deux modes d'identification, ensemble ouvert et ensemble fermé. En validant ces systèmes sur une base de données de 165 personnes, nous avons dégagé une amélioration considérable du taux d'identification (100%).

Conclusion Générale

Conclusion Générale

Le travail présenté dans ce mémoire s'inscrit dans le contexte de l'identification automatique des personnes basée sur leurs descripteurs biométriques. Nous avons utilisé une nouvelle modalité biométrique, à savoir l'empreinte des articulations des doigts, pour réaliser nos systèmes biométriques proposés, uni-modaux et multimodaux. Après avoir introduit les concepts généraux de la biométrie, nous avons présenté un état de l'art de méthodes de fusion des modalités biométriques, en utilisant les différentes techniques et niveaux de fusion. Nous avons également présenté quelques méthodes d'extraction des caractéristiques basées sur la texture. Nos tests sur la base des données d'empreinte de FKP de l'Université Polytechnique de Hong Kong (PolyU) ont montré que notre méthode 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.

A l'issu des conclusions retenues de nos travaux réalisés, nous nous envisageons dans les futures travaux d'utiliser d'autres méthodes(PCA ,GABOR..etc) pour l'extraction des caractéristiques des modalités biométriques. Ainsi, nous viserons à utiliser d'autre niveau de fusion (niveau image, niveau caractéristique et niveau décision).

Bibliographie

Bibliographie

[1] F.Perronnin, J. Dugelay, “An Introduction to Biometrics Audio and Video-Based Person Authentification ”. Volume 19 – n4,2002

[2] S.Boudjelial, " detection et identification d’individu par méthode biométrique ".UMMTO.2014

[3] M.Moulay, M.Arbaoui, "authentification des personnes par l’articulation du doigt " UNIVERSITE KASDI MERBAH OUARGLA.2015

[4] A.Murhula, " Conception et mise en place d'une plateforme de sécurisation par synthese et reconnaissance biométrique de documents de traffic ". Polytechnique_INITELEMATIQUE_BURUNDI - Ingénieur Civil en Informatique et télécommunications 2015

[5] A.Meraoumia, "Modèle de Markov caché applique à la multi biométrie " USTHB. 2014

[6] A. Ross and A. K. Jain, "Information Fusion in Biometrics", Pattern Recognition Le Vol. 24, Issue 13, pp. 2115-2125, September, 2003.

[7] K. Nanda kumar, A. Ross, and A. K. Jain, "Biometric Fusion: Does Modeling Correla Really Matter? ", Proc. 3rd Int`l Conf. on Biometrics: Theory, Applications and Syst Washington DC, Sept. 2009.

[8] Y.Lee, K.Lee, Hyung keun Jee, Youn-Hee Gil, Woo-Yong Choi, Dosung Ahn, Sung Bum Pan, "Fusion for Multimodal Biometric Identification",5th International conference on Audio and video-based biometric person authentication-AVBPA, Hilton Rye Town, N.Y. USA, July 2005, pp. 1071-1079.

[9] S.Jidong, L.Xiaoming, "Fusion of Radar and AIS Data", 7th International Conference on Signal Processing-ICSP'04, Beijing, China, Vol.3, 2004, pp, 2604-2607.

[10] C.Berger ; M.Voltersen ; R.Eckardt ; Eberle, J. ; Heyer, T. ; Salepci, N. ; Hese, S. ; Schmullius,C. ; Tao, J. ; Auer, S. ; Bamler, R. ; Ewald, K. ; Gartley, M. ; Jacobson, J. ; Buswell, A. ; Du, Q. ;Pacifici, F., "Multi-Modal and Multi-Temporal Data Fusion", IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing, Jun 2013, Vol.6, N.3, pp.1324-1340,.

[11] Julian Fièrrez-Aguilar, Javier Ortega-Garcia, Daniel Garcia-Romero, and Joaquin Gonzalez-Rodriguez, "A comparative evaluation of fusion strategies for multimodal biometric veri_cation",4th International Conference on Audio-and Video-Based Biometric Person Authentication-AVBPA, Guildford, UK, Jun 2003, pp. 830-837.

[12] A. Ross and A. Jain. “Information fusion in biometrics”. *Pattern Recognition Letters*, Vol. 24, No. 13, pp. 2115–2125, 2003.

[13] Ismahène Dehache &Labiba Souici-meslati, " UNE APPROCHE MULTIMOD POUR LA VERIFICATION BIOMETRIQUE ".2011

[14] Lorène Allano, ‘‘stratégies de fusion de scores et mesures de dépendance appliquées aux bases de personnes virtuelles’’ UNIVERSITE D’EVRY-VAL D’ESSONNE,2009

[15] A. A. Ross, A. K. Jain and K. Nandakumar, "Levels of Fusion in Biometrics", Handbook of Multibiometrics, Springer, US, 2006.

