REPUBLIQUE DEMOCRATIQUE POPULAIRE D'ALGERIE

ENSEIGNEMENT SUPÉRIEUR DU MINISTÈRE ET RECHERCHE SCIENTIFIQUE

UNIVERSITÉ KASDI MERBAH OUARGLA

Faculté des nouvelles technologies de l'information et de la communication

Département d'électronique et de télécommunications

Mémoire

MASTER ACADÉMIQUE

Domaine: Science et technologie

Spécialité: Systèmes de télécommunications

Présentée par:

HALIMI Abir SEDDIKI Amel

THEME

Système Biométrique pour la Reconnaissance des Articulations des Doigts et la Méthode de Quantification de phase Local

Devant le jury:

Mr. M. Chaa	MCA	President	UKM Ouargla
Mme. F. Charif	MCA	Examinateur	UKM Ouargla
Mr. K. BEN SAID	MAB	Encadreur	UKM Ouargla
Mr. Z. TIDJANI	MAA	Co-encadreur	UKM Ouargla

Année Académique:2019/2020

Remerciements

Tous d'abord, Nous Remercions à Allah Tout puissant de nous avoir donné la force, la volonté ,et le privilège d'étudier et de réaliser ce travail

Nous à remercier notre encadreur monsieur Dr ***BEN SAID KHALD*** *s'est toujours montré l'écoute et était très disponible tout au long de réalisation de ce mémoire*

Nous Remercions les membres du jury pour leur éminentes contributions à l'évaluation de ce projet .

Enfin , nous adressons nos plus sincères remerciements à les familles Halimi et Seddiki et tous nos proches et amis ,qui ont toujours soutenu et encouragé au cours de la réalisation de ce travail.

Dédicace

Je dédie ce travail

À la princesse des femmes, chère mère et à mon cher père, je garde la tête haute et fière de l'être

À mes sœurs et frères

À Toute ma famille

Et à tous ceux qui m'ont soutenu de loin ou de près pour terminer mon voyage d'étude

ABIR HALIMI

Dédicace

Premièrement, louange à Dieu et merci à Dieu, par la grâce duquel Sont fait les bonnes œuvres

Je dédie ce modeste travail À qui c'était ont été la raison de ma présence dans la vie à mon cher père (que Dieu ait pitié de lui) et à ma mère bien-aimée (Que Dieu la protège)

A frères et à mes chers sœurs (chacun en son nom) et Leurs enfants.

A tous ceux qui m'ont enseigné un lettre .

A tous ceux mes amis.

A tous ceux que l'encre a oublié mais le cœur n'oublie pas.

AMEL SEDDIKI

Résumé

L'identification automatique des individus est devenue une exigence importante pour une variété d'applications telles que le contrôle d'accès et les systèmes de surveillance. Les systèmes biométrique offrent une identification automatique de l'identité, basée sur des mesures physiologiques ou comportementales ou biologiques d'un individu. C'est ce que nous apprendrons à connaître au début, le concept du système biométrique et ses composants et méthodes de base dans l'identification des personnes.

Le travail proposé dans ce mémoire étudie reconnaissance des personnes par la empreintes articulation de doigts (FKP). Les empreintes articulation de doigts FKP sont importantes en raison de leurs avantages, tels que la facilité d'utilisation, la haute sécurité et la simplicité. Sur cette base, nous avons développé un système d'identification des empreintes articulation de doigts (FKP). Dans tous les systèmes biométriques il existe différentes techniques d'extraction de caractéristiques pour décrire les informations tissulaires, Dans nos travaux, nous avons utilisé la méthode de quantification de phase locale (LPQ) .

Notre travail dans Matlab est appliqué à une base de données bien connue «PolyU-FKP», qui a donné des résultats acceptables.

Mots Clés: Biométrique, Les articulations des doigts, extraction de caractéristiques, Réduction de dimension, quantification de phase locale LPQ.

Abstract

Automatic identification of individuals has become an important requirement for a variety of applications such as access control and surveillance systems. Biometric systems provide automatic identification of identity, based on physiological or behavioral or biological measurements of an individual. This is what we will get to know in the beginning, the concept of the biometric system and its components and basic methods in the identification of people.

The work proposed in this dissertation studies recognition of people by finger joint prints (FKP). FKP finger joint impressions are important because of their advantages, such as ease of use, high security and simplicity. Based on this, we have developed a finger joint fingerprint identification (FKP) system. In all biometric systems there are different feature extraction techniques to describe tissue information, In our work, we used the local phase quantification (LPQ) method.

Our work in Matlab is applied to a well-known “PolyU-FKP” database, which gave acceptable results.

Keywords: Biometric, Finger joints, Feature extraction, Dimension reduction ,LPQ local phase quantification.

ملخص

أصبح التحديد التلقائي للأفراد مطلبا مهما لمجموعة متنوعة من التطبيقات مثل أنظمة التحكم في الوصول و المراقبة ، حيث توفر الأنظمة الحيوية التعرف التلقائي للهوية ، بناءا على القياسات الفسيولوجية أو السلوكية أو البيولوجية للفرد وهذا ما سنتعرف عليه في البداية ، مفهوم نظام القياسات الحيوية ومكوناته وطرقه الأساسية في تحديد الهوية الشخصية.

العمل المقترح في هذه المذكرة يدرس التعرف على الأشخاص بواسطة بصمات مفاصل الأصابع اليد (FKP). حيث تعد بصمات FKP مهمة بسبب مزاياها , مثل سهولة الاستخدام والأمان العالي والبساطة . على أساس هدا قمنا بتطوير نظام تحديد باستخدام بصمات مفاصل الأصابع اليد (FKP) . في جميع أنظمة المقاييس الحيوية توجد تقنيات مختلفة لاستخراج الميزات لوصف معلومات النسيج ، في عملنا استخدمنا طريقة تكميم المرحلة المحلية LPQ .

يتم تطبيق عملنا في برنامج ماتلاب على قاعدة بيانات معروفة في هدا المجال ”PolyU-FKP “ وقد أعطت نتائج مقبولة.

الكلمات المفتاحية: بيومتري، مفاصل الأصابع، استخراج الميزات، تقليل الأبعاد، تكميم المرحلة المحلية LPQ .

Table des Matières

Remerciements I
Dédicace II
Dédicace III
Résumé IV
Table des Matières VI
Liste des Figures VIII
Liste des Tableaux X
Liste des Abréviations XI
Introduction générale 1

CHAPITRE I: Biométrie Multimodal

I.1 Introduction 3
I.2 Biométrie 3
I.3 Evolution de la Biométrie 4
I.4 Types de Modalités Biométries 4
I.4.1 Modalités Morphologiques 5
I.4.2 Modalités Comportementales 8
I.4.3 Modalités Biologiques 10
I.5 Système Biométrique Unimodal 11
I.5.1 Composants de base d'un Systéme Biométrique 11
I.6 Fonctionnement général d'un Systéme Biométrique 12
I.6.1 Mode d'Enrôlement 12
I.6.2 Mode de Reconnaissance 12
a) Mode de vérification 13
b) Mode de d'identification 13
I.7 Performances de Système Biométrique 14
I.8 Systéme Biométrique Multimodal 17
I.8.1 Différents multi-possibles 17
I.9 Fusion au Système Biométrique Multimodal 18
I.9.1 Fusion au niveau du capteur 18
I.9.2 Fusion au niveau Extraction de caractéristique 19
I.9.3 Fusion au niveau score 19
I.9.4 Fusion au niveau décision 20
I.10 Conclusion 21

CHAPITRE II : Extraction des caractéristiques des image et Réduction de dimension

II.1 Introduction 23
II.2 Image numérique 23
II.2.1 Images en niveaux de gris (monochrome) 24
II.3 Extraction des Caractéristiques 24
II.4 Quantification de phase Locale (LPQ) 24
II.4.1Quantification de phase locale Multi-blocs (MB-LPQ) 26
II.4.2Quantification de phase locale à plusieurs Niveau (ML-LPQ) 26
II.5 Réduction de dimension 27
II.5.1 Analyse de Composent principal (ACP) 27
II.5.2 Whatening ACP(WACP) 28
II.6 Classification 28
II.6.1 Support Vector Machine (SVM) 28
II.7 Conclusion 29

CHAPITRE III: Résultats expérimentaux et discussions

III.1 Introduction 31
III.2 Systeme de Reconnaissance FKP 31
III.2.1 La Base de données FKP 33
III.2.1.1 Séparation de la base de données 33
III.3. Expérimentations sur la FKP 34
III.3.1 Protocole Experimentale 34
III.4. Résultats et Discussion 35
III.5 Conclusion 39
Conclusion générale 41
Références 42

Liste des Figures

CHAPITRE I : Biométrie Multimodal

Figure I. 1 Structure des Types de Modalités Biométriques 5
Figure I. 2 trait biométrique :visage. 6
Figure I. 3 trait biométrique : Le empreinte digitale. 6
Figure I. 4 trait biométrique : Iris 7
Figure I. 5 trait biométrique : la main. 7
Figure I. 6 images de Empreintes des articulation des doigts 8
Figure I. 7 t rait biométrique : Signature 8
Figure I. 8 Système de reconnaissance de frappe sur un clavier 9
Figure I. 9 trait biométrique: la Voix 9
Figure I. 10 trait biométrique: démarche 10
Figure I. 11 trait biométrique : ADN 10
Figure I. 12.Composants d'un système biométrique 12
Figure I. 13 Enrôlement d'une personne dans le système biométrique 12
Figure I. 14 Vérification de la personne dans le système biométrique 13
Figure I. 15 Identification de la personne dans le système biométrique 14
Figure I. 16 Illustration du FRR et du FAR 15
Figure I. 17 Graph démonstratif de l'EER 15
Figure I. 18 Courbe ROC 16
Figure 1.19 : Courbe CMC.....16
Figure I. 20 Les différents systèmes multimodaux 18
Figure I. 21 Processus de Fusion au niveau du capteur 19
Figure I. 22 Processus de Fusion au niveau Extraction de caractéristique 19
Figure I. 23 Processus de Fusion au niveau score.....20
Figure I. 24 Processus de Fusion au niveau décision.....20

CHAPITRE II :Extraction des caractéristiques des image et Réduction de dimension

Figure II. 1 Image numérique 23
Figure II. 2 Images en niveaux de gris.....24
Figure II.3 Organigramme de l'ensemble des étapes nécessaire à la construction du descripteur LPQ 25
Figure II. 4 Exemple sur d'application de la méthode MB-LPQ …… 26
Figure II. 5 Exemple d'approche ML-LPQ d'extraction de caractéristiques avec (n=3 niveaux) 26

CHAPITRE III : Résultats expérimentaux et discussions

Figure III. 1 Structure du système d'authentification personnelle d'FKP 32
Figure III. 2 dispositif d'acquisition d'image FKP.....32
Figure III. 3 Exemple d'images de FKPs 33
Figure III. 4 Courbe ROC de système unimodal 36
Figure III. 5 Courbe CMC de système unimodal 37
Figure III. 6 Courbe ROC de système multimodal.....37
Figure III. 7 Courbe CMC de système multimodal 38

Liste des Tableaux

Table III. 1: Performance de système unimodal par ML-LPQ pour le doigt milieu gauche 35
Table III. 2: Performance de système unimodal par ML-LPQ et WPCA 35
Table III. 3: Performance de système unimodal 36
Table III. 4: Performance de système Multimodal 37
Table III. 5: Performance de système Multimodal pour différents régle de fusion….....38

Liste des Abréviations

FKP :Fingir Knuckle print

ADN : Acide Désoxyribonucléique

RAM : Random Access Memory

DSP : Digital signal processor

PIN : Personal Identification Number

FRR : False Rejection Rate

FAR : False Acceptante Rate

ERR : Equal Error Rate

ROC: Receiver Operating Characteristic

CMC : Cumulative Match Characteristics

IRM: Imagerie par Résonance Magnétique

LPQ : Local phase Quantization

MB-LPQ : Multi-blokc Local phase Quantiziation

ML-LPQ : Multi-Level Local phase Quantiziation

ACP : Analyse de Composent Principal

WACP : Whitening Analyse de Composent principal

SVM : Support Vector Machine

LED : Light-Emitting Diode

CCD : Charged Coupled Device

ROI : Région Of Interrest

LIF: Left Index Fingers

LMF: Left Middle Fingers

RIF : Right Index Fingers

RMF : Right Middle Fingers

ROR : Rank One Recognition

RPR : Rank of Perfect Recognition

Introduction générale

Introduction générale

Dans le passé, le monde utilisait des techniques d'authentification telles que le mot de passe et la carte d'identité pour sécuriser des biens tels que des armes et des informations confidentielles, en particulier dans le domaine du renseignement mais n'est pas suffisant, car il y a ceux qui peuvent deviner ou voler le mot de passe ou falsifiable la carte d'identité. donc nous sommes réfugiés d'établir une nouvelle méthode pour mettre fin et des limités à ce problème, cette méthode est dénommée "système de biométrique". La reconnaissance des individus a connu plus d'importance dans la vie humaine quotidienne. La reconnaissance biométrique est utilisée dans de nombreuses applications telles que la protection de l'accès à un ordinateur, un téléphone portable, un établissement, et des cartes bancaires…etc.

