



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
Filière : Télécommunication
Spécialité : Signal et Communication

Présenté par :

BENOUAER Aichouche TAHRINE Soumia

Thème

*Systeme biométrique basé sur les
motifs locaux binaires orientés
(LBP_θ)*

Soutenu publiquement

Le: 25/05/2016

Mme.	F. CHERIF	MCB	Président	UKM Ouargla
Mr.	A. MERAOUMIA	MCA	Encadreur	U.TEBESSA
Mr	M. KORICHI	Doctorant	Co-Encadreur	UKM Ouargla
Mme.	S. OURAGH	MAA	Examinatrice	UKM Ouargla

Année Universitaire : 2016 /2017

Remerciements

En premier lieu, nous tenons à remercier notre **DIEU**, notre créateur pour nous avoir donné la force pour accomplir ce travail.

Nos sincères gratitudes à **MR.MERAOUZIA Abdallah** pour accepter de nous encadrer, et pour ses instructions incontestables

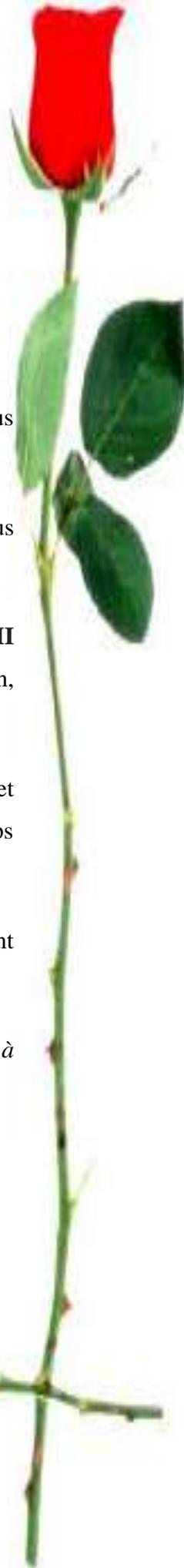
Nous adressons nos vifs remerciements à notre Co-encadreur **MR.KORICHI Maarouf** pour nous avoir diligentés tout au long de ce travail, pour sa compréhension, sa patience, ses compétences, et ses remarques qui nous ont été bénéfiques.

Nous tenons tout particulièrement à remercier **Mr.SAMAI Djamel** et **Mr.BENSID Khaled**, qui nous ont soutenus, conseillés et nous ont offert leur temps précieux.

Nos remerciements les plus vifs à tous les enseignants du département d'électronique et tous les collègues de la promotion.

Nos derniers remerciements à ceux qui ont contribué de près ou de loin à l'élaboration de notre mémoire.

BENOUAËR Aichouche, TAHRINE Soumia



Dédicace

Je dédie ce modeste travail à :

Mes parents:

Ma mère, qui ne cesse jamais de m'offrir, son amour, son soutien, tous les sacrifices consentis et ses précieux conseils, pour toute son assistance et sa présence dans ma vie.

Mon père, j'espère qu'il est fier de trouver ici le résultat d'années de sacrifices pour m'aider à avancer dans la vie. Merci pour les valeurs nobles, l'amour, l'éducation et le soutien permanent venu de vous.

Mes frères et sœurs qui n'ont cessé d'être pour moi des exemples de persévérance, de courage et de générosité. Ma grand-mère que Dieu protège et mes chers neveux nièces.

Mes amies, tout particulièrement ma cher binôme Soumia, mes collègues, et ma grande familles BENOUAER et BENMOUSSA qui m'on toujours poussé et m'encouragé.

Mes enseignants du département d'électronique.

Benouaer Aichouche



Dédicace

Je dédie ce modeste travail

A mes chers parents, qui ont tout sacrifié pour mon bien et qui ont éclairé ma route par leur compréhension, leurs soutiens

Mon Père *Abdelhafid* Ma Mère *Khaoula*.

A mes deux frères Mourad et Hassan ainsi que Mes Sœurs.

A mes anges *Nihad* et *Khoulod* sans oublier ma neveu

Mohammed Raed.

A ma Sœur et binôme *Aichouche*.

A celui que m'a soutenue tout au long de ce projet

Mon fiancé *Haroun*.

A toute ma famille, Mes amies et mes collègues d'études.

A tous ceux qui ont contribué de près ou de loin
pour que ce projet soit possible.

Je vous dis merci

TARME Soumia



Table des Matières

Table Des Matières.....	i
Liste Des Figures.....	iii
Liste Des Tableaux.....	V
Liste D'abréviations.....	Vi
INTRODUCTION GENERALE.....	1
<u>CHAPITRE I : Sécurité de l'information et la biométrie</u>	
I.1 Introduction.....	3
I.2 Sécurité de l'information.....	3
I.3 Méthodes de reconnaissance.....	4
I.4 Biométrie.....	4
I.5 Modalités biométriques.....	5
I.5.1 L'analyse physiologique (morphologique).....	5
I.5.2 L'analyse comportementale.....	9
I.6 Architecture d'un système biométrique.....	11
I.7 Applications de la biométrie.....	13
I.8 L'évaluation de performances des systèmes biométriques.....	13
I.9 Conclusion.....	15
<u>CHAPITRE II: Biométrie Multimodale et Fusion d'Information</u>	
II.1 Introduction.....	17
II.2 Limitation des systèmes biométriques uni-modal.....	17
II.3 Système biométrique multimodal.....	18
II.3.1 Catégories de la multi-modalité.....	18
II.3.2 Architecteur de des systèmes multimodaux.....	19
II.4 Fusion multimodale.....	20
II.5 Fusion au niveau des scores.....	23
II.5.1 Approche de combinaison des scores.....	23
II.5.2 Approche de classification des scores.....	24
II.6 Normalisation des scores.....	24

II.7 Conclusion.....	26
<u>Chapitre III : Extraction Des Caractéristiques d'Empreinte Palmaire en utilisant LBP_θ</u>	
III.1 Introduction.....	28
III.2 Choix l'empreinte palmaire.....	28
III.3 Empreinte palmaire.....	29
III.3.1 Avantages de l'empreinte palmaire.....	29
III.3.2 Les caractéristiques biométriques d'une empreinte palmaire et les types de reconnaissance.....	29
III.4 Système proposé.....	32
III.4.1 Extraction des Caractéristiques.....	33
III.4.2 Motifs binaires locaux LBP.....	33
III.4.3 Contribution.....	34
III.4.4 LBP Orienté (LBP _θ).....	34
III.5 Conclusion.....	36
<u>Chapitre IV : Expérimentations Et Résultats</u>	
IV.1 Introduction.....	38
IV.2 Objectif.....	38
IV.3 Base de données de l'empreinte palmaire multi-spectrale (PolyU-MSP)	38
IV.4 Séparation des bases de données.....	39
IV.5 Environnement du travail	39
IV.6 Expérimentations sur l'identification des individus par leurs empreintes palmaire....	40
IV.6.1 Système uni-modal.....	40
IV.6.2 Système multimodale.....	49
IV.7 Compte rendu des résultats	55
IV. 8 Conclusion.....	59
Conclusion générale.....	58

Liste des figures

Figure I.1	Catégories technologiques de la biométrie.....	5
Figure I.2	a) Image de la geometrie de main ;b) Dispositif de reconnaissance de la geometrie de main.....	6
Figure I.3	a) Image d'une empreinte digitale ;b) Dispositif de reconnaissance d'une empreintes digitales.....	6
Figure I.4	a) Image du visage ; b) Dispositif de reconnaissance de visage.....	7
Figure I.5	a) Image du retine ; b) Dispositif de reconnaissance de retine.....	7
Figure I.6	a) Image d'un Iris;b) Dispositif de reconnaissance de l'Iris.....	8
Figure I.7	Image de l'ADN.....	8
Figure I.8	a) Image de la voix ; b) Dispositif de reconnaissance de la voix.....	9
Figure I.9	Image d'un clavier.....	9
Figure I.10	a) Image de signature ; b) Dispositif de reconnaissance de signature.....	10
Figure I.11	a) Images d'une démarche.....	10
Figure I.12	Architecture d'un système de reconnaissance biométrique.....	11
Figure I.13	Phase d'enrôlement.....	12
Figure I.14	Processus d'Identification.....	12
Figure I.15	Processus de Vérification.....	13
Figure I.16	La courbe CMC.....	15
Figure I.17	La courbe ROC.....	15
Figure II.1	Catégories de la multi-biométrie.....	19
Figure II.2	Architecture d'un système multi-biométrique en parallèle.....	20
Figure II.3	Architecture d'un système multi-biométrique en série.....	20
Figure II.4	Différents niveaux de fusion biométrique.....	21
Figure II.5	Schéma de fusion au niveau du capteur.....	21
Figure II.6	Schéma de fusion au niveau du l'extraction des caractéristiques.....	22
Figure II.7	Schéma de fusion au niveau de la décision.....	23
Figure II.8	Schéma de fusion au niveau de scores.....	23
Figure III.1	a) Image du empreinte palmaire ; b) Dispositif de reconnaissance de L'empreinte palmaire.....	29
Figure III.2	La paume de main et ses plis.....	30

Figure III.3	Empreintes différentes avec des lignes principales similaires.....	30
Figure III.4	Points de référence de l'empreinte palmaire (a et b).....	31
Figure III.5	Caractéristiques d'une empreinte palmaire : a) image basse résolution, b) image haute résolution.....	32
Figure III.6	Description de système.....	32
Figure III.7	Construction d'un motif binaire et calcul du code LBP.....	34
Figure III.8	Illustration de la méthode proposée LBP_{θ}	35
Figure IV.1	Schéma de principe de dispositif d'acquisition des images multi spectrales	40
Figure IV.2	Quelques images de la base de données PolyU-MSP.....	40
Figure IV.3	Schéma du principe d'un système d'identification Uni-modal.....	42
Figure IV.4	Courbe ROC de LBP basique.....	43
Figure IV.5	Courbe CMC de LBP basique.....	43
Figure IV.6	Courbe ROC de LBP_{var}	44
Figure IV.7	Courbe CMC de LBP_{var}	45
Figure IV.8	Courbe ROC de NIR_PLM en utilisant LBP_{θ}	46
Figure IV.9	Courbe CMC de NIR_PLM en utilisant LBP_{θ}	47
Figure IV.10	Courbe ROC de NG_PLM en utilisant LBP_{θ}	47
Figure IV.11	Courbe CMC de NG_PLM en utilisant LBP_{θ}	48
Figure IV.12	Courbe ROC de LBP_G	49
Figure IV.13	Courbe CMC de LBP_G	49
Figure IV.14	Schéma de principe de système multimodal proposé.	50
Figure IV.15	Courbe ROC de fusion biométrique dans l'angle 150°	52
Figure IV.16	Courbe CMC de fusion biométrique dans l'angle 150°	52
Figure IV.17	Courbe CMC de fusion 30NG/150NIR.....	53
Figure IV.18	Courbe ROC de fusion 30NG/150NIR.	54
Figure IV.19	Courbe CMC de fusion 150NG/30NIR.....	55
Figure IV.20	Courbe ROC de fusion 150NG/300NIR.....	55
Figure IV.21	Courbe ROC des différentes variantes de LBP.	57
Figure IV.22	Courbe CMC des différentes variantes de LBP.....	57

Liste des tableaux

Tableau I.1 : Comparaison entre les modalités morphologiques.....	8
Tableau I.2 : Comparaison entre les modalités comportementales.....	10
Tableau III.1: Classification des modalités biométriques.....	28
Tableau IV.1 : Tableau de résultats de LBP basique.....	42
Tableau IV.2 : Tableau de résultats de LBP _{var}	44
Tableau IV.3: Tableau de résultats de LBP _θ	45
Tableau IV.4: Tableau de résultats de LBP _G	48
Tableau IV.5 : Résultats de fusion biométrique en ensemble ouvert.....	51
Tableau IV.6 : Résultats de fusion biométrique en ensemble fermée.....	51
Tableau IV.7 : Résultats de fusion algorithmique.....	53
Tableau IV.8 : Résultats des différentes variantes de LBP.....	56

Liste des Abréviations

ADN:	Acide Désoxyribose Nucléique
DB:	Data Base
CMC:	Cumulative Match Curve
EER:	Equal Error Rate
FAR:	False Accept Rate
FRR:	False Rejection Rate
LBP:	Local Binary Pattern
LBP_θ:	LBP orienté
LBP_G:	LBP Gradient
LED:	Light Emission Diode
MAX:	la règle maximum
MIN:	la règle minimum
MUL:	la règle multiplication
NG:	Niveau de Gris
NIR:	Near Infra-Red
PLM:	Empreinte palmaire
ROC:	Receiver Operating Characteristic
ROI:	Region Of Interest
ROR:	Rank One Recognition
RPR:	Rank of Perfect Recognition
SUM:	la règle somme
Th:	Threshold
WHT:	Weighted sum rule (la règle somme pondérée)

INTRODUCTION

GENERALE

INTRODUCTION GENERALE

La nécessité d'accès sécurisés automatisés à des environnements physiques ou virtuels est en pleine croissance. Ce besoin requiert des moyens fiables pour vérifier l'identité d'une personne qui se présente au système d'accès. Or les moyens classiques reposant sur des mots de passe ou des cartes magnétiques associées à un code personnel présentent un certain nombre d'inconvénients. Un mot de passe peut être oublié ou volé par un autre individu, ou même cédé à quelqu'un d'autre ; les cartes d'accès peuvent également être perdues ou volées. C'est ainsi que l'exploitation de caractéristiques ou mesures liées à la physiologie même de l'individu est apparue naturellement comme la solution la plus fiable, chacune de ces différentes mesures est appelée "modalité biométrique".

La biométrie est devenue l'une des tâches les plus importantes qui intéressent plusieurs chercheurs en informatique. Dans les applications de contrôle d'accès, la biométrie constitue une solution efficace, simple et surtout pas chère, qui assure de bonnes performances. La biométrie est « la reconnaissance automatique d'une personne en utilisant des traits distinctifs ». Elle regroupe aussi « toutes les caractéristiques ou traits physiologique et comportementale personnels automatiquement mesurables, robustes et distinctives qui peuvent être utilisées pour identifier un individu ou pour vérifier l'identité prétendue d'un individu ». Ces traits sont des caractéristiques universelles et uniques pour chaque personne, par ailleurs, il existe plusieurs traits biométriques à savoir : les empreintes digitales, l'iris, le visage, la rétine, les veines... et bien d'autres que l'on découvre au cours de ce travail. La biométrie regroupe deux axes principaux, en effet elle peut être une identification ou une vérification. Dans une application d'identification, le dispositif biométrique requiert une information biométrique et la compare avec chaque information stockée dans la base de données, c'est une comparaison un à plusieurs (1:N). Alors que pour la vérification ou l'authentification, l'utilisateur annonce son identité par une information biométrique, et le système compare la donnée caractéristique obtenue à partir de l'information entrée, avec la donnée enregistrée correspondante à l'identité prétendue, c'est une comparaison un à un (1:1).

L'inconvénient majeur de certaines techniques biométriques est qu'elles peuvent être reproduites par d'autres personnes, par exemple on peut reproduire les empreintes digitales sur du silicone, cela a conduit à développer d'autres techniques, en effet, le fait d'introduire deux ou plusieurs traits biométriques augmente la performance du système, c'est ce qu'on appelle "La biométrie Multimodale", elle consiste à la multiplication des modalités biométriques, des algorithmes d'analyse ou des bases de données utilisées, elle est de plus en plus utilisée, car elle offre des systèmes de reconnaissance performants et fiables.

INTRODUCTION GENERALE

Dans ce contexte, la modalité biométrique choisie est l'empreinte palmaire à cause de ses caractéristiques textuelles ou nous avons appliqué notre approche proposée "le descripteur de texture LBP orienté" comme étant une méthode d'extraction des caractéristiques.

Nous avons choisi d'articuler notre étude autour de quatre chapitre principaux. Le premier chapitre est consacré à la présentation générale de la biométrie. Il décrit le principe de fonctionnement de système biométrique, puis définit les outils utilisés pour évaluer leur performance.

Le système multi-modale est introduit dans le deuxième chapitre avec ses différentes catégories et leur architecture. Ensuite nous avons expliqué les niveaux de fusion des données. Il existe un grand nombre des méthodes de fusion de scores dont l'opération de normalisation est nécessaire pour rendre tous les scores dans le même intervalle.

Le troisième chapitre présente la méthode LBP orienté d'extraction des caractéristiques textuelles d'empreinte palmaire qui est définie au début de chapitre.

Le quatrième chapitre est dédié aux résultats expérimentaux de notre méthode proposée LBP orienté avec un compte-rendu des résultats obtenu.

Enfin, la conclusion générale résume notre contribution de notre méthode proposée.

CHAPITRE I

SECURITE DE L'INFORMATION ET LA BIOMETRIE

I.1 Introduction

Dans l'environnement quotidien, un individu a besoin de s'identifier dans une multitude de contextes : accéder à un aéroport, entrer dans des endroits militaires, entrer à son lieu de travail, pour retirer de l'argent à un distributeur ou payer en magasin, pour demander un service social...Autant de codes et de mots de passe à mémoriser et à protéger. Afin de développer les moyens de reconnaissance, la recherche connaît depuis quelques années un renouveau spectaculaire et manifeste un intérêt majeur aux données biométriques.

Dans ce chapitre nous allons introduire la notion de la sécurité de l'information, puis exposer la biométrie et leur modalité (techniques biométriques). Ensuite nous allons développer le système biométrique et son fonctionnement et citer quelques exemples d'application.

I.2 Sécurité de l'information

Avec la croissance remarquable des communications, tant en volume qu'en diversité (déplacement physique, transaction financière, accès aux services, etc.), les préoccupations internationales ont fait ressortir ces nécessités en vue de lutter contre les problèmes du vol d'identité, la fraude, le crime et le terrorisme. Nous pouvons définir le vol d'identité comme l'utilisation abusive ou non autorisée d'une information personnelle volée (i.e., mot de passe, carte ID, empreinte digitale, etc.) pour profiter d'un service ou pour le saboter, ou une combinaison de ces types d'abus. Ce qui donne une image claire sur les grandes menaces de ce problème sur plusieurs niveaux.

Les systèmes traditionnels d'authentification personnelle (connaissance et possession) qui font usage des mots de passe ou des cartes d'identité ne sont pas en mesure de répondre à toutes ces exigences. Par exemple, la plupart des gens utilisent des mots de passe basés sur des lettres ou des nombres qu'ils peuvent se rappeler facilement, comme les noms, les dates d'anniversaires et les personnalités connues ou la musique préférée. En effet, cela rend ces mots de passe faciles à deviner en utilisant une attaque à force brute ou une attaque par dictionnaire. En outre, bien qu'il soit conseillé d'utiliser des mots de passe différents pour des applications différentes, la plupart des gens utilisent le même mot de passe sur différentes applications. Si un seul mot de passe est compromis, toutes les applications seront menacées. En pratique, les mots de passe, qui sont aléatoires et longs, sont plus sécurisés, mais ils sont plus difficiles à retenir, ce qui incite certains utilisateurs à les écrire dans des endroits accessibles (par exemple, un fichier texte ou un papier).

Par contre, les systèmes d'authentification basés sur la biométrie qui utilisent des propriétés physiologiques (visage, empreintes digitales, etc.) et comportementales (signature, voix, etc.) ont prouvé une priorité par rapport aux systèmes traditionnels.

Le système biométrique présentent l'avantage, par rapport aux systèmes traditionnels puisque l'information biométrique ne peut pas être perdue, oubliée, ou devinée facilement.[1]

I.3 Méthodes de reconnaissance

Il existe traditionnellement deux manières d'identifier un individu :

- 1) **Méthode basée sur une connaissance (knowledge-based)** : Cette connaissance correspond par exemple au mot de passe qui permet d'activer un téléphone portable.
- 2) **Méthode basée sur une possession (token-based)** : Il peut s'agir d'une pièce d'identité, une clef, un badge,...etc.

Ces deux méthodes d'identification peuvent être utilisés de manière complémentaire afin d'obtenir une sécurité accrue comme pour la carte bleue. Cependant, elles ont leurs faiblesses respectives. Dans le premier cas, le mot de passe peut être oublié par son utilisateur ou bien deviné par une autre personne. On estime ainsi qu'une personne sur quatre écrits directement sur sa carte bleue son code secret afin de ne pas l'oublier. Dans le second cas, le badge (ou la pièce d'identité ou la clef) peut être perdu ou volé.