[16] Rui Zhao, Kunlun Li, Ming Liu, Xue Sun, "A Novel Approach of Personal Identification Based on Single Knuckle-print Image", Asia-Pacific Conference on Information Processing-APCIP, 2009.

[17] Ville Ojansivu et Janne Heikkilä, *"Blur Insensitive Texture Classification Using Local Phase Quantization*". Dans *ICISP ’08 : Proceedings of the 3rd international conference on Image and Signal Processing*, pages 236–243, Berlin, Heidelberg, 2008.

[18] Shahid Akbar, Ashfaq Ahmad,Maqsood Hayat,Faheem Ali, “Face Recognition Using Hybrid Feature Space in Conjunction with Support Vector Machine”.2015

[19] Wael Ben Soltana, "Optimisation de stratégies de fusion pour la reconnaissance de visages 3D ".2014

[20] Timo Ahonen, Esa Rahtu, Ville Ojansivu et Janne Heikkilä, *"Recognition of blurred faces using Local Phase Quantization".* Dans *ICPR*, pages 1–4, 2008.

[21] Cécile Fiche,"Repousser les limites de l’identification faciale en contexte de vidéo-surveillance". GRENOBLE 2012

[22] Matti Pietikäinen et Janne Heikkilä, "*Image and Video Description with Local Binary Pattern", Variants*, June 2011.

[23] Mohamed Ibn Khedher "Ré-identification de personnes à partir des séquences vidéo ".2015

[24] Nicolas Morizet, " Reconnaissance Biométrique par Fusion Multimodale du Visage et de l'Iris ".2010

[25] Abdallah Meraoumia,, "Personal Recognition by Finger-Knuckle-Print Based on Gabor Filter Response". INTERNATIONAL CONFERENCE ON ELECTRONIC OIL - ICEO'11 OUARGLA, ALGERIA, FEBRUARY 07-09, 2011

[26] The Hong Kong Polytechnic University, PolyU FKP Database, Http: //www.comp.polyu.edu.hk/sbiometrics/FKP/polyudb.htm.

[27] L. Zhang, L. Zhang, D. Zhang," Finger-knuckle-print verification based on band-limited phase only Correlation", the 13th International Conference on Computer Analysis of Images and Patterns-CAIP, Munster, Germany, pp. 141-148, 2009.

ANNEXE

Prétraitement d'image FKP

Afin d'extraire la région d'intérêt (Region Of Interest ROI) qui contient les textures autour de l'articulation. Cette opération a pour but d'éliminer le fond (réduction de la taille d'image) et d'avoir des résultats plus précis.

A.1.Etape 1 : Filtrage et sous-échantillonnage

La taille de chaque image de la base des données est 768×576 pixels avec une résolution de 400dpi. Il n'est pas nécessaire d'utiliser cette résolution pour l'extraction des caractéristiques (une faible résolution peut représenter bien les lignes principales et secondaires autour de l'articulation). Par conséquent, l'image du doigt subit une opération de filtrage suivi par une opération de sous-échantillonnage. L'objectif de l'opération de filtrage est de réduire le bruit dans l'image. Un filtre passe-bas (filtre gaussien), peut être appliqué pour réduire ce bruit et améliorer la qualité de l'image originale. L'opération de sous-échantillonnage permet de réduire la résolution de l'image jusqu'à 150dpi. L'avantage de cette opération est de réduire considérablement le coût de calcul en réduisant la quantité de données. Nous notons ID l'image résultante. Le résultat de cette étape est illustré dans la figure (A.1).

Figure A.1: Filtrage et sous-échantillonnage de l'image de doigt.

A.2.Etape 2 : Détermination de l'axe X

Une fois l'image de l'empreinte a été filtrée et sous-échantillonnée, l'algorithme détermine l'axe horizontal X. La limite inférieure du doigt peut être facilement extraite par un détecteur de contour de type Canny. Le filtre de Canny est utilisé en raison de ses avantages (bonne détection, bonne localisation). En fait, cette limite inférieure est presque conforme à toutes les images parce que tous les doigts sont mis sur le bloc de base dans l'acquisition de l'image. En adaptant cette frontière comme une ligne droite, l'axe X est déterminé. La figure(A.2) montre l'axe X dans la frontière basse du doigt.

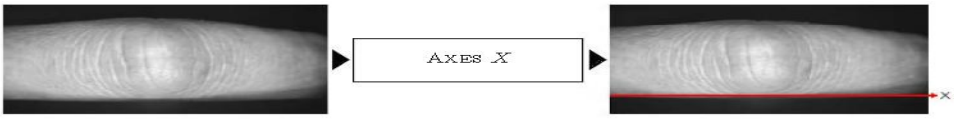


Figure A.2 : Détermination de l'axe X.