De nombreuses technologies biométriques ont été développées, toutes basées sur les identificateurs biométriques biologiques et physiologiques et comportementales telles que : l'iris, la voix, les empreintes digitales, le visage, FKP... etc. Ces derniers sont plus fiables que les systèmes classiques (clé, mot de passe...) car ils sont difficilement falsifiables.

Le système qui viennent d'être étudiés c'est celui de la reconnaissance des personnes par leurs images des surfaces extérieures des doigts, un système qui utilise l'empreinte des articulations des doigts(Finger knuckle Print "FKP":(Index gauche (LIF), médian gauche (LMF), index droit (RIF), médian droit (RMF)) . Cette modalité a été choisie parce qu'elle a de nombreux avantages remarquables dans ce domaine de la biométrie, en plus c'est une technique, simple et facile à utiliser. L'objectif de cette étude est de développer un système biométrique idéal pour identifier les articulations des doigts.

Dans cette étude , nous allons essayer d'atteindre cet objectif à travers trois chapitres, plusieurs notions et concepts de la biométrie et réalisation de système de reconnaissance vont être abordé :

- **Le premier chapitre:** Nous parlerons de la biométrie en général et ses différentes méthodes, avec une reconnaissance à la biométrique unimodal et à la biométrie multimodale, et c'est ce sur quoi nous nous concentrerons pendant l'étude.
- **Le deuxième chapitre:** On exposera dans ce chapitre, les méthodes utilisées pour l'extraction des caractéristiques, réduction de dimension, et la classification des données.
- **Le troisième chapitre:** Nous parlerons du système FKP en tant que méthode

biométrique, de ses caractéristiques exploitées dans différents types de reconnaissance ainsi que du processus général de son identification. Ensuite, nous analysons les résultats expérimentaux obtenus par chaque méthode, suivis d'une discussion des résultats.

Chapitre I

Biométrie Multimodal

I.1 Introduction

La sécurité des systèmes d'information est devenue un domaine de recherche d'une grande importance. La conception d'un système d'identification fiable, efficace et robuste est une tâche prioritaire. L'identification de l'individu est également nécessaire pour assurer la sécurité des systèmes et des institutions, pour contrôler l'accès à une zone très sûre qui n'est accessible qu'à un nombre limité de personnes (enregistré dans une base de données) Ceci est cohérent avec la recherche de l'identité de la personne apparaissant dans la base de données et de la personne qui a les fonctionnalités compatibles avec celle-ci . Il existe plusieurs technologies d'identification différentes, dont certaines sont utilisées à grande échelle depuis des années; La méthode d'authentification ou de vérification de personne la plus courante est la biométrie .

Dans le premier chapitre, nous présenterons le système biométrique et ses différentes modalités ,par ailleurs nous parlerons du système biométrique multimodal en passant par quelques problèmes de système biométrique uni-modal.

I.2 Biométries

La biométrie est une technique naissante qui nous permet de vérifier L'identité de la personne en employant un ou plusieurs de ses caractéristiques personnelles. Il existe plusieurs appondus biométriques, les plus connues étant: physiques (Empreinte digitale, géométrie de la main…etc.) ou traits personnels automatiquement mesurables (démarche, voix, signature…etc.) , robustes et distinctives qui peuvent être utilisées pour Identifier la personne ou pour vérifier l'identité prétendue d'un individu" .ou Biologiques comme(l'ADN..etc.) d'une personne et a pour objectif de déterminer son identité de manière irréfutable. biométrie est basée sur ce que l'on est permet ainsi d'éviter la duplication, le vol, l'oubli ou la perte.

Pour assurer leurs fiabilités, les modalités biométriques doivent être déterminées par quelques caractéristiques. Parmi les propriétés d'une modalité biométrique, on trouve [1]:

- **Universelles:** exister chez tous les individus
- **Uniques :** permettre de différencier un individu par rapport à un autre
- **Permanentes :** invariables dans le temps

- **Mesurables :** collectez facilement les données des fonctionnalités
- **Performance :** c'est l'efficacité du système en termes de précision, de vitesse de gestion des défauts et de rugosité
- **Acceptabilité:** le système doit respecter certains critères (facilité d'acquisition, rapidité, etc.) afin d'être employé.

I.3 Evolution de la Biométries

Depuis l'existence de l'homme, il a toujours cherché à trouver les différences qui existent entre lui et son entourage et à les exploiter dans ses besoins quotidiens.

Les chinois ont été les premières à utiliser, il y a 1000 ans, les empreintes digitales à des fins de signature de documents. Après, c'était le tour de l'anatomiste MARCELLO MALPIGHI(1628-1694)qui les a étudiées avec un nouvel instrument nommé microscope. Puis le physiologiste tchèque JAN EVANGELISTA PURKINGE(1787-1869) a essayé de les catégoriser selon certaines caractéristiques [2].

Vers la fin du XIX^{é} sicle, le DR HANRY FAULDS (1843-1930),chirurgien à Tokyo, a marqué le premier pas vers l'élaboration d'un système d'identification d'individus en se basant sur des méthodes statistiques pour la classification des empreintes.

En ce moment, un de ses contemporains, le français ALPHONSE BERTILLON (1853-1914), était en train de tester une méthode d'identification des prisonniers nommée anthropométrie judiciaire. BERTILLON procédait à la pris de photographies de sujets humains, mesurait certaines parties de leur corps(tète, membres,..etc.)et on notait les dimensions sur les photos et sur les photos et sur des fiches à des fins d'identification ultérieur. C'était la naissance de la première base de données contenant des information des individus [2]. Et depuis, ces systèmes de reconnaissance ne cessent de se développer et de devenir plus performants.

I.4 Types de Modalités Biométries

La technologie biométrique est sophistiquée, plus intelligente, super sensible et mise en place pour aider à protéger les entreprises et les particuliers. Plus important encore, il est impossible de voler ou de dupliquer, comme son nom l'indique. Il existe divers traits

présents chez l'homme, qui peuvent être utilisés comme modalités biométriques. Les modalités biométriques relèvent de trois types : morphologiques , comportementale et biologiques

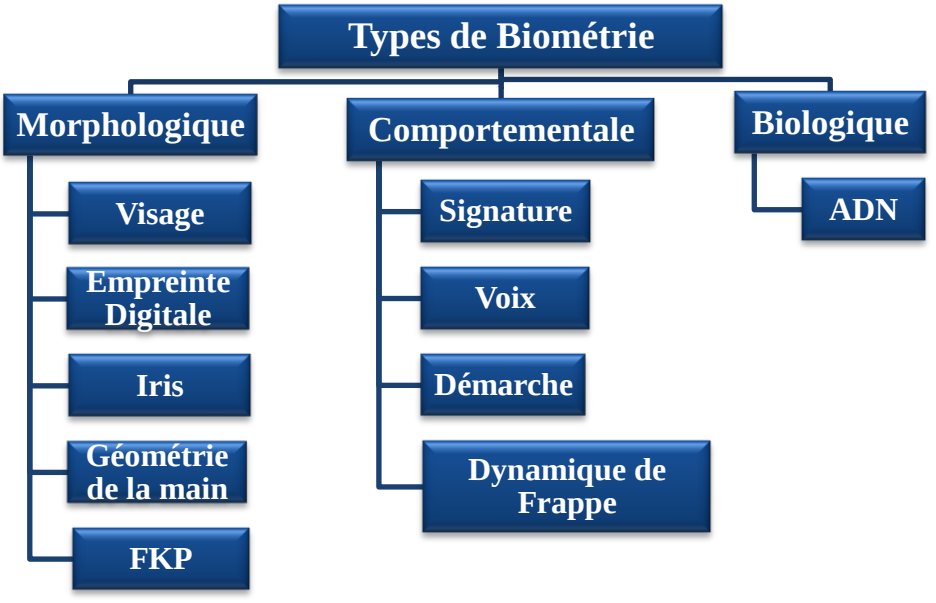

Figure I.1 : Structure des Types de Modalités Biométries

I.4.1 Modalités Morphologiques .

a) La Forme du visage

Le visage est la biométrie la plus commune et la plus populaire. Elle reste la plus acceptable puisqu'elle correspond à ce que les humains utilisent dans l'interaction visuelle. Les caractéristiques jugées significatives pour la reconnaissance du visage sont : les yeux , la bouche et la tour du visage. Utilise des caractéristiques faciales distinctes pour créer une autorisation , ces caractéristiques comprennent les contours supérieurs de l'orbite oculaire, les zones autour des pommettes, les côtés de la bouche et l'emplacement du nez et des yeux.

Les systèmes traditionnels utilisent des algorithmes pour identifier les caractéristiques faciales par des points de repère et comparer la taille ou la forme relative . des yeux, du nez , des pommettes et de la mâchoire, mais la reconnaissance tridimensionnelle améliore la précision en utilisant des capteurs tridimensionnels pour reconnaître les caractéristiques

faciales distinctes.

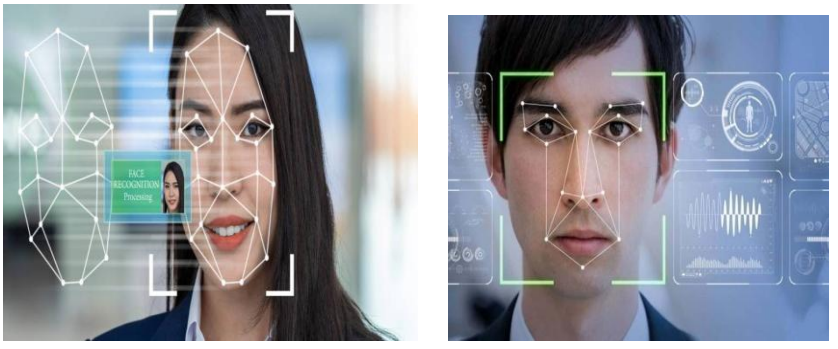

Figure I.2: trait biométrique :visage

b) Les empreintes digitales

Considéré la méthode d'identification de la personne la plus efficace et la plus populaire. Les empreintes digitales sont composées de lignes localement parallèles présentant des points singuliers (minuties) et constituent un motif unique, universel et permanent [3].
minutie prétendaient être uniques à chaque doigt; c'est la collection de points de minutie dans une empreinte digitale qui est principalement utilisée pour faire correspondre deux empreintes digitales.

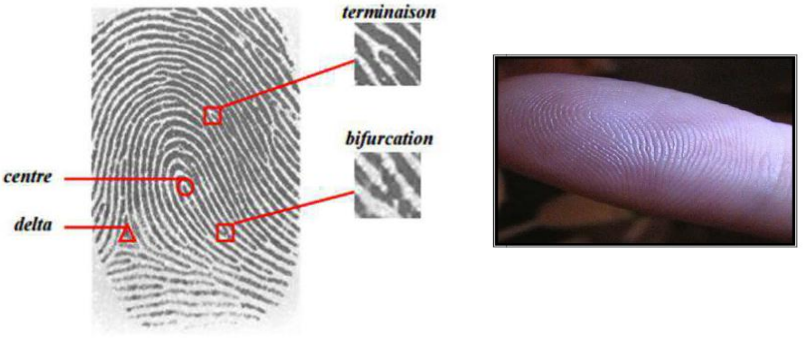

Figure I.3 : trait biométrique : Le empreinte digitale

c) L'iris

Elle est considérée comme la modalité la plus précise pour l 'identification et l'authentification [4]. Son seul inconvénient est son coût assez élevé, ce qui la rend pas autant répondu pour des applications quotidiennes. Alors, son utilisation s'est limitée dans des endroits où la sécurité est primordiale et même critique. La reconnaissance par l'iris [1] est utilisée aussi dans le secteur financier pour les employés et les clients, dans les

hôpitaux et dans les grands aéroports. Une personne voulant s'identifier place son œil à quelques centimètres du capteur et l'image de l'iris est prise par une caméra. Ensuite, les caractéristiques sont extraites de l'image de l'iris et comparées à celles enregistrées dans la base de données.

Figure I.4 : trait biométrique : Iris

d) La géométrie de la main

Chaque individu à sa propre forme de la main. Les paumes des mains humaines contiennent un motif de crêtes et de vallées, tout comme les empreintes digitales [5] .La zone de la paume est beaucoup plus grande que la zone d'un doigt et par conséquent les empreintes de paume devraient être encore plus distinctives que les empreintes digitales .On peut l'acquérir en utilisant un scanner spécialisé. La longueur des doigts, leur épaisseur et leur position relative sont des paramètres qui sont extraits de l'image et comparés à ceux existant dans une base de données. Néanmoins, cette biométrie est sujette à certaines modifications qui sont dues au vieillissement .

Les systèmes biométriques utilisant la forme de la main sont simples à mettre en œuvre, et sont très bien acceptée par les utilisateurs.

