

وزارة التعليم العالي والبحث العلمي

BADJI MOKHTAR- ANNABA UNIVERSITY
UNIVERSITE BADJI MOKHTAR ANNABA



جامعة باجي مختار- عنابة

Année : 2019

Faculté: Sciences de l'ingénieur
Département: Electronique

MEMOIRE

Présenté en vue de l'obtention du diplôme de : MASTER

Intitulé

Identification Biométriques des Personnes par
les Empreintes d'Articulation du Doigt.

Domaine : Sciences et Technologie
Filière : Electronique
Spécialité: Instrumentation

Par :
Chakour Alla Eddine

DEVANT Le JURY

| | | | |
|------------------------------|--------------------|------------|-------------|
| PRESIDENT: | D. MESSADEG | Pr | UBMA |
| DIRECTEUR DE MEMOIRE: | M. BOUGHAZI | Pr | UBMA |
| EXAMINATEURS: | K. BOUKHARI | MCA | UBMA |
| | T. HAFS | MCB | UBMA |

Remerciement

Je tiens à remercier tout d'abord dieu qui a aidé à

Réaliser ce modeste travail, et pour sa grâce toutes à la longue de notre vie professionnelle et personnelle. Je remercie chaleureusement mon encadreur et Professeur: M. Boughazi pour son aide, sa disponibilité, son sérieux ainsi que ses encouragements et ses conseils. Je tiens aussi à remercier :

- Tous les enseignants de département de génie électrique.**
- Mademoiselle, Daas sara, pour sa disponibilité, sa patience, son suivi constant de ce travail.**

Sans oublier qui ont contribué de près ou de loin à la réaffirmation de notre travail.

Enfin, j'adresse mes plus sincères remerciements à tous mes proches et amis, qui m'ont toujours soutenu et encouragé au cours de la réalisation de ce travail, Merci à toutes et à tous.

Dédicace

Je dédie ce travail à :

A mes chers parents, à ma mère, à mon père,
pour tout leur amour et leur soutien

A tous mes maîtres et professeurs : du primaire
au supérieur.

A Mes amis et camarades de la classe qui
m'ont soutenu

A tous ceux qui nous ont aidés de proche et de
loin.

Et aux professeurs, aux enseignants qui
travaillent au sein du département
électronique

ملخص

منذ قديم الزمن سعى الإنسان إلى إنشاء وسائل موثوقة وفعالة لضمان هوية الأشخاص الذين يتفاعلون معهم. منذ العصور القديمة كانت أفضل طريقة للتأكد من أن الشخص الذي أمامنا هي مشاركة سر يعرفه فقط كل من المحاورين أو مجموعة (مثل الاستخدام كلمة مرور على سبيل المثال).

النظام البيومتري هو التحليل الرياضي للخصائص البيولوجية للشخص وله غرض عام هو تحديد هوية الفرد ومعرفة ماهيته. بالنظر إلى أنه من بين العديد من طرق تحديد الهوية مثل استخدام بصمات الأصابع ، فإن الهدف (LPP) من هذا العمل المقدم هو استخدام هذه الطريقة لتحقيق نظام للتحقق التلقائي للأشخاص ، في عملنا أيضا نستخدم تكتل تعد المرحلة الكمي المحلي من التقنيات المستخدمة لاستخراج الخصائص أيضا نمط البت المحلي (LBQ)، التمييزية للبصمات اليد

على الرغم من التقدم الكبير الذي تم إحرازه في مثل هذه الأنظمة ، إلا أن . الأداء لا يزال غير مرضٍ ، وهو ما يتطلب أيضًا تطوير أنظمة بيومترية متعددة الوسائط (تجمع بين العديد من القياسات الحيوية لزيادة الموثوقية)

Résumé:

Depuis toujours, l'homme a cherché à mettre en place des moyens fiables et efficaces pour s'assurer de l'identité des personnes avec lesquelles elles interagissent. Depuis l'antiquité, le meilleur moyen de s'assurer que la personne que l'on a en face de soi est bien la bonne restera le partage d'un secret seulement connu des deux interlocuteurs ou d'un groupe (comme l'utilisation d'un mot de passe par exemple).

La biométrie consiste en l'analyse mathématique des caractéristiques biologiques d'une personne et a pour but général de déterminer son identité et l'identifier. Vu que parmi les nombreuses méthodes d'identification biométrique comme l'utilisation des empreintes d'articulations des doigts, le but de ce travail, est d'utiliser cette modalité pour réaliser un système de vérification automatique de personnes, Dans notre travail, un bloc Quantification de la Phase locale (LPQ) et Motif binaire locale (LBP) sont des techniques utilisées afin d'en extraire les caractéristiques discriminantes de la modalité FKP. Bien que des progrès significatifs aient été enregistrés pour de tels systèmes, la performance est encore loin d'être satisfaisante, ce qui plaide d'ailleurs en faveur du développement des systèmes biométriques multimodaux (combiner plusieurs biométries pour augmenter la fiabilité)

Abstract:

Ever since, man has sought to establish reliable and effective means to ensure the identity of the people with whom they interact. Since antiquity, the best way to ensure that the person we have in front of us is the good will remain the sharing of a secret only known to both interlocutors or a group (as the use a password for example).

Biometrics is the mathematical analysis of a person's biological characteristics and has the general purpose of identifying and identifying oneself. Given that among the many methods of biometric identification such as the use of fingerprint fingerprints, the purpose of this work is to use this modality to achieve a system of automatic verification of people, In our work, a block Local Phase Quantification (LPQ) and Local Bit Pattern (LBP) are techniques used to extract the discriminates characteristics of the FKP modality. Although significant progress has been made for such systems, the performance is still far from satisfactory, which also calls for the development of multimodal biometric systems (combining several biometrics to increase reliability).

Table de Matières

| | |
|-----------------------------|-----|
| Remerciement..... | I |
| Dédicace..... | II |
| Résumé..... | III |
| Liste des Figures..... | 1 |
| Liste de Tableau..... | 3 |
| Liste des abréviations..... | 4 |
| Introduction générale..... | 5 |

Chapitre I : Principes De La Biométrie

| | |
|--|-----------|
| I-1 Introduction..... | 8 |
| I-2 La biométrie..... | 8 |
| I-2.1 Définition..... | 8 |
| I-3 Les systèmes biométriques..... | 9 |
| I-3.1 Définition et fonctionnement..... | 9 |
| I-4 Les Modalités biométrique..... | 9 |
| I-4.1 Principaux modalités biométriques..... | 10 |
| I-5 L'architecture des systèmes biomtriques | 15 |
| I-6 L'État de L'art sur l'empreinte d'articulation (FKP) | 17 |
| I-7 Les performances des systèmes biométriques | 20 |
| I-7.1 caractéristiques des systèmes biométriques..... | 20 |
| I-8 Conclusion | 23 |

Chapitre II: La Biométrie Pour L'identification

| | |
|---|----|
| II-1 introduction..... | 24 |
| II-2 La biométrie Uni-modal et multimodale..... | 24 |
| II-2.1 système uni-modal | 24 |
| II-2.2 système multimodal | 26 |
| II-3 Des méthodes de prétraitement d'image..... | 26 |
| II-3 .1 Méthode d'Extraction de Caractéristiques..... | 28 |
| II-3 .2 Mesures de distance..... | 31 |
| II-3.3 Mesure des similarités | 31 |
| II.3.5 Décision..... | 32 |
| II-4- conclusion..... | 32 |

Chapitre III: programmation du processus d'analyse des images.

| | |
|--|----|
| III-1 Introduction..... | 33 |
| III-2 Explication du programme par étapes | 33 |
| III-2.1 Comment reconnaître les empreintes d'articulation..... | 33 |
| III-2.2 La Base de données..... | 33 |
| III-2.3 L'acquisition des données..... | 34 |
| III-2.4 La manipulation des images..... | 35 |
| III-3 Partie programmation..... | 36 |
| III-3.1 Premier partie | 36 |
| III-3.2 Deuxième partie..... | 37 |