A.3.Etape 3 : Extraction d'une sous-image

Les informations utiles qui peuvent être utilisées pour une identification biométrique ne réside que dans une partie de l'image du doigt. Par conséquent, nous avons d'abord coupé

Figure A.3 : Sous-image extraite avant l'extraction de la ROI

Une sous-image, IS, à partir de l'image originale. Les limites gauche et droite d'IS sont deux valeurs xées empiriquement. Les limites hautes et basses sont estimées selon la limite de vrais doigts. La figure (A.3) montre un exemple d'une sous-image. Cette sous-image est utilisée pour calculer l'axe Y.

A.4.Etape 4 : Détection de contour

En appliquant le détecteur de contour de type Canny à l'image IS, l'image des contours IE peut être obtenue. Voir la figure(A.4) pour un exemple

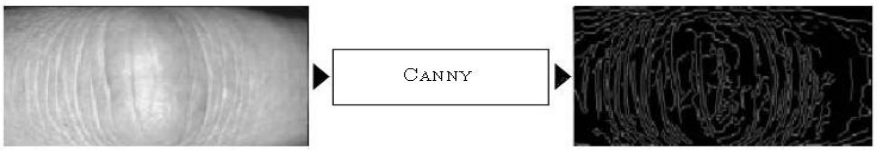


Figure A.4 : Image des contours obtenue.

A.5.Etape 5 : Codage des directions convexes

Basé sur les caractéristiques des courbes des contours dans l'image, IE, nous pouvons coder IE pour obtenir une image codée, ICD, qui représente les directions convexes des courbes. À cette étape, chaque pixel dans IE sera donc désigné par un code afin de représenter la direction (convexe) locale de ce pixel. Basé sur l'observation des images de doigt, nous pouvons représenter un modèle idéal des courbes dans l'image de doigt comme indiqué dans la figure (A.5). Dans ce modèle, une courbe dans l'image est soit convexe vers la gauche

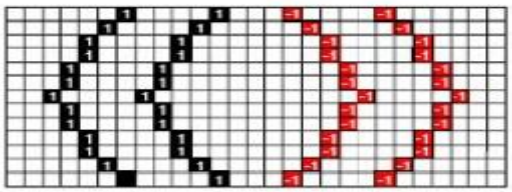


Figure A.5 : Courbes sur l'image de doigt.

Ou convexe vers la droite. Nous pouvons coder les pixels sur les courbes convexes (vers la gauche) par « 1 », les pixels sur les courbes convexes (vers la droite) par « 1 » et les autres pixels (n'appartiennent pas _a ces deux courbes) par « 0 ». La figure A.6 montre les directions convexes ICD.

A.6.Etape 6 : Détermination de l'axe Y

Pour une image de doigt, la plupart des courbes sur la partie gauche de l'image sont dirigées vers la gauche et ceux sur la partie droite sont dirigés vers la droite. Cependant, il n'y a pas

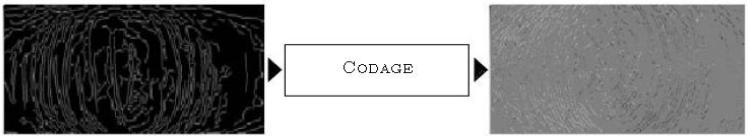


Figure A.6 : Image obtenue par l'application de codage de la direction convexe

Des directions convexes évidentes dans une petite zone autour de l'articulation. A partir de cette observation, nous pouvons définir une grandeur de convexité,ϱ, comme suit :

$$\boldsymbol{\varrho(x) = abs(\sum_w I_{CD})} \quad \textbf{(A.1)}$$

Où x est la position horizontale (représente une colonne) de la fenêtre. W est une fenêtre symétrique par rapport à l'axe X = x. La fenêtre W est de taille d×h, avec h égale à l'hauteur de l'image IS et d est choisi, dans notre travail, égale à 35. La grandeur ϱ (x) peut atteindre sa minimale autour du centre de l'articulation. La fenêtre doit réaliser un trajet qui part de la gauche et qui va balayer les différents x. L'axe Y est définit comme suit :

$$Y = \arg min_{\infty}[\boldsymbol{\varrho(x)}] \quad (A.2)$$

Cette position peut être utilisée pour définir l'axe Y. La figure (A.7) montre la position de l'axe Y dans l'image du doigt.