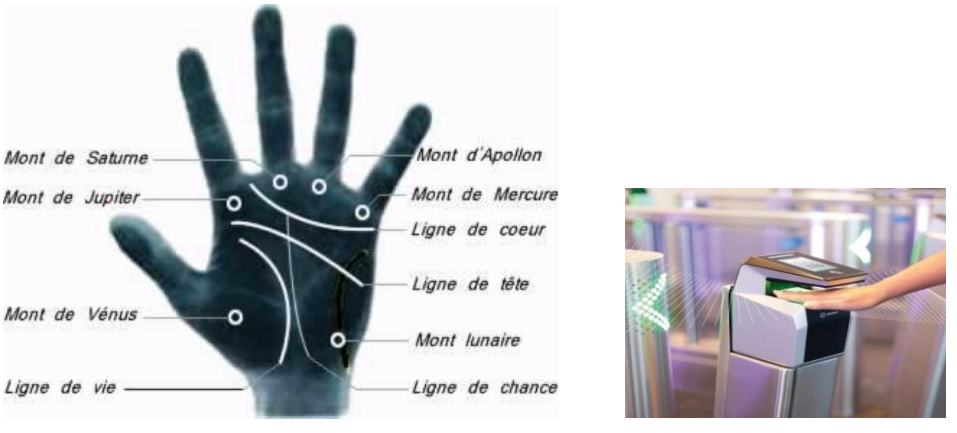

Figure I.5: trait biométrique : la main

e) Empreintes des articulation des doigts (FKP :Fingir Knuckle print)

C'est la technologie biométrique basée sur la surface arriére de doigt ,elle contient des caractéristiqes distinctives, telles que les lignes pricipales, les lignes secondaires et les crétes, qui peuvent étre extraites à partir des images à basse résolution .La main contient plusieurs doigts, pour cela , il faut conserver les information à chaque doigt pour une reconnaissance précise dans le domaine d'identification [6] .

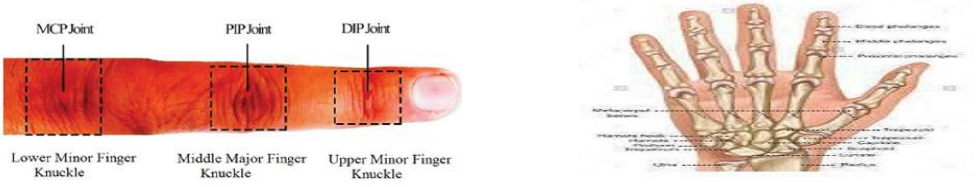

Figure I.6 : images de Empreintes des articulation des doigts

I.4.2 Modalités Comportementales

a) La dynamique de 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. Il existe deux approches pour vérifier la signature statique et dynamique. Dans la vérification de signature statique, seules les formes géométriques de la signature sont utilisées pour authentifier une personne. Dans cette approche, en règle générale, la signature est normalisée à une taille connue ensuite décomposée en éléments simples.

La forme et les relations de ses éléments sont utilisées comme caractéristiques d'identification. Quant à la deuxième approche de la vérification de signature elle utilise ,en plus de la forme géométrique, les caractéristiques dynamiques telles que l'accélération, la vitesse et les profils de trajectoire de la signature. Il est à noter que la signature est une physiques et émotionnelles de la personne[3].

Figure I.7: trait biométrique : Signature

b) Dynamique de Frappe sur un clavier

Il s'agit d'une technique de reconnaissance des personnes basée sur le rythme de frappe qui leur est propre. Elle est appliquée au mot de passe qui devient ainsi beaucoup plus difficile à « imiter » Lors de la mise en place de cette technique, il est demandé à l'utilisateur de saisir son mot de passe un dizaine de fois de suite.

A l'aide d'un algorithme qui exploite le temps d'appui sur chaque touche et le temps entre chaque touche, la dizaine de saisie est « moyennée »pour bâtir un profil de frappe de l'utilisateur qui servira de référence. Aux accès suivants, en suivants le même approche, la saisie du mot de passe donnera sera couplée à un profil de frappe qui sera comparé au profil de référence[7].

Figure I.8 : Système de reconnaissance de frappe sur un clavier

c) La Voix (ou la parole)

Les systèmes de reconnaissance vocale ou vocale identifient une personne en fonction de ses paroles. La génération de la voix humaine implique une combinaison de caractéristiques comportementales et physiologiques. La composante physiologique de la voix dépend de la forme et de la taille des voies vocales, des lèvres, des cavités nasales et de la bouche.

La reconnaissance des haut-parleurs convient parfaitement aux applications comme la télé-banque, mais elle est assez sensible au bruit de fond et à l'usurpation de lecture . Encore une fois, la modalité vocale est principalement utilisée en mode de vérification.

Figure I.9: trait biométrique: la Voix

d) La démarche

Il s'agit de reconnaître un individu par sa façon de marcher et de bouger (vitesse, accélération, mouvements du corps…),en analysant des séquences d'images. La démarche serait en effet étroitement associée à la musculature naturelle et donc très personnelle. Mais des vêtements amples, par exemple, peuvent compromettre une bonne identification.

Figure I.10: Analyse de la démarche

I.4.3 Modalités Biologiques

a) L'ADN

Acide **D**ésoxyribonucléique (ADN) Présent dans les cellules du corps, il est spécifique d'un individu à un autre et permet de l'identifier de manière certaine à partir d'un simple fragment de peau, d'une trace de sang ou goutte de salive.

Actuellement, le temps requis pour une analyse et le coût associé à celle-ci restreignent son utilisation dans des domaines autres que celui de l'identification judiciaire .Cependant, ce procédé biométrique fait l'objet de recherche intensive puisqu'il représente la technologie d'identification par excellence avec une marge d'erreur bien en dessous des autres moyens biométriques.

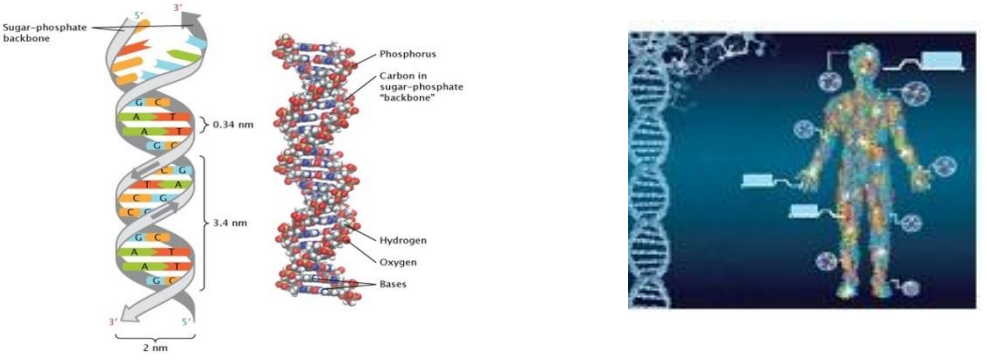

Figure I.11 : trait biométrique : ADN

I.5 Système Biométrique Unimodal

Est un système biométrique à statut unique , peuvent reconnaître des personnes sur la base d'une seule source d'informations vitales, mais ils souffrent de certains problèmes, notamment les données de capteurs alarmantes, l'incapacité de distinguer les caractéristiques biométriques, le manque d'universalité et usurper les attaques [8].

I. 5.1 Composants de Base d'un Système Biométrique

Le système biométrique se compose de quatre (04) éléments importants, à savoir :

- **Interface d'entrée (capteurs)** : Fait au niveau du capteur ,qui est la partie responsable de la conversion des données biologiques humaines sous forme numérique. Par exemple: la photo en cas de systèmes de reconnaissance visage.
- **Base de données Stocke** : La base de données stocke l'échantillon enregistré après son appel pour effectuer une correspondance et en même temps s'authentifier. Pour l'identification, nous pouvons y trouver n'importe quel marqueur d'accès aléatoire (RAM) ou serveur de données .

  pour vérification, nous notons que l'élément de stockage est amovible tel qu'un contact ou une carte utilisée.
- **Unité de traitement** : La partie responsable du traitement est le microprocesseur, ordinateur qui traite les données capturées par les capteurs ou un processeur de signal numérique (DSP).

  Pour traiter un échantillon biométrique, il doit contenir :

  - Un échantillon d'amélioration d'image.
  - Un échantillon de normalisation d'image.
  - Extraction de caractéristiques.
  - Comparaison de l'échantillon biométrique avec tous les échantillons stockés dans la base de données.
- **Interface de sortie :** L'interface de sortie , Il s'agit de la dernière étape où nous

sommes informés de la décision d'approuver ou non.

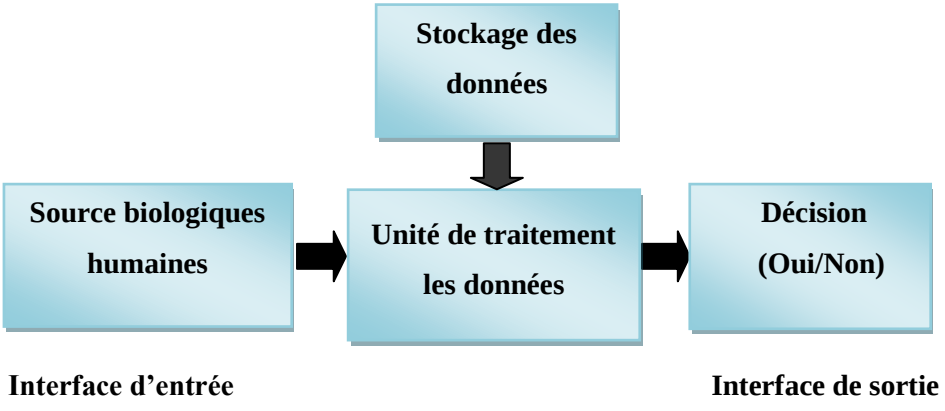

Figure I.12: Composants d'un système biométrique

I.6 Fonctionnement général d'un Système Biométrique

Les systèmes biométriques ont deux modes de fonctionnement, le premier est l'enrôlement, et le second est la reconnaissance.

I.6.1 Mode d'Enrôlement

Pour enregistrer un utilisateur dans un système biométrique pour la première fois, il faut d'abord passer par cette étape.et où une ou plusieurs modalités biométriques sont capturées et enregistrées dans une base de données [9].

Cette inscription peut être accompagnée de l'ajout d'information biographique dans la base de données

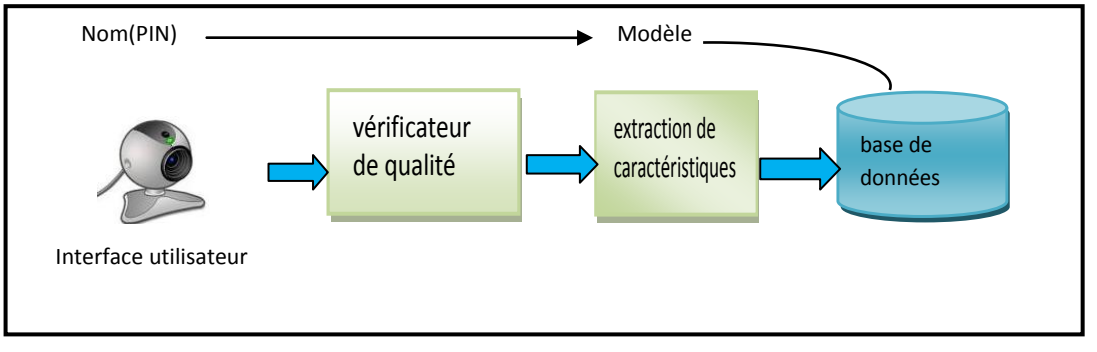

Figure I.13: Enrôlement d'une personne dans le système biométrique

I.6.2 Mode de Reconnaissance

Ce mode est compose de deux modes est vérification (authentification) et l'identification.

a) Mode de vérification (authentification)

Ce processus est chargée de vérifier si l'Identité utilisateur est correct ou non. Pour illustrer ce principe le système récupère les données biométriques et les compare uniquement avec le modèle enregistré correspondant à M.X en entrant le code d'identification personnel (code PIN) et en fournissant une méthode biométrique On parle alors de correspondance (1:1). Ainsi, si l'entrée biométrique de l'utilisateur et le modèle enregistré dans la base de données correspondant à l'identité affirmée possèdent un degré de similitude élevé, l'affirmation est validée et l'utilisateur est considéré comme étant un authentique. Dans le cas contraire, l'affirmation est rejetée et l'utilisateur est considéré comme étant un imposteur. En résumé, un système biométrique opérant en mode vérification répond à la question "Suis-je bien M. X ?".

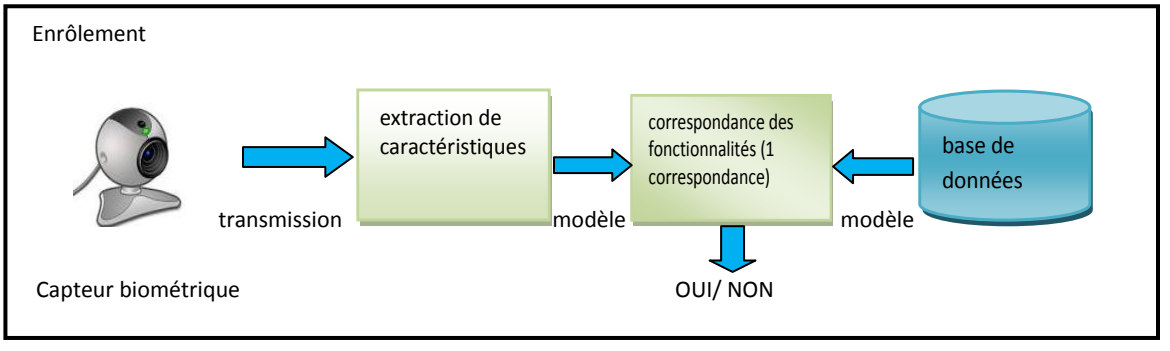

Figure I. 14: Vérification de la personne dans le système biométrique

b) Mode d'identification

Dans ce processus, l'utilisateur ne révèle pas explicitement son identité, mais elle doit être déjà enregistrée dans le système afin qu'elle puisse être identifiée en comparant l'échantillon biométrique de l'individu avec des modèles pour toutes les personnes dans la base de données, puis nous parlons de correspondance (1: N). La sortie du système biologique consiste en l'identité de la personne dont le modèle présente le plus haut degré de similitude avec l'échantillon biométrique fourni en entrée. Après cela, la personne est acceptée si la plus grande similitude entre l'échantillon et tous les modèles est supérieure à une sécurité minimale fixe, ce qui signifie qu'une des personnes inscrites dans le système refuse par ailleurs [9].