III-4 conclusion..... 37

Chapitre IX: interprétation expérimentale des résultats

IX-1 Introduction.....38

IX-2 La méthode basée sur la méthode LPQ.....38

IX-2.1 les résultats pour chaque doigt de main avec la méthode LPQ.....38

IX-3 La méthode basée sur la méthode LBP.....41

IX-3.1 les résultats pour chaque doigt de main avec la méthode LBP.....41

IX-4 Etude comparative entre les deux méthodes.....43

IX-5 Conclusion.....44

Conclusion générale.....45

Bibliographie.....46

Liste des Figures

| | |
|---|----|
| Figure I.1 Classification d'un certain nombre de modalités biométrique..... | 10 |
| Figure I.2 : Image de la géométrie de main ;b) Dispositif de reconnaissance de la géométrie de main | 10 |
| Figure I.3 : Image d'une empreinte digitale..... | 11 |
| Figure I.4 : la reconnaissance de visage. | 11 |
| Figure I.5 : image iris | 12 |
| Figure I.6 : reconnaissance de signature. | 13 |
| Figure I.7 : reconnaissance de frappe au clavier..... | 13 |
| Figure I.8 : Image de la Reconnaissance vocale..... | 14 |
| Figure I.9 : image d'ADN. | 14 |
| Figure I.10 : Image de système configuration des veines..... | 15 |
| | |
| Figure I.11 : phase d'enrôlement..... | 16 |
| Figure I.12 : Phase vérification | 17 |
| Figure I.13 : Phase Identification | 17 |
| Figure I.14 : :(a) FKP image, (b) ROI image, (c) Code des FKP..... | 19 |
| Figure I.15 : Graphe démonstratif de l'EER. | 22 |
| Figure I.16 : courbe de ROC | 23 |
| Figure I.17 : Illustration du FRR et du FAR. | 24 |
| Figure II.1 : Des empreintes d'articulations | 26 |
| Figure II.2 : Construction d'un motif binaire et calcul du code LBP.. | 30 |
| Figure II.3:Organigramme de l'ensemble des étapes nécessaire à la génération du vecteur des caractéristiques par la méthode LPQ. | 32 |
| Figure III.1 : Le dispositif d'acquisition des données | 38 |
| Figure III.2 : Des images d'empreintes d'articulations acquises | 38 |
| Figure IX.1: Genuine and Impostor Distribution of LBQ Méthode.... | 42 |
| Figure IX.2: FAR and FRR vs Threshold graph of LBQ Méthode..... | 42 |
| Figure IX.3: ROC curve_1 of LBQ Méthode..... | 42 |
| Figure IX.4: ROC curve_2 of LBQ Méthode..... | 43 |

Figure IX.5: CMC curve of LBQ Méthode43
Figure IX.6: Genuine and Impostor Distribution of LBP Method44
Figure IX.7: FAR and FRR vs Threshold graph of LBP Method44
Figure IX.8: ROC curve_1 of LBP Method.....45
Figure IX.9: CMC curve of LBP Method.....45

Liste de Tableaux

| | |
|---|----|
| Tableau I.1 : Comparaison des Technologies Biométriques | 15 |
| Tableau III. 2 : Résultats obtenus selon la méthode LBQ | 42 |
| Tableau III.3: Résultats obtenus selon la méthode LBP..... | 44 |
| Tableau III.4: Comparaison entre les deux méthodes..... | 44 |

List des abréviations:

ADN : AcideDésoxyriboseNucléique

BDD : Base de données

FKP: Finger knuckle print

CMC : Cumulative Match Curve

EER : Equal Error Rate FAR : False Accept Rate

FRR : False Rejection Rate

LBP : Local Binary Pattern

LPQ : Local Phase Quantization

ROC : Receiver Operating Characteristic

RIF : Right Index Fingers

RMF : Right Middle Fingers

GAR :Genuine Acceptance Rate

ROR: Rank of Perfect Recognition

Introduction générale :

L'être humain a connu avec le temps plusieurs changements importants dans tous les aspects de sa vie surtout avec l'arrivée de l'informatique qui a changé le monde, c'était une révolution technologique spécialement au domaine de communication, pour lutter et faire face contre le taux de criminalisation élevé, comme l'espionnage, le piratage, ce dernier touche même nos renseignements privés. Pour cela, il est incontournable d'établir une nouvelle méthode pour mettre fin à ce problème, cette méthode est dénommée "système de reconnaissance". La reconnaissance des individus a une grande importance dans notre vie humaine quotidienne. Elle assure les transactions des personnes en différents domaines afin d'assurer une sécurité pertinente. Dans ces derniers temps, l'utilisation des systèmes de reconnaissance n'est pas si répandue aux grands secteurs tels que le secteur militaire et d'autres secteurs où la sécurité est cruciale. Actuellement, la reconnaissance biométrique est utilisée dans de nombreuses applications telles que la protection de l'accès à un ordinateur, un téléphone portable, une clé USB, un établissement, des cartes bancaires.... De nombreuses technologies biométriques ont été développées, toutes basées sur les identificateurs biométriques physiologiques et comportementaux telles que : l'iris, la voix, les empreintes digitales, le visage, la signature.... Ces derniers sont plus fiables que les systèmes classiques (clé, mot de passe...), Car ils sont difficilement falsifiables.

Dans ce travail, les systèmes qui viennent d'être étudiés c'est celui de la reconnaissance des personnes par leurs images des surfaces extérieures des doigts, ou bien c'est, un système qui utilise l'empreinte des articulations des doigts, Finger knuckle Print (FKP). 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. Donc en final, la combinaison de tous les doigts (des deux mains) peut être utilisée afin d'établir un système biométrique robuste, pertinent et précis et donc efficace.

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

Notre mémoire est scindé en quatre chapitres : Dans le premier chapitre nous avons défini la biométrie ainsi que les différents techniques et modalités biométriques utilisées. Ce chapitre est constitué d'un aperçu sur les principaux domaines d'utilisation de la biométrie et aussi leur

contribution dans le marché mondial, en constatant que Les systèmes biométriques sont actuellement de plus en plus demandés. Le deuxième chapitre Dans ce chapitre nous avons défini plusieurs notions de traitement d'images, comme aussi la façon d'utiliser et de combiner plusieurs modalités dans notre système a été abordée. Notre travail à l'extraction de caractéristiques ou les traits spécifiques des empreintes est également présenté dans ce chapitre. Dans ce chapitre, des notions sur les deux techniques LPQ et LBP, ainsi que la façon de les appliquer pour extraire les caractéristiques discriminantes sont présentés. Dans le troisième chapitre, est fait principalement, pour l'explication détaillée de notre programme réalisé, qui vise à identifier les personnes à partir des empreintes d'articulations de doigts et fait l'évaluation du système étudié.

Enfin, le quatrième chapitre est consacré pour les résultats expérimentaux. Premièrement on fait l'extraction des caractéristiques des empreintes et ensuite l'identification des personnes grâce à la méthode LBQ avec les différents doigts des deux mains, deuxièmement on répète ce travail avec la méthode LBP. Et dernièrement une partie comparative entre ces différentes méthodes est illustrée dans ce chapitre. Et on termine avec la conclusion générale.

Chapitre I : Principes de la Biométrie

I-1 Introduction

Connaître de manière à la fois efficace et pertinente l'identité d'un individu reste un grand problème dans notre société. En effet, même si ne nous savions pas, notre identité est vérifiée quotidiennement par de plusieurs organisations ou personnes : lorsque nous utilisons notre carte bancaire, lorsque nous accédons à notre lieu de travail ou lors d'un accident, lorsque nous nous connectons à un réseau informatique, etc.

La biométrie est une solution parfaite et plus simple et plus efficace des méthodes d'authentification traditionnelles basée sur une connaissance qui correspond par exemple au mot de passe utilisé au démarrage ou au code qui permet d'activer un téléphone portable.

I-2 La Biométrie :

I-2.1 Définition :

La biométrie consiste à identifier une personne à partir de ses caractéristiques physiques comme le visage, les empreintes digitales, l'iris,...etc. Ou comportementales par exemple la voix, l'écriture, le rythme de frapper sur un clavier....etc. En plus les caractéristiques biologiques comme L'ADN, les veines et le thermo-gramme facial. Ces caractéristiques qu'elles soient innées comme les empreintes digitales ou bien acquises comme la signature, sont attachées a chaque

individu et ne sont donc pas des faiblesses des méthodes basés sur une connaissance ou une possession. En effet, un attribut physique ou comportemental ne peut être oublié, perdu ou volé. (1)

I-3 Systèmes biométriques :

I-3.1 Définition et fonctionnement :

Un système biométrique est un système automatique de mesure basé sur la reconnaissance de caractéristique propre à un individu : physique ou comportementale.