Les caractéristiques biométriques sont une solution alternative aux deux méthodes d'identification précédente. [2]

I.4 Biométrie

Le terme "**biométrie**" provient des mots grecs, «**bios**» qui veut dire la vie et du mot «**métrique**» qui veut dire mesure. Elle englobe toutes les caractéristiques physiques ou traits personnelles automatiquement mesurable, robuste et distinctives qui peuvent être utilisées pour identifier un individu ou pour vérifier l'identité prétendue d'un individu. [3]

L'individu ne souffre donc pas aux faiblesses des méthodes basées sur une connaissance ou une possession. En effet, un attribut physique ou comportemental ne peut être oublié ou perdu général, ils sont très difficiles à « deviner » ou à « voler » ainsi qu'à « dupliquer ».

Nous décrivons maintenant les propriétés souhaitables d'une caractéristique biométrique. Cette caractéristique doit être:

- Universelle, c'est-à-dire que toutes les personnes de la population à identifier doivent la posséder.
- Facile et quantitativement mesurable.

- Unique, c'est-à-dire que deux personnes ne peuvent posséder exactement la même caractéristique.
- Permanente, ce qui signifie qu'elle ne doit pas varier au cours du temps.
- Performante, c'est-à-dire que l'identification doit être précise et rapide.
- Bien acceptée par les utilisateurs du système. [4]

I.5 Modalités biométriques

Il y a deux catégories technologiques de la biométrie. La première est l'analyse physiologique qui est la plus répandue et qui traite les empreintes digitales, les empreintes palmaires, la forme de la main, les traits du visage, l'ADN...etc. La deuxième est l'analyse comportementale, elle traite la dynamique de la signature, la façon d'utiliser un clavier, la voix ou la manière de marcher.

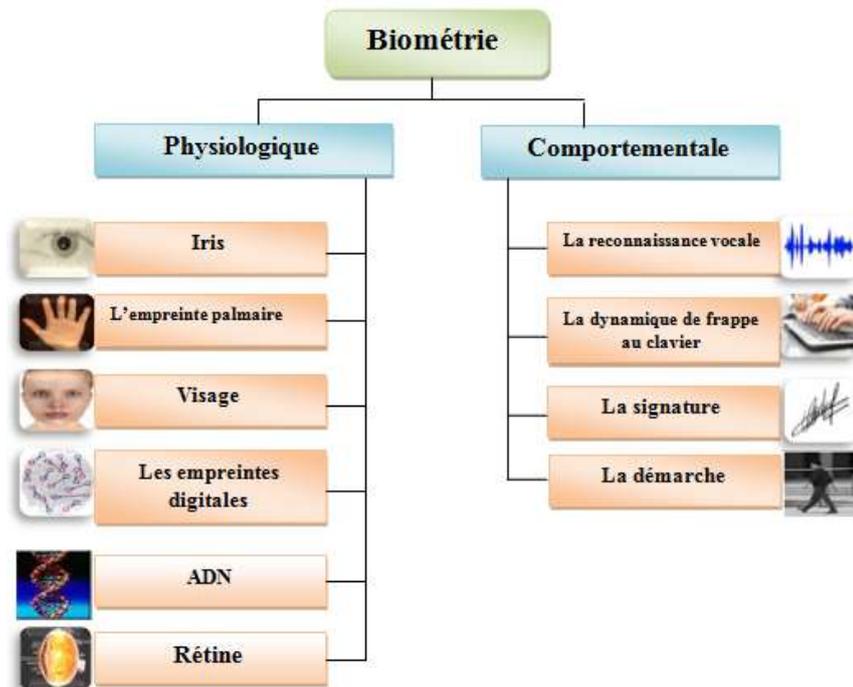


Figure I.1: Catégories technologiques de la biométrie.

I.5.1 Analyse physiologique (morphologique)

Elle est basée sur l'identification de traits physiologique particuliers qui, pour toute personne, sont uniques et permanents. Cette catégorie regroupe l'iris de l'œil, la forme de la main, les empreintes digitales, les traits du visage, etc.

1) **La géométrie de main** : Cette modalité consiste à analyser, la forme de la main sa longueur, sa largeur, son hauteur, la courbure des doigts...etc. Cette technique est récente, simple, et bien acceptée par les utilisateurs qui suivent des guides des capteurs (LEDs

infrarouge, des appareils photos numériques) pour qu'ils bien positionner leurs doigts, ce qui rende ainsi la détection / la segmentation plus aisée, cependant ce genre de système peut être trompé par de vrais jumeau ou même par des personnes ayant des formes de la main proches.[5]

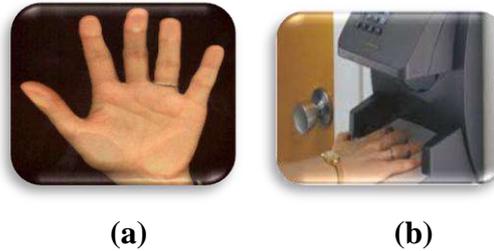


Figure I.2 : a) Image de la géométrie de main ;b) Dispositif de reconnaissance de la géométrie de main.

2) Les empreintes digitales : Les empreintes digitales sont composées de lignes localement parallèles présentant des points singuliers (minutes) et constituent un motif unique, universel et permanent. Pour obtenir une image de l'empreinte d'un doigt, on utilise des capteurs. Les avancées technologiques ont permis d'automatiser la tâche au moyen de capteurs intégrés, remplaçant ainsi l'utilisation classique de l'encre et du papier. [6]

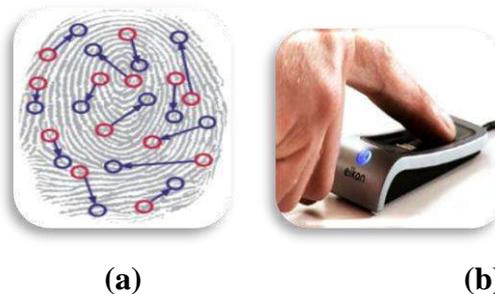


Figure I.3 : a) Image d'une empreinte digitale ;b) Dispositif de reconnaissance d'une empreintes digitales.

3) Visage : Les systèmes actuels de reconnaissance du visage sont composés d'un module d'acquisition d'images avec une caméra. Il procède d'abord à une détection du visage dans l'image acquise. Ensuite, qui va la traiter en utilisant des algorithmes afin d'extraire une signature du visage.

Finalement, cette signature est comparée, à l'aide d'un classificateur, avec les signatures déjà existantes dans une base de données locale, afin d'identifier l'individu.[6]

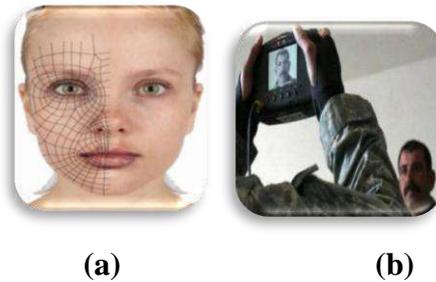


Figure I.4: a) Image du visage ; b) Dispositif de reconnaissance de visage

4) La rétine: Elle se base sur le schéma et le dessin formés par les vaisseaux sanguins de la rétine qui sont uniques pour chaque personne et assez stables tout au long de la vie. Elle est très peu utilisée et mal acceptée par le public et les utilisateurs car il doit placer son œil près de la caméra (quelques centimètres). Elle est utilisée essentiellement dans des environnements de haute sécurité comme l'accès aux sites nucléaires militaires.[3]

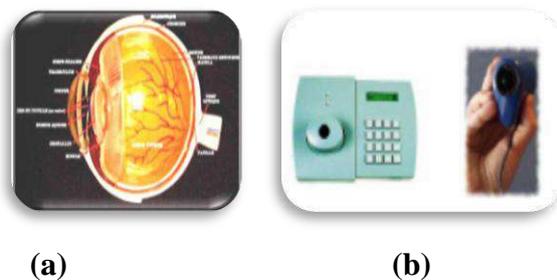


Figure I.5 : a) Image du retine ; b) Dispositif de reconnaissance de retine.

5) Iris : L'iris est la région, sous forme d'anneau, situé entre la pupille et le blanc de l'œil. L'iris a une structure extraordinaire et offre de nombreuses caractéristiques de texture qui sont uniques pour chaque individu. Les algorithmes utilisés dans la reconnaissance de l'iris sont précis que la planète toute entière pourrait être inscrite dans une base de données de l'iris avec peu d'erreurs d'identification.

L'image de l'iris est généralement capturée à l'aide d'une caméra standard. Cependant, cette étape de capture implique une coopération de l'individu. De plus, il existe plusieurs contraintes liées à l'utilisation de cette technologie.[7]



Figure I.6: a) Image d'un Iris;b) Dispositif de reconnaissance de l'Iris.

6) ADN : L'analyse des empreintes génétiques est une méthode d'identification d'individus extrêmement précise, elle est issue directement de l'évolution de la biologie moléculaire. L'information génétique d'un individu est unique, car aucun membre de l'espèce ne possède la même combinaison de gènes codés dans l'acide désoxyribonucléique (ADN).[8]



Figure I.7: Image de l'ADN.

Tableau I.1: Comparaison entre les modalités morphologiques.

	Avantages	Inconvénients
La géométrie de la main	<ul style="list-style-type: none"> • Acceptance par les individus. • Pas d'effet en cas d'humidité ou d'impropriété des doigts. 	<ul style="list-style-type: none"> • Perturbation possible par des blessures. • Système encombrant.
Les empreintes digitales	<ul style="list-style-type: none"> • Facilité d'utilisation et traitement rapide. • La plus éprouvée. 	<ul style="list-style-type: none"> • Possibilité d'attaques. • Sensible en cas d'humidité ou malpropreté des doigts.
Visage	<ul style="list-style-type: none"> • Bien accepté par les usagers. • Elle n'est pas très coûteuse. 	<ul style="list-style-type: none"> • Jumeaux identiques.
Rétine	<ul style="list-style-type: none"> • Fiabilité. • Durabilité. 	<ul style="list-style-type: none"> • Mauvaise acceptation • Coûteuse.
Iris	<ul style="list-style-type: none"> • Contient grande quantité d'information. • Pas de confusion pour les vrais jumeaux. 	<ul style="list-style-type: none"> • Méthode invasive et non conviviale. • Facilement photographié.
ADN	<ul style="list-style-type: none"> • La plus distinctive. 	<ul style="list-style-type: none"> • Analyse trop lente à donner des résultats. • Coût élevé.

I.5.2 Analyse comportementale

Elle se base sur l'analyse de certains comportements d'une personne. Cette catégorie regroupe la reconnaissance vocale, la dynamique de frappe au clavier, la dynamique de la signature, etc.

1) La reconnaissance vocale: La biométrie de la voix traite des données qui proviennent à la fois de facteurs physiologiques dépendants de l'âge, du sexe, de la tonalité, de l'accent et de facteurs comportementaux comme la vitesse et le rythme. Ils ne sont en général pas imitables. C'est la seule technique qui permette à l'heure actuelle de reconnaître une personne à distance et qui est en général bien accepté par les usagers. Cependant cette technique est très facilement falsifiable et nécessite en plus une excellente qualité d'enregistrement. En outre peu de différences existent entre deux voix ce qui rend cette technique peu fiable.[9]



Figure I.8: a) Image de la voix ; b) Dispositif de reconnaissance de la voix.

2) La dynamique de frappe au clavier : Le système est basé sur la dynamique de frappe au clavier, il ne nécessite aucun équipement particulier, chaque ordinateur disposant d'un clavier. Il s'agit d'un dispositif logiciel qui calcule le temps où un doigt effectue une pression sur une touche et le temps où un doigt est dans les airs (entre les frappes). Cette mesure est capturée environ 1000 fois par seconde. La séquence de frappe est prédéterminée sous la forme d'un mot de passe. Initialement l'utilisateur doit composer son mot de passe à quelques reprises afin qu'il soit constitué un gabarit de référence.[8]



Figure I.9: Image d'un clavier.

3) **La signature** : La vérification de la signature analyse la façon dont un utilisateur signe son nom. Les caractéristiques dynamiques de la signature comme la vitesse et la pression sont aussi importantes que la forme géométrique de la signature.[7]



Figure I.10: a) Image de signature ; b) Dispositif de reconnaissance de signature.

4) **La démarche** : Il s'agit de reconnaître un individu par sa façon de marcher et de bouger. En analysant les déformations des jambes et bras au niveau des articulations. La démarche serait en effet étroitement associée à la musculature naturelle donc elle est très personnelle.[3]

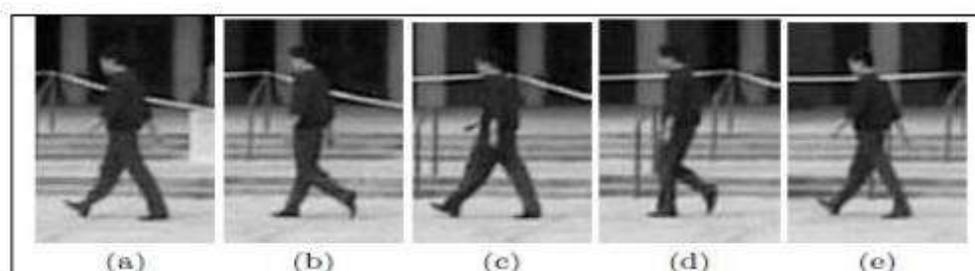


Figure I.11: a) Images d'une démarche.

Tableau I.2 : Comparaison entre les modalités comportementales.

	Avantages	Inconvénients
La reconnaissance vocale	<ul style="list-style-type: none"> • Facilité. 	<ul style="list-style-type: none"> • Sensible à l'état physique et émotionnel de l'individu. • Vulnérabilité aux attaques.
La dynamique de frappe au clavier	<ul style="list-style-type: none"> • Acceptation forte par l'utilisateur. 	<ul style="list-style-type: none"> • Ne sont pas plus pratiques pour autant.
La signature	<ul style="list-style-type: none"> • Acceptation forte par l'utilisateur. 	<ul style="list-style-type: none"> • couteuse. • Dépend de la fiabilité de la signature.
La démarche	<ul style="list-style-type: none"> • Peut être repérée à grande distance à l'aide d'une caméra à faible résolution • Observée ainsi de n'importe quel angle. 	<ul style="list-style-type: none"> • Il est sensible aux changements d'habits, chaussures et surface.

I.6 Architecture d'un système biométrique[10]

Il existe toujours deux phases dans un système biométrique: la phase d'apprentissage et celui de reconnaissance. Pendant l'apprentissage, le système va acquérir une ou plusieurs mesures biométriques qui serviront à construire un modèle de l'individu. Ce modèle de référence servira de point de comparaison lors de la reconnaissance.

Chaque une des phases est composées de plusieurs unités peut être résumé comme suit :

- 1) **Unité de Capteur biométrique** : correspond à la lecture de certaines caractéristiques physiologiques, comportementales d'une personne, au moyen d'un terminal de capture biométrique.
- 2) **Unité d'extraction des données** : extrait les informations pertinentes à partir des données biométriques brutes, par exemple des images de visage ou des régions caractéristiques de visage.
- 3) **Unité création d'une signature** : crée un modèle numérique afin de représenter la donnée biométrique acquise. Ce modèle, appelé aussi signature, sera conservé sur un support portable (puce ou autre) ou dans une base de données.
- 4) **Unité de comparaison** : compare les caractéristiques biométriques d'une personne soumise à contrôle (volontairement ou à son insu) avec les signatures mémorisées. Cette unité fonctionne soit en mode vérification (pour une identité proclamée) ou bien en mode identification (pour une identité recherchée).
- 5) **Unité de base de données** : stocke les modèles biométriques des utilisateurs enrôlés.

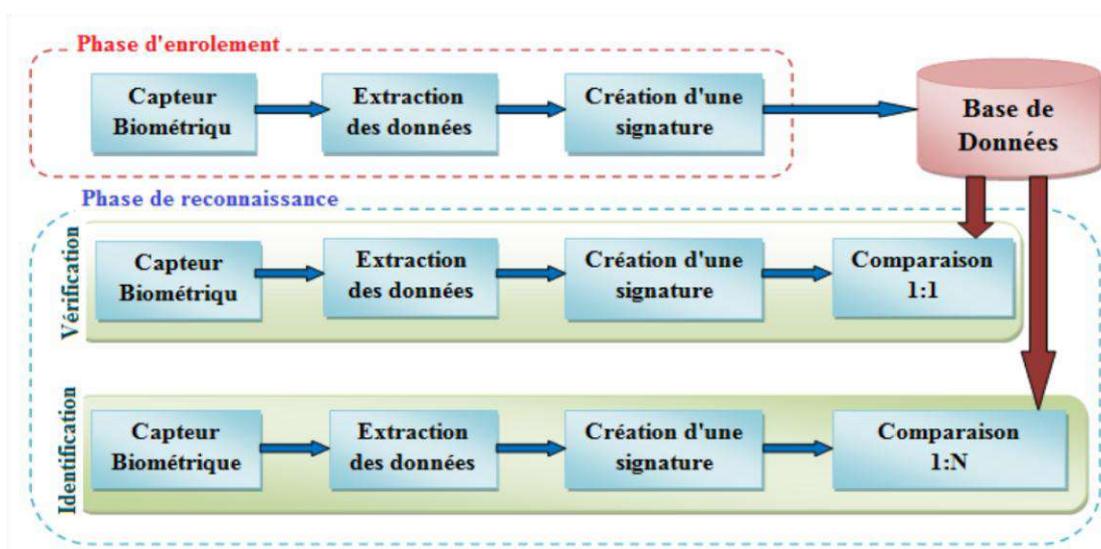


Figure I.12: Architecture d'un système de reconnaissance biométrique.

I.6.1 Fonctionnement d'un système biométrique

Un système biométrique peut fonctionner en phase d' enrôlement ou en phase de reconnaissance (Identification et Vérification).

a) Phase d' enrôlement

L' enrôlement est une phase d' apprentissage. Pendant cette phase, les caractéristiques biométriques des individus sont saisis par un capteur biométrique, puis représentées sous forme numérique (signatures) ou seuls les paramètres pertinents sont extraits, et enfin stockées dans la base de données.[7]



Figure I.13:Phase d' enrôlement.

b) Phase de reconnaissance

Au cours de la reconnaissance, la caractéristique biométrique est mesurée et un ensemble de paramètres est extrait comme lors de l' apprentissage. Le capteur utilisé doit avoir des propriétés aussi proches au celles utilisé durant la phase d' apprentissage et la suite de cette phase sera différente suivant le mode opératoire du système: Identification ou Vérification.[7]

1) Processus d' Identification : En mode d' Identification, le système doit deviner l' identité de la personne à partir d' une comparaison "1 à N", dans lequel, le système compare le signal mesuré avec les différents modèles contenus dans la base de données: accepte si l' utilisateur existe dans la base de données ou refuse s' il n' existe pas. Donc on aura une réponse à une question de type : « Qui suis-je ? ».

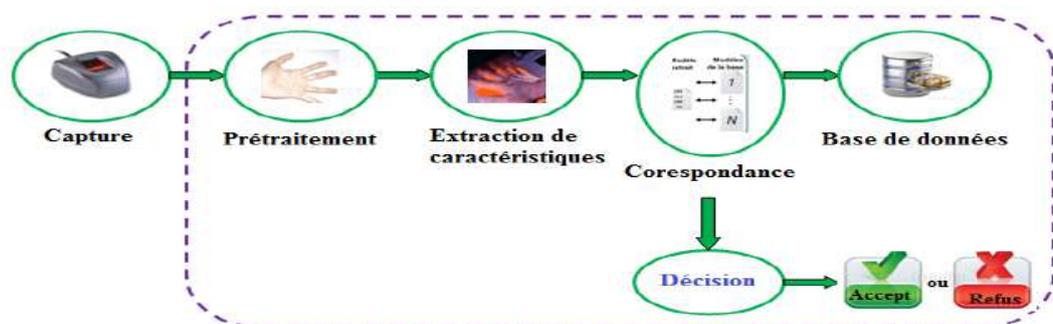


Figure I.14:Processus d' Identification.