Un exemple de système qui fonctionne en mode d'identification est d'entrer dans la salle de renseignement par des personnes spécifiques, chacune soumettant d'abord ses données biologiques au système et selon l'identification de l'utilisateur, le système lui donne le droit d'entrer ou non. En résumé, un système biométrique opérant en mode identification répond à la question "Suis-je bien connu du système ? ".

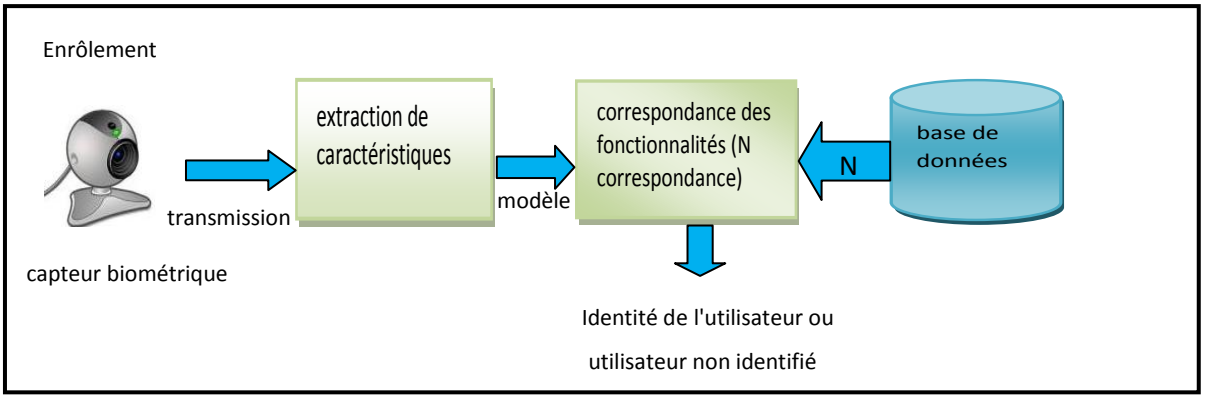

Figure I.15: Identification de la personne dans le système biométrique

I.7 Performances des Systèmes Biométriques

Un système biométrique peut faire deux types d'erreurs. Il peut rejeter un utilisateur légitime et dans ce premier cas on parle de faux rejets (false rejection). Il peut aussi accepter un imposteur et on parle dans ce second cas de fausse acceptation (false acceptante). La performance d'un système se mesure donc à son taux de faux rejet (False Rejection Rate ou FRR) et à son taux de fausse acceptation (False Acceptante Rate ou FAR) [10]

- **Taux de faux rejet (False Rejection Rate ou FRR):** Ce taux représente le pourcentage de personnes censées être reconnues mais qui sont rejetées par le système :

$$\textbf{FRR} = \frac{\text{Nombre de faux rejet}}{\text{Nombre de clients présentes}}$$

- **Taux de fausse acceptation(False Acceptante Rate ou FAR):** Ce taux représente le pourcentage de personnes censées ne pas être reconnues mais qui sont tout de même acceptées par le système :

$$\textbf{FAR} = \frac{\text{Nombre de faux acceptations}}{\text{Nombre d'imposteurs présentes}}$$

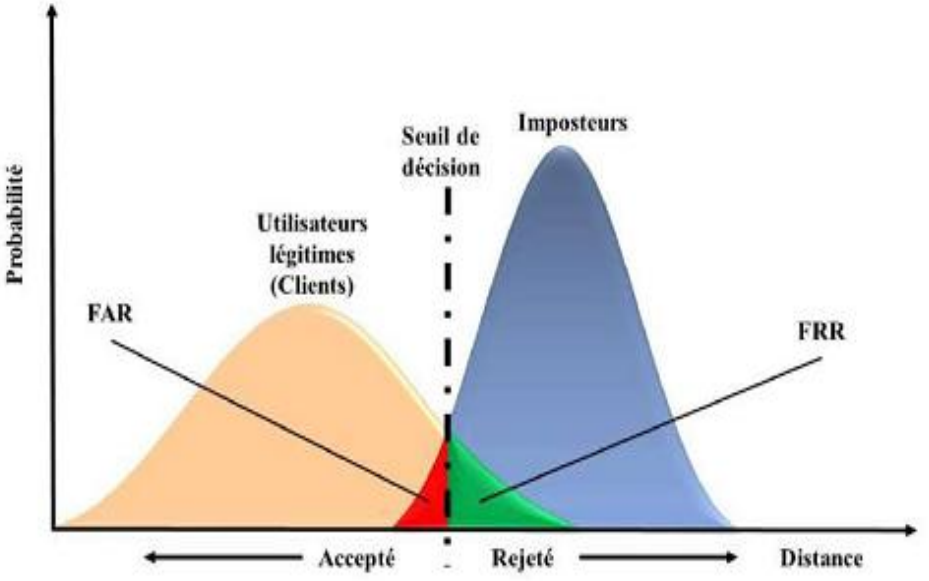

Figure I.16: Illustration du FRR et du FAR

❖ **Taux d'égale erreur(Equal Error Rate ou ERR):** Ce taux calculé à partir des deux premiers critères et constitue un point de mesure de performance courant .

Ce point correspond à l'endroit où FRR = FAR **,** c'est-à-dire est le point d'intersection entre la courbe du taux de fausses acceptations et la courbe du taux de faux rejets .

$$\textbf{ERR} = \frac{\text{Nombre de fausse acceptations+ Nombre de faux rejet}}{\text{Nombre totale d'accès}}$$

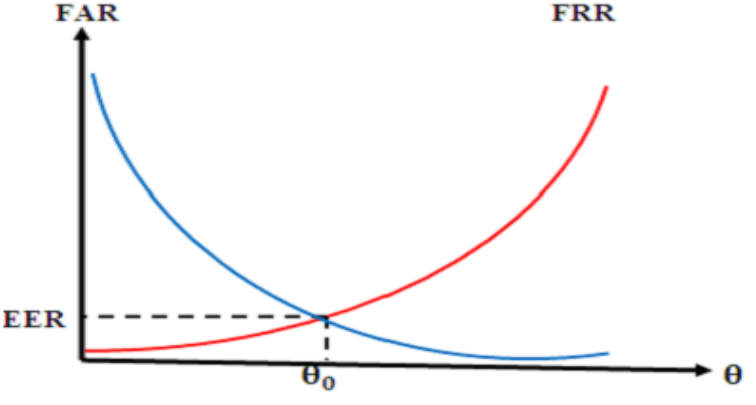

Figure I.17: Graph démonstratif de l'EER

θ0 : Seuil correspondent onle point d'équivalence des erreurs.

Les performances d'un système biométrique peuvent être présentées graphiquement à l'aide de la courbe ROC (Receiver Operating Characteristic), illustrée par à la (Figure. I.18). Cette courbe permet de représenter graphiquement la performance d'un système de vérification pour les différentes valeurs de θ. Le taux d'erreur égal (Equal Error Rate ou EER) correspond au point FAR=FRR, c'est-à-dire graphiquement à l'intersection de la courbe ROC avec la première bissectrice.

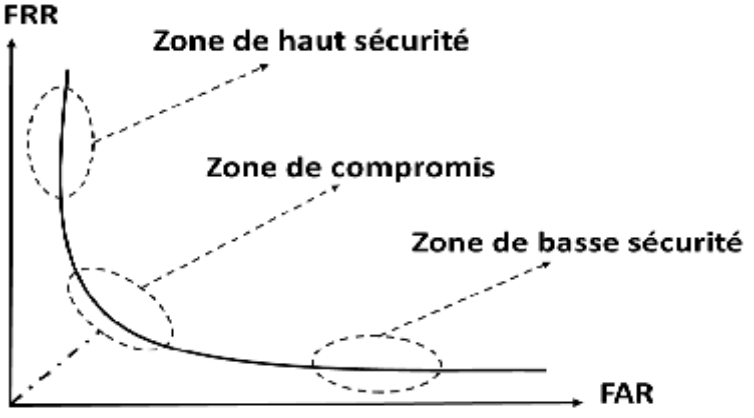

Figure 1.18 : Courbe ROC

En mode identification, il peut être utile de savoir si le bon choix se trouve parmi les N premières réponses du système. On trace alors la courbe ''Cumulative Match Characteristics'' (**CMC**) qui représente la probabilité que le bon choix se trouve parmi les N premiers résultats . Comme l'illustre la Fig1.19[11] .

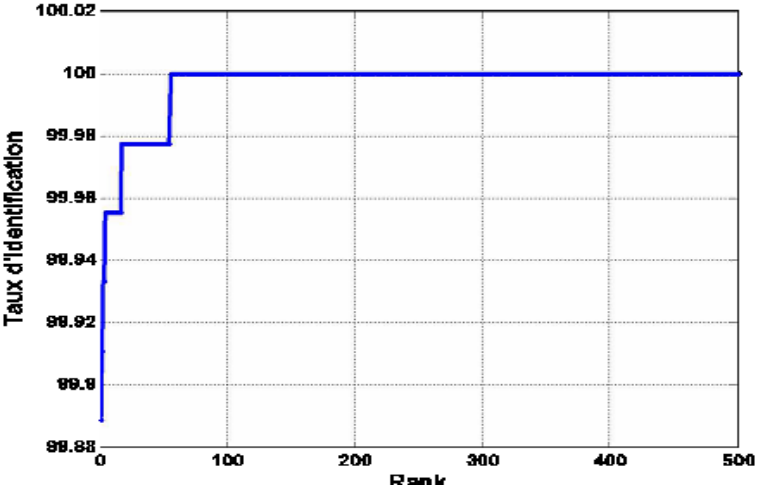

Figure 1.19 : Courbe CMC

I.8 Système Biométrique Multimodal

Système biométrique multimodal est un Système combiner de plusieurs biométrique . L'objectif de la combinaison de plusieurs systèmes est de réduire l es restrictions et d'améliorer les performances de reconnaissance et augmenter la quantité d'informations qui distingue chaque personne en plus de cela nous voulons augmenter le pouvoir de reconnaissance du système. De plus, les systèmes multi-biométriques [12] fournissent des mesures anti-usurpation en rendant difficile pour un intrus d'usurper plusieurs traits biométriques simultanément.

I.8.1 Différents multi-possibles

On peut différencier 5 types de systèmes multimodaux selon les systèmes qu'ils combinent :

1) **Systèmes multi-capteurs :** une seule modalité biométrique est acquise en utilisant un certain nombre de capteurs.
2) **Systèmes multi-instances:** ces systèmes utilisent plusieurs états du même corps. Par exemple, plusieurs cas du visage peuvent être pris du côté gauche et droit pour vérifier l'identité d'un individu.
3) **Systèmes multi-algorithmes:** une seule entrée biométrique est traitée avec différents algorithmes d'extraction. cette multiplicité des algorithmes peut intervenir dans le module d'extraction en considérant plusieurs ensembles de caractéristiques et /ou dans le module de comparaison en utilisant plusieurs algorithmes de comparaison.
4) **Systèmes multi-échantillons:** un seul capteur peut être utilisé pour acquérir plusieurs échantillons du même trait biométrique afin de tenir compte des variations qui peuvent se produire dans le trait, ou pour obtenir une représentation plus complète du trait sous-jacent.
5) **Systèmes multimodaux:** les systèmes multimodaux définissent l'identité sur la base de preuves de multiples caractéristiques biométriques. Par exemple, l'utilisation de fonctionnalités physiquement indépendantes (telles que les empreintes digitales et l'iris) améliore les performances que les fonctionnalités associées (telles que les mouvements

de la voix et des lèvres).