Il est basé sur l'analyse de données liées à l'individu qui peuvent être classées en trois grandes catégories : Analyse basée sur la morphologie, Analyse de traces biologiques, L'analyse comportementale.

Il peut être représenté par 4 principales étapes :

- Le module de capture.
- Le module d'extraction de caractéristiques.
- Le module de correspondance.
- Le module décision. (2)

I-4 Modalités biométriques :

Il existe plusieurs modalités biométriques utilisées dans divers secteurs, on peut distinguer 3 catégories :

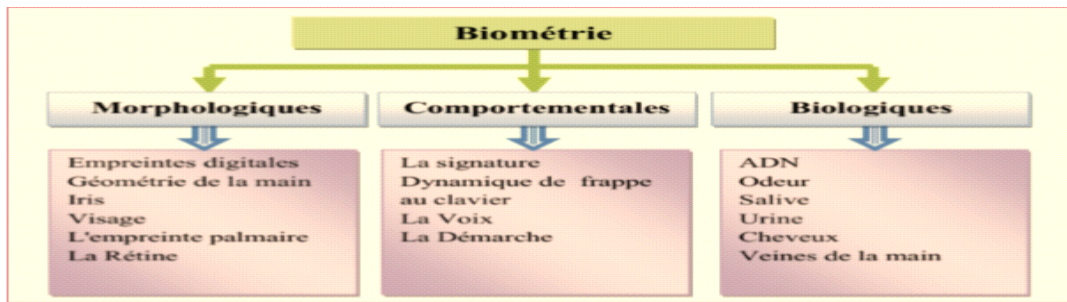


Figure (1) : Classification d'un certain nombre de modalités biométriques.

I-4.1 Principaux modalités biométriques :

1-Modalités morphologiques (physiologiques) : Elle est basée sur l'identification de traits physiologiques particuliers qui pour tout 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. (4).

- **La géométrie de la main** : Cette modalité consiste à analyser la forme de la main, sa longueur, sa hauteur, la courbure de doigt etc.



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

- **Empreinte digitale** : L'empreinte digitale est la caractéristique d'un doigt. On croit que chaque empreinte digitale est unique, chaque personne a ses propres empreintes digitales. (4)

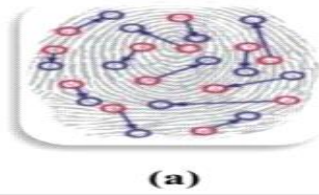


Figure (3) : Image d'une empreinte digitale.

- Visage :

Les systèmes actuels de reconnaissance du visage sont composés d'un module d'acquisition d'image 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. (5)



Figure (4) : la reconnaissance de visage.

- **Iris**: Est la membrane colorée de l'œil. Une caméra proche des infrarouges photographie une tranche de l'iris, elle relève les caractéristiques particulières du relief. C'est une technologie fiable et semble être beaucoup plus précise que certains autres moyens biométriques. (6)



Figure (5) : image iris.

La rétine : Cette mesure biométrique se base sur le fait que les vaisseaux sanguins d'une rétine sont différents d'une

personne à une autre et stable durant la vie. Cette technologie est la plus complexe à falsifier, mais probablement à cause de son coût élevé elle n'est pas utilisée que dans les cas où la sécurité est primordiale (7).

2-Modalité comportementale :

Elle est basée sur l'analyse de certains comportements d'une personne.

- L'écriture (La signature) :

Les systèmes de reconnaissance de l'écriture consistent à analyser les caractéristiques spécifiques d'une signature comme, La vitesse, la pression sur le crayon, le mouvement, les points et les intervalles de temps où le crayon est levé, elle base généralement sur le fait que l'utilisateur signe avec un stylo électronique sur une plaquette graphique et au même temps elle examine l'ensemble de dynamiques. (3)



Figure (6) : reconnaissance de signature.

- La dynamique de frapper au clavier :

C'est une caractéristique de l'individu. Les caractéristiques suivantes sont généralement prises en compte :

Vitesse de frappe, suite de lettres, mesure de temps de frappe, pause entre chaque mot, reconnaissance de mots précis (8).



Figure (7) : reconnaissance de frappe au clavier.

La voix : La reconnaissance par voix utilise les caractéristiques vocales pour identifier les personnes en utilisant des phrases, Mot de passe, un téléphone ou un microphone peut être comme dispositif d'acquisition. (4)

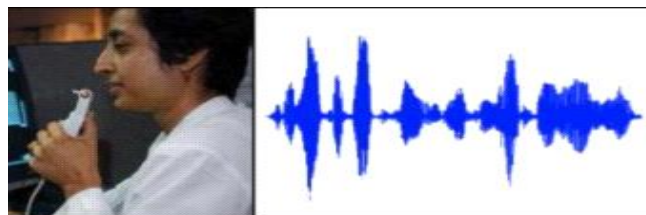


Figure (8) : Image de la Reconnaissance vocale

- **La Démarche :** La biométrie de la marche est une biométrie basée sur la marche de la personne, ça devrait être mentionné que la marche n'est pas affectée par la vitesse de la marche de la personne. (9)

3-Modalité biologique :

Elle est basée sur l'identification de traits biologiques particuliers

- **L'ADN :** L'Analyse des empreintes génétiques est une méthode

Extrêmement précise d'identification, 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 gène codé dans l'acide désoxyribose nucléaire (ADN). (10)



Fig (9) : image d'ADN.

- **Vaine de la main** : On a longuement considéré que le modèle des veines dans l'anatomie humaine peut être unique aux individus. (11)



Fig(10): Image de système configuration des veines.

Et chaque modalité citée au-dessus est utilisée selon le besoin de l'utilisateur, et il faut savoir les avantages et les inconvénients de chaque modalité.

Tableau (1) : Comparaison des Technologies Biométriques.

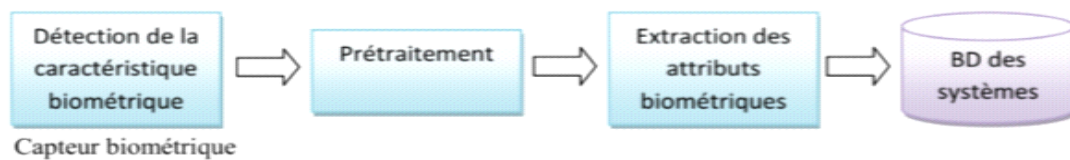
| Technique | Avantages | Inconvénients |
|----------------------|---|--|
| Empreintes digitales | - Coût - Ergonomie moyenne | - Acceptabilité moyenne - Possibilité d'attaque |
| Forme de la main | - Très ergonomique - Bonne acceptabilité | - Système encombrant et coûteux - Perturbation possible par des blessures |
| Visage | - Coût - Bonne acceptabilité | - Jumeaux, déguisement vulnérabilité aux attaques (facile à falsifier) |
| Rétine | - Fiabilité - Pérennité | - Acceptabilité très faible - Contrainte d'éclairage |
| Iris | - Fiabilité | - Acceptabilité très faible - Contrainte d'éclairage |
| Voix | - Facilité | - Vulnérable aux attaques (faciles à falsifier) |
| Signature | - Ergonomie | - Dépendant de l'état émotionnel de la personne peu fiable |
| Frappe au clavier | - Ergonomie | - Dépendant de l'état physique de la personne peu fiable |

I-5 Architecture des systèmes biométriques :

I-5.1 Différent modes des systèmes biométriques

Les systèmes biométriques peuvent fournir trois modes de fonctionnement à savoir, mode d'enrôlement, mode vérification et le mode identification. Donc, le Mode de fonctionnement :

Le mode d'enrôlement : c'est une phase d'apprentissage qui a pour but de recueillir des informations biométriques sur les personnes à identifier pendant cette phase, les caractéristiques biométriques des individus sont saisies par un capteur biométrique, puis représentées sous forme numérique et enfin stockées dans une base de données (12)

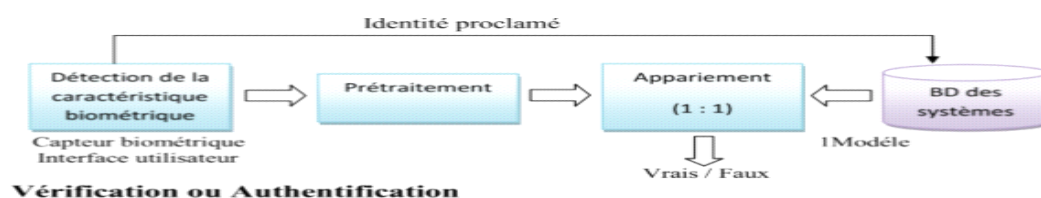


Enrôlement

Fig(11) : phase d'enrôlement

Le mode vérification ou authentification :