2) **Processus de Vérification** : En mode de vérification ou authentification, l'utilisateur propose une identité au système et le système doit vérifier que l'identité de l'individu est bien celle proposée à partir d'une comparaison "1 à 1". Dans un tel mode, le système doit alors répondre par accepter ou refuser à la question suivante: «Suis-je bien la personne que je prétends être? ».

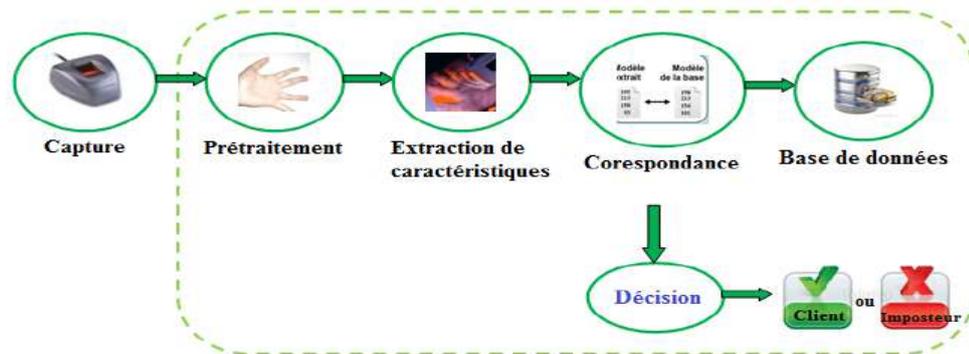


Figure I.15: Processus de Vérification.

I.7 Applications de la biométrie:

Les applications de la biométrie peuvent être divisées selon trois groupes : service public, application de la loi et transaction commerciale et bancaire.

1) **Service public:** La biométrie est fréquemment utilisée dans plusieurs services de type gouvernementale telles que la carte d'identité nationale, le permis de conduire, la sécurité sociale, le contrôle des frontières, le contrôle des passeports, etc..[11]

2) **Application de la loi:** L'identification judiciaire utilise depuis longtemps la biométrie telle que l'identification de corps, la recherche criminelle, l'identification de terroriste...etc.

3) **Transaction commerciale et bancaire:** Les techniques biométriques peuvent être utilisées dans les activités bancaire et commerciale, par exemple, l'apparition de machines de retrait automatique d'argent disposant d'un système de vérification d'individu basé sur l'empreinte palmaire. Ainsi que l'ouverture de réseau informatique, la sécurité de données électroniques, l'e-commerce, l'accès Internet, le contrôle d'accès physique, le téléphone cellulaire, la gestion des registres médicaux, l'étude à distance,... etc.

I.8 Evaluation de performances des systèmes biométriques : [9]

L'évaluation de performance comprend de nombreux aspects, tels que : la précision, l'efficacité, le volume de données stockées pour chaque individu, l'échec à l'acquisition ou à l'enrôlement, le coût des matériels et des logiciels, la facilité d'usage pour les utilisateurs, etc.

Nous nous intéressons dans ce qui suit à la précision, qui est considérée comme étant un point important pour estimer la performance d'un système biométrique. Tout d'abord, nous introduisons les trois critères principaux suivants :

- **FAR** (*False Acceptation Rate*) : représente le pourcentage des personnes déclarées par le système comme clients alors qu'ils sont des imposteurs. Il est égale au nombre de fausse acceptation divisé par le nombre total d'accès imposteurs.

$$FAR = \frac{\text{Nombre des imposteurs acceptés}}{\text{Nombre total d'accès d'imposteurs}} \quad (I.1)$$

- **FRR** (*False Reject Rate*) : représente le pourcentage des personnes censées être clients mais ils sont rejetés par le système. C'est le ratio entre le nombre de faux rejets et le nombre de tests des personnes légitimes.

$$FRR = \frac{\text{Nombre des clients rejetés (FR)}}{\text{Nombre total d'accès de clients}} \quad (I.2)$$

- **EER** (*Equal Error Rate*), c'est le taux d'erreurs égales un compromis entre les fausses acceptations et les faux rejets, autrement dit c'est le point de mesure sur lequel FAR = FRR.

$$EER = \frac{\text{Nombre de fausse acceptations} + \text{nombre de faux rejets}}{\text{Nombre total d'accès}} \quad (I.3)$$

Dans le cas d'un système utilisé en processus identification, les applications peuvent être déployées en monde fermé ou en monde ouvert qu'on a mentionné précédemment :

a) En monde fermé : le taux d'identification est la mesure la plus 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 premières réponse. On trace alors ce que l'on appelle une courbe de scores cumulés CMC. La courbe (CMC)(voir figure I.16) donne le pourcentage de personnes reconnues en fonction d'une variable que l'on appelle le rang. [9]

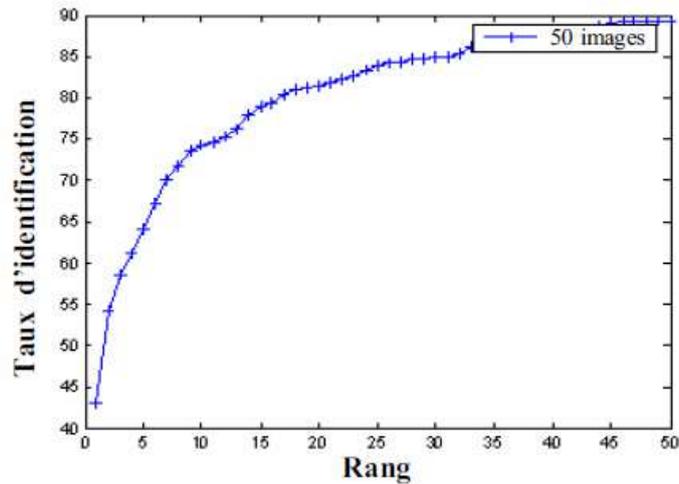


Figure I.16: La courbe CMC.

b) **En monde ouvert** : lorsque on mesure les performances d'un système biométrique, on utilise ce qu'on appelle une courbe ROC ("Receiver Operating Characteristic"). La courbe ROC (voir figure I.17) trace le taux de faux rejet en fonction du taux de fausse acceptation. Plus cette courbe tend à épouser la forme du repère, plus le système est performant, c'est-à-dire possédant un taux de reconnaissance global élevé. [9]

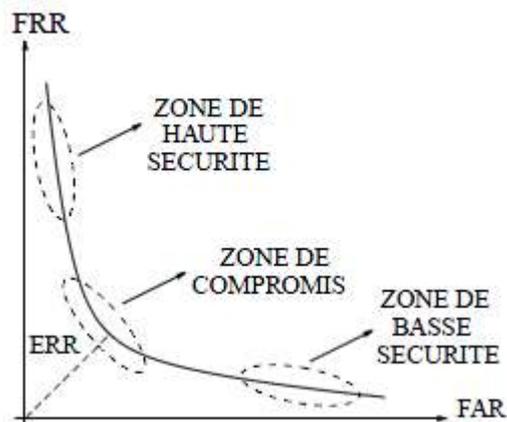


Figure I.17: La courbe ROC

Conclusion

Dans ce chapitre nous avons référé à la nécessité de la biométrie pour assurer la sécurité d'identité des individus. Ensuite nous avons présenté la biométrie, ses diverses technologies et les principaux modules des systèmes biométriques.

Enfin nous avons cité leurs différentes applications et aussi donné un aperçu sur les techniques de mesure de leurs performances.

CHAPITRE II

BIOMETRIE MULTIMODALE ET FUSION D'INFORMATION

II.1 Introduction

Le système biométrique optimal et robuste doit impérativement avoir les propriétés d'universalité, d'acceptabilité, d'unicité, de collectabilité et de sécurité. Mais comme il n'existe pas de modalités qui puissent avoir toutes ces propriétés, la solution est d'utiliser plusieurs caractéristiques biométriques dans un unique système pour améliorer ses performances.

Dans ce chapitre, nous allons traiter la multi-biométrie et ses diverses catégories, ensuite présenter les niveaux de fusion d'information. Enfin nous avons expliqué le principe de fusion de score et ses approches et la normalisation des scores.

II.2 Limitation de système biométrique uni-modal[5]

Bien qu'il existe un grand nombre des techniques de reconnaissance biométrique uni-modales (utilisant une seule modalité) améliorées, cependant celles-ci souffrent de plusieurs facteurs qui dégradent leurs performances tels que :

- **Le bruit:** introduit par le capteur défaillant ou mal entretenu (exemple l'accumulation de poussière sur le capteur d'empreinte digitale), il peut sérieusement compromettre la précision du système.
- **Non-universalité :** C'est le cas où des personnes peuvent avoir des empreintes non enregistrables à cause d'un accident ou d'un travail manuel prolongé.
- **Manque d'individualité :** nous pouvons avoir une similarité des caractéristiques extraites de deux personnes différentes cela dû à des facteurs génétiques (exemple les jumeaux, les membres de la même famille, ou même les membres de la même population), ce qui affecte significativement la performance de système biométrique en augmentant le taux de fausse acceptation.
- **Manque de représentation invariante :** C'est les variations à l'intérieur d'une même modalité biométrique, par exemple nous pouvons avoir deux signatures différentes correspond à la même personne.
- **Sensibilité aux attaques :** le problème de la fraude et du vol semble s'éliminer par les méthodes biométriques, cependant on ne fait que les réduire. Des études ont montré qu'il est possible de voler une empreinte digitale et de la produire (en utilisant par exemple la silicone), c'est le cas des modalités signature et voix qui sont faciles à falsifier.

II.3 Système biométrique multimodal

La multi-modalité est l'utilisation de plusieurs modalités biométriques. La combinaison de plusieurs modalités à pour objectif de diminuer les limitations des systèmes uni-modaux. De plus, le fait d'utiliser plusieurs modalités biométriques réduit le risque d'impossibilité d'enregistrement ainsi que la robustesse aux fraudes. [12]

Il existe des facteurs qui impactent sur la structure d'un système biométrique multimodal : [13]

- Les avantages liés au coût : on doit mettre un compromis entre le coût supplémentaire et l'amélioration de la performance du système.
- La détermination des sources d'information biométrique.
- L'acquisition et la séquence de traitement.
- Le type d'information : (caractéristiques, scores de correspondance, décision, etc.).
- La méthode de fusion: la méthode de combiner les informations présentées par de multiples sources biométriques.

II.3.1 Catégories de la multi-modalité

La multi-biométrie au sens large se réfère à cinq scénarios différents (**figure II.1**) qui sont :

- 1) **Systèmes multi-instances** : il s'agit d'utiliser un seul capteur pour extraire des instances du même caractère biométrique, afin d'obtenir plusieurs variations de ce trait en enrichissant le modèle biométrique de l'individu. Par exemple l'acquisition de plusieurs images de visage en changeant la pose, l'expression, et/ou l'illumination. [5]
- 2) **Systèmes multi-capteurs** : Dans ce système nous utilisons plusieurs capteurs pour acquérir la même modalité, afin d'extraire plusieurs informations de même trait biométrique. Exemple la capture de la texture 2D, de la surface 3D, ainsi que l'image infrarouge de visage de l'individu avec différents gamme de capteurs. [5]
- 3) **Systèmes multi-algorithmes** : Dans ces systèmes, plusieurs algorithmes d'extractions de caractéristiques et/ou plusieurs algorithmes de calcul de similarité sont utilisés sur la même modalité biométrique. Par exemple, des algorithmes d'analyse de texture et de minuties peuvent être associés pour traiter la même image d'empreinte palmaire afin d'extraire diverses caractéristiques qui peuvent améliorer la performance du système. [5]
- 4) **Systèmes multi-échantillons** : Un seul capteur peut être utilisé pour acquérir plusieurs échantillons du même trait biométrique dans le but de prendre en compte les

variations qui peuvent se produire au sein de ce trait, ou pour obtenir une représentation plus complète du caractère sous-jacent.[5]

- 5) **Systèmes multi-biométries** : Dans ce cas, plusieurs modalités biométriques sont combinées afin d'établir l'identité d'un individu. Le nombre de traits biométriques utilisés dans une application spécifique est également limité par des considérations pratiques, telles que le cout de déploiement, le temps d'enrôlement, le temps de retour ou encore le taux d'erreur attendu.[5]

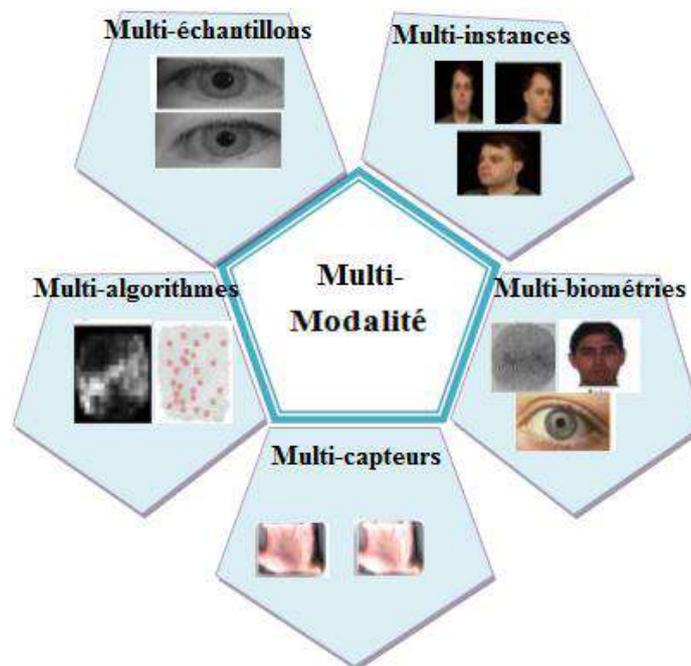


Figure II.1: Catégories de la multi-modalité.

II.3.2 Architecture de système multimodal [6]

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

- 1) **Architecture en parallèle** : C'est la plus utilisée car elle permet d'utiliser toutes les informations disponibles et donc d'améliorer les performances du système. En revanche, l'acquisition et le traitement d'un grand nombre de données biométriques sont coûteux en temps et en matériel, et réduisent le confort d'utilisation (voir **figure II.2**). [8]

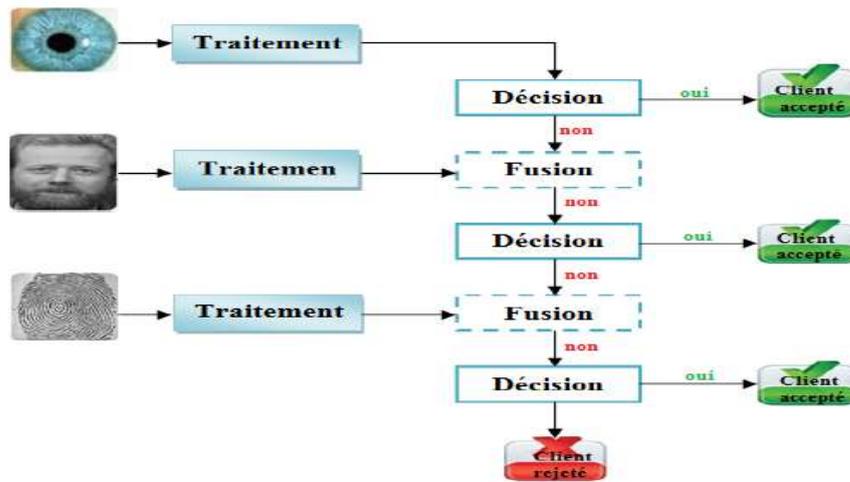


Figure II.2: Architecture d'un système multimodal en parallèle.

- 2) **L'architecture en série :** Elle peut être privilégiée dans certaines applications ; par exemple si la multi-modalité est utilisée pour donner une alternative pour les personnes ne pouvant pas utiliser l'empreinte digitale (voir figure II.3). [8]

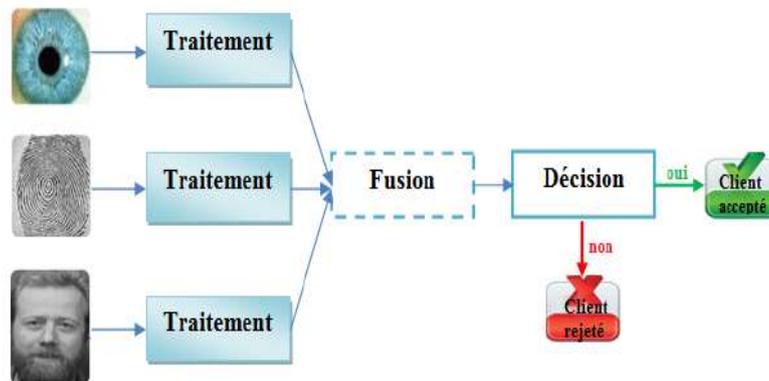


Figure II.3 : Architecture d'un système multi-modal en série.

II.4 Fusion multimodale

La fusion biométrique multimodale combine des mesures de différents traits biométriques pour renforcer les points forts et réduire les points faibles des différents processus biométriques fusionnés. Ainsi, la fusion des informations biométriques peut se faire dans différents niveaux : niveau capteur, niveau caractéristiques, niveau score ou niveau décision (Figure II.4).

CHAPITRE II BIOMETRIE MULTIMODALE ET FUSION D'INFORMATION

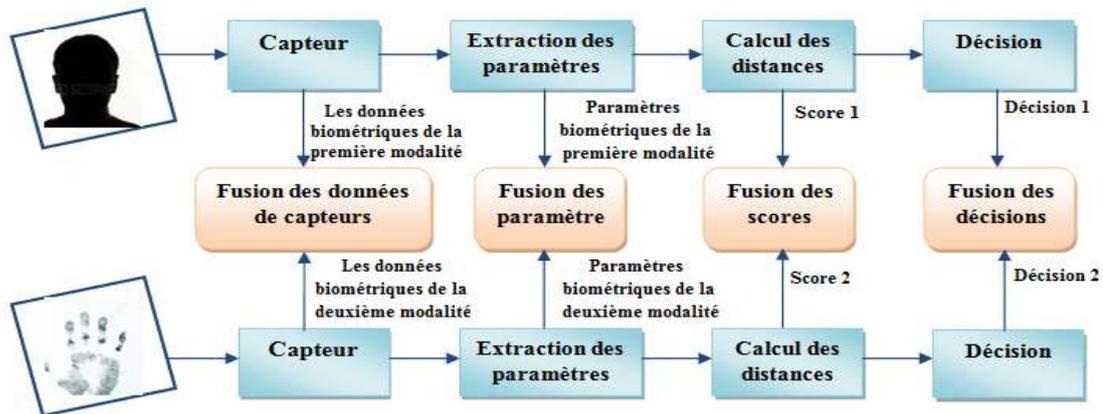


Figure II.4: Différents niveaux de fusion biométrique.

II.4.1 Niveaux de fusion

La fusion des informations biométriques peut se diviser en deux classifications: Fusion pré-classification et Fusion post-classification.

a) Fusion Pré-classification

La fusion pré-classification correspond à la fusion des informations issues de plusieurs données biométriques au niveau du capteur (images brutes) ou au niveau des caractéristiques extraites par le module d'extraction de caractéristiques.

- **Niveau capteur**

Ce type de fusion peut se faire uniquement si les diverses captures sont des instances du même trait biométrique obtenu à partir de plusieurs capteurs compatibles entre eux ou plusieurs instances du même trait biométrique obtenu à partir d'un seul capteur. Un exemple du niveau de fusion de capteurs consiste à détecter un signal de parole simultanément avec deux différents microphones.[14]

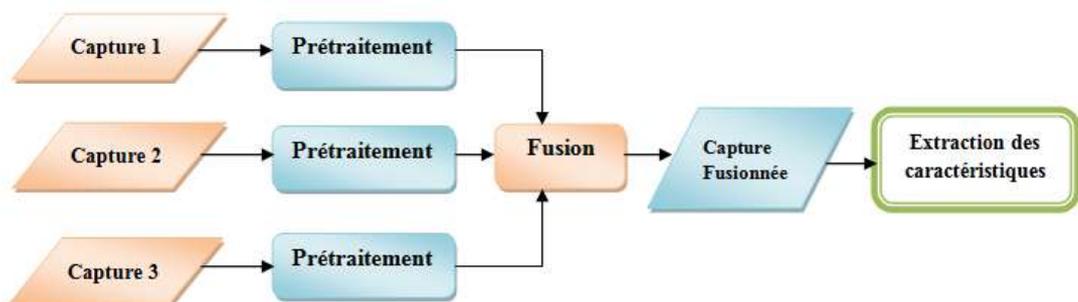


Figure II.5: Schéma de fusion au niveau du capteur.