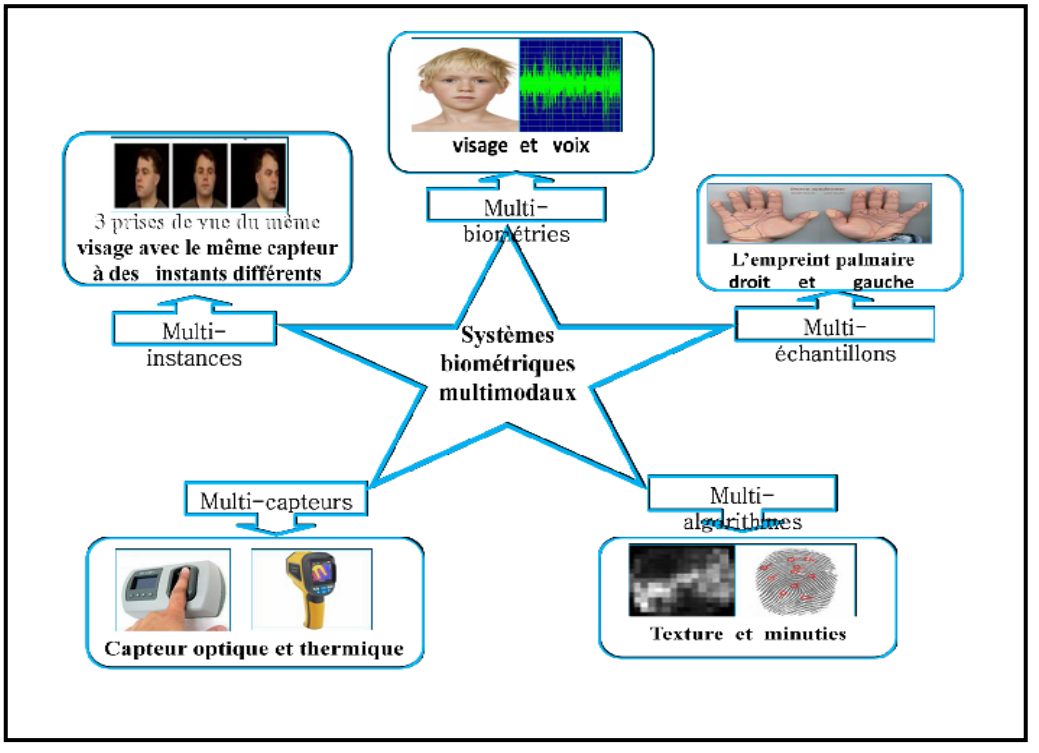

Figure I.20: Les différents systèmes multimodal

I.9 Fusion au Système Biométrique Multimodal

C'est la combinaison d'informations ou de preuves produites par de multiples sources biométriques. Il y'a quatre niveaux différents pour combiner deux ou plusieurs systèmes biométriques ,qui sont les suivants :[13]

- Données,
- Caractéristiques extraites,
- Scores issus du module de comparaison,
- Décisions du module de décision.

I.9.1 Fusion au niveau du capteur (donnée)

Les systèmes biométriques multi capteurs prélèvent le même exemple d'une modalité Biométrique avec deux capteurs distinctement différents [14].Le traitement des échantillons capturés peut se faire avec un ou plusieurs algorithmes. Comme exemple de

ce niveau, on peut citer l'emploi d'une caméra lumière visible et une caméra IRM pour l'identification du visage.

La fusion au niveau du capteur est relativement peu utilisée, car les captures doivent être compatibles entre elles et la correspondance entre les points dans les données brutes doit être connue par avance.

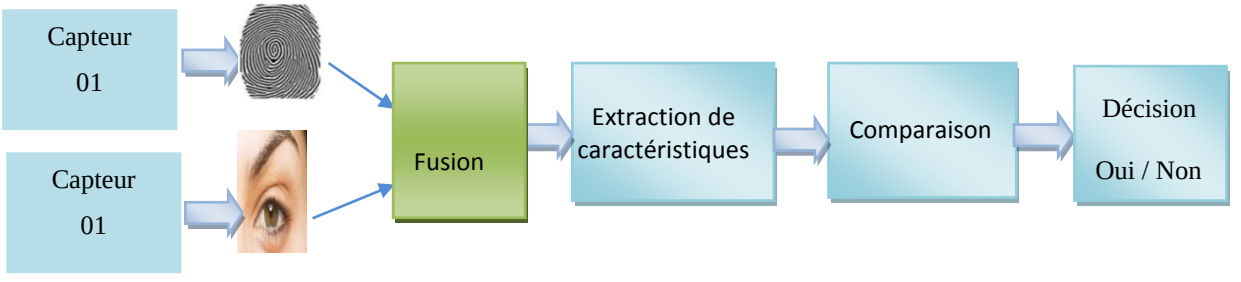

Figure I.21 : Processus de Fusion au niveau du capteur

I.9.2 Fusion au niveau Extraction de caractéristique

La fusion au niveau caractéristique consiste à combiner différents vecteurs de caractéristiques [15], obtenus à partir de l'une des sources suivantes: plusieurs capteurs du même trait biométrique, plusieurs instances du même trait biométrique, plusieurs unités même trait biométrique ou encore plusieurs traits biométriques.

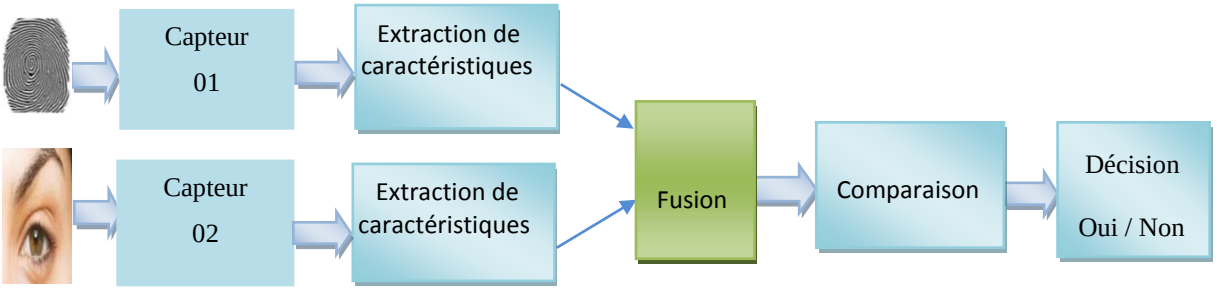

Figure I.22 : Processus de Fusion au niveau Extraction de caractéristique

I.9.3 Fusion au niveau score

Dans ce cas, le système biométrique multimodal combine informations après deux comparaison ou plus . ont montré que cette méthode plus utilisé par rapport autre

méthodes .

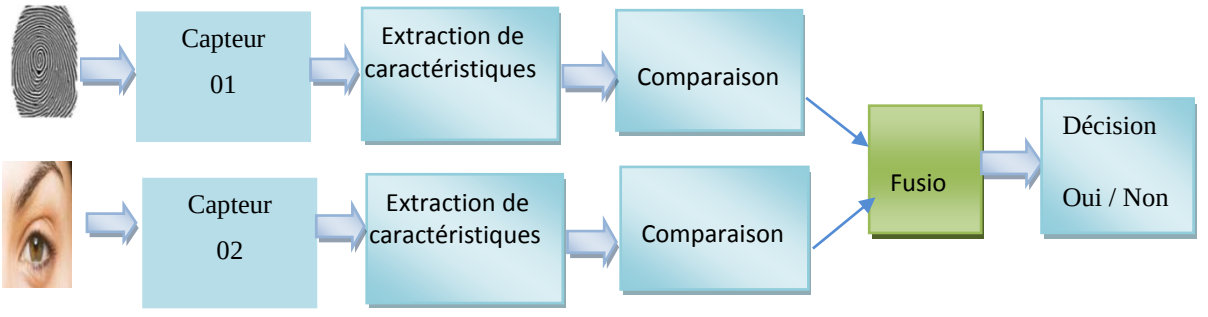

Figure I.23 : Processus de Fusion au niveau score

I.9.4 Fusion au niveau décision

Dans ce cas, les résultats finaux de plusieurs classeurs sont combinés via des technologies telles que La plupart des décisions prises sont similaires.

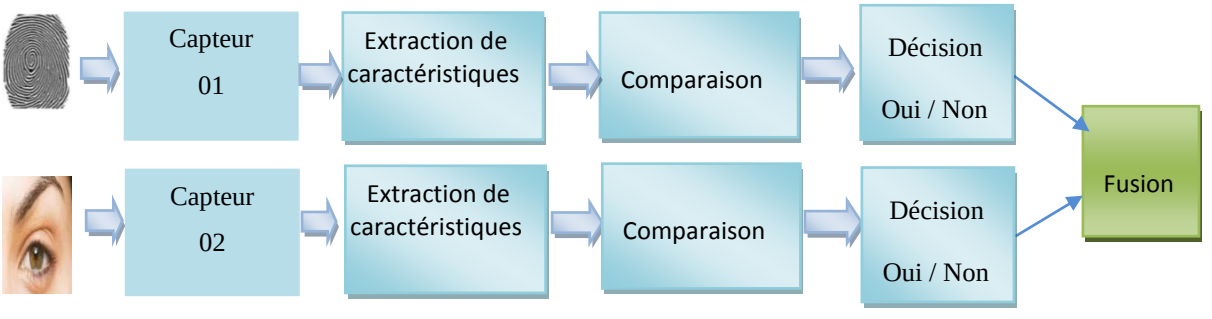

Figure I.24 : Processus de Fusion au niveau décision

I.10 Conclusion

À la fin de ce chapitre, après avoir fourni quelques définitions et concepts liés aux systèmes et méthodes biométriques .

Nous avons découvert un système de biométrie multimodale de processus de fusion, qui est l'une des solutions pour améliorer l'efficacité et réduire les restrictions sur les systèmes biométriques unimodal. Dans deuxième chapitre, nous parlerons de la façon d'extraire les caractéristiques d'une image à l'aide d'un algorithme utilisées dans le but d'extraire des informations biométriques ,ainsi que les méthodes de Réduire ses dimensions.

Chapitre II

Extraction des Caractéristique des images et Réduction de dimension

II.1 Introduction

L'objective de l'étape d'extraction des caractéristiques réduire les dimensions des images de originales tout en préservant et en extrayant les informations importantes codées dans ces images. Un ensemble soigneusement sélectionné de caractéristiques transformera les images afin qu'il devienne plus facile de distinguer entre les classes authentiques et falsifiée, nous avons utilisées dans le but d'extraire des informations biométriques .

Nous intéresserons dans cette étude par les méthode LPQ d'extraction des caractéristiques d'image et techniques de Réduction du dimension et ainsi classification pour modéliser les paramétres extraits d'une modalité d'un individu en basant sur leur caractéristiques communes.

II.2 Images numérique

L'image numérique est un fichier de différentes tailles et formats pouvant être ouvert sur les écrans des appareils numériques tels que les ordinateurs, le plus petit composant de l'image est les pixels .chacun ayant comme caractéristique un niveau de gris ou des couleurs prises à partir de l'emplacement correspondant dans l'image réelle .

La numérisation d'une image est sa conversion de son état analogique en une image numérique représentée par une matrice bidimensionnelle de valeurs numériques f (x, y) comme indiqué sur la figure (II.1), où m et n sont des coordonnées cartésiennes d'un point de l'image et f (x, y) le niveau d'intensité .

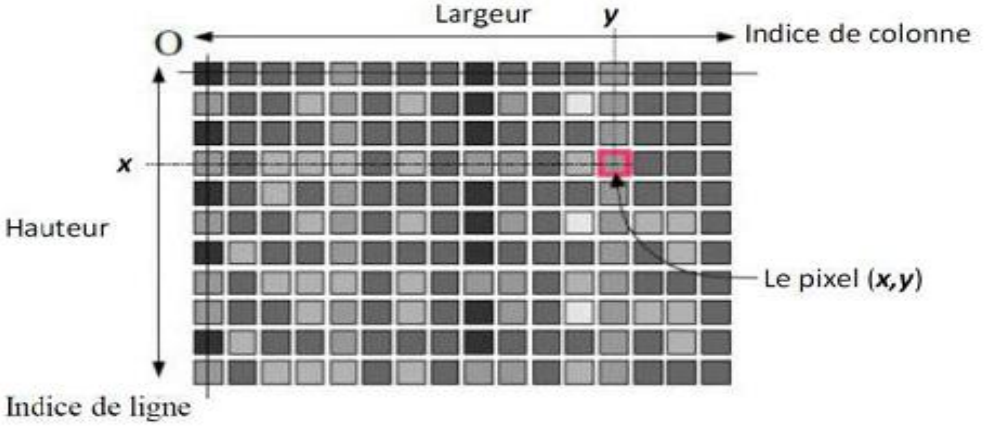

Figure II.1 : Image numérique

II.2.1 Images en niveaux de gris (monochrome)

Le niveau de gris est la valeur de l'intensité lumineuse à un point .La couleur du pixel peut prendre des valeurs allant du noir au blanc en passant par un nombre fini de niveaux intermédiaires .Donc pour représenter les images à niveaux de gris on peut attribuer à chaque pixel de l'image une valeur correspondant à la quantité de lumière renvoyée [16].

Le nombre de niveaux de gris dépend du nombre de bits utilisés pour décrire la "couleur" de chaque pixel de l'image. Plus le nombre est élevé, plus les niveaux possibles sont nombreux .

Figure II.2 : Images en niveaux de gris.

II.3 Extraction des caractéristiques

La méthode d'extraction de caractéristiques est une étape très importante dans la conception d'un système d'identification . Cette étape représente le cœur du système d'identification; Les informations sont extraites de l'image qui sera sauvegardée en mémoire pour une utilisation ultérieure dans la phase de comparaison. L'extraction des caractéristiques utilise plusieurs méthodes, parmi lesquelles nous citons LPQ.

II.4 Quantification de phase Locale (LPQ)

L'informations de LPQ peut être extraite en utilisant la transformée discrète de Fourrier à fenêtre à deux dimensions (2DWFT).

$$Fu(x) = \sum h(m-x)f(m)e^{-j\pi u}\, T\ m = Eu\ T f x \quad ,m \epsilon Nx \qquad (II.1)$$

Où $Eu\ T$, de taille = 1 ×M², est un vecteur de base de 2DWFT avec la fréquence u, et fx, taille = M² × N, est un vecteur contenant les valeurs des pixels d'image dans Nx à chaque position x. La fonction fenêtre, h (x) est une fonction rectangulaire.