C'est la comparaison 1 à 1 entre les données biométriques capturées (modèle test) et les données stockées dans sa propre base (les modèles d'apprentissage). Dans un tel système un individu qui désire être identifié réclame une identité, habituellement par l'intermédiaire d'un PIN (numéro d'identification personnelle), d'un nom d'utilisateur, d'une carte d'identité etc. Le système doit répondre à la question suivante : suis-je réellement la personne qui suis-je entrain de proclamer (13)



Fig(12)

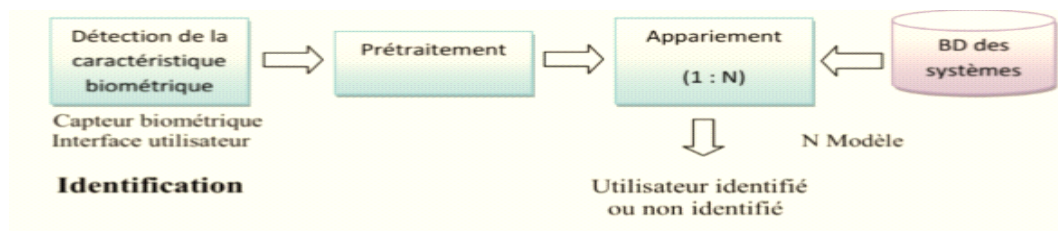
: Phase vérification.

Le mode identification :

Le Système doit deviner l'identité de la personne. Il répond à la question de type : qui suis-je ?

Dans ce mode, le système compare le signal mesuré et les différents modèles contenus dans la base de données. En général, lorsque l'on parle d'identification, on suppose que le problème soit fermé, c'est-à-dire toute personne qui utilise le système possède un modèle dans la base de données. Le

système effectue un appariement (1 :N) pour la personne en question comme illustré à la figure (4) :



Fig(13) : Phase Identification.

I-6 L'état de L'art sur l'empreinte d'articulation (FKP) :

Récemment on constate que l'empreinte d'articulation du doigt, qui se réfère aux formes inhérentes de la surface externe autour du doigt et spécialement la partie haute de doigt, est fortement unique et peut servir à une modalité biométrique distinctive. L'articulation du doigt est encore à la phase de développement et peut être considérée comme nouvelle tendance dans la biométrie.

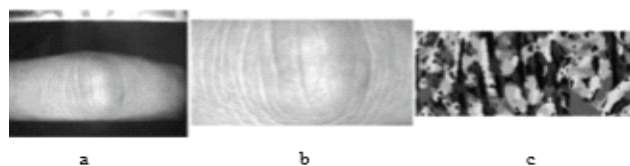
Woodard and Flynn (2005), (14) ont d'abord étudié la surface du doigt pour l'authentification des individus. Ils ont utilisé un capteur minolta 900/910 pour l'acquisition de la surface du dos de doigt 3D. Leur effort valide l'unicité de la surface arrière du doigt comme un trait biométrique potentiel. Cependant leur travail n'est pas entièrement consacré aux points d'articulation et ils ont utilisé la surface complète du dos des doigts dans l'authentification.

En outre, l'utilisation de minolta 900/910 soulève le coût globalement prétraitement de la surface du doigt à 3D augmente le temps et la complexité du système qui limite son utilisation pour les applications biométrique en ligne. En 2009, Kumar et Ravikanth (14) ont présenté une analyse détaillée sur l'acquisition et l'extraction de points

d'articulation de la partie dorsale de la main. Ils utilisent un faible coût à l'aide d'un appareil photo numérique (Canon Powershot A620) pour l'acquisition du dos de la main. L'image de la main acquise est ensuite utilisée pour extraire les points d'articulation comme une région d'intérêt (ROI).

La PCA, linear discriminant analysis (LDA) et Independent component Analysis (ICA) sont des caractéristiques extraites à partir de points d'articulation. Ces travaux ont mis un grand effort pour valider l'unicité de la surface externe supérieure du doigt. Cependant ils n'ont pas fourni une solution pratique.

En outre la méthode (14) exploite principalement les informations de la forme 3D du dos du doigt mais n'utilise pas entièrement l'information de la texture externe tandis que les méthodes d'analyse de sous-espace utilisées dans (15), ne peuvent pas extraire efficacement les lignes distinctives et les attributs de la surface du dos du doigt. Par contre dans l'article (16), ils ont développé un système de reconnaissance de l'empreinte d'articulation y compris spécifiquement l'appareil d'acquisition ensuite une détection de la région d'intérêt a été implémentée et par la suite un filtre de Gabor 2D a été utilisé pour extraire l'information de l'orientation locale pour le Matching ils ont utilisé la distance angulaire pour mesurer la similarité entre 2 codes qui correspondent aux images.



Fig(14) :(a) FKP image, (b) ROI image, (c) Code des FKP.

Malgré le développement d'un appareil d'acquisition, le temps d'exécution reste un problème et ce problème est dû au Matching (16, 585,920 au total) et à la mesure de similarité (le temps total d'exécution pour une seule vérification prend environ 1s) comme résultat, ils ont trouvé un taux de reconnaissance 97% et un FAR de 0.02% et EER de 1.09%. Le centre biométrique de recherche à l'université polytechnique de Hong Kong a développé un appareil en temps réel pour la capture de l'empreinte d'articulation et l'utiliser pour les constructions d'une base de données à grande échelle. Dans (17) les images de l'empreinte d'articulation contiennent plus de bruit en les comparant avec les empreintes palmaires. Dans ce cas ils ont proposé 2 étapes :

L'application du filtre de Gabor 2D pour améliorer les lignes de l'empreinte d'articulation et les descripteurs scale-Invariant feature transform (SIFT). Après le filtre de Gabor l'Algorithme Contrast Limited adaptive Histogramme Equalization (CLAHE) est appliqué pour améliorer le contraste des lignes d'articulation. Dans (28) une méthode par la fusion de plusieurs algorithmes pour l'extraction des caractéristiques est représentée. Ils utilisent LG (Log Gabor), LPQ (Local Phase Quantization),

PCA et LPP (Locally Preserving Projections) pour l'extraction des caractéristiques

Dans la première expérience, ils utilisent un seul algorithme pour l'extraction des caractéristiques. Les résultats obtenus font apparaître que l'algorithme des LG à une exactitude élevée en le comparant avec les autres algorithmes. Une fusion entre deux algorithmes a été utilisée. La meilleure

fusion est la fusion entre LG et LPP avec un taux de reconnaissance de 89.67%. En cet article ils se concentrent juste sur la phase d'extraction des caractéristiques.

I-7 Les performances des systèmes biométriques :

I-7.1 caractéristiques des systèmes biométriques :

Chaque caractéristique (ou modalité) biométrique a ses forces et ses faiblesses, et le choix dépend de l'application visée.

On s'attend ce qu'aucune modalité biométrique ne répond efficacement aux exigences de toutes les applications, plusieurs études ont été menées afin d'évaluer les performances des systèmes biométriques (19).

Ces études sont basées sur quatre critères d'évaluation :

Intrus : Ce critère permet de classer les systèmes biométriques en fonction de l'existence d'un contact direct entre le capteur utilisé et l'individu à reconnaître.

Fiabilité : Dépend de la qualité de l'environnement (éclairage par exemple) dans lequel l'utilisateur se trouve. Ce critère influe sur la reconnaissance de l'utilisateur par le système considérablement.

Coût : Doit être modéré. À cet égard nous pouvons dire que la reconnaissance faciale ne nécessite pas une technologie coûteuse. En effet, la plupart des systèmes fonctionnent en utilisant un appareil à photo numérique de qualité standard

Effort : Requis par l'utilisateur lors de la saisie de mesures biométriques, et qui doit être réduit le plus possible.