- **Niveau des caractéristiques[15]**

La fusion au niveau caractéristiques consiste à combiner différents vecteurs de caractéristiques qui sont obtenus à partir d'une des sources suivantes : plusieurs capteurs du

CHAPITRE II BIOMETRIE MULTIMODALE ET FUSION D'INFORMATION

même trait biométrique, plusieurs algorithmes du même trait biométrique, ou encore plusieurs traits biométriques. Quand les vecteurs de caractéristiques sont homogènes (par exemple, plusieurs images d'empreinte palmaires d'un utilisateur), un unique vecteur de caractéristiques résultant peut être calculé comme une somme pondérée des vecteurs de caractéristiques individuels. Lorsque les vecteurs de caractéristiques sont hétérogènes (par exemple, des vecteurs de caractéristiques de différentes modalités biométriques comme le visage et la géométrie de la main), nous pouvons les concaténer pour former un seul vecteur de caractéristiques.

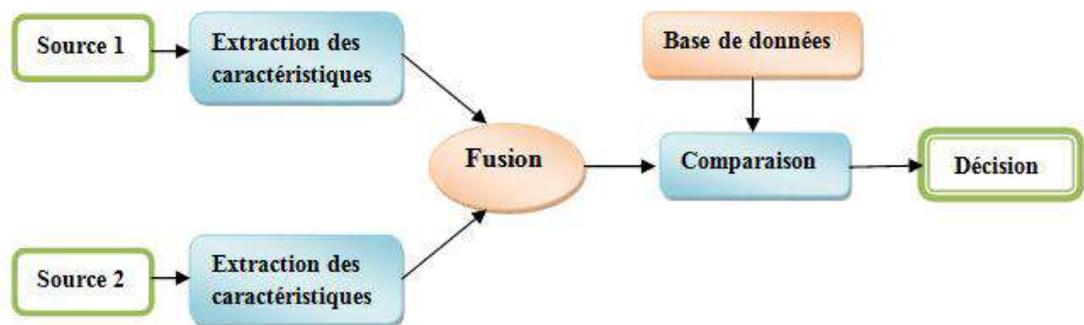


Figure II.6: Schéma de fusion au niveau de l'extraction des caractéristiques.

b) Post-classification

La fusion post-classification est très étudiée par les chercheurs. Cette fusion peut se faire au niveau des scores issus des modules de comparaison ou au niveau des décisions.

- **Niveau de décision**

Chaque modalité est d'abord identifiée de façon indépendante, puis la décision finale est prise en se basant sur la fusion des décisions des différents processus biométriques. Les résultats finaux de plusieurs classificateurs sont consolidés par des techniques comme celle de la majorité de votes. La fusion au niveau décision est considérée comme rigide en raison de la disponibilité des informations limitées.[14]

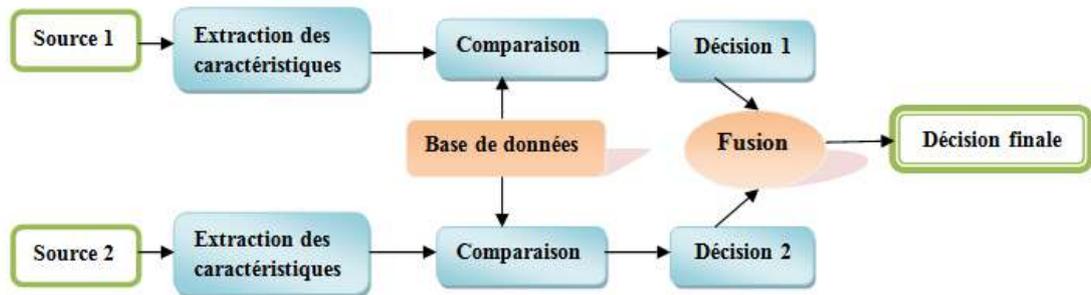


Figure II.7: Schéma de fusion au niveau de la décision.

- **Niveau des scores**

Les différents sous-systèmes du système multi-biométrique produisent des scores après l'étape de la comparaison. Après les vecteurs de caractéristiques, les scores d'appariement contiennent l'information la plus riche à propos du modèle biométrique. Par conséquent, la fusion au niveau score donne le meilleur compromis entre la richesse d'information et la facilité d'implémentation(voir figure II.8).[16]

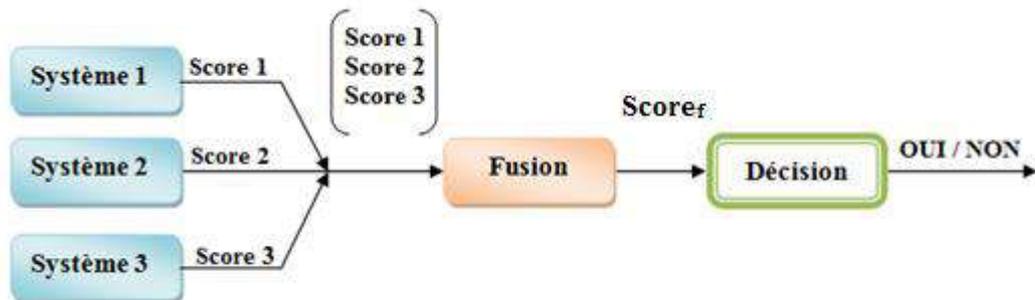


Figure II.8: Schéma de fusion au niveau de scores.

II.5 Fusion au niveau des scores

II.5.1 Approche de combinaison des scores[14]

Dans les méthodes de combinaison, les scores sont traités séparément avant de les combiner pour construire un unique score qui sert à prendre une décision finale. Cependant, les scores provenant de différents classifieurs doivent être cohérents entre eux, pour cela, une étape de normalisation qui transforme les scores dans un domaine commun est nécessaire avant de les combiner.

Les méthodes de combinaisons de scores simples 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, La somme pondérée ou la médiane.

- Combiner les scores par la moyenne consiste à calculer S tel que :

$$S = \frac{1}{N} \sum_{i=1}^N S_i \quad (\text{II.1})$$

- Combiner les scores par le produit consiste à calculer S tel que :

$$S = \prod_{i=1}^N S_i \quad (\text{II.2})$$

- Combiner les scores par le minimum consiste à calculer S tel que :

$$S = \min (s_i) \quad (\text{II.3})$$

- Combiner les scores par le maximum consiste à calculer s tel que :

$$S = \max (s_i) \quad (\text{II.4})$$

- Combiner les scores par la médiane consiste à calculer S tel que :

$$S = \text{med} (s_i) \quad (\text{II.5})$$

- La somme pondérée est une méthode un peu plus évoluée qui nécessite une adaptation par le réglage de paramètres. Elle consiste à calculer S tel que :

$$S = \sum_{i=1}^N W_i S_i \quad (\text{II.6})$$

II.5.2 Approche de classification des scores

Dans les méthodes de classification de scores, on construit un vecteur de caractéristiques en utilisant les scores de correspondance en sorties de chaque classifieur, puis on l'affecte à l'une des deux classe : client ou imposteur. Le classifieur adopté, afin de réaliser ce processus, est apte à prendre la décision sans tenir compte de la manière dont le vecteur de caractéristiques a été créé, autrement dit ; les scores en sortie de différents sous-systèmes peuvent être non homogènes, et ils n'exigent aucun traitement avant de les envoyer dans le classifieur.[14]

II.6 Normalisation des scores[14]

Les méthodes de normalisation de scores ont pour objectif de transformer individuellement chacun des scores issus des systèmes pour les rendre homogènes avant de les combiner. Certains systèmes produisent des scores de similarité (plus le score est grand, plus la référence ressemble au test, donc l'utilisateur est un Client), d'autres produisent des distances (plus la distance est faible, plus la référence et le test sont proches, plus l'utilisateur est un Client).

Les différentes techniques de normalisation de scores sont :

1) Normalisation par la méthode Min-Max

Cette méthode n'est pas robuste (insensible aux valeurs aberrantes). La normalisation Min-Max conserve la distribution de scores originale à un facteur d'échelle près et transforme tous les scores dans l'intervalle [0,1].

CHAPITRE IIBIOMETRIE MULTIMODALE ET FUSION D'INFORMATION

Le score normalisé Min-Max pour le score de test s_{ik} est donné par :

$$S'_{ik} = \frac{s_{ik} - \min(\{s_i\})}{\max(\{s_i\}) - \min(\{s_i\})} \quad (II.7)$$

S_{ik} le $k^{\text{ème}}$ score de sortie du $i^{\text{ème}}$ système, où $i = 1, 2, \dots, N$ et $k = 1, 2, \dots, M$.

2) Normalisation par la méthode Z –Score

Cette méthode n'est pas robuste. De plus, la normalisation Z-Score ne garantit pas un intervalle commun pour les scores normalisés provenant de différents systèmes. Pour une distribution arbitraire, la moyenne et l'écart-type sont respectivement des estimateurs raisonnables de position et d'échelle, mais ne sont pas optimaux.

$$S'_{ik} = \frac{s_{ik} - \mu}{\sigma} \quad (II.8)$$

Où μ est la moyenne arithmétique et σ l'écart -type des données.

3) Normalisation par la médiane et l'écart absolu médian (MAD)

C'est une méthode robuste. Cependant, les estimateurs issus de la médiane et de la MAD ont une faible efficacité comparée aux estimateurs issus de la moyenne et de l'écart -type, c'est-à-dire que lorsque la distribution de score n'est pas gaussienne, la médiane et la MAD sont de pauvres estimateurs des paramètres de position et d'échelle. Ainsi, cette technique de normalisation ne conserve pas la distribution d'entrée et ne transforme pas les scores dans un intervalle commun.

$$S'_{ik} = \frac{s_{ik} - \text{median}}{\text{MAD}} \quad (II.9)$$

$$\text{MAD} = \text{median} (\{|S_i - \text{median} (\{S_i\})|\}) \quad (II.10)$$

4) Normalisation Par une fonction Quadratique-Linéaire-Quadratique (QLQ)

Snelick Et al. utilisent une fonction Quadratique-Linéaire-Quadratique (QLQ) pour normaliser des scores au préalable transformés dans l'intervalle [0,1] (S_{MM}) grâce à une normalisation Min Max (S_{MM}). Cette normalisation QLQ prend comme paramètres le centre c et la largeur w de la zone de recouvrement des distributions des scores Imposteurs et Client.

$$S_{QLQ} \begin{cases} \frac{1}{c - \frac{w}{2}} S_{MM}^2, & \text{si } S_{MM} \leq \left(c - \frac{w}{2}\right) \\ S_{MM}, & \text{si } \left(c - \frac{w}{2}\right) < S_{MM} \leq \left(c + \frac{w}{2}\right) \\ \left(c + \frac{w}{2}\right) + \sqrt{\left(1 - c - \frac{w}{2}\right) \left(S_{MM} - c - \frac{w}{2}\right)}, & \text{sinon} \end{cases} \quad (II.11)$$

5) Normalisation Par la méthode tangente hyperbolique "Tanh"

Les scores normalisés sont donnés par :

$$s'_{ik} = \frac{1}{2} \left\{ \tanh \left(0.001 \frac{s_{ik} - \mu}{\sigma} \right) + 1 \right\} \quad (\text{II.12})$$

Où μ est la moyenne arithmétique, σ l'écart - type des données et \tanh la tangente hyperbolique. La méthode tangente hyperbolique met chaque score normalisé dans l'intervalle [0, 1].

6) Normalisation par une fonction double sigmoïde

Cappelli et al. [308] ont utilisé une fonction double sigmoïde pour la normalisation de score dans un système biométrique multimodal qui combine différents systèmes d'empreinte digitale. Le score normalisé est donné par :

$$s'_{ik} = \begin{cases} \frac{1}{1 + \exp\left(-2\left(\frac{s_{ik} - t}{r_1}\right)\right)} & , \text{si } s_{ik} < t, \\ \frac{1}{1 + \exp\left(-2\left(\frac{s_{ik} - t}{r_2}\right)\right)} & , \text{sinon} \end{cases} \quad (\text{II.13})$$

II.7 Conclusion

Dans ce chapitre nous avons abordé la multi-biométrie qui fournit une alternative au système biométrique uni-modale afin d'améliorer sa performance. Ensuite nous avons déterminé les différentes formes de multi-biométrie, ainsi que l'architecture qui peuvent être utilisées. Enfin nous avons étudié la fusion des données avec ses divers niveaux.

CHAPITRE III

EXTRACTION DES

CARACTERISTIQUES

D'EMPREINTE PALMAIRE EN

UTILISANT LBP_θ

CHAPITRE III : EXTRACTION DES CARACTERISTIQUES D'EMPREINTE PALMAIRE EN UTILISANT LBP_θ

III.1 Introduction

L'identification des individus par leurs empreintes palmaires (Palprints) considérée comme nouveau membre de la famille des modalités biométriques, est devenue un domaine de recherche très actif durant ces dernières années. Les travaux réalisés, jusqu'à présent, sur la reconnaissance des individus par leurs l'empreinte palmaire se sont basés sur le prétraitement et l'extraction des caractéristiques principales des images d'empreinte palmaire dont nous avons présentés dans ce chapitre avec leur processus de reconnaissance.

Ce chapitre, est basé sur l'extraction des caractéristiques d'empreinte palmaire en utilisant la méthode LBP (Motifs binaires locaux) qui est devenue très populaire dans la reconnaissance des textures qu'on va mieux expliquer dans ce qui suit.

III.2 Choix d'empreinte palmaire

L'identification en employant des caractéristiques de l'empreinte palmaire est une biométrie fréquemment utilisable. Les empreintes palmaires contiennent plus d'information que les autres modalités, ainsi elles sont plus discriminantes. Elles contiennent des caractéristiques distinctives additionnelles qui peuvent être extraites à partir des images à basse résolution.

Dans le tableau suivant nous avons classifié les différentes modalités selon le coût d'utilisation et leur sensibilité à l'état physique et émotionnel des individus.[18]

1^{ère} classe : ADN, Iris et Rétine.

2^{ème} classe : Visage, Voix, Signature, Démarche, Frappe au clavier.

3^{ème} classe : Modalités liées à la main.

Tableau III.1: Classification des modalités biométriques.

	1 ^{ère} CLASSE	2 ^{ème} CLASSE	3 ^{ème} CLASSE
Acceptabilité	↓↓	↑↑	↑↑
Permanence	↑↑	↓↓	↑↑
Taux d'indentification	↑↑	↓	↑

A partir de tableau suivant, nous avons conclue que les modalités liées à la main sont les plus réponsus à notre exigence : permanent, très bien accepté par les individus avec un taux d'erreur acceptable.

CHAPITRE III : EXTRACTION DES CARACTERISTIQUES D'EMPREINTE PALMAIRE EN UTILISANT LBP₀

III.3 Empreinte palmaire

On appelle paume de la main la partie intérieure de la main du poignet aux racines des doigts, elle peut être définie comme étant le modèle de la paume de la main illustrant les caractéristiques physiques du motif de sa peau tel que les lignes (principales et rides), points, minutie et texture.[3]

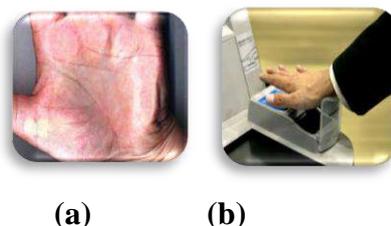


Figure III.1:a) Image du empreinte palmaire ; b) Dispositif de reconnaissance de L'empreinte palmaire.

III.3.1 Avantages de l'empreinte palmaire [18]

- Les empreintes palmaires contiennent plus d'information que les empreintes digitales.
- Elles sont plus discriminantes.
- les sources de capture d'empreintes palmaires sont beaucoup moins chères que celles de capture des iris.
- Les empreintes palmaires contiennent des caractéristiques distinctives additionnelles telles que les lignes principales et les ridules.
- En combinant toutes les caractéristiques d'une paume, il est possible d'établir un système robuste de biométrie.

III.3.2 Les caractéristiques biométriques d'une empreinte palmaire et les types de reconnaissance [3]

L'empreinte palmaire présente différents types de caractéristiques qui peuvent être exploitées dans la reconnaissance des individus.

a) Des caractéristiques géométriques

Comme toute image, l'empreinte palmaire présente des caractéristiques géométriques telles que : la longueur, la largeur, et la surface. Ces caractéristiques ne sont pas distinctives mais peuvent tout de même être utiles pour une première vérification.

b) Les lignes principales (Plis de flexion)

L'empreinte palmaire est caractérisée par trois plis de flexion, dites lignes principales : la ligne de tête, la ligne de vie et celle du cœur. La Figure III.2 montre les différents plis de la paume.

CHAPITRE III : EXTRACTION DES CARACTERISTIQUES D'EMPREINTE PALMAIRE EN UTILISANT LBP_θ

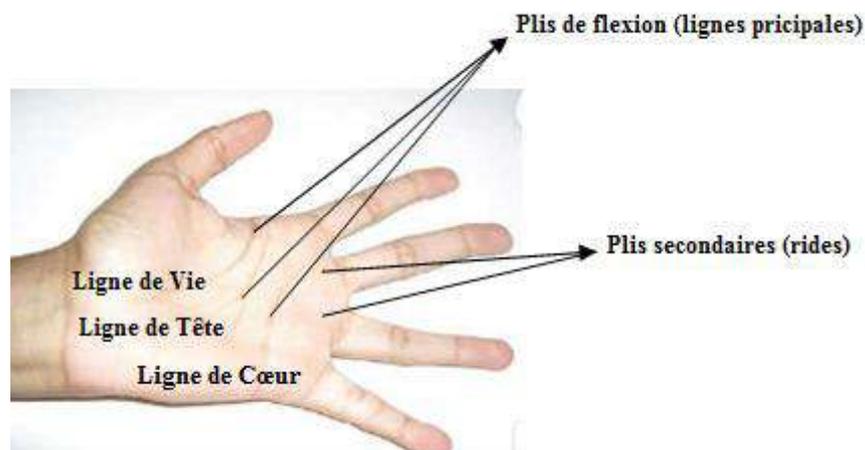


Figure III.2: La paume de main et ses plis.

Ces plis ne varient que peu à travers le temps. Ils sont faciles à extraire par des algorithmes de détection de contour. Leur positionnement et leur forme sont importants pour la reconnaissance. Mais ils sont génétiquement liés (2 jumeaux ont la même forme de plis de flexion) et restent peu distinctifs. Ainsi, seuls, ils ne peuvent pas fournir une information suffisante pour une reconnaissance efficace (**Figure III.3**).

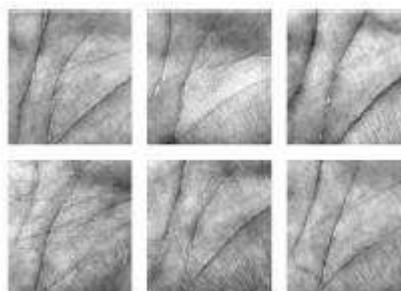


Figure III.3: Empreintes différentes avec des lignes principales similaires.

c) Les rides (Plis secondaires)

L'empreinte palmaire contient de nombreux autres plis qui diffèrent de ceux de flexion du fait qu'ils sont plus minces et plus irréguliers. Certains d'entre eux sont congénitaux, d'autres sont dus aux activités musculaires. Les lignes principales et les rides peuvent être observées facilement sur les images capturées à basse résolution. Comme les lignes principales seules ne fournissent pas une information distinctive suffisante, les rides jouent un rôle important dans la reconnaissance palmaire. Combinées aux lignes principales, elles fournissent une information distinctive pour la reconnaissance.

CHAPITRE III : EXTRACTION DES CARACTERISTIQUES D'EMPREINTE PALMAIRE EN UTILISANT LBP₀

d) Les points de référence (Datum points)

Les points représentant les deux extrémités de la paume de la main sont appelés point de références. Ce sont les points a et b dans la **Figure III.4**



Figure III.4: Points de référence de l'empreinte palmaire (a et b).