La transformation est calculée à quatre valeurs de la fréquence, u = [u0, u1, u2, u3] où u0= $[a, 0]^T$, u1= $[0, a]^T$, u2 = $[a, a]^T$ et u3 = $[a, -a]^T$. La valeur a est la plus haute fréquence scalaire pour laquelle $\boldsymbol{Hui} > 0$. Ainsi, seuls quatre fonctions complexes comme un banc de filtres sont nécessaires pour produire huit images résultantes, composées de 4 images de la partie réelle et 4 images de la partie imaginaire de la transformée. Chaque pixel de l'image complexe résultant peut être codé en une valeur binaire représentée dans l'équation (II.2) en appliquant (the quadrant bit coding). [17]

$$Bui^{Re}(x) = \begin{cases} 1 \ Si \ Fui^{Re}(x) > 0 \\ 0 \ Si \ Fui^{Re}(x) \leq 0 \end{cases} \qquad Bui^{Im}(x) = \begin{cases} 1 \ Si \ Fui^{Im}(x) > 0 \\ 0 \ Si \ Fui^{Im}(x) \leq 0 \end{cases} \qquad (II.2)$$

Ce procédé de codage attribue deux bits pour chaque pixel pour représenter le quadrant dans lequel se trouve l'angle de phase [18].

En fait, il fournit également la quantification de la fonction de phase de Fourier. En général, LPQ est une chaîne binaire, présentée dans l'expression (II.3), obtenue pour chaque pixel par la concaténation des codes quadrant bits réelles et imaginaires des huit coefficients de Fourier de ui .

$$LPQ(x) = [B_{u0}^{Re}(x), B_{u0}^{Im}(x), \ldots B_{u3}^{Re}(x), B_{u3}^{Im}(x)] \qquad (II.3)$$

La chaîne binaire est convertie en nombre décimal par l'expression (II.4)pour produire une étiquette de LPQ. La figure II.2 résume l'ensemble de ces étapes.

$$LPQ(x) = B_{u0}^{Re}(x) + B_{u0}^{Im}(x) \times 2^1 + \ldots + B_{u3}^{Re}(x) \times 2^{K-1} + B_{u3}^{Im}(x) \times 2^k \qquad (II.4)$$

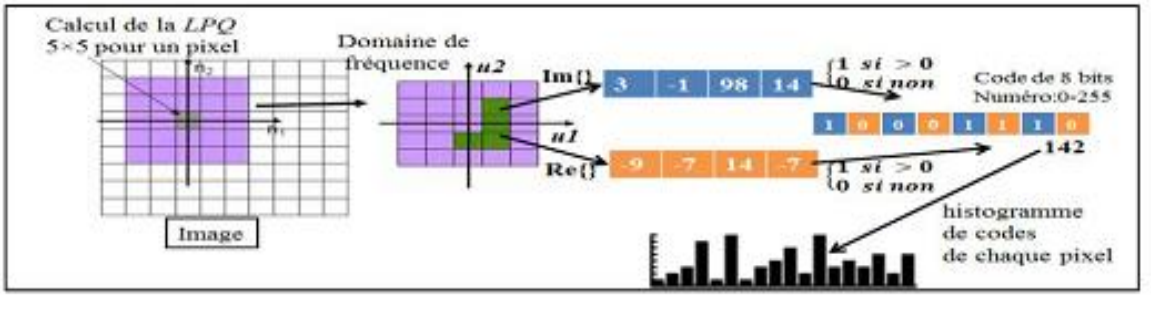

Figure II.3: Organigramme de l'ensemble des étapes nécessaire à la construction du descripteur LPQ

II.4.1 Quantification de phase locale Multi-blocs (MB-LPQ)

Nous avons divisé l'image acquissent régions d'intérêt (région of inter est :ROI) en (n x n) sous-blocs et on applique la méthode de LPQ sur chaque sous-bloc n = 1,2 ,3,4 et 5 . Cette méthode est appelée LPQ Multi-Blocs.

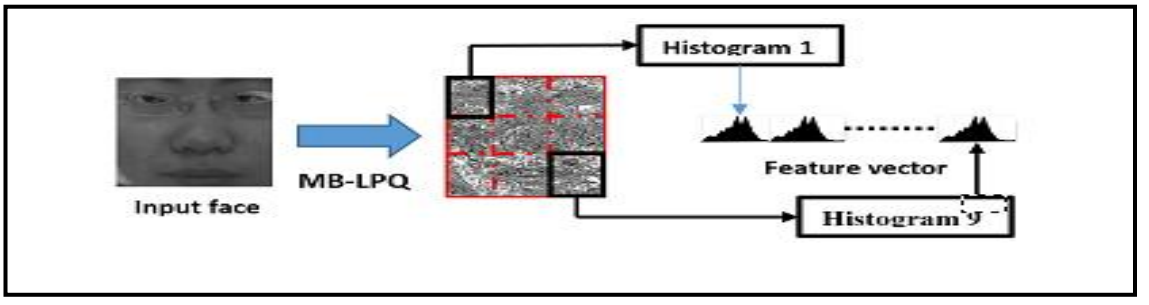

Figure II.4: Exemple sur d'application de la méthode MB-LPQ

II.4.2Quantification de phase locale à plusieurs niveaux(Multi Level: ML-LPQ)

L'idée principale de ML-LPQ est d'extraire des caractéristiques de différentes (MB-LPQ) divisions, puis les combiner. En d'autres termes , l'extraction de caractéristiques de l'ensemble de l'image, puis en divisant l'image en n^2 sous-blocs et extraire les caractéristiques de chaque sous-blocs et ainsi de suite jusqu'à ce qu'on atteigne le niveau prévu. Le résultat final de ML-LPQ est $1^2+2^2+3^2+\ldots\ldots+n^2$ histogrammes [19]. Nous combinons ces histogrammes pour obtenir le vecteur de caractéristiques. Donc, nous avons maintenant besoin d'expliquer comment utiliser les histogrammes image parce que nos bases de données ne contiennent que l'image. Chaque image est divisé en trames multiples et sur chaque cadre de notre approche est utilisée et la fonctionnalité dans termes d'histogramme est extrait, puis la moyenne de tous les histogrammes est calculé. Enfin la sélection de score pêcheur [20] est utilisé sur la dire de tous les histogrammes pour réduire le banc histogramme Figure II.5.

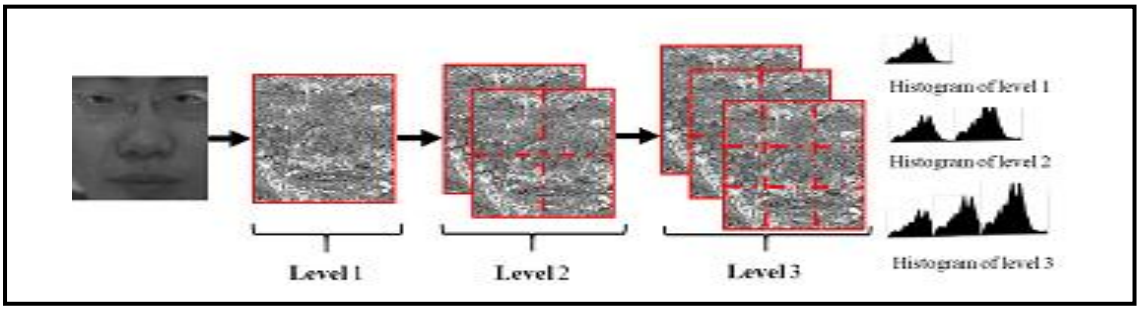

Figure II.5: Exemple d'approche ML-LPQ d'extraction de caractéristiques avec (n=3 niveaux)

II.5 Réduction de dimension

La réduction de dimension est la technique de conversion de l'ensemble de données de la matrice X en un nouvel ensemble de la matrice Y de dimension d (où d est la dimension intrinsèque située dans un espace de plus grande dimension D c'est-à-dire d <D), tout en conservant autant que possible les informations de base de l'ensemble de départ.

II.5.1 Analyse de Composent principal (ACP)

L'algorithme ACP, en anglais PCA (Principal Component Analysis) est né des travaux de MA. Turk et AP. Pentland au MIT Media Lab , en 1991 [3] .

ACP est une méthode mathématique qui peut être utilisée pour simplifier un ensemble de données, en réduisant sa dimension [21], Elle est utilisée pour représenter efficacement les compression d'image.

L'ACP est méthode d'analyse de données multi variées les plus utilisées, un des résultats les plus importants de l'algèbre linéaire appliquée et peut-être son utilisation la plus courante est qu'on l'utilise comme la première étape en essayant de analyser de grands ensembles de données, qui consiste à transformer nombreuses variables en quelques variables (les composants principaux), ou axes principaux. ACP permet explorer des jeux de données multidimensionnels constitués de variables quantitatives .elle est largement utilisée en biométrique que bien d'autres domaines.

Les étapes principales pour calculer la matrice de projection mathématique(UPCA) de PCA sont:

- Chaque image est représentée par un vecteur de taille *N*.

$$X^{i} = [X^{i}_{1}, X^{i}_{2}, \ldots\ldots X^{i}_{N}] \qquad (II.5)$$

- Toutes les images sont centrées en soustrayant l'image moyenne de chaque vecteur image.

$$\overline{X}^{i} = X^{i} - m\ ,\ \ m = \frac{1}{P}\sum_{i=1}^{P} \mathrm{Xi} \qquad (II.6)$$

m: moyenne de toutes les images d'apprentissage.

Ces vecteurs sont combinés, côte-à-côte, pour créer une matrice $\overline{X}$ de données d'apprentissage de taille N × P (où P est le nombre d'images d'apprentissage, N la taille de

la vectrice image). Le calcul de la matrice de covariance (C) qui est définie par la formule:

$$C = \overline{X}\,\overline{\mathrm{Xi}} \qquad (II.7)$$

On calcule ensuite les vecteurs propres V et les valeurs propres D de la matrice C. Les valeurs propres de la matrice C représentent le taux de variation le long de l'axe du vecteur propre associé. La matrice de transformation de PCA est donc les R premiers vecteurs propres ordonnés par ordre décroissant des valeurs propres correspondantes (UPCA) [22] .

II.5.2 Whitening ACP (WACP)

Sur la base de la méthode ACP proposée, il s'agit d'un algorithme de réduction dimensionnelle qui peut être utilisé pour accélérer l'algorithme d'apprentissage des fonctionnalités. Nous dérivons l'algorithme de whitening ACP car il s'agit d'une étape de pré-traitement importante pour de nombreux algorithmes. Supposons, par exemple, que nous formions notre modèle sur des images. Les entrées initiales sont redondantes, car les valeurs de pixels adjacents sont fortement corrélées. Le but du whitaning est de réduire la redondance, c'est-à-dire de rendre les entrées moins redondantes, Plus formellement .

II.6 Classification

La classification C'est un propos de modèle les paramètres extraits et discriminantes d'un individu ou d'un plusieurs individus ayant des similarités nous les mettons dans la même classe, Distinguer deux classes ou plus par séparation linéaire . Le classifieur se présente sous la forme d'une combinaison linéaire des variables. Donc, il est utilisé pour la machine vectorielle de support SVM.

II.6.1 Support Vector Machine (SVM)

SVM c'est une technique de discrimination et de classification. L'idée originale des SVMs est basée sur l'utilisation de fonctions noyau kernel, qui permettent une séparation optimale des points du plan en différentes catégories. La méthode fait appel à un ensemble de données d'apprentissage, qui permet d'établir un hyperplan séparant au mieux les points.

SVM a été initialement conçu pour résoudre des problèmes de second ordre, mais après diligence et étude la généralisation peut être faite dans le cas multi-classes en utilisant trois méthodes différentes. La première méthode et la deuxième méthode (une contre toutes,

une contre une) dépendent du doublement des couches binaires de classeur tandis que la dernière propose (Méthode globale) Précision globale [23].

II.7 Conclusion

Dans ce chapitre, après avoir fourni une définition d'image et l'utilisation de l'algorithme LPQ pour extraire les caractéristiques d'une image, nous avons conclu que cet algorithme extrait des informations biométriques qui sont coordonnées afin qu'il soit facile de distinguer entre les classes d'origine et les classes forgées. et pour réduire les dimensions de l'image, nous avons utilisé la méthode ACP et sur cette base est venue l'étape de prétraitement requise pour certains algorithmes appelée Bleaching (WACP).Les différentes classes ont été classées et distinguées à l'aide de la technique SVM.

Chapitre III

Résultats expérimentaux

et discussions

III.1 Introduction

L'authentification et la vérification des FKP possèdent plusieurs avantages sur les autres technologies biométriques: elle est naturelle, non intrusive et facile à utiliser. Les systèmes biométriques uni-modaux permettent de reconnaître une personne en utilisant une seule modalité biométrique, mais ne peuvent pas garantir avec certitude une bonne authentification. Alors la solution est la mise en place de systèmes biométriques multimodaux obtenus en fusionnant plusieurs systèmes de reconnaissance de FKP, c'est ce que nous allons vérifier dans une expérience que nous allons faire. Dans ce présent travail, nous familiariser avec le système que nous allons utiliser pour reconnaissance des images FKP , après avoir dressé un état de l'art de la reconnaissance de FKP Tout d'abord ,et étudié plusieurs méthodes pour sélectionner les meilleurs systèmes d'authentification de FKP. Ensuite, nous présentons les multi-échantillons des FKP (l'index gauche avec médian gauche ,puis index droit avec médian droit , puis tous les quatre doigts) et la multi cela se fait à l'aide d'un algorithme ML-LPQ et propriété WPCA afin de connaître les performances du système en calculant Le taux d'erreur égal (EER) et Rang de reconnaissance parfaite (ROR). enfin on va comparer les différentes méthodes de combinaison de score pour choisir la meilleur parmi eux .