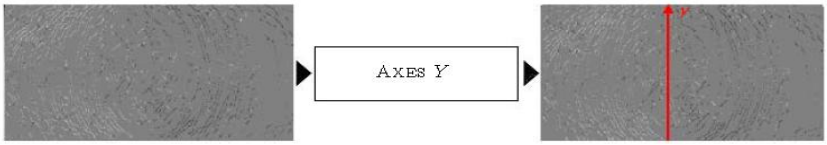


Figure A.7 : Détermination de l'axe Y.

A.7.Etape 7 : Localisation de la ROI

Après avoir localisé les axes X et Y, nous pouvons déterminer une zone dans l'image ID, nommée IROI, qui représente la région d'intérêt. D'après la figure(A.8), la ROI, avec une taille fixe, peut être extraite à partir de l'image ID

Figure A.8 : Localisation de la ROI dans l'image de doigt

A.8.Etape 8 : Extraction de ROI

Une région d'intérêt de l'empreinte est définie et découpée autour du l'axe Y (comme le montre la figure(A.9). Une région rectangulaire, qui correspond au ROI, avec une dimension fixe (110×220 pixels) et contenant la majorité de l'empreinte, est ensuite extraite.

Figure A.9 : Extraction de la ROI à partir l'image de doigt.

Enfin, nous pouvons constater que la méthode de localisation des axes X et Y, ainsi que la méthode d'extraction de la ROI, peuvent aligner efficacement les différentes images des doigts, en normalisant la zone qui fait l'objet des différents traitements pour extraire les caractéristiques biométriques du doigt. Ces opérations réduisent considérablement les variations causées par les différentes poses du doigt dans le système d'acquisition.

Abstract.
In recent years, automatic personal identification is becoming an important requirement in variety 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, which offers more properties and several advantages over the traditional security. Finger-Knuckle-Print (FKP) is one important biometric feature. Which provides uniqueness, stability and high distinguish ability. In our work,a Multi-Block Local Phase Quantization (MB-LPQ) and Local Binary Pattern (LBP) techniquesare used in order to extract the discriminant characteristics of the FKP modality. 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 are used. Our experimental results, using FKP database (PolyU), demonstrate the higher performance of the proposed FKP based identification system.

Key words: Biometrics, FKP, Feature extraction, Identification, MB-LPQ, LBP, multimodal, fusion.

Résumé.
Au cours des dernières années, l'identification personnelle automatique devient une exigence importante variété d'applications telles que le contrôle d'accès, les systèmes de surveillance et des bâtiments physiques. Biométrie, qui traite de l'identification des individus en fonction de leurs caractéristiques physiques ou comportementales, est apparue comme une technologie d'identification automatique efficace, qui offre plus de propriétés et plusieurs avantages par rapport à la sécurité traditionnelle. L'empreinte de l'articulation de doigts (FKP) est une caractéristique biométrique importante. Qui fournit l'unicité, la stabilité et la haute distinction capacité. Dans notre travail, un multi-bloc Quantification de la Phase locale (MB-LPQ) et Motif binairelocale (LBP) sont des techniques utilisées afin d'en extraire les caractéristiques discriminantes de la modalité FKP. Le système biométrique uni-modal souffre comme les données du capteur de bruit, 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 estutilisé. Nos résultats expérimentaux, en utilisant la base de 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 الاخيرة , اصبحت الهوية الشخصية مطلب هام وأساسي في عدة تطبيقات مثل الامن , انظمة المراقبة والعمارات ....الخ. تعالج الانظمة البيومترية هويات الأشخاص بدلالة مميزاتهم الفيزيائية او المعنوية .وقد تبين انها تقنية فعالة للتعرف التلقائي على الأشخاص , وتتميز بكثير من المميزات على الانظمة التقليدية . بصمة مفصل الاصبع (FKP), هي ميزات بيومترية هامة , والتي تتوفر فيها الوحدانية ,الثبات ,وقدرة تمييز عالية .
وفي عملنا هذا , قمنا بتطبيق خوارزميتين LPQ وLBP, لأنهما تقنيتان تقومان باستخراج مميزات مفاصل الاصابع على شكل مصفوفات .النظام البيومتري احادي الوسائط يعاني من حساسية الملتقطات كالطفيليات ,اللاعمومية ....الخ, ومن اجل هذه السلبيات ,تطرقنا الى أنظمة متعددة الوسائط . وقد استعملنا في نتائجنا التجريبية قاعدة المعطيات لجامعة (PolyU),كما اننا بينا من خلال هذه النتائج الاداء الافضل لانظمة الهوية على القاعدة (FKP) المقترحة .

***الكلمات المفتاحية*-البيومترية , FKP, استخراج الميزات ,الهوية , احادي الوسائط ,متعدد الوسائط ,الدمج ,LBP, LPQ**