Ils servent de points de repère lors de l'alignement et l'extraction des caractéristiques de l'empreinte palmaire. La taille de cette dernière peut être aussi estimée grâce à ces deux points.

e) Les crêtes papillaires

Les crêtes papillaires sont des épaissements permanents de l'épiderme (la couche cellulaire extérieure de la peau). Elles se trouvent sur la face antérieure de la main (paume et doigts) ainsi que sur la plante du pied. Ce sont des surfaces représentant les zones principales de préhension et d'appui, simulant les bandes de roulement sur un pneu d'automobile. Elles sont élevées au-dessus du niveau général de la peau dans des formes parallèles droites ou en séries de courbes. Ces crêtes permettent de distinguer différents types de points pouvant être considérés comme caractéristiques palmaires :

- Les minuties
- Les points singuliers

Comme le montre la **Figure III.5**, selon la résolution utilisée dans l'acquisition de l'empreinte, une ou plusieurs de ces caractéristiques peuvent être observées et par conséquent exploitées dans la reconnaissance palmaires des individus. Cela a permis de classifier les approches de reconnaissance en deux grandes catégories principales : approches haute résolution et approches basse résolution.

CHAPITRE III : EXTRACTION DES CARACTERISTIQUES D'EMPREINTE PALMAIRE EN UTILISANT LBP_θ

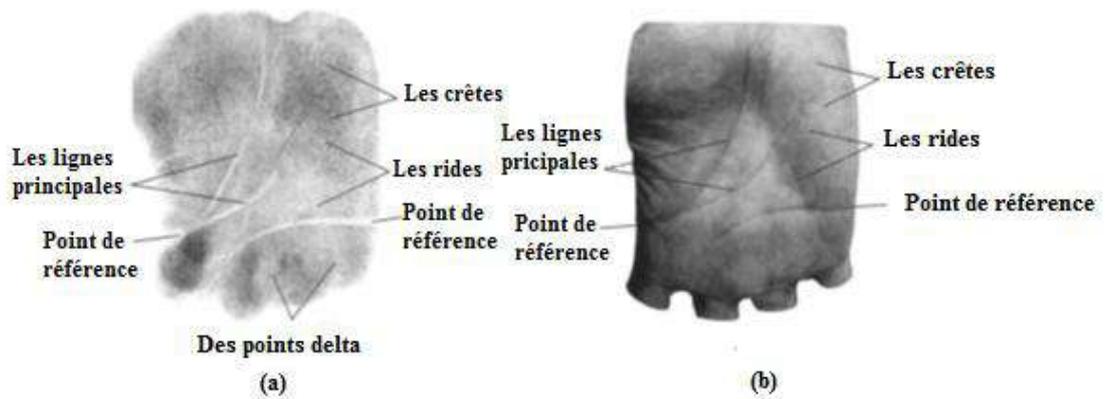


Figure III.5: Caractéristiques d'une empreinte palmaire : a) Image basse résolution, b) Image haute résolution.

D'après les caractéristiques citées au-dessus, Il est difficile d'obtenir un bon taux de reconnaissance en utilisant seulement les lignes principales à cause de leur ressemblance parmi différents individus. Donc La représentation en textures pour la classification des images d'empreinte palmaire à basse résolution a fourni une approche efficace par rapport aux autres caractéristiques. L'une des solutions pour résoudre ce problème est d'extraire les caractéristiques de texture des images des empreintes palmaires à basse résolution en utilisant la méthode des motifs binaires locaux (LBP).

III.4 Système proposé

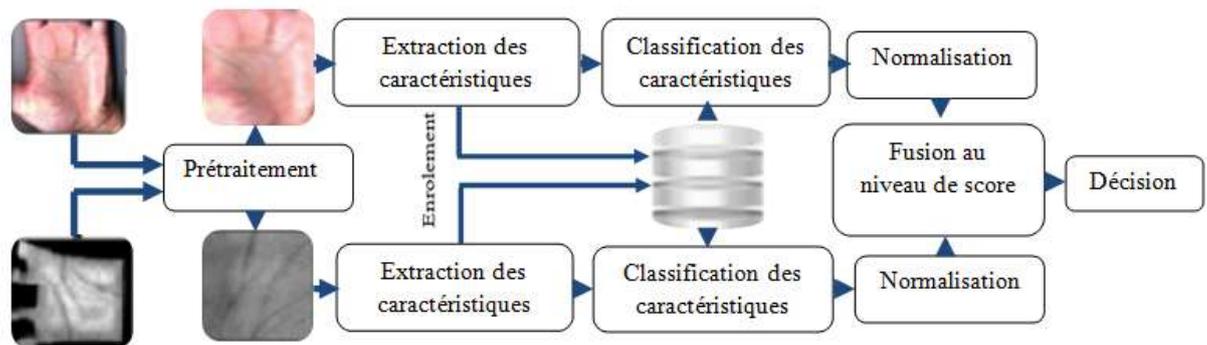


Figure III.6 : Description de système.

Le schéma fonctionnel du système d'identification proposé, présenté à la **Figure III.6**, est composé de deux sous-systèmes qui échangent des informations au niveau de score correspondant. Chaque sous-système exploite différentes techniques d'extraction des caractéristiques. Il y a deux phases dans chaque sous-système: les phases d'enrôlement et de reconnaissance. Les deux phases, pour les deux sous-systèmes, comprennent deux sous-modules: prétraitement pour la région d'intérêt (ROI) localisation et extraction des

CHAPITRE III : EXTRACTION DES CARACTERISTIQUES D'EMPREINTE PALMAIRE EN UTILISANT LBP_θ

caractéristiques pour extraire les caractéristiques biométriques discriminantes. Cependant, la phase d'identification se compose de sous-modules supplémentaires: correspondance, normalisation et fusion, pour calculer la similitude, normaliser les distances obtenues et fusionner les deux scores d'appariement normalisés. Enfin, sur la base de ce score de correspondance unique, une décision finale, soit d'accepter ou de rejeter un utilisateur, est faite.[19]

III.4.1 Extraction des Caractéristiques

L'extraction des caractéristiques est une tâche cruciale dans toutes les applications de reconnaissance de formes, car les bons résultats sont directement liés à l'unicité et à la variabilité des caractéristiques extraites utilisées pour distinguer les différentes textures. En raison de sa propriété texturale discriminative, sa simplicité et son coût de calcul très bas, LBP devient très populaire dans la reconnaissance de formes.

III.4.2 Motifs binaires locaux LBP [20]

Les motifs binaires locaux ont initialement été proposés par Ojala en 1996 afin de caractériser les textures présentes dans des images en niveaux de gris. Ils consistent à attribuer à chaque pixel P de l'image à analyser, une valeur caractérisant le motif local autour de ce pixel. Ces valeurs sont calculées en comparant le niveau de gris du pixel central P aux valeurs des niveaux de gris des pixels voisins.

Le concept du LBP est simple, il propose d'assigner un code binaire à un pixel en fonction de son voisinage. Ce code décrivant la texture locale d'une région est calculé par seuillage d'un voisinage avec le niveau de gris du pixel central. Afin de générer un motif binaire, tous les voisins prendront alors une valeur "1" si leur valeur est supérieure ou égale au pixel courant et "0" autrement (**Figure III.8**). Les pixels de ce motif binaire sont alors multipliés par des poids et sommés afin d'obtenir un code LBP du pixel courant. On obtient donc pour toute l'image, des pixels dont l'intensité se situe entre 0 et 255 comme dans une image à 8 bits ordinaire. Plutôt que de décrire l'image par la séquence des motifs LBP, on peut choisir comme descripteur de texture un histogramme de dimension 255.

CHAPITRE III : EXTRACTION DES CARACTERISTIQUES D'EMPREINTE PALMAIRE EN UTILISANT LBP_θ

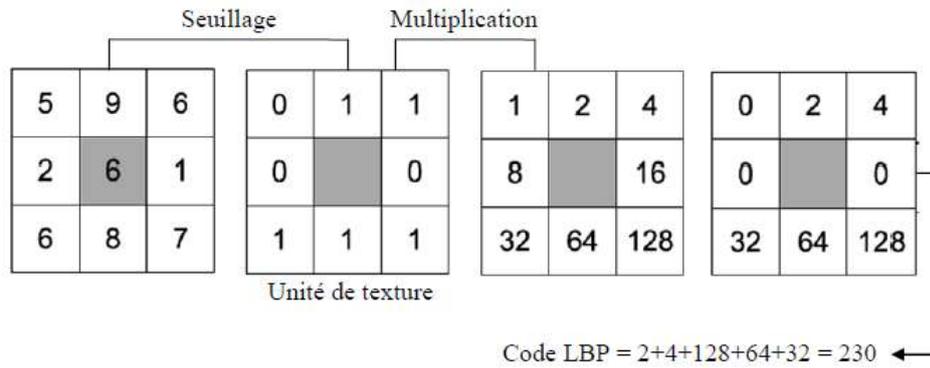


Figure III.7 : Construction d'un motif binaire et calcul du code LBP.

Pour calculer un code LBP dans un voisinage de P pixels, dans un rayon R, on compte simplement les occurrences de niveaux de gris g_p plus grands ou égaux la valeur centrale.

$$LBP(X_c, Y_c) = \sum_{n=0}^{P-1} U(g_i - g_c) * 2^n \quad (III.1)$$

Où x_c et y_c les coordonnées du pixel central, $u()$ est la fonction signe et où g_i et g_c sont respectivement les niveaux de gris d'un pixel voisin et du pixel central.

$$U(x) = \begin{cases} 1 & \text{si } x \geq 0 \\ 0 & \text{autrement} \end{cases} \quad (III.2)$$

III.4.3 Contribution [19]

Malgré la performance et l'efficacité de LBP basic, mais il reste toujours un inconvénient major c'est que la méthode LBP est sensible à la rotation et au bruit ce que pousse les chercheurs de proposer plusieurs variantes basées sur LBP de base. L'une des variétés est le LBP orienté.

Nous avons tenté d'améliorer la méthode LBP afin de rendre plus efficace pour caractériser l'image de l'empreinte, pour avoir un système plus performant on propose une nouvelle appelé méthode LBP orienté.

III.4.4 LBP Orienté (LBP_θ)

Comme mentionné ci-dessus, il existe diverses extensions et réformes du LBP original suite à sa première introduction par Ojala et al. La plupart de ces variantes ignorent les lignes d'image aux fins de classification ou de reconnaissance. Pour résoudre ce problème, nous proposons une technique LBP_θ pour améliorer les lignes d'image dans une orientation choisie.

Le schéma proposé peut extraire plusieurs vecteurs de caractéristiques en utilisant plusieurs orientations, puis améliorer la classification et le taux de reconnaissance en fusionnant plusieurs de ces vecteurs caractéristiques. La **figure III.9** montre le modèle binaire local orienté proposé. Le vecteur de caractéristiques LBP_θ est créé de la manière

CHAPITRE III : EXTRACTION DES CARACTERISTIQUES D'EMPREINTE PALMAIRE EN UTILISANT LBP_θ

suivante: Sélection d'un bloc de 9×9 autour du pixel examiné (pixel central), gc. Ensuite, pour une orientation souhaitée, calculer les coordonnées des voisins (gp). Lorsque la valeur du pixel central est supérieure à la valeur du voisin, écrivez 1. Sinon, écrivez 0. Cela donne un nombre binaire à 8 chiffres, qui sont habituellement convertis en valeur décimale. Notez qu'il y a une ambiguïté d'un facteur de 180° en orientation des lignes, c'est-à-dire que la ligne orientée à 30° et la ligne orientée à 210° ne peuvent pas être différenciées l'une de l'autre. Pour cela, dans un domaine d'image numérique, les orientations des lignes varient de 0° à 180° . Ainsi, les coordonnées des voisins pixels gp, où $p \in [0 \dots P]$ et $P = 7$, sont données par:

- si $0^\circ \leq \theta \leq 45^\circ$ ou $135^\circ \leq \theta \leq 180^\circ \Rightarrow$

$$(x_p, y_p) \equiv \begin{cases} x_p = x_c + \alpha - p \\ y_p = y_c + \lfloor x_p \tan(\theta) \rfloor \end{cases} \quad (\text{III.4})$$

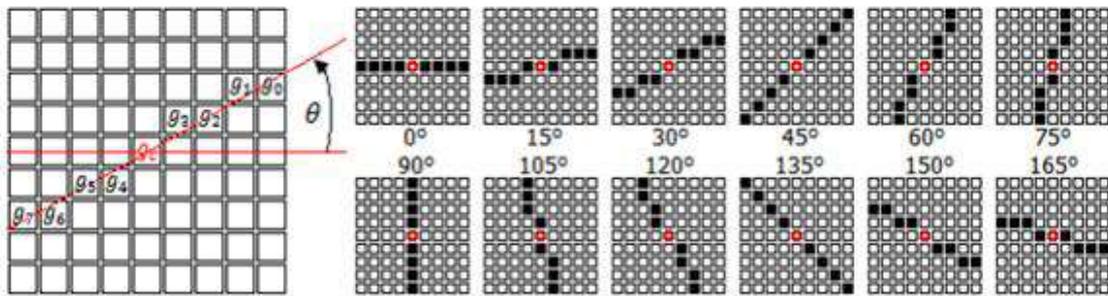


Figure III.8 : Illustration de la méthode proposé LBP_θ

- si $45^\circ \leq \theta \leq 135^\circ \Rightarrow$

$$(x_p, y_p) \equiv \begin{cases} y_p = y_c + \alpha - p \\ x_p = x_c + \lfloor y_p \left(\frac{1}{\tan(\theta)}\right) \rfloor \end{cases} \quad (\text{III.5})$$

Où

$$\alpha = \begin{cases} 4, & \text{si } p \in [0, P - 4] \\ 3, & \text{si } p \in [P - 3, P] \end{cases} \quad (\text{III.6})$$

CHAPITRE III : EXTRACTION DES CARACTERISTIQUES D'EMPREINTE PALMAIRE EN UTILISANT LBP_{θ}

Et $[x]$ désigne toute la partie de x . Quelques exemples sont présentés à la **figure III.9** Avec le LBP_{θ} où $\theta = [0^{\circ} \dots 165^{\circ}]$. Dans cette figure, les pixels centraux sont représentés en cercles rouges, et les pixels de quartier sont des carrés noirs.

III.5 Conclusion

L'empreinte palmaire présente une texture assez riche en lignes et en stries pour différencier les individus. C'est pourquoi on a bénéficié de cette particularité dans notre étude pour réaliser l'extraction des caractéristiques des textures en utilisant une nouvelle méthode LBP Orienté.

Dans ce chapitre, nous avons défini l'empreinte palmaire et ses caractéristiques, puis nous avons présenté la méthode LBP et leur développement. Enfin nous avons expliqué notre approche proposée LBP Orienté (LBP_{θ}).

Chapitre IV
EXPERIMENTATIONS ET
RESULTATS

IV.1 Introduction

Notre étude a été faite en testant l'algorithme proposé d'extraction des caractéristiques d'empreinte palmaire (LBP orienté) qui est mentionné dans le chapitre précédent. Elle est réalisée sur la base de données PolyU-Multi-spectrale (multi spectral palmprint).

Cette étude concerne quatre types de descripteur des textures (LBPbasique, LBP var, LBP orienté, LBPG), en utilisant des systèmes uni-modal et multi-modal. Nous donnerons Les résultats qui ont été obtenus sous forme de courbes ROC, CMC et des tableaux, l'analyse de ces résultats nous permettons de prouver l'avantage de LBP orienté.

IV.2 Objectif

Dans notre travail, les méthodes décrites ci-dessus sont utilisées comme descripteurs de caractéristiques pour représenter l'empreinte palmaire. Dans nos tests, les résultats obtenus pour LBP_{θ} Ont été comparés à ceux du précédent travail (LBP et LBP / VAR). Ensuite, la méthode proposée, LBP_{θ} a également été comparé. Les systèmes développés utilise deux représentations d'image d'empreinte palmaire, des images de niveau de gris (NG) et des infrarouges(NIR), pour cela, la performance de ces représentations est déterminée individuellement (systèmes uni-modaux) et plusieurs règles de fusion sont appliquées pour développer un système multimodal basés sur la fusion au niveau de score correspondant. Enfin, il est à noter que nos systèmes sont testés dans les deux modes d'identification (ensemble ouvert et ensemble fermé).

IV.3 Base de données de l'empreinte palmaire multi-spectrale (PolyU-MSP)

La base de données que nous avons utilisée dans nos expérimentations est PolyU Data-base qui contient 500 individus créés par des chercheurs de l'université polytechnique de Hong Kong. Les images des empreintes palmaires ont été assemblées en utilisant un dispositif de capture d'images, ensuite elles ont été prises dans deux périodes différentes séparées par un intervalle de temps d'environ deux mois. Chaque individu devait prendre au moins six images de ses des empreintes palmaires durant une période précise. De plus, dans la deuxième période, la source de lumière et l'objectif de la caméra CCD ont été ajustés de telle sorte que les images de la première et deuxième période donnent l'impression d'avoir été prises par deux dispositifs des empreintes palmaires différents.

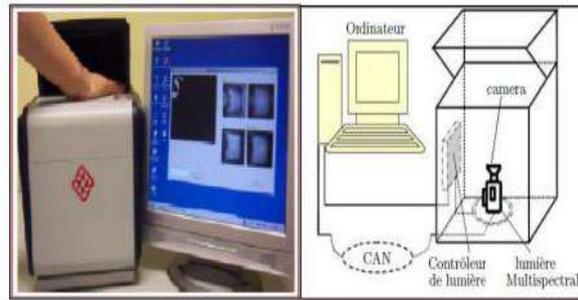


Figure IV.1: Schéma de principe de dispositif d'acquisition des images multi-spectrales.

Le système collecte quatre images depuis quatre bandes (Rouge, Vert, Blue et NIR). **La figure IV.1** montre des échantillons d'empreinte palmaire multi-spectrale sous les quatre bandes spectrales. La taille de chaque image est de 128×128 pixel avec une résolution de 75 dpi et cette base d'images contient 6000 images pour chaque bande provenant des 500 paumes différentes [38].



Figure IV.2 : Quelques images de la base de données PolyU-MSP.

IV.4 Séparation des bases de données

Notre base de données est divisée en deux parties: une base pour effectuer l'apprentissage et l'autre pour tester les techniques et déterminer leurs performances. Il n'y a pas de règles pour déterminer ce partage de manière quantitative.

Dans les séries de test que nous avons effectué, la base de données a été scindée de la façon suivante :

- ❖ **Images d'apprentissages :** La première, la cinquième et la neuvième image de chaque personne servent pour la phase d'apprentissage.
- ❖ **Images de Tests :** Les 9 images restantes de chaque individu nous ont servi pour la réalisation des différents tests.

IV.5 Environnement du travail

Dans cette section, nous présenterons les environnements matériel et logiciel de notre travail.

IV.5.1 Environnement matériel

Afin de mener à bien ce projet, il a été mis à notre disposition un ensemble de matériels dont les caractéristiques sont les suivantes :

Un ordinateur FUJITSU-PC avec les caractéristiques suivantes :

- ✓ Processeur : Intel(R) Pentium(R)
- ✓ RAM: 4.00 Go de RAM.
- ✓ Disque Dur: 500 Go.
- ✓ OS: Microsoft Windows 7 32bits.

IV.5.2 Outils de développement

Nous avons eu recours lors de l'élaboration de notre système à Matlab 2014a que nous présenterons ci-dessous.

Matlab 8.3 (R2014a) et son environnement interactif est un langage de haut niveau qui permet l'exécution de tâches nécessitant une grande puissance de calcul et dont la mise en œuvre sera bien plus simple et rapide qu'avec des langages de programmation traditionnels. Il dispose de plusieurs boîtes à outils en particulier celle du traitement d'images « Image ProcessingTool Box » qui propose un ensemble d'algorithmes et d'outils graphiques de référence pour le traitement, l'analyse, la visualisation et le développement d'algorithmes de traitement d'images.

IV.6 Expérimentations sur l'identification des individus par leurs empreintes palmaires

Dans le but d'analyser notre système d'identification, et afin d'arriver à des résultats satisfaisants, nous avons divisé notre travail en deux parties :

IV.6.1 Système uni-modal

Dans ce système d'identification, Nous avons effectué une étude sur les quatre descripteurs : LBP basique, LBP var, LBP_G, LBP orienté. Cette étude est faite pour évaluer la performance de la méthode LBP orienté.