III.2 Système de Reconnaissance FKP

Les systèmes de reconnaissance des personnes par FKP est un nouveau type de systèmes biométriques qui peut discriminer différents individus en fonction des lignes et des textures existantes dans la surface du doigt externe [24].

Pour que des personnes soit reconnue par FKP, nous doit passer par deux étapes:

- **l'identification FKP:** il est nécessaire d'avoir des images de référence, sous la forme d'une base de données de FKP de toutes les personnes connues par le système. A chaque image est associé un vecteur de caractéristiques, ces caractéristiques invariantes pour une même personne, et différentes d'une personne à l'autre, donc deux personnes ne peuvent pas posséder exactement la même caractéristique.
- **La vérification FKP:** c'est une comparer le vecteur de caractéristiques du FKP à reconnaitre avec celui de chacun des FKP de la base . Ceci permet de retrouver la personne ayant le FKP le plus ressemblant, qui est celui dont le vecteur est le plus similaire.

Le système d'authentification personnelle FKP se compose de deux unités, la première d'acquisition des images et la seconde traitement des images: Le module d'acquisition des images FKPs est**(**composé d'un support de doigt, d'une source de lumière LED sous forme d'un anneau, d'une lentille, d'une caméra CCD et d'une carte d'acquisition**)**.L'image FKP capturé est entrée dans le module de traitement de images **(**qui comprend trois étapes de base: ROI (région d'intérêt)extraction, extraction des caractéristiques et codage, et l'appariement ''maching''**)**.

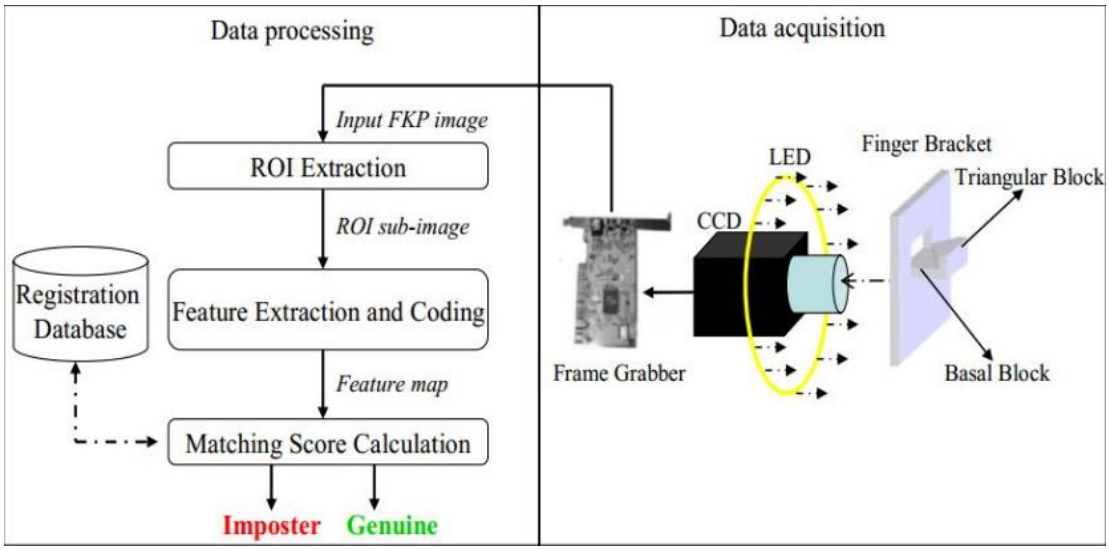

Figure III.1 : Structure du système d'authentification personnelle d'FKP

Figure III.2 montre le dispositif d'acquisition d'image FKP dont la taille globale est 160mm × 125mm × 100mm[25].

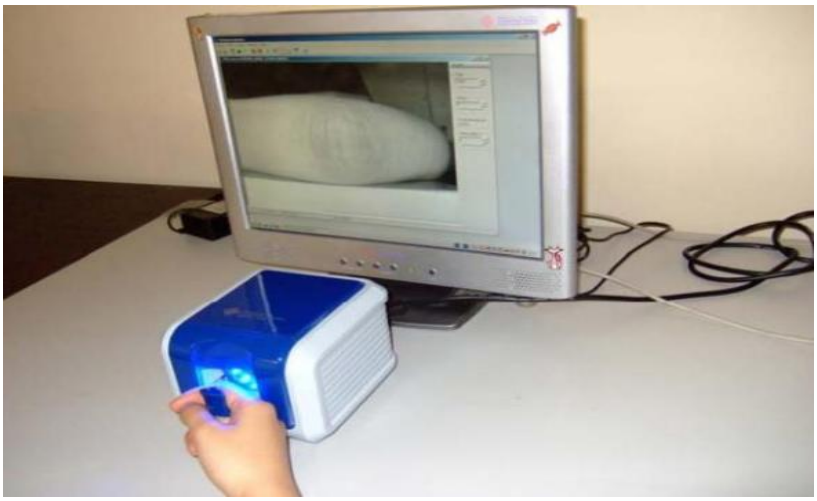

Figure III.2: Dispositif d'acquisition d'image FKP

III.2.1 La Base de données FKP

Pour évaluer le système d'authentification personnelle proposé pour FKP. les images Existant la base de données sont capturées à l'aide d'un appareil d'acquisition d'images FKP. les bénévoles étaient des étudiants et des enseignants de l'Université polytechnique de Hong Kong et à Harbin Institute of Technology (PolyU). La base de données PolyU-FKP contient à 165 personnes (125 mâles et 40 femelles). Parmi eux 143 personnes ayant l'âge compris entre 20 et 30 ans et les autres d'âge compris entre 30 et 50 ans.

Nous avons recueilli les échantillons en deux séances distinctes, Prenez Six images de pour quatre doigts (l'index gauche LIF en anglais «Left Index Fingers», médian gauche LMF en anglais «Left Middle Fingers», index droit RIF en anglais «Right Index Fingers» et médian droit RMF en anglais «Right Middle Fingers»). Par conséquent, 48 des images différentes de FKP pour chaque personne étaient recueillies auprès, Au total, la base de données contient 7920 images différentes.

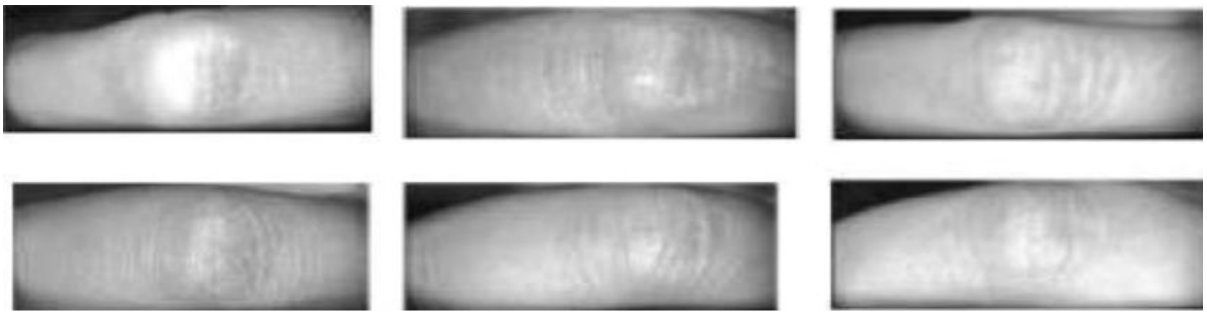

Figure III.3: Exemple d'images de FKPs

III.2.1.1 Séparation de la base de données

pour développer une application de reconnaissance de FKP, il est nécessaire de disposer de deux bases de données : une base pour effectuer l'apprentissage et l'autre pour tester les techniques et déterminer leurs performances, mais Il n'y a pas de règles pour déterminer ce partage de manière quantitatif. Il résulte souvent d'un compromis tenant compte du nombre de données dont on dispose et du temps pour effectuer l'apprentissage. dans les séries de test , nous séparons la base de données en deux parties principales:

- **Images apprentissages:** La première, la cinquième et la neuvième image de chaque personne servent pour la phase d'apprentissage.

- **Images Tests:** Les 9 images restantes de chaque individu nous ont servi pour la Réalisation des différents tests.

III.3 Expérimentations sur la FKP

III.3.1 Protocole Experimentale

Des exemples d'images pour chaque sujet ont été recueillis en deux sessions. Dans nos expériences, nous avons pris des images collectées dans la première session comme l'ensemble de l'apprentissage et des images recueillies lors de la deuxième session, comme l'ensemble de test. Par conséquent, il y avait 660 (165 × 4) classes 3960 et 1980 (660 × 3) images dans l'apprentissage. Pour obtenir des résultats statistiques, chaque image de l'ensemble test a été jumelé à toutes les images dans l'ensemble d'apprentissage. Si les deux images sont de la même classe, la mise en correspondance entre eux a été comptée comme un véritable appariement; sinon il a été considéré comme une adaptation d'imposteur.

Le taux d'erreur égal (EER), qui est le point où le taux de fausses acceptations (FAR) est égal au taux de faux rejet (FRR), est utilisé pour évaluer la précision de vérification. Par ailleurs, la courbe caractéristique de fonctionnement récepteur (ROC), qui est un terrain de FRR contre FAR pour tous les seuils possibles, obtenus par l'utilisation de chaque méthode de codage évalué seront fournis.

Pour évaluer la performance de notre système, on procède aux expérimentations suivantes :

Les tests sur la base FKP ont été réalisés en quatre expérimentations :

1-Première expérimentation: Nous avons étudié l'effet du LPQ sur le taux de détermination du système biométrique, et nous sélectionnons le meilleur paramètre du ML-LPQ pour le majeur gauche. Les résultats des caractéristiques obtenues à partir du blanchiment (Whitening en anglais) de l'analyse des composants principaux WPCA .

2- Deuxième expérimentation: Dans cette étape, nous utiliserons l'algorithme ML-LPQ. Ces algorithmes sont parmi les meilleurs descripteurs de tissu actuellement pour extraire des caractéristiques de l'empreinte commune (LIF, LMF, RIF, RMF); Nous avons fait de nombreuses expériences pour savoir quel doigt fonctionne le mieux.

3-Troisième expérimentation: Nous avons combiné quatre échantillons d'empreintes digitales différents pour augmenter les performances du système d'identification (l'index gauche LIF «Left Index Fingers» avec médian gauche LMF «Left Middle Fingers»,puis index droit RIF «Right Index Fingers» avec médian droit RMF «Right Middle Fingers» puis tous les quatre doigts)

4- Quatrième expérimentation: Dans cette étape, nous utiliserons les différentes règles de fusion: (Sum, Mul, Min, Max, W Sum, W Mu) pour la fusion obtenue à partir de la somme des doigts.

III.4 Résultats et Discussion

Plusieurs tests ont été effectués et les résultats de sont illustrés dans les tableaux suivent :

❖ Les Résultats de Système Unimodal

Table III.1: Performance de système unimodal par ML-LPQ pour le doigt milieu gauche

Nombre de niveau	EER	ROR
1	0.202	99.19
2	0.067	99.46
3	0.067	99.59
4	**0.067**	**99.73**
5	0.067	99.73

À travers le tableau, nous remarquons que la valeur de EER à nombre de niveau = 4 est la plus faible. En outre, le rapport ROR à nombre de niveau = 4 est le plus élevé, donc nombre de niveau = 4 est le meilleur.

Table III.2: Performance de système unimodal par ML-LPQ et WPCA

Nous prenons ce résultat et y appliquons la méthode WPCA:

Taille de vector WPCA	EER	ROR
50	0.336	98.18
100	0.206	99.12
150	0.062	99.32
200	0.067	99.66
250	0.067	99.73

300	0.067	99.73
350	0.066	99.79
400	**0.027**	**99.79**
450	0.032	99.86
500	0.032	99.86

À travers le tableau, on constate que la taille de vecteur WPCA = 400 est la meilleure, car la valeur EER est la plus faible et le ratio ROR est le plus élevé.

Table III.3: Performance de système unimodal

	Ensemble ouverte		**Ensemble fermé**	
	EER	T_0	ROR	RPR
LIF	0.027	0.6724	99.79	09
LMF	$6.65\ 10^{-3}$	0.8180	99.93	09
RIF	0.035	0.6095	99.73	11
RMF	0.067	0.5186	99.93	47

À travers le tableau, nous notons que la valeur EER du le doigt milieu gauche (LMF) est la plus basse et la meilleure. Nous notons également que le rapport ROR du le doigt milieu gauche (LMF) et du le doigt milieu droit (RMF) est le plus élevé, mais le LMF nous l'avons obtenu du rang 09 et le RMF nous l'avons obtenu du rang 47 Donc LMF est le meilleur.