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). [20]

Le FAR (False Acceptance Rate): Ce taux représente le pourcentage d'individus reconnus par le système biométrique. Les systèmes classent alors deux caractéristiques provenant de deux personnes différentes comme appartient à la même personne. [21]

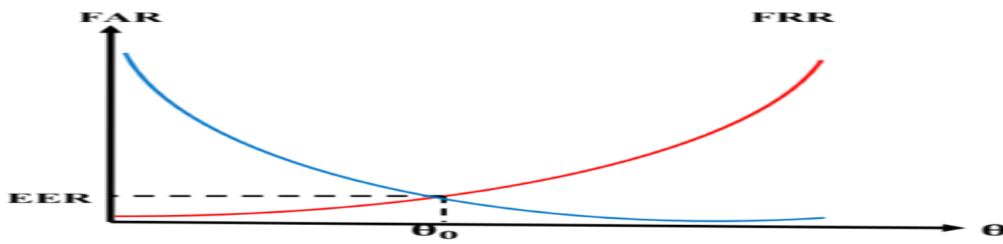
***FAR = Nombre des imposteurs acceptés /
Nombre total d'accès imposteurs***

Le FER (False Rejection Rate): La fréquence des rejets par rapport aux personnes qui doivent être correctement vérifiés. Quand un utilisateur autorisé est rejeté il ou elle doit représenter leurs caractéristiques biométriques au système [24]

***FER = Nombre des clients rejetés /
Nombre total d'accès clients***

L'EER (Equal Error Rate): Le point d'équivalence des erreurs est le taux d'exactitude croisée EER, il est déterminé par le point d'intersection entre la courbe du taux de fausses acceptations et la courbe du taux de faux rejets, on peut aussi définir le taux d'erreur égal (Equal Error Rate ou EER) comme suit :

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



Fig(15):Graphe démonstratif de l'EER.

θ_0 = Seuil correspondant au point d'équivalence des erreurs [21]

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.

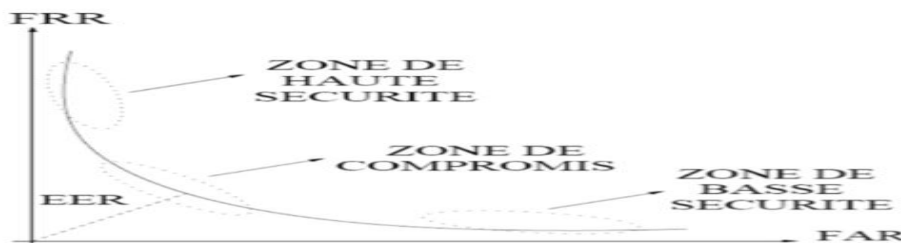


Fig (16) : courbe de ROC.

Il est fréquemment utilisé pour donner un aperçu de la performance d'un système biométrique. Cependant, il est important de souligner que l'EER ne résume en aucun cas toutes les caractéristiques d'un système biométrique. Le seuil

doit donc être ajusté en fonction de l'application ciblée : haute sécurité, basse sécurité ou compromis entre les deux. [22]

Le but fondamental de tout système biométrique opérant au niveau score, est de pouvoir séparer au maximum les distributions de score des imposteurs et des authentiques. En minimisant la zone de recouvrement entre ces deux distributions, on améliore la performance globale du système en augmentant le taux de reconnaissance.



Fig(17) : Illustration du FER et du FAR

I-8 Conclusion :

Dans ce chapitre, nous avons donné des définitions de certaines notions principales de la biométrie, nous avons présenté quelques techniques biométriques ainsi que l'architecture d'un système biométrique. La performance et la fiabilité d'un système biométrique se déterminent par le taux d'identification et les taux d'erreurs commises par le système. Pour bien obtenir de meilleurs résultats de performances, les chercheurs préfèrent la combinaison de deux ou plusieurs modalités différentes.

Chapitre II : La Biométrie pour l'identification

II-1 introduction :

Dans ce chapitre, nous allons parler sur les limitations des systèmes Uni-modal et ses inconvénients, qui utilisent une seule modalité biométrique d'un individu et il souffre pour identifier une personne avec une grande précision. Le système de reconnaissance des empreintes d'articulations, comme tous les systèmes biométriques est constitué de trois étapes primordiales : Le prétraitement, l'extraction des caractéristiques et la classification. Dans l'étape de prétraitement, les images sont traitées pour faciliter l'extraction des caractéristiques. Ce processus sert à éviter les informations inutiles. Le deuxième module sert à traiter l'image afin d'extraire uniquement les caractéristiques biométriques, sous forme d'un vecteur ou Template, qui ensuite peuvent être utilisées pour connaître les personnes. Ces caractéristiques sont uniques à chaque personne et stables. La reconnaissance est faite par la comparaison (classification) du vecteur de caractéristique avec une base de données.

II-2 La biométrie Uni-modal et multimodale:

II-2.1 Système Uni-modal :

Le système Uni-modal, c'est un système qui utilise une seule modalité biométrique pour l'identification, comme l'utilisation d'une seule empreinte d'articulation ou un seul algorithme pour identifier les personnes. Ces types des

systemes généralement ne sont pas assez sécurisés et ont un taux d'erreur élevé.

1-Limitations des Systèmes Uni-modaux : On ne peut pas garantir un excellent système d'identification des personnes (un excellent taux de reconnaissance) en utilisant une modalité biométrique seulement. Les systèmes biométriques Uni-modaux ont plus d'avantages et d'intelligence par rapport aux systèmes traditionnels, mais leur utilisation souffre de plusieurs limitations qui peuvent diminuer considérablement leur efficacité. En général, les systèmes Uni-modaux sont souvent affectés par les problèmes suivants :

2-Les problèmes des caractéristiques biométriques : Et cela signifie que parfois des modalités biométriques qui ne sont pas possédées ou assez claires par la personne à reconnaître pour permettre la reconnaissance de son identité. Certaines personnes peuvent avoir les articulations des doigts ou empreintes abîmés à cause d'un accident ou d'un travail manuel prolongé.

3- Différence entre les captures : c.-à-d. que les données biométriques acquises à partir d'un utilisateur lors de la phase de reconnaissance ne sont pas les mêmes données qui ont été prises pour créer le modèle de ce même utilisateur lors de la phase d'enrôlement. Ces changements peuvent être à cause d'une mauvaise interaction de l'utilisateur avec le capteur (comme changer de position ou d'expression faciale lorsque l'utilisateur se pose devant la caméra).

4- système fragile et Sensibilité : Dans certains cas, il est relativement simple de reproduire une signature ou imiter la voix d'une personne (les modalités biométriques comportementales sont plus sensibles à ce genre d'attaque), il est moins facile de reproduire, par exemple l'empreinte digitale, mais cela est possible et parfois y aurait de tricheries dans ce domaine.

5-Des biométries non-unique : Parfois certaines personnes peuvent avoir une apparence faciale plus ou moins identique due à des facteurs génétiques (ex : père et fils, vrais jumeaux). Ces biométries non-unique sont parfois presque identiques permettent à augmenter le taux d'erreur d'un système biométrique (acceptation des imposteurs) [25]

II-2.2 Les systèmes multimodal dans la biométrie :
En effet, c'est la combinaison de plusieurs modalités et algorithmes en même temps, pour améliorer les performances de la reconnaissance. En enrichissant le nombre d'informations discriminant de chaque personne, on souhaite augmenter le taux de reconnaissance du système (vérification ou l'identification)

II-3 Des méthodes de prétraitement d'images:

- Rehaussement des niveaux de gris : Le prétraitement de rehaussement des niveaux de gris consiste à renforcer certaines plages de niveaux de gris au détriment d'autres plages, pour mettre des objets en valeur.

- **Égalisation d'histogramme** : L'égalisation d'histogramme sert à améliorer le contraste. Il faut la faire en s'assurant que les niveaux de gris des pixels de l'image résultante sont uniformément répartis (distribution uniforme des niveaux de gris). Cette transformation consiste à rendre le plus plat possible l'histogramme des niveaux de gris de l'image.

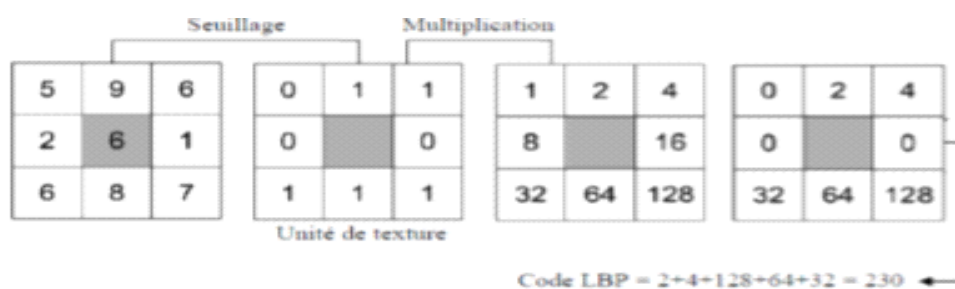
Filtre gaussien : C'est également un filtre passe-bas. Une gaussienne à deux dimensions est donnée par l'expression suivante m :

II-3.2 Méthode d'Extraction des Caractéristiques :

Extraction des Caractéristiques : l'extrait des caractéristiques de l'image de modalité (dans notre cas c'est FKP) est une phase très importante pour concevoir la pertinence d'un système d'identification. Par contre, le choix de la méthode d'extraction des caractéristiques biométriques est basé sur trois informations essentielles la texture, les lignes et l'apparence de l'empreinte. La plupart des expériences nous disent que l'information la plus distinctive de l'empreinte réside dans la texture, pour cela, on choisit parmi des algorithmes (quantification de la phase local (LPQ) et motifs binaires locaux (LBP) qui sont très utilisés et donnent des bons résultats surtout dans la reconnaissance faciale.

Méthode du Local Binary Pattern(LBP) : Les motifs binaires locaux ont initialement été proposés par Ojala en 1996 afin de Caractériser les textures présentées 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 2). 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.



fig(2): 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.

$$LBP(X_c, Y_c) = \sum_{n=0}^p U(g_i - g_c) 2^n$$

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.

Local phase Quantization(LPQ) : L'information de LPQ peut être extraite en utilisant la transformée discrète de Fourier à fenêtre à deux dimensions (2DWFT).

$$Fu(x) = \sum_{m \in Nx} h(m - x) f(m) e^{-j\pi u^T m} = E_u^T f x$$

Où E_u^T , de taille = $1 \times M^2$, est un vecteur de base de 2DWFT avec la fréquence u , et $f x$, taille = $M^2 \times N$, est un vecteur contenant les valeurs des pixels d'image dans Nx à chaque position de x . La fonction fenêtre, $h(x)$ est une fonction rectangulaire. La transformation est calculée à quatre valeurs de la fréquence:

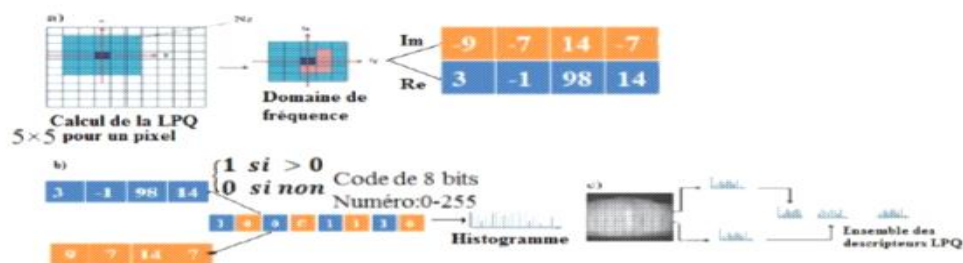
$u = [u_0, u_1, u_2, u_3]$ où $u_0 = [\mathbf{a}, \mathbf{0}]^T$, $u_1 = [\mathbf{0}, \mathbf{a}]^T$, $u_2 = [\mathbf{a}, \mathbf{a}]^T$ et $u_3 = [\mathbf{a}, -\mathbf{a}]^T$.

La méthode LPQ peut être résumée en quatre étapes distinctes. Dans un premier temps, l'opérateur (LPQ) est appliqué sur l'image d'entrée pour obtenir l'image labélisée. Ensuite, l'image obtenue est divisée en petites régions. Pour chacune d'entre elles, un histogramme des étiquettes est construit afin d'obtenir des vecteurs des caractéristiques (Templates) locaux de articulation de doigt (FKP). La représentation globale (vecteur des caractéristiques global qui représente l'image entière) de l'articulation de doigt (FKP) est obtenue par combinaison de tous les vecteurs. La Fig(3) résume l'ensemble des étapes nécessaires à la génération de ce vecteur ce procédé de codage, attribue deux bits pour chaque pixel pour représenter le quadrant dans lequel se

trouve l'angle de phase. 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 précédente, obtenue pour chaque pixel par la concaténation des codes quadrant bits réels et imaginaires des huit coefficients de Fourier de ui .

La chaîne binaire est convertie en nombre décimal pour produire une étiquette de LPQ.

La figure II.3 résume l'ensemble de ces étapes.



Fig(3):Organigramme de l'ensemble des étapes nécessaire à la génération du vecteur des caractéristiques par la méthode LPQ

Filtre de Gabor : Pour les applications nécessitant une analyse par orientations, les fonctions de Gabor qui produisent une décomposition en ondelettes est très utilisée. De nombreuses applications en traitement d'images font appel à l'utilisation ces types des fonctions, comme par exemple l'analyse de textures ou objets par attributs fréquentiels. En effet, les lignes de l'empreinte sont caractérisées par leur fréquence locale et leur orientation.

En utilisant des filtres de Log Gabor, bien choisis, il est possible d'en extraire les caractéristiques biométriques. Cependant, lorsque ceux-ci sont correctement paramétrés, ils permettent de préserver les lignes et fournissent des informations sur l'orientation locale de la texture.

II-3.3 Mesures de distance : Lorsqu'on souhaite comparer deux vecteurs de caractéristiques issus du module d'extraction de caractéristiques d'un système biométrique, on peut soit effectuer une mesure de similarité (ressemblance), soit une mesure de distance (divergence). La première catégorie de distances est constituée de distances Euclidiennes et est définie à partir de la distance de Minkowski d'ordre p dans un espace euclidien (déterminant la dimension de l'espace euclidien).

La distance Euclidienne : La distance Euclidienne est une distance géométrique dans cet espace multidimensionnel.

II-3.4 Mesure des similarités :

L'étape de l'identification, commence une fois le vecteur des caractéristiques sont obtenus par le module de traitement, le système va ensuite effectuer le calcul de similarité entre un vecteur enregistré dans la base de données et un vecteur de test.

II.3.5 Décision :

La dernière étape dans le processus de reconnaissance et après l'identification est le fait d'accepter ou de rejeter la personne en question en se basant sur un seuil déterminé, Le choix de ce seuil est prise généralement selon les erreurs produites par le système. Sur cela, on fait la comparaison entre la distance trouvée et le seuil nous permet d'accepter la personne en question ou la refuser.

$$\begin{cases} D0 \leq T0 \Rightarrow \textit{Accepté} \\ D0 > T0 \Rightarrow \textit{Rejeté} \end{cases}$$

Souvent dans les travaux réalisés, la valeur de seuil se trouve dans le point de l'intersection et égal à $EER = FAR = FRR$.

II-4 conclusion :

Au jour d'aujourd'hui, il y a une nouvelle tendance qui se reprend avec le temps et qui commence à attirer l'attention et à susciter les efforts, c'est le multimodal, dans lequel on combine plusieurs technologies, ou plusieurs algorithmes de reconnaissance, ou on utilise de différents systèmes afin d'améliorer ces systèmes et leurs performances de reconnaissance. C'est pour cela et dans ce contexte de l'évolution de la biométrie, nous avons mentionné dans ce chapitre la biométrie multimodale.

Chapitre III: programmation du processus et traitement des images.

III-1 Introduction :

Dans ce chapitre nous allons expliquer avec détails le fonctionnement et le processus de notre programme d'identification des individus d'une manière générale et abrégé, plusieurs programmes et méthodes sont mises en œuvre pour pouvoir faire l'opération de la reconnaissance, en utilisant la simulation sur Matlab ou un autre logiciel on visualise les résultats à vouloir obtenir.

III-2 Explication du programme par étapes.

III-2.1 Comment reconnaître les empreintes d'articulation :

L'identification de l'identité de la personne est faite par la reconnaissance des Empreintes d'Articulation du Doigt (EAD ou FKP), on commence par avoir les images des empreintes, dans une base de données des empreintes (FKP) de ces personnes qui seront connues et enregistrées dans le système. Toutes les images sont associées à un vecteur de caractéristiques. Ces caractéristiques ne changent pas pour une même personne, mais elles sont différentes d'une personne à l'autre. La reconnaissance consiste alors à la comparaison du vecteur de caractéristiques du FKP à reconnaître avec ceux des FKP de la base de données.

III-2.2 La Base de données de FKP: Les images de cette base de données sont capturées à l'aide du dispositif d'écrit ci-

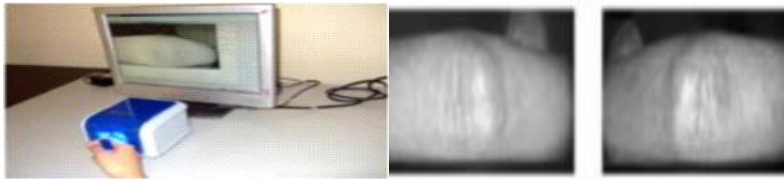
dessus au sein de (Poly U). La base de données PolyU-FKP contient 165 personnes dont 125 personnes sont des masculins. 143 personnes ayant l'âge compris entre 20 et 30 ans et les autres ayant l'âge entre 30 et 50 ans. Les images de chaque doigt sont capturées en deux sessions avec un intervalle de 25 jours entre les deux sessions. Six images de chaque doigt ont été collectées. Quatre doigts pour chaque personne sont capturés, à savoir, l'index gauche (Left Index Finger-LIF), l'index droit (Right Index Finger-RIF), le milieu gauche (Left Middle Finger-LMF) et le milieu droit (Right Middle Finger-RMF). Par conséquent, 48 images des quatre doigts sont collectées pour chaque personne. La base de données finale rassemble un total de 7920 images en niveaux de gris des doigts, gauches et droits. La figure III.2 illustre quelques exemples d'images de cette base de données [1]. Notre base de données composé des images d'empreintes d'articulations du doigt de 5 personnes du : l'index et middle fingers, de la main gauche et droite. Il y a 12 images qui sont prises pour chaque empreinte d'articulation du doigt. Et on a des images des empreintes de la main gauche et droite de 5 personnes qui sont filtrés et mise en gris.

III-2.3 L'acquisition des données :

Pour avoir les meilleures conditions lors de l'acquisition des données l'environnement d'acquisition devrait être stable le plus possible afin que les perturbations sur les images de la base, de la même personne, soient minimales. En général, le

processus d'acquisition stable permet d'améliorer les performances de la reconnaissance des personnes.

Le dispositif qu'on dispose pour l'acquisition des données se compose d'un support de doigt, une source de lumière LED a une forme d'un anneau, une lentille, une caméra CCD et une carte d'acquisition.



Fig(1) : Le dispositif d'acquisition des données Fig(2) : Des empreintes d'articulations

III-2.4 La manipulation des images :

Ces 12 images de l'empreinte (De chaque doigt) seront scindées en deux groupes : un groupe pour faire l'enrôlement et l'autre pour le test des techniques, et après en savoir plus sur leurs performances. Dans notre test que nous avons fait, la base de données a été construite de deux étapes :

Images d'enrôlement : La première, la cinquième, et la neuvième image de chaque personne servent pour l'étape d'apprentissage.

Images Tests : Les 9 images restantes de chaque personne servent à réaliser les différents tests.

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

comme un imposteur, l'objectif est d'évaluer le taux de reconnaissance de l'algorithme utilisé, en suivant un protocole de test se base sur la mesure du taux de reconnaissance.

III-3 Partie programmation:

III-3.1 Premier partie:

- On commence par définir la base de données qui contient les empreintes, on choisit le type d'empreinte à enrôler, soit: Left-index, right-middle etc., en choisissant par des vecteurs les images voulus.

- La phase d'enrôlement, consiste à lire les images contenues dans la base de données.

On aligne les images choisies, après on extrait les caractéristiques de chaque une en utilisant premièrement la Méthode Local Phase Quantization (LPQ) ensuite la méthode Local Binary Pattern(LBP).

- La phase précédente, on la refait plusieurs fois avec les autres images d'empreintes d'articulation de doigts des deux mains

- La phase de reconnaissance :

Après l'extraction des caractéristiques et des traits uniques de chaque image, on va pouvoir comparer entre ces dernières afin de savoir si elles se correspondent ou pas, en utilisant la méthode de la distance euclidienne.

- On conserve nos résultats de ce teste dans un fichier .mat pour les garder et les utiliser dans la Deuxième partie

III-3.2 Deuxième partie :

- Evaluation et l'identification :

- Initialiser les valeurs des points et des vecteurs et des matrices.
- Créer deux fonctions, une pour charger les résultats de partie une, et l'autre pour normaliser la distance des matrices chargés.
- Calculer le nombre des imposteurs et les clients.
- Calculer les erreurs FRR (False Reject Rate), FAR (False Acceptance Rate), GAR (Genuine Acceptance Rate) du système pour la courbe en boucle ouvert .
- Calculer le range et le taux d'identification pour la courbe en boucle fermé.
- illustration des figures des courbes des erreurs FRR FAR GAR et des courbes CMC et ROC

III-4. Conclusion :

Ce chapitre nous avons montré, le programme réalisé pour la reconnaissance à partir de base de données, en traitant les images avec la méthode de distance euclidienne, ensuite nous avons vu le calcul du taux des différentes erreurs de système afin d'évaluer les performances de système et ses méthodes utilisées.

Chapitre IX: Interprétation expérimentale des résultats

IX-1 Introduction

Ce chapitre regroupe les résultats expérimentaux de la reconnaissance des images FKP et puis l'identification des personnes, faites avec les algorithmes LPQ et LBP sur la base de données qui contient plusieurs images des empreintes de plusieurs personnes. Donc sur cela, on voit que notre travail consiste à concevoir un système d'identification biométrique des individus par la reconnaissance FKP en se basant sur LPQ et LBP qui sont essentiellement utilisées pour extraire les caractéristiques des images pour chaque modalité (index gauche (LIF), médian gauche (LMF), index droit (RIF), médian droit (RMF)).

IX-2 La méthode basée sur la méthode LPQ :

La méthode LPQ est basée sur quatre paramètres importants : la taille de fenêtre (windows size), le nombre des blocs et le nombre des filtres. Pour cela, des tests empiriques ont été exécutés afin d'en choisir les meilleurs paramètres de cette méthode. Dans le tableau suivant, nous avons mis les résultats de cette expérience en calculent à chaque fois erreur (EER) des différentes empreintes (FTP) des mains droite et gauche.

IX-2.1 les résultats pour chaque doigt de main avec la méthode LPQ :

D'après les courbes ROC et CMC du système en boucle ouvert et fermé d'empreintes d'index de la main gauche (Left-index) :

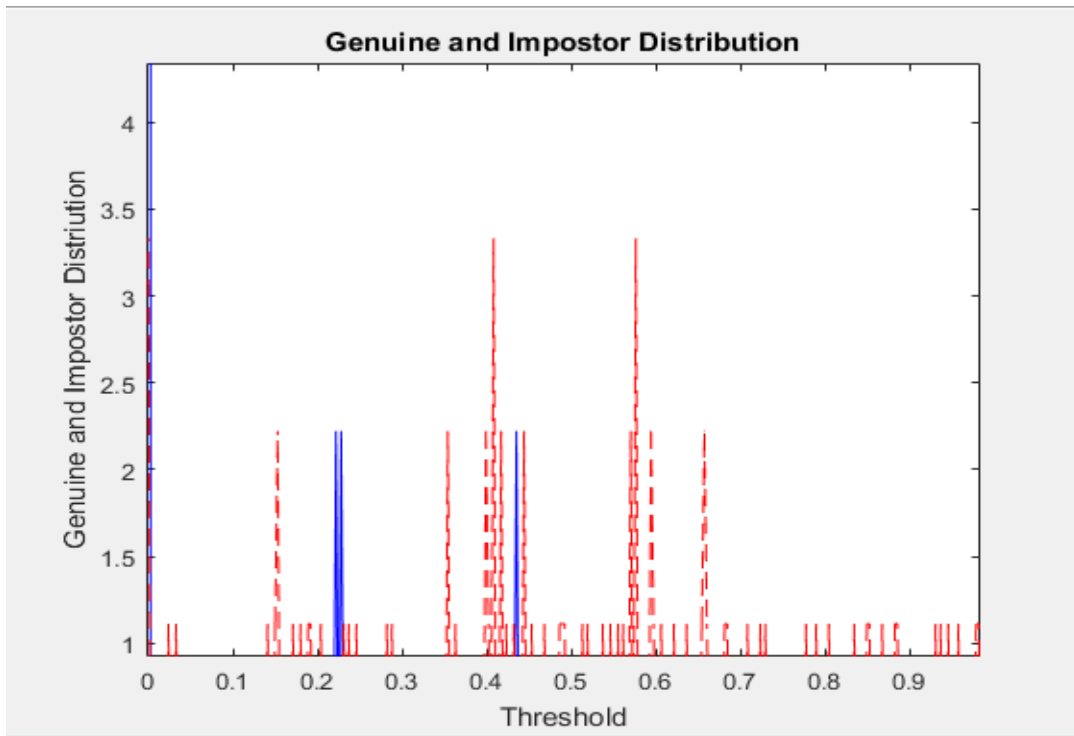


Figure IX.1: Genuine and Impostor Distribution of LBQ Method

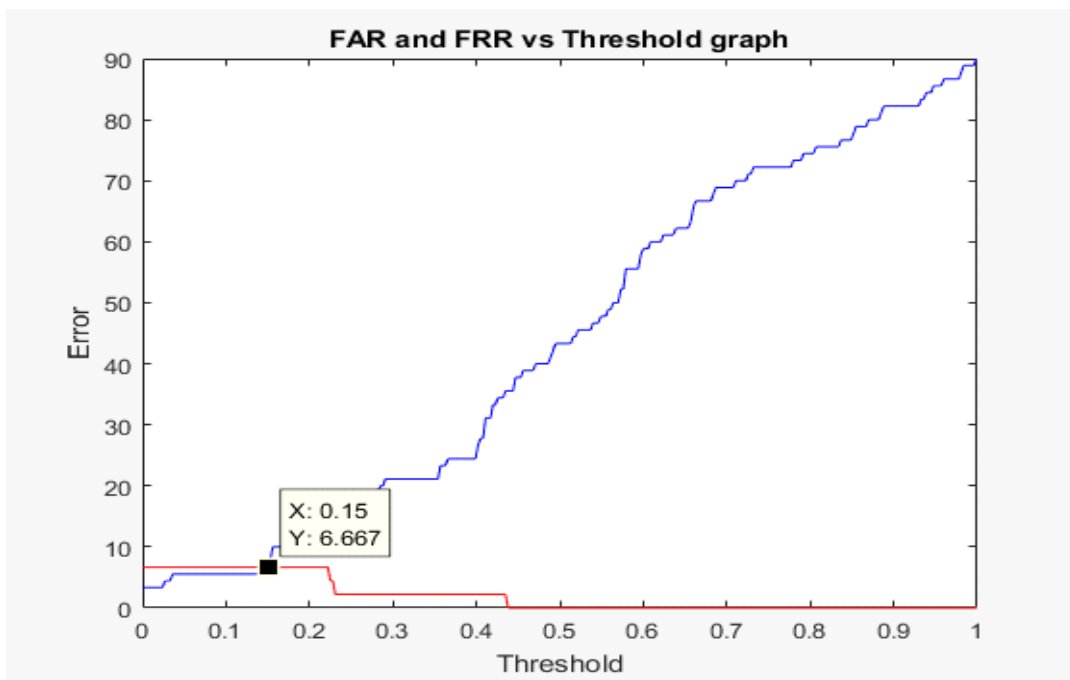


Figure IX.2: FAR and FRR vs Threshold graph of LBQ Met

Boucle fermé :

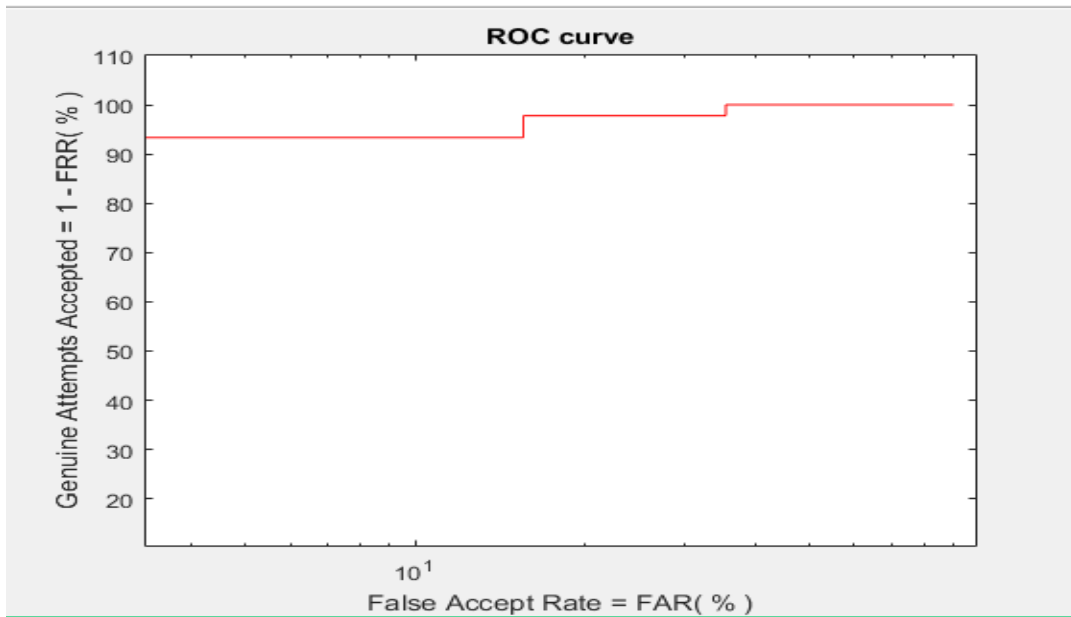


Figure IX.3: ROC curve_1 of LBQ Method

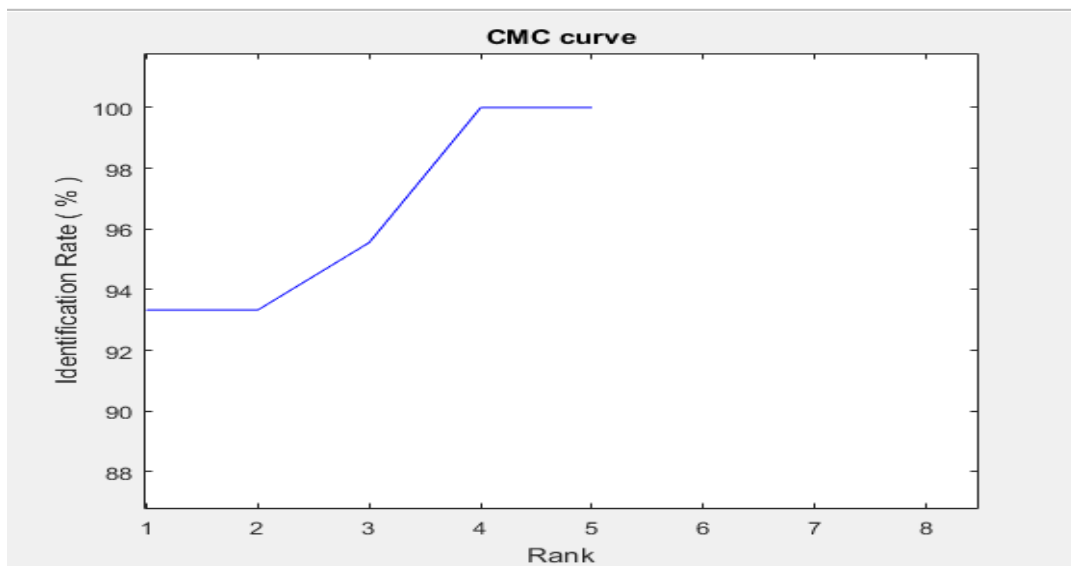


Figure IX.5: CMC curve of LBP Method

En faisant la même chose avec les autres empreintes de doigt Left-middle..., on peut en déduire les paramètres suivants :

| Modalité | Ensemble ouvert | | Ensemble fermé | |
|----------|-----------------|-------|----------------|-----|
| | EER | TO | ROR | RPR |
| LIF | 6.667 | 0.147 | 93.33% | 1 |
| LMF | 0 | 0.28 | 100% | 1 |
| RIF | 0 | 0.393 | 100% | 1 |
| RMF | 0 | 0.288 | 99,94% | 1 |

Tableau III.1: Résultats obtenus selon la méthode LBQ IX-3-La méthode basée sur la méthode LBP :

C'est basées sur les images des FKP, qui ont été examinées pour l'évaluation du taux d'identification on fait notre expérience en fonction de la méthode LBP

IX-3.1 les résultats pour chaque doigt de main avec la méthode LBP :

D'après les courbes ROC et CMC du système en boucle ouvert en utilisant la méthode LBP :