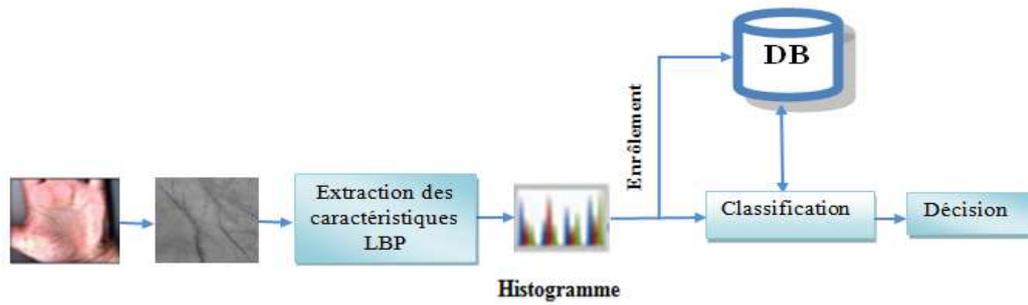


Figure IV.3 : Schéma du principe d'un système d'identification Uni-modal.

Le système (voir **Figure IV.3**) est composé de trois modules principaux: Extraction des caractéristiques, Mesure de similarité, et Décision. Notre travail est basé sur le module d'extraction des caractéristiques en utilisant l'approche proposée appelée LBP orienté pour extraire les caractéristiques des empreintes palmaires. L'image d'entrée est une modalité parmi les quatre modalités existantes dans notre base de données. Les résultats obtenus ont été présentés à la suite.

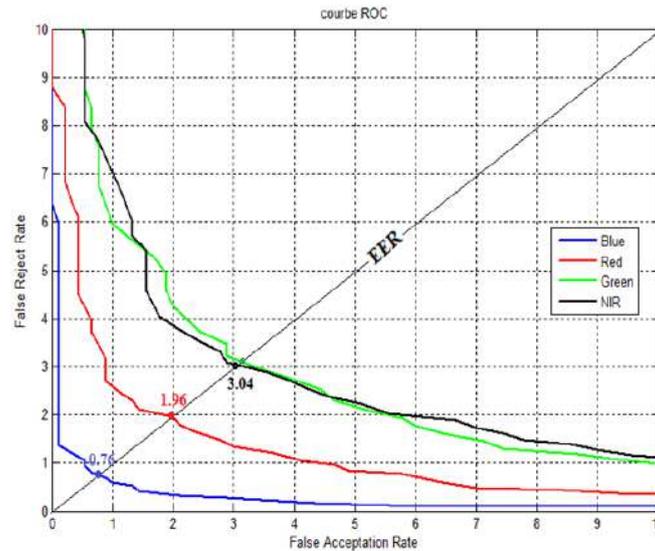
❖ **Algorithme LBP Basique**

Dans cette section on va appliquer le descripteur des textures LBP basique pour l'extraction des caractéristiques de l'image. Les résultats sont illustrés dans les figures et le tableau suivant.

Tableau IV.1 : Tableau de résultats de LBP basique.

Base de données	Open set		Closed set	
	T ₀	EER%	ROR%	RPR
Red	0.066	1.962	83.11	17
Blue	0.034	0.761	92	13
NIR	0.080	3.048	73.89	16
Green	0.070	3.114	76.89	42

Dans ce tableau, nous remarquons que la bande spectrale Blue (**B**) offre la meilleure performance en comparant avec les autres bandes. Dans ce cas, le système fonctionne avec une erreur minimale égale à **EER= 0.761%**.



La figure IV.4 montre les courbes caractéristiques (Receiver Operating Characteristic (ROC)) du système, dans le mode ensemble ouvert, en utilisant quatre bandes des empreintes palmaires. La méthode d'extraction des caractéristiques basée sur LBP basique est utilisée pour tous les PLM. Il est clair, d'après cette figure, que la bande bleu (B) offre le meilleure EER ($EER = 0.761\%$) avec un seuil $T_o = 0.034$, en comparaison avec les autres bandes (R, G, NIR).

Nous avons aussi testé les performances de cette méthode dans un système d'identification opérant en mode ensemble fermé. La figure IV.5, montre la courbe des scores cumulés (Cumulative Match Curve (CMC)) du système basé sur les différents PLM d'empreinte palmaire.

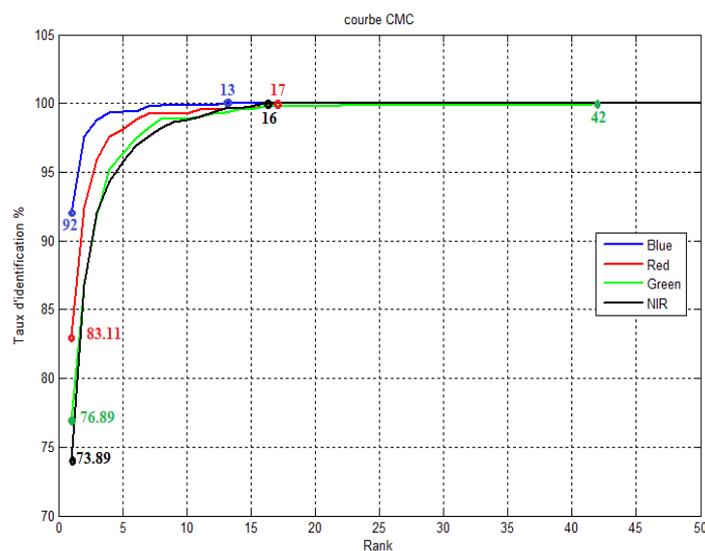


Figure IV.5: Courbe CMC de LBP basique.

D'après cette figure, nous obtenons un taux d'identification (ROR : Rank One Recognition) égal à **ROR=92%** et un rang d'identification (Rank of Perfect Recognition-RPR) égal à **RPR=13**, mais il est à noter, d'après tous les résultats, que la méthode LBP basique donne des résultats acceptables pour tous les bandes dans les deux modes d'identification.

❖ **AlgorithmeLBP_{var}**

LBP_{var} est une des variantes de LBP basic. Nous avons exécuté un algorithme LBP_{var} pour le test de notre base de données, et les résultats sont mentionnés au- dessous.

Tableau IV.2 : Tableau de résultats de LBP_{var}.

Base de donné	Open set		Closed set	
	T ₀	EER%	ROR%	RPR
Red	0.024	1.148	92.67	19
Blue	0.029	1.084	91.89	20
Green	0.040	2.801	80.89	31
NIR	0.049	1.472	88.67	13

Dans ce tableau, nous remarquons que le système uni modale avec la modalité Blue nous a donné des résultats acceptable avec un **EER=1.084%** et un **ROR=91.89%**.

Afin de comprendre l'affluence de l'algorithme LBP_{var} sur le comportement du système, nous avons présenté la courbe caractéristique (ROC) montré dans la **figure IV.6** qui nous informe des résultats du système dans l'ensemble ouvert.

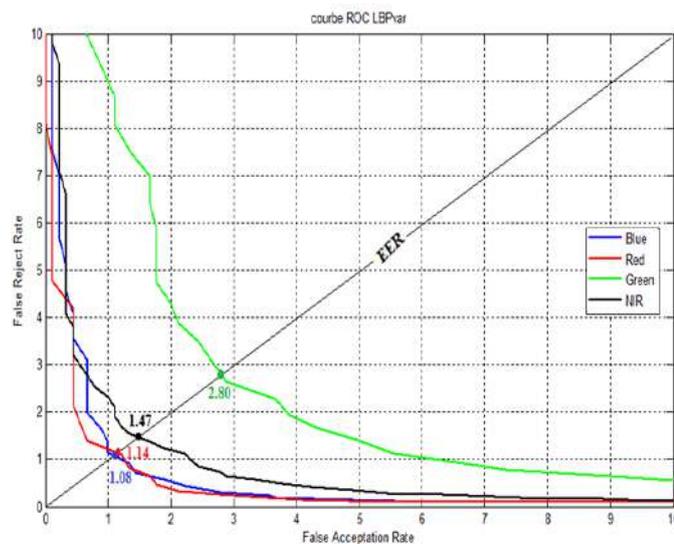


Figure IV.6: Courbe ROC de LBP_{var}.

Il est à noter d’après cette figure que la bande Blue offre les meilleur résultats EER ($EER=1.084\%$) avec un seuil $T0=0.029$ par rapport à les autres bandes

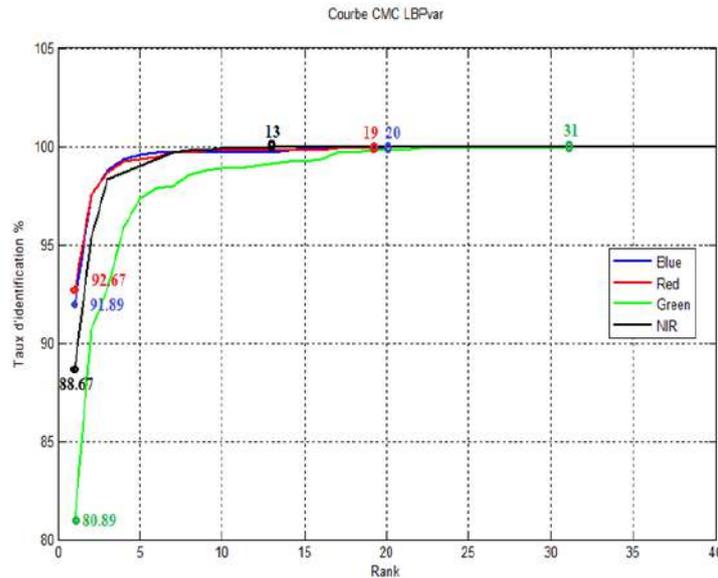


Figure IV.7: Courbe CMC de LBP_{var}.

Nous avons aussi testé les performances de cet algorithme sur le système dans le mode ensemble fermé. La Figure IV.7 montre la courbe des scores cumulés (CMC) du système qui indique que la bande Blue est la plus performante avec un ROR= 92%.

❖ Algorithme LBP Orienté

La nouvelle approche LBP orienté (LBP_θ) est caractérisée par orientation de son voisinage qui peut être choisie dans le but d’améliorer les lignes d’image. Dans ce qui suit on va tester l’algorithme LBP_θ avec plusieurs orientations afin de trouver l’orientation qui nous donne un résultat optimal avec deux modalités PLM_NG et PLM_NIR. Les résultats sont présentés sur le tableau suivant :

Tableau IV.3: Tableau de résultats de LBP_θ.

	NIR_PLM				NG_PLM			
	open set		closed set		open set		closed set	
	EER%	T0	ROR%	RPR	EER%	T0	ROR%	RPR
0°	0.215	0.327	99.33	17	0.345	0.345	99	96
30°	0.098	0.252	99.44	16	0.444	0.384	98.78	98
60°	0.541	0.318	98.11	63	1.351	0.438	97.67	99
90°	1.226	0.312	95.22	58	2.992	0.453	94.67	100
120°	0.211	0.273	99.11	25	0.534	0.366	98.33	89
150°	0.015	0.171	99.78	2	0.112	0.282	99.11	16

A travers les résultats de tableau (IV.3), on peut clairement constater que LBP_{θ} a donné les meilleurs résultats en utilisant NIR_PLM à l'angle 150° avec $EER=0.015\%$ et $ROR=99.78\%$

Nous allons présenter les résultats sous forme des courbes en divisant en deux parties : Résultats de NIR_PLM et Résultats de NG_PLM.

❖ Résultats de NIR-PLM:

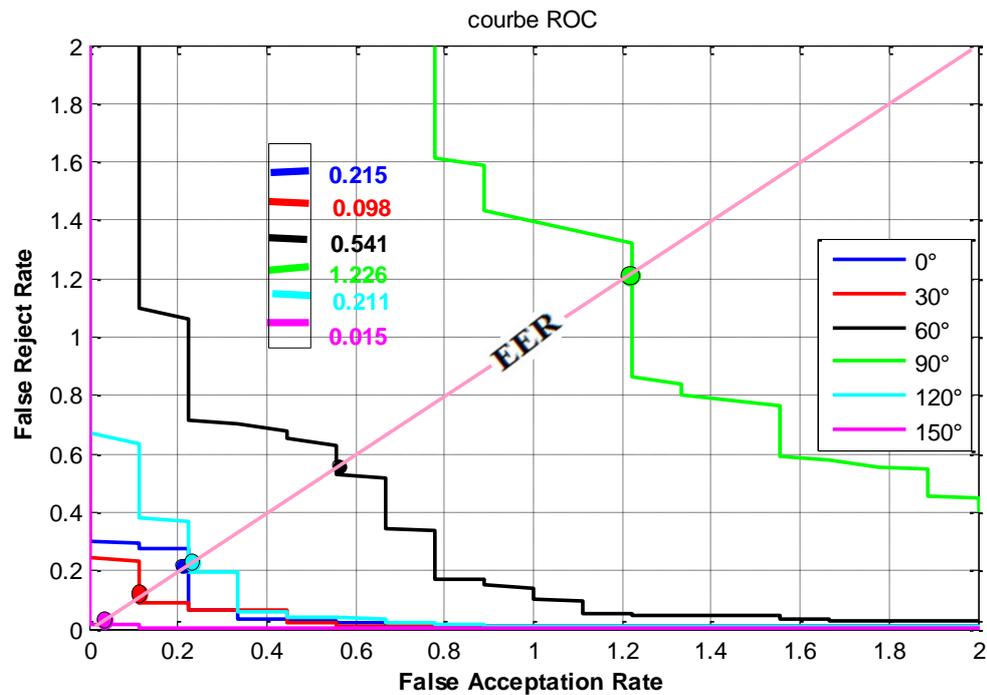


Figure IV.8: Courbe ROC de NIR_PLM en utilisant LBP_{θ} .

La figure IV.8 illustre les résultats d'application de l'algorithme LBP_{θ} en mode d'identification ensemble ouvert sur la modalité NIR-PLM sous forme courbes caractéristiques (ROC). Ces résultats sont montrant que l'orientation 150° est la plus performante avec la PLM-NIR ou' on a réussi à avoir un taux d'erreur minimale $EER=0.015\%$.

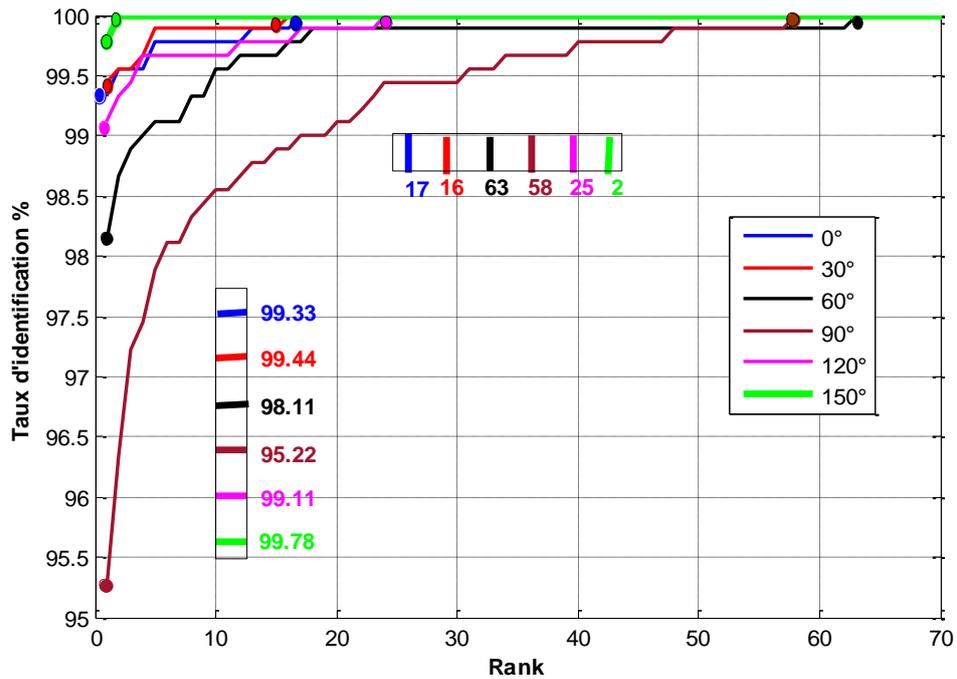


Figure IV.9: Courbe CMC de NIR_PLM en utilisant LBP₀.

Cette courbe (CMC) mentionné sur la figure IV.9 montre les résultats de l'application de l'algorithme LBP₀ en mode d'identification ensemble fermé, où on a trouvé des excellentes résultats ROR= 99.78%.

❖ Résultats de NG-PLM :

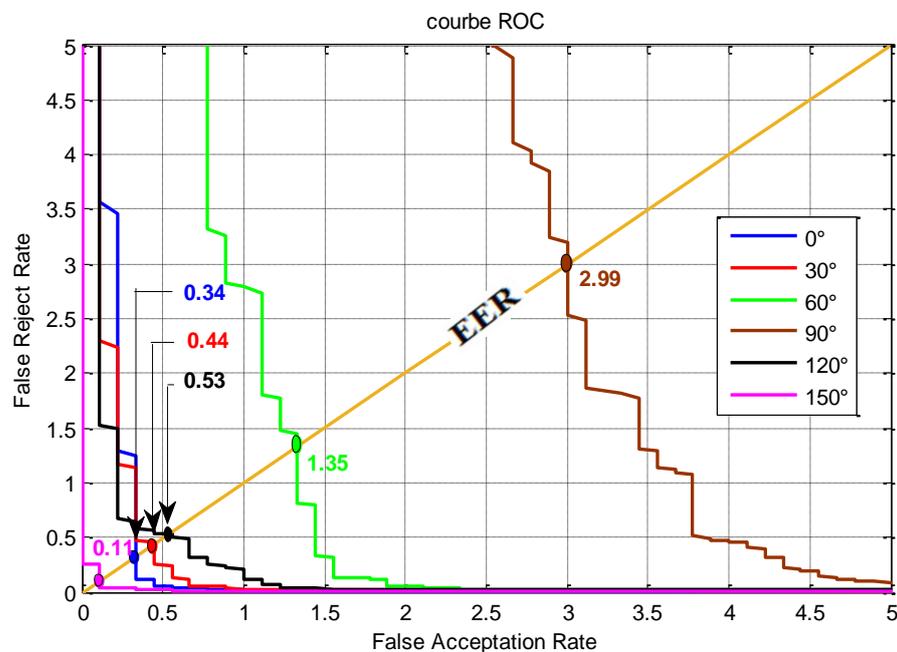


Figure IV.10: Courbe ROC de NG_PLM en utilisant LBP₀

La figure IV.10 illustre les résultats d'application de l'algorithme LBP₀ en mode d'identification ensemble ouvert sur la modalité NG-PLM-sous forme courbes

caractéristiques (ROC). Ces résultats montrent que l'orientation 150° est la plus performant avec la NG-PLM ou' on a réussi à avoir un taux d'erreur minimale **EER=0.112%**.

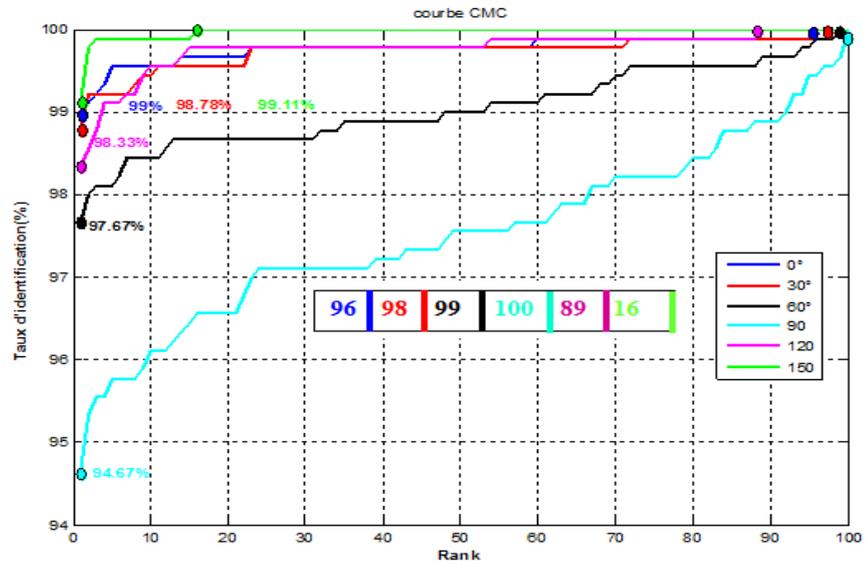


Figure IV.11: Courbe CMC de NG_PLM en utilisant LBP_0 .

Une deuxième courbe des scores cumulés (CMC) mentionné sur la **figure IV.7** montre les résultats de l'application de l'algorithme LBP_0 en mode d'identification ensemble fermé ou' on a trouvé des excellentes résultats **ROR= 99.11%**.

❖ **Algorithme LBP Gradient (LBP_G)**

Le fonctionnement de LBP_G se base sur le gradient d'image. Pour évaluer la performance de cet algorithme, nous avons l'appliqué sur les modalités NIR-PLM et NG-PLM ou' on a trouvé les résultats suivants:

Tableau IV.4: Tableau de résultats de LBP_G .

	Open set		Closed set	
	EER%	T0	ROR%	RPR
NIR_PLM	1.1	0.3	95.33	85
NG_PLM	1.012	0.363	97.22	100

Le **tableau IV.4** montre que lorsque nous avons appliqué l'algorithme LBP_G sur les modalités NIR et NG, nous avons remarqué que la modalité NG est la plus performante avec **EER=1.01%** et **ROR=97.22%**

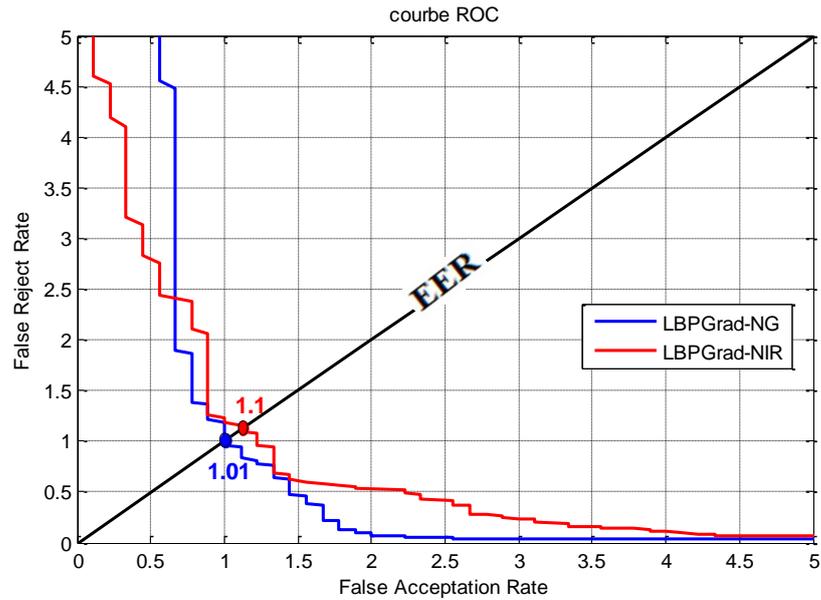


Figure IV.12: Courbe ROC de LBP_G

La figure IV.12 nous permet de voir que l’algorithme LBP_G a donné avec la modalité NG des résultats mieux qu’avec la modalité NIR dans le mode d’identification ensemble ouvert. La courbe caractéristique (ROC) montre l’avantage de NG -PLM selon les résultats trouvés EER (EER=1.01%) avec un seuil T₀=0.363.

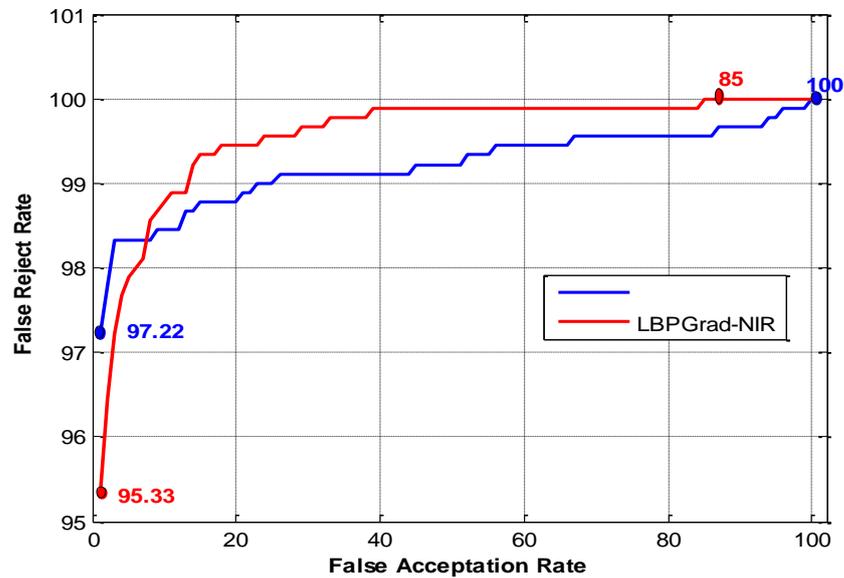


Figure IV.13: Courbe CMC de LBP_G.

La courbe (CMC) montrée dans la figure IV.13 illustre les valeurs trouvées en testant l’algorithme LBP_G mode ensemble fermé avec les modalités NIR et NG d’où on peut extraire les valeurs ROR=97.22% et RPR=100 qui prouvent l’avantage de NG -PLM par rapport aux NIR-PLM.

IV.6.2 Système multimodaux

En vue d'améliorer nos résultats, nous allons fusionner les différents scores des différentes bandes afin d'obtenir un système multimodal. **La figure IV.14** illustre le schéma de principe le système proposé.

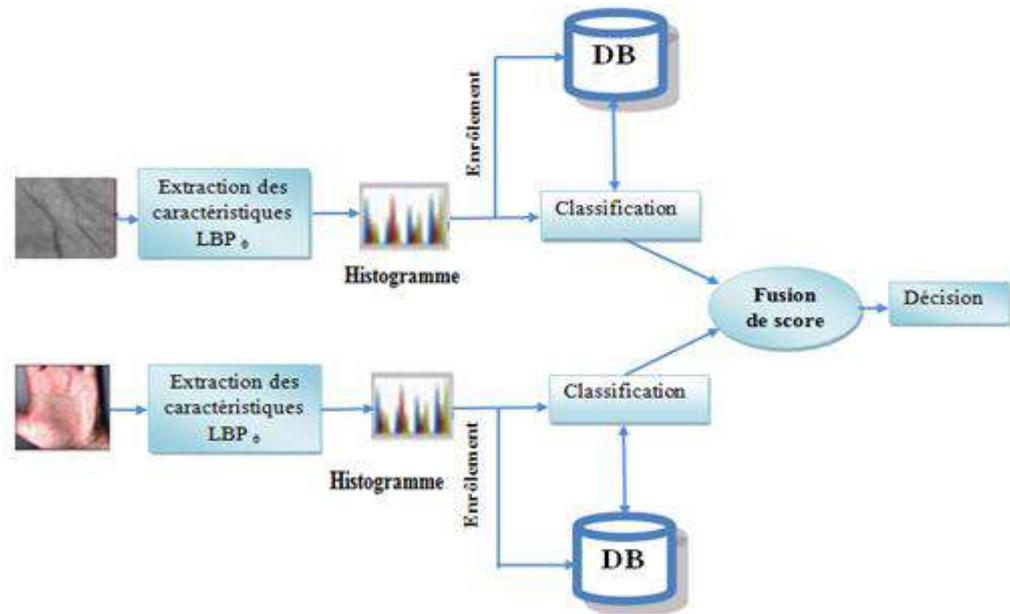


Figure IV.14 : Schéma de principe de système multimodal proposé.

Nous allons mettre en commun deux types de fusion. Premièrement: la fusion algorithmique où on fusionne les deux bandes NIR et NG en utilisant les deux orientations qui nous donne un taux d'erreur minimale. Deuxièmement: la fusion biométrique qui est réalisée par la fusion des deux bandes NIR et NG d'empreinte palmaire toutes les orientations.

Dans notre méthodologie, deux représentations différentes de l'empreinte palmaire ont été fusionnées au niveau des scores par les règles : la somme, moyenne, Max, Min, somme pondérée et la multiplication.

❖ Fusion biométrique

La fusion biométrique a été faite pour évaluer les performances de la méthode LBP_{θ} dans un système d'identification en modes ensemble ouvert et fermé. Elle sera appliquée entre les deux palm : NIR-PLM et NG-PLM avec tous les niveaux angles. Les résultats ont été présentés sur les tableaux suivants :

Tableau IV.5 : Résultats de fusion biométrique en ensemble ouvert.

		Open set									
		SUM		MUL		MIN		MAX		WHT	
		EER%	T0	EER%	T0	EER%	T0	EER%	T0	EER%	T0
NG-NIR	0°	0.231	0.399	0.195	0.375	0.136	0.345	0.226	0.285	0.181	0.387
	30°	0.119	0.276	0.112	0.267	0.074	0.225	0.211	0.294	0.121	0.276
	60°	0.455	0.357	0.457	0.351	0.397	0.321	1.239	0.408	0.363	0.318
	90°	1.392	0.384	1.351	0.372	1.046	0.327	2.875	0.438	1.109	0.336
	120°	0.076	0.213	0.098	0.231	0.105	0.267	0.422	0.339	0.051	0.201
	150°	0.026	0.294	0.026	0.285	0.022	0.165	0.101	0.285	0.013	0.204

Tableau IV.6 : Résultats de fusion biométrique en ensemble fermée.

		Closed set									
		SUM		MUL		MIN		MAX		WHT	
		ROR%	RPR	ROR%	RPR	ROR%	RPR	ROR%	RPR	ROR%	RPR
NG-NIR	0°	99.67	33	99.67	33	99.56	19	99.33	96	99.56	27
	30°	99.33	28	99.33	23	99.44	18	99.22	98	99.56	14
	60°	98.67	53	98.67	52	98.33	50	98	99	98.67	48
	90°	96	80	96	80	95.89	58	95	100	96	65
	120°	99.44	32	99.44	32	99.44	24	98.33	88	99.56	28
	150°	99.88	3	99.88	3	99.67	2	99.78	14	99.88	2

On constate sur ces tableaux que pour les même combinaisons, le système donne le meilleur résultat dans l'angle 150° avec un ROR égal à 99.88% et un RPR égale à 2 et EER=0.013% ceci avec la règle WHT.

La figure IV.15 montre les courbes caractéristiques (ROC) du système, dans le mode ensemble ouvert, en utilisant différent règles de fusion.

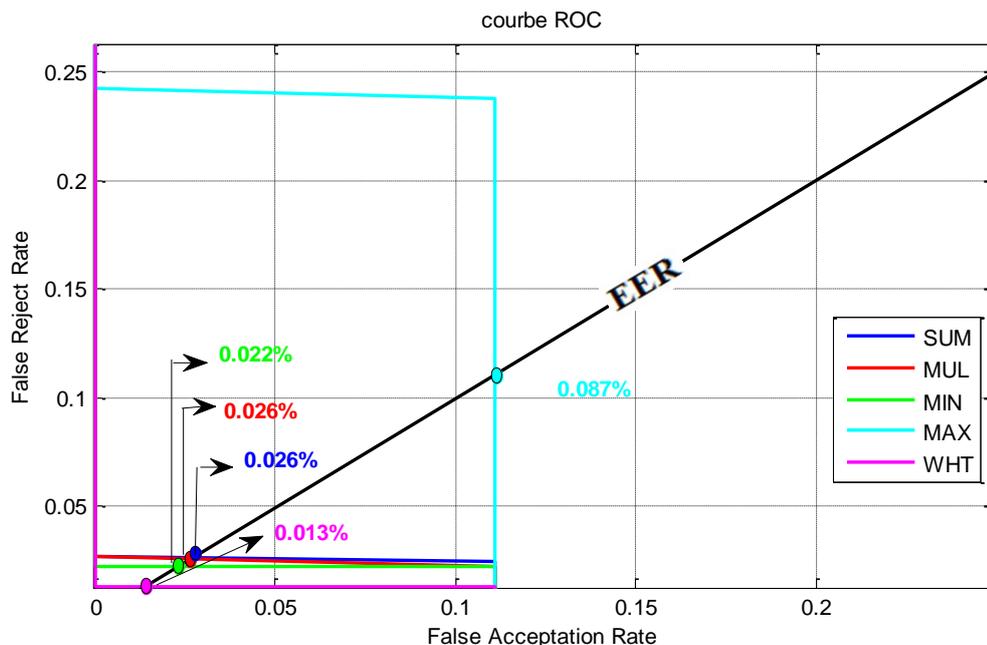


Figure IV.15: Courbe ROC de fusion biométrique dans l'angle 150°.

D'après cette figure, Il est clair que la règle WHT offre la meilleure **EER** (**EER = 0.013%**) avec un seuil **To= 0.204**.

Nous avons aussi testé les performances de cette méthode dans un système d'identification opérant en mode ensemble fermé. La **figure IV.16**, montre la courbe des scores cumulés (CMC) du système.

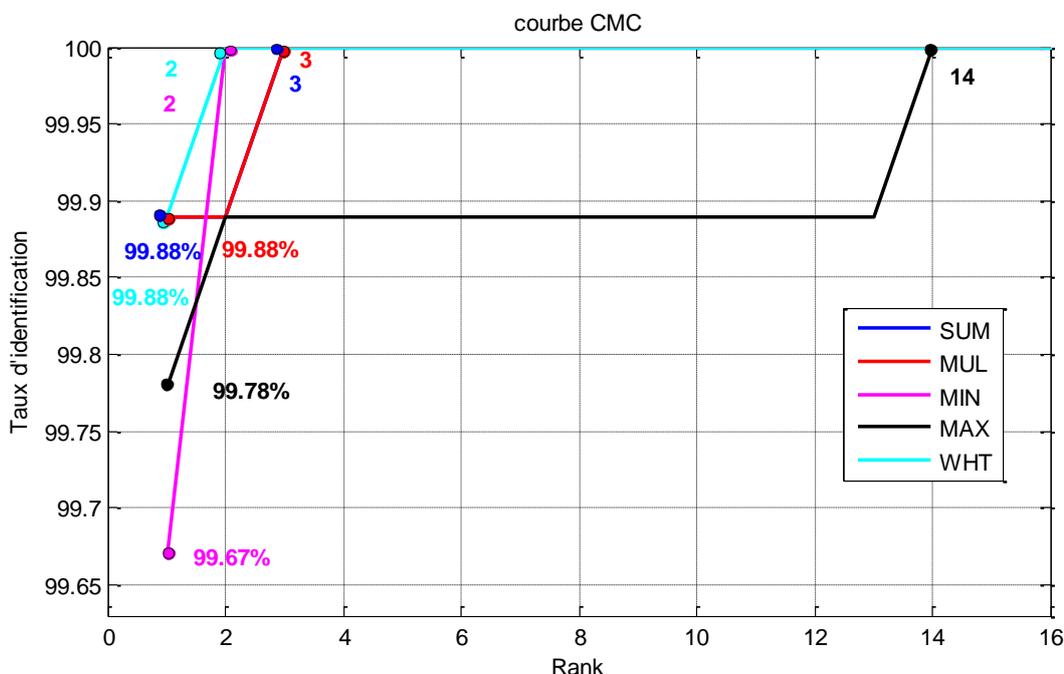


Figure IV.16 : Courbe CMC de fusion biométrique dans l'angle 150°.

La **figure IV.16** indique que les meilleurs résultats obtenus en utilisant la règle WHT. Elle donne un **ROR= 99.88%** avec un **RPR** égale **2**.

❖ Fusion algorithmique

La fusion algorithmique a été appliquée entre les deux palm: NIR-PLM et NG-PLM. Nous avons choisi les deux orientations qui nous donnent les meilleurs résultats dans le système uni modaux avec LBP orienté pour les combinant.

Dans les modes d'identification ensemble ouvert et fermé, le **Tableau IV.7** présente les taux d'identification retenus pour les différents systèmes en respectant les différentes règles de fusion.

Tableau IV.7 : Résultats de fusion algorithmique.

	NIR-150°/NG-30°				NIR-30°/NG-150°			
	open set		closed set		open set		closed set	
	EER%	T0	ROR%	RPR	EER%	T0	ROR%	RPR
SUM	0.017	0.198	99.56	46	0.044	0.306	99.78	4
MUL	0.096	0.339	99.56	42	0.042	0.297	99.78	4
MIN	0.006	0.165	99.56	42	0.040	0.219	99.67	4
MAX	0.305	0.339	99.22	98	0.1051	0.261	99.56	11
WHT	0.017	0.198	99.89	2	0.044	0.306	99.78	4

Dans ce tableau, nous remarquons que la fusion NG-30°/NIR-150° donnés un bon résultat avec la règle MIN. Dans ce cas, le système fonctionne avec une erreur minimale égale à **EER= 0.006%** en même temps que le seuil **To = 0.165**.

❖ Résultat de 30NG/150NIR

La **figure IV.17** montre la courbe des scores cumulés (CMC) du système basé sur les différentes règles de fusion qui sont : SUM, MUL, MIN, MAX et WHT.

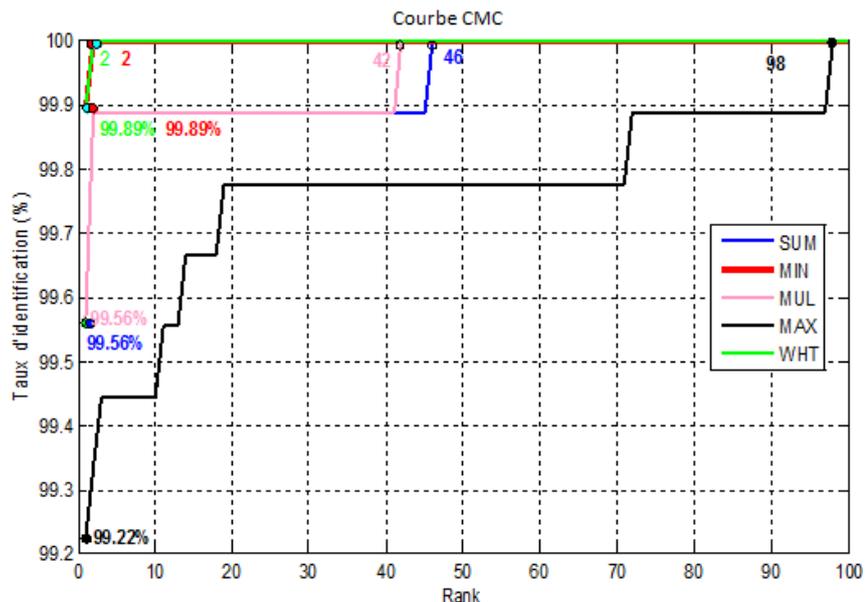


Figure IV.17: Courbe CMC de fusion 30NG/150NIR.

D'après cette courbe, le système fonctionne en mode ensemble fermé avec un taux d'identification au rang un **ROR** égal à **99.89%** et un rang d'identification parfait (**RPR**) égal à **2** avec les règles MIN et WHT.

Nous avons aussi testé les performances de la méthode dans un système d'identification opérant en mode ensemble fermé. La **figure IV.18** montre la courbe ROC.

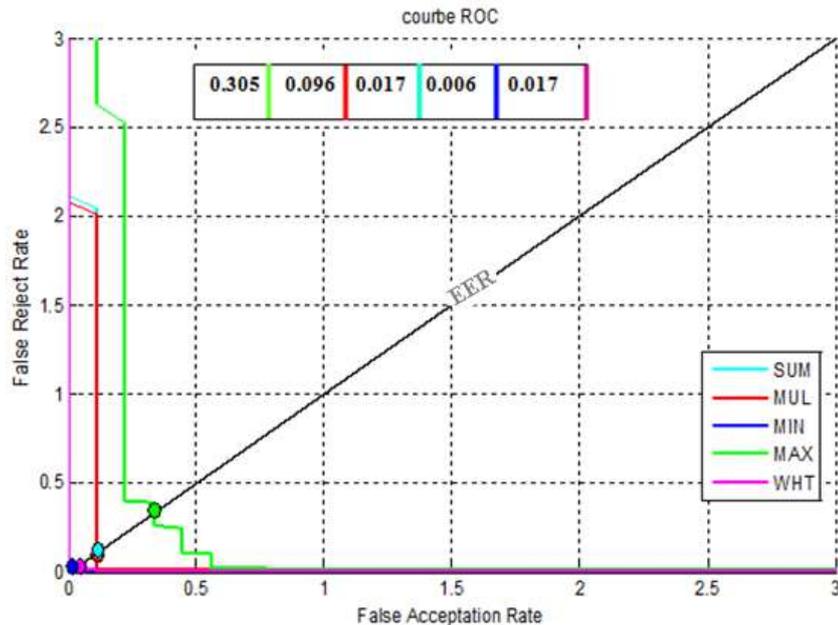


Figure IV.18: Courbe ROC de fusion 30NG/150NIR.

Il est clair, d'après cette figure, que la règle MIN offre la meilleure EER (**EER = 0.006%**) avec un seuil $T_o = 0.165$, en comparaison avec les autres règles (SUM, MUL, MAX et WHT).

❖ **Résultats : 150NG/30NIR**

La **figure IV.19** montre la courbe des scores cumulés (CMC) du système basé sur les différentes règles de fusion.

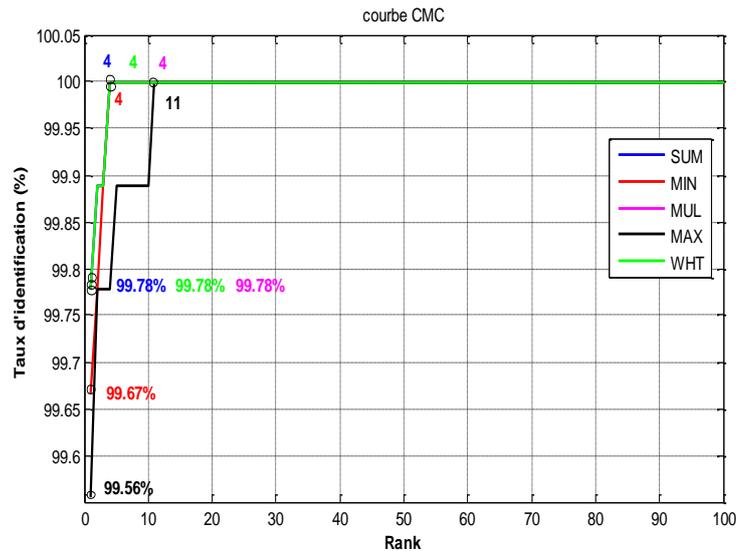


Figure IV.19: Courbe CMC de fusion 150NG/30NIR.

D’après cette courbe, le système fonctionne en mode ensemble fermé avec un taux d’identification **ROR** égal à **99.78%** et un rang d’identification (**RPR**) égal à **4** avec les règles SUM, MUL et WHT.

Nous avons aussi testé les performances de la méthode dans un système d’identification opérant en mode ensemble fermé. La **figure IV.20** montre la courbe ROC.

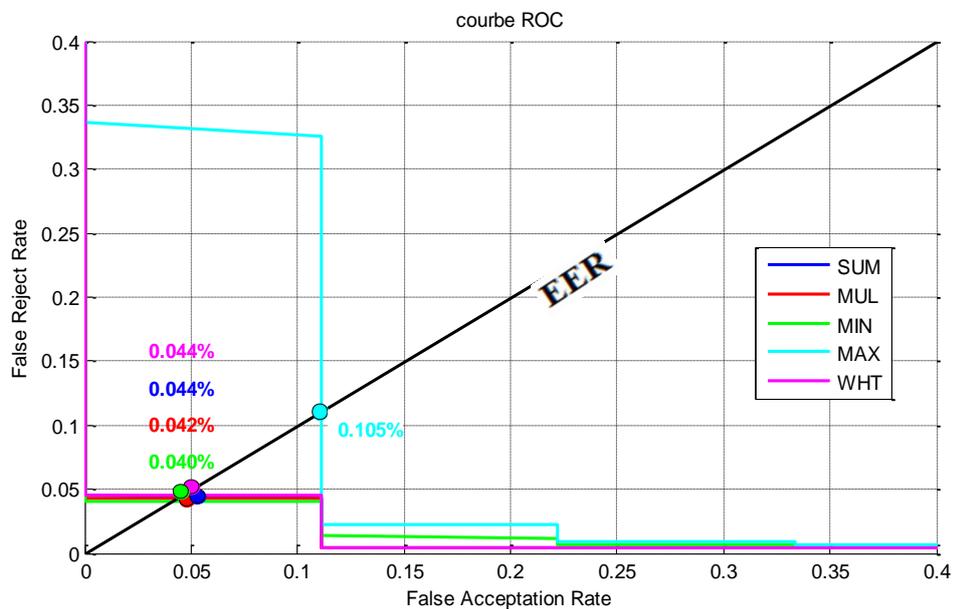


Figure IV.20: Courbe ROC de fusion 150NG/300NIR.

D’après cette figure, nous remarquons que les règles MIN offre la meilleure EER où **EER** = **0.040%** avec un seuil **To** = **0.219**, en comparaison avec les autres règles (SUM, MUL, MAX et WHT).

IV.7 Compte rendu des résultats

LBP orienté est la nouvelle approche proposée dans ce mémoire et afin de montrer son efficacité par rapport aux variantes existantes, nous avons réalisé des tests sur des différentes variantes de LBP. L'ensemble des résultats obtenus est résumé dans le tableau suivant:

Tableau IV.8 : Résultats des différentes variantes de LBP.

	Système uni-modale			Système multimodale		
	LBP basic (bande Blue)	LBP var (bande Blue)	LBP orienté (150°)	LBP gradient (NG- PLM)	Fusion algorithmique (NIR150°- NG30°)	Fusion biométrique (150°: NG- NIR)
Open set (EER%)	1.084	0.7617	0.015	1.012	0.006	0.013
Closed set (ROR%)	91.89%	92	99.78%	97.2%	99.89	99.88

Ce qui ressort du tableau (**Tableau IV.8**) confirme que l'utilisation de l'algorithme LBP₀ offre un taux d'identification élevé dans le système uni-modale en mode d'identification ensemble ouvert avec un taux d'erreur **EER=0.015%** et pour le mode d'identification ensemble fermé nous a donné un **ROR= 99.78%**. L'usage de système multimodale en basant sur la technique de fusion nous permettre de renforcer nos résultats ou' la fusion algorithmique a donné en mode ensemble ouvert **EER= 0.006%**et en mode ensemble fermé **ROR=99.89%**, mais la fusion biométrique a donné **EER=0.013ROR=99.88%**.

Pour mieux comprendre l'allure du système, nous suggérons les courbes suivantes (**Figure IV.21**), (**Figure IV.22**):

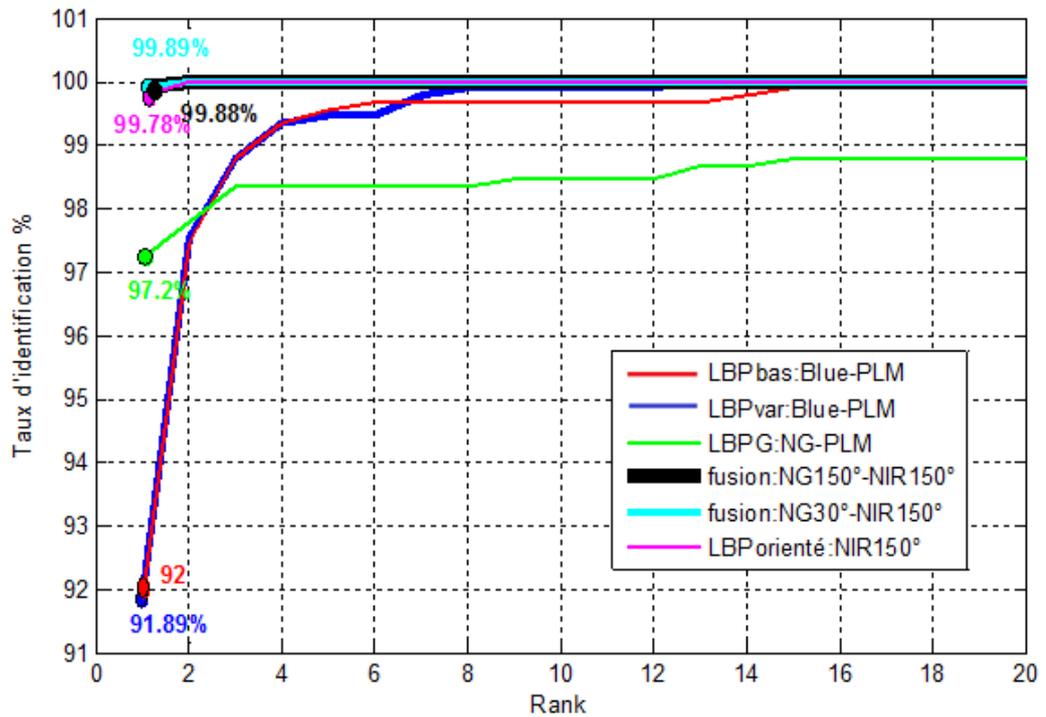


Figure IV.21: Courbe ROC des différentes variantes de LBP.

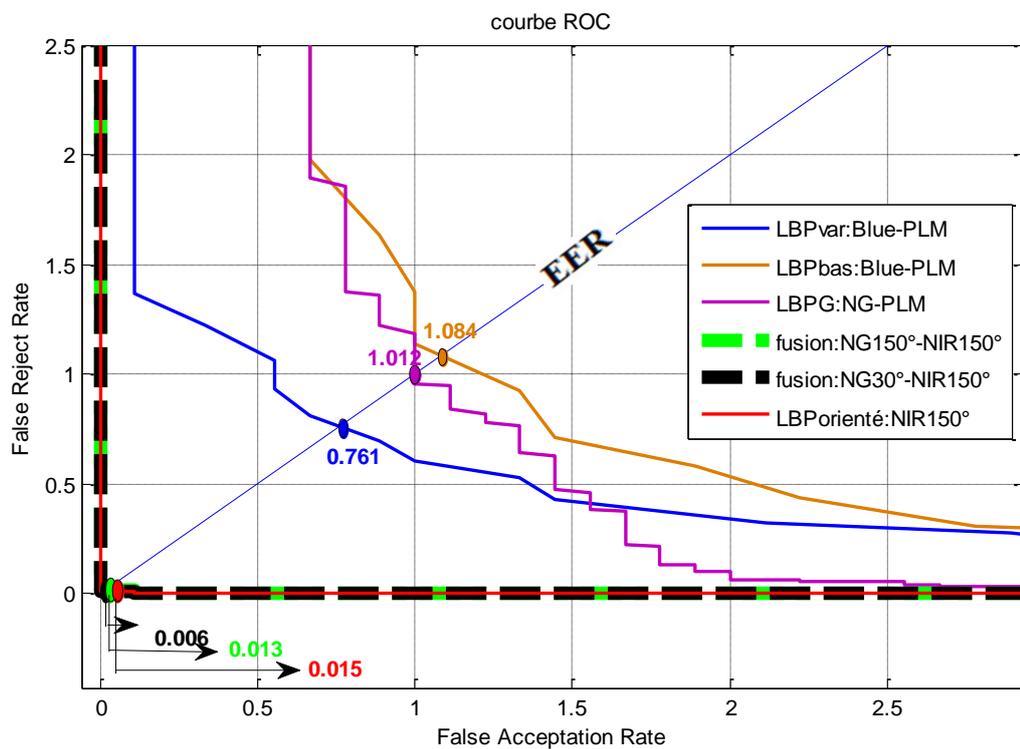


Figure IV.22: Courbe ROC des différentes variantes de LBP.

Ces courbes montrent le taux d'erreur et le taux d'identification de chacune des différentes méthodes. La méthode LBP orienté donnera les meilleurs résultats

(**ROR=99.78%** ; **EER=0.015%**) dans le système uni modale et dans le système multi modale, et à l'aide de fusion algorithmique, les résultats ont évolué avec **EER=0.006%**, **ROR=99.89%**.

IV.8 Conclusion

Dans ce chapitre nous avons présenté des applications sur l'extraction des caractéristiques des images d'empreinte palmaire en utilisant l'algorithme LBP et ses types LBP var LBP gradient et l'approche proposé LBP orienté, en appliquant deux systèmes de test systèmes uni-modal et systèmes multimodale afin de prouver la robustesse de la nouvelle méthode par rapport à les méthodes déjà existant.

Les résultats des calculs effectuées sont présenté dans des courbe ROC, courbe CMC et des tableaux. En analysant ces résultats, on a trouvé que LBP orientés est le meilleur algorithme (**EER=0.015%**, **ROR=99.78%**). Pour le système multimodal, on a suivi la procédure de fusion pour améliorer la performance de notre méthode proposé, et la fusion algorithmique nous a donné les meilleurs résultats (**EER=0.013%**, **ROR=99.89%**).

CONCLUSION GENERALE

CONCLUSION GENERALE

La biométrie est en constante évolution technologique, elle est largement utilisée dans de nombreux domaines pour des applications d'identification.

Le but principal des méthodes d'identification biométriques est de comparer une donnée de référence à une donnée étrangère qui sera obtenue via un capteur externe, cela dans le but de prouver l'identité de la personne soumise aux tests et éventuellement de l'autoriser ou non à accéder à un élément sécurisé.

Dans le domaine de la reconnaissance des empreintes palmaire, les caractéristiques texturales peuvent être décrites comme étant un moyen permettant de distinguer une empreinte d'une autre empreinte. Les caractéristiques sont généralement définies par expérience.

Nous avons tenté de proposer la méthode d'extraction des caractéristiques texturale LBP. Des nombreux travaux ont été proposés par des chercheurs. Notre étude s'est focalisée sur les caractéristiques texturale en utilisant LBP orienté dans le système uni-modal et multimodal.

Nous avons enfin présenté les résultats expérimentaux de LBP basique, LBP_{var}, LBP_G et la nouvelle approche LBP orienté. Ces résultats sont exposés à partir des courbes CMC et ROC de chaque algorithme. Pour LBP orienté, nous avons fait plusieurs tests d'orientation afin d'obtenir un taux d'erreur minimale suivant l'orientation idéale.

Au cours de ce travail, nous avons obtenu un taux d'erreur égale **EER=0.006%** à avec l'orientation **150°** qui traduit l'intérêt, et **ROR=99.89%**. Ces résultats sont très encourageants et montrent l'efficacité du descripteur LBP orienté.

BIBLIOGRAPHIE

- [1] C. Moujahdi, A. Hakim, and A. El, "Protection des systèmes de sécurité biométriques : contributions à la protection des modèles biométriques.", Thèse de Doctorat, Université Mohammed V – Agdal Maroc vol. 212, no. 0. 2014.
- [2] A.Ben Hamed O.Medjadji, "Reconnaissance des empreintes digitales" Mémoire de Master, Université Abou Bakr Blkaid Tlemcen. 2016
- [3] S.Zitouni, A.Saci, , "Authentification et identification biométrique des personnes par les empreintes palmaires " Mémoire de Master, Université Kasdi Merbah Ouargla.2016
- [4] F. Perronnin and J. Dugelay, "Introduction à la Biométrie Authentification des Individus par Traitement Audio-Vidéo" "An Introduction to Biometrics Audio and Video-Based Person Authentication", Article,vol. 19. 2002.
- [5] S.Benkhaira, " Systèmes multimodaux pour l'identification et l'authentification biométrique " Mémoire de Magister, Université 20 aout 1955-Skikda. 2010
- [6] H.Ahmed, "Identification des individus par la biométrie multimodale" Mémoire de Magister, Université Mohamed Boudiaf Oran. 2014
- [7] S.Boudjella, "detection et identification de personne par méthode biométrique" Mémoire de Magister, Université Mouloud Mammeri Tizi-Ouzou
- [8] I.Benchennane, "Etude et mise au point d'un procédé biométrique multimodale pour la reconnaissance des individus" Thèse de Doctorat, Université Mohamed Boudiaf Oran 2016
- [9] M. Mohamad El Abed, "Evaluation de systemes biometriques Liming" Thèse de Doctorat, Universitécaen/Basse-Normandie.2011
- [10] S.Guerifi Ababssa, "authentification d'individus par reconnaissance de caractéristiques biométriques liées aux visages 2D/3D" Thèse de Doctorat, Université D'evry Val D'essonne [Île-De-France](#). 2008
- [11] .A.Z.Aghiles, " Segmentation d'images appliquée en biométrie: Cas des images de l'iris " Mémoire de Magister, Université Mouloud Mammeri Tizi-Ouzou. 2013
- [12] R.Laouar, R.Chelawa, " Reconnaissance des personnes par leur empreintes palmaires multi-spectrales basées sur la DCT et le GMM " Mémoire de Master, Université Kasdi Merbah - Ouargla .2011
- [13] N.Morizet, " Reconnaissance Biométrique par Fusion Multimodale du Visage et de l'Iris " Thèse de Doctorat, École Doctorale D'informatique, Telecommunications Et Électronique De Paris. 2009
- [14] H. Guesmi, " Identification de personnes par fusion de différentes modalités biométriques" Thèse de Doctorat, Université Européenne De Bretagne en Habilitation Conjointe Avec L'université De Rennes 1 Co-Tutelle Avec L'université De Sfax. 2014
- [15] R. Mokhtari, M.Salhi, " L'identification de l'empreinte palmaire basée sur la fusion des données pour la reconnaissance des personnes" Mémoire d'ingénieur d'état, Université Kasdi Merbah - Ouargla .2010

- [16] A.Bouchemha, "Etude et Application des transformées géométriques à la Compression des images hautes résolutions et à la Biométrie (Authentification/Vérification de l'empreinte palmaire)" Thèse de Doctorat, Université Badji Mokhtar Annaba. 2016.
- [17] A.Meraoumia, "Modèle de Markov caché appliqué à la multibiométrie" Thèse de Doctorat, Université Houari Bomedienne Alger . 2014
- [18] K.Barka, Y.Boukhris, "Système d'identification biométrique à base d'un modèle flou " Mémoire de Master, Université Kasdi Merbah - Ouargla .2016
- [19] A. Meraoumia, H. Bendjenna, and S. Chitroub, Oriented Local Binary Pattern : A new scheme for an efficient feature extraction technique. Article, 2013.
- [20] .L. Houam, " Contribution À L'Analyse De Textures De Radiographies Osseuses Pour Le Diagnostic Précoce De L'Ostéoporose" Thèse de Doctorat, Univesite D'orleans, Univesite de Guelma. 2013

Résumé

Dans les systèmes biométrique, il existe diverses techniques d'extraction des caractéristiques pour décrire des informations de texture, parmi lesquelles on trouve le motif local binaire (Local Binary Pattern : LBP). Bien que LBP soit un descripteur efficace de texture, il ne parvient pas à caractériser suffisamment l'image. Dans ce travail, afin d'améliorer la capacité de discrimination qui conduit à une précision très acceptable du système de classification, nous proposons une nouvelle approche pour analyser la texture des images. Cette technique représente une version améliorée de LBP (appelée LBP orienté LBP_0). elle utilise les voisinages de chaque pixel dans des orientations choisies [19]. pour évaluer notre méthode, un système d'identification des empreintes palmaires est utilisé.

Mots clé : Biométrie, Extraction des caractéristiques, Texture, LBP, LBP_0 .

Abstract

In biometric systems, there are various feature extraction techniques for describing texture information, including the local binary pattern (LBP). Although LBP is an effective texture descriptor, it fails to adequately characterize the image. In this work, we propose a new approach to analyze the texture of images in order to improve the discriminating capacity which leads to a very acceptable precision of the classification system. This technique represents an improved version of LBP (called LBP -oriented LBP, using the neighborhoods of each pixel in selected orientations). In order to evaluate our method, a palm fingerprint identification system is used.

Key words: Biometric, Feature extraction, Texture, LBP, LBP_0 .

ملخص

في الأنظمة البيومترية، هناك تقنيات مختلفة لاستخراج مميزات لوصف معلومات اللمس، ومن بينها النمط الثنائي المحلي LBP. على الرغم من أن LBP هو واصف ملمس فعال إلا أنه يفشل في تمييز الصورة بما فيها الكفاية. في هذا العمل، ولتحسين قدرة التمييز التي تؤدي نظام التصنيف بدقة مقبولة، نقترح نهجاً جديداً لتحليل ملمس الصور. هذا الأسلوب هو نسخة محسنة من LBP تدعى LBP الموجهة. ويستخدم جوار البكسل في كل الاتجاهات التي يتم تحديدها. و لتقييم أسلوبنا، نستخدم نظام تحديد بصمة الراحة.

كلمات البحث: البيومترية، استخراج المميزات، اللمس، النمط الثنائي المحلي LBP, LBP الموجهة.