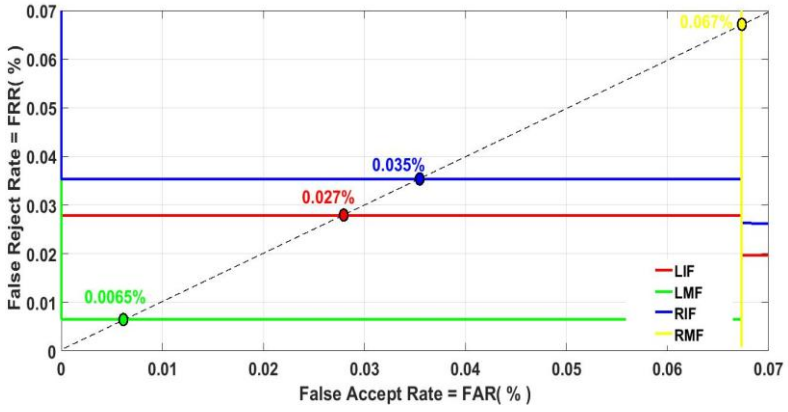

Figure III.4: Courbe ROC de système unimodal

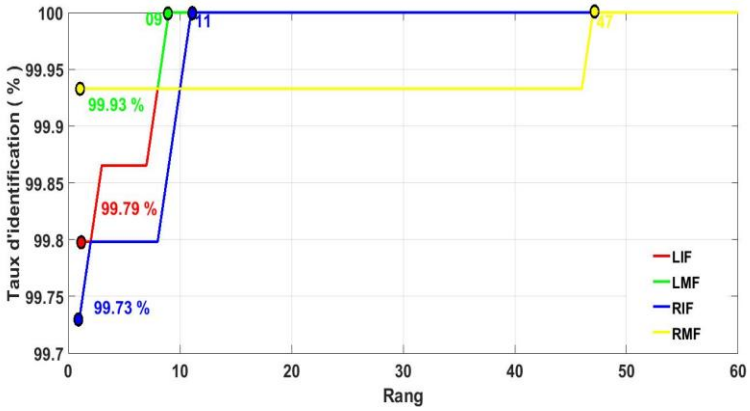

Figure III.5 : Courbe CMC de système unimodal

❖ Les Résultats de Système Multimodal

Dans cette étape, nous combinons: le doigt index droit (RIF)avec du doigt milieu droit(RMF), et le doigt index gauche(LIF) avec le doigt milieu gauche(LMF) . Ensuite, nous rassemblons les quatre doigts ensemble.

Table III.4: Performance de système Multimodal

	Ensemble ouverte		**Ensemble fermé**	
	EER	T_0	ROR	RPR
LIF+LMF	0.00	0.693	100	01
RIF+RMF	0.00	0.703	100	01
ALL Finger	0.00	0.690	100	01

A travers le tableau, on note que pour toutes les étapes de combinaison a on obtient EER =0 et ROR = 100% et dès le premier ordre .Donc ce système est un système optimal.

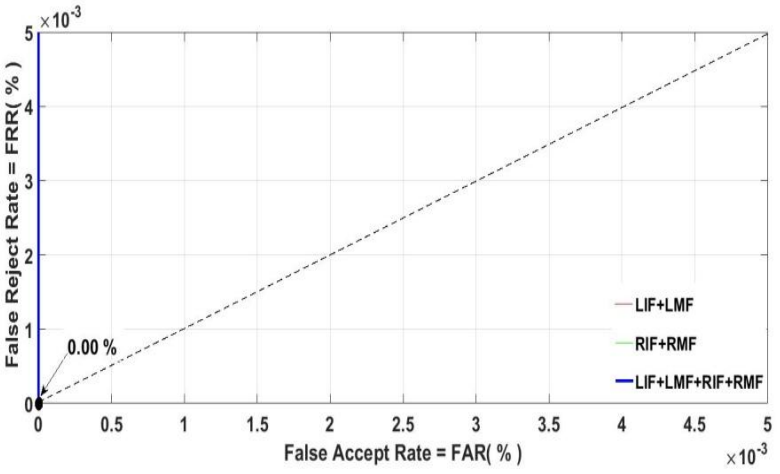

Figure III.6: Courbe ROC de système multimodal

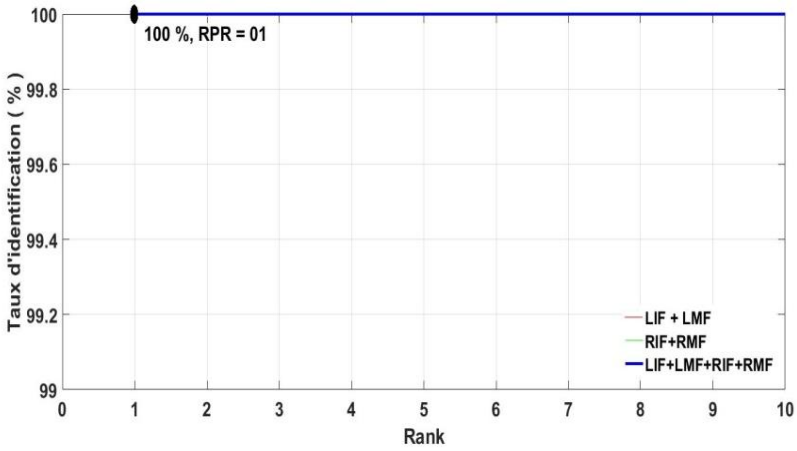

Figure III.7: Courbe CMC de système multimodal

❖ Différents Règles de Fusion

Table III.5 : Performance de système Multimodal pour les différents règle de fusion

Règle De Fusion	**Ensemble ouverte**		**Ensemble fermé**	
	EER	T_0	ROR	RPR
Sum	0.00	0.690	100	01
Mul	/	/	100	01
Min	0.00	0.25	100	01
Max	/	/	99.39	02
W Sum	0.00	0.833	100	01
W Mul	0.00	0.574	100	01

À travers le tableau, nous remarquons qu'en entrant les différentes règles de fusion sur un système multimédia(FKP), nous obtenons un système plus optimal , et c'est ce que nous avons remarqué lorsque les résultats du rapport EER=0 et ROR=100% étaient du premier ordre, à l'exception de la règle Max, Il a atteint le ROR=99.39% de au second ordre.

❖ Discussion

D'après les résultats obtenus, nous pouvons conclure que le système d'authentification FKP est un système fiable. Il permet de faire la distinction entre acceptable et imposteur . Nous considérons les résultats obtenus comme très satisfaisants, et en introduisant les

méthodes ML-LPQ et WPCA, la précision des résultats a augmenté. L'ensemble des tests effectués a permis de conclure, qu'avec l'utilisation de la fusion des échantillons (quatre doigts) et entrant les différentes règles de fusion (sum ,Mul ,Min....) ; Nous apportons augmentation des performances de système d'authentification grâce a ces fusions.

III.5 Conclusion

Dans ce chapitre, nous avons défini notre système d'authentification biométrique par FKP, en présentant comment le système FKP peut identifier, distinguer et séparer les personnes. Nous avons appris à connaître les informations les plus importantes de la base de données PolyU-FKP, de la capture d'image à la prise de décision, et finalement nous avons obtenu un système idéal qui montre les meilleurs résultats en mettant en œuvre un processus d'intégration de système multimédia.

Conclusion générale

Conclusion générale

La biométrie est considéré le domaine concerné par l'identification des personnes en fonction de leurs caractéristiques physiques ou comportementales ou biologies. Dans cette mémoire, nous avons fourni un aperçu de la biométrie et un aperçu de certaines techniques biométriques, et nous avons également essayé d'intégrer des technologies à différents niveaux, c'est-à-dire le passage d'un système unimodal à un système multimodal, afin d'obtenir un système plus sûr et plus efficace.

L'objectif suivis dans ce mémoire propose une démarche qui consiste à améliorer la performance de l'identification biométriques via l'empreinte FKP,qui est basé sur quatre doigts: (index gauche (LIF), médian gauche (LMF), index droit (RIF), médian droit (RMF). Sur cette base, la méthode la plus appropriée pour notre problème a été choisie, à savoir la méthode LPQ pour extraire les caractéristiques. En outre, un ensemble de processus différents a été utilisé : a été utilisé Analyse en composantes principales (ACP) pour simplifier l'ensemble de données en réduisant sa taille et WACP pour représenter efficacement les images FKP, qui peuvent être reconstruites grossièrement en un petit ensemble de poids et une image standard), suivie d'une classification de support de machine vectorielle (SVM).

Et nous avons combiné deux doigts, puis quatre doigts, c'est-à-dire que nous sommes passés d'un système unimodal à un système multimodal. et nous avons également eu recours aux l'amélioration du système à règles de fusion telles que (sum, Mul, Max, Min. ..) .

En fin, les résultats obtenus, sont très intéressants. En effet on est arrivé à un Taux d'erreur égal (EER) =0 est un taux idéal et un taux de reconnaissance idéal de 100 %, Ces deux tarifs sont intéressants ce qui rend notre système fiable où il répond bien à l'objectif que nous nous sommes fixés au départ, à savoir la mise en œuvre d'un système permettant la reconnaissance d'individus.

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

Bibliographie

[1] T.Hafs, "Reconnaissance Biométrique Multimodale basée sur la fusion en score de deux modalité " ,Mémoire de Doctorat en Electronique, Université de Annaba ,2016.

[2] T.H.Betaouaf, "Caractéristisation de la rétine pour la reconnaissance biométrique des personnes ", Mémoire de magister en Informatique, Université de Tlemcen ,2011.

[3] S.Boudjallel,"Détection et Identification de personne par méthode biométrique" ,Mémoire de magister en Electronique, Université de Tizi-Ouzou,2014 .

[4] Li.Guoqiang, C.Busch , BianYang ,"A novel approach used for measuring fingerprint orientation of arch fingerprint",in Information and Communication Technology, Electronics and Microelectronics, 2014.

[5] Arun A.Ross , Karthik Nandakumar , Anil K. Jain " Handbook of Multibiometric" ,

24 May 2006

[6] A.Benagga, L.Telbi, "Reconnaissance des personnes basée sur l'empreintes de l'articulation de doigt", Mémoire de Master, Université Kasdi Merbah Ouargla,2016.

[7] K.Sadalah, "Identification Biométrique des personnes par les empreintes palmaires", Mémoire de Master, Université de Annaba ,2019.

[8] E.B. BELALEM, A.HAFIANE, "Biometric System based on Neural Network ", Mémoire de Master, Université Kasdi Marbah Ouragla ,2019.

[9] N. HEZIL, " Méthode hybride en biométrie: Application à la paume de la main & l'Oreille", Mémoire de Doctorat**,** Université de Guelma 2017.

[10] A.E.Chakour, "Identification Biométriques des personnes par les Empreintes d'Articulation du Doigt ", Mémoire de Master, Université Badji Mokhtar- Annaba ,2019.

[11] EL.M .Hadjadji, k.Mahdadi, "Modélisation d'empreinte biométrique par un modèle flou de Sugeno optimisé ", Mémoire de Master, Université kasdi-Merbah Ouargla ,2017.

[12] R.Lamraoui, H.Benhmidcha,"Reconnaissance Biométrique Multimodale ", Mémoire de Master en Informatique, Université de Oum-El Bouaghi ,2016.

[13] Faundez-Zanuy, M.,"Data fusion in biometrics", In: IEEE Aerospace and Electronic Systems Magazine, vol. 20, pp. 34-38 (2005).

[14] Dasarathy, V.B, "Sensor fusion potential exploition-innovative architecture and illustrative applications", Proc.of IEEE. Vol.85,PP;24-39,1997.

[15] Oxenham, M.G. Kewley, D. Nelson, M. J, "Measure of information for multi-level data fusion", SPIE conference, Vol.2755,PP.271-282,1996.

[16] M .SANDELI,"Traitement d'images par des approches bio-inspirées Application à la segmentation d'images", Mémoire de Master, Université Constantine 2, 2014.

[17] J.Flusseret,T.Suk, "Degraded Image Analysis: An Invariant Approach. IEEE Trans " , Pattern Analysis and Machine Intelligence ,Vol.20,no.590-603,1998.

[18] C.Fiche ,"Repousser les limites de l'identification faciale en contexte de vidéo surveillance", Docteur de l'Université de Grenoble Spécialité :Signal-Images-Parole-Télécoms (SIPT),31 Janvier 2012 .

[19] DANG HOANG VU, "Biométrie pour l'identification", Rapport final, Institut de la Francophonie pour l'informatique, Hanoï, Vietnam, 07-2005.

[20] N. Morizet," Reconnaissance Biométrique par Fusion Multimodale du Visage et de l'Iris", Thèse présentée pour obtenir le grade de Docteur, Ecole Nationale Supérieure des Télécommunications, paris ,18 Mars 2009.

[21] N.MERAMRIA,"Reconnaissance de visages par Analyse Discriminante Linéaire (LDA)", Mémoire de Master **,** Université Badji Mokhtar- Annaba, 2016 .

[22] S.E.ZITOUNI, A.SACI,"Authentification et Identification biométrique des personnes par les empreintes palmaires", Mémoire de Master **,** Université Kasdi Marbah Ouragla, 2016 .

[23] H.Seggar, M.Djarallah, "Multi-modal biometric des person Identifiction system Based on Finger knuckle print Features ", Mémoire de Master **,** Université Kasdi Marbah Ouragla, 2016 .

[24] M.CHAA,"Système de Reconnaissance de Personne par des Techniques, Biométriques ", Mémoire de Doctorat **,** Université Ferhat Abbas Sétif 1, 2017 .

[25] O.Moulai Brahim,M.I.Arbaoui ,"Authentification des personnes par les articulations des doigts ", Mémoire de Master**,** Université Kasdi Marbah,2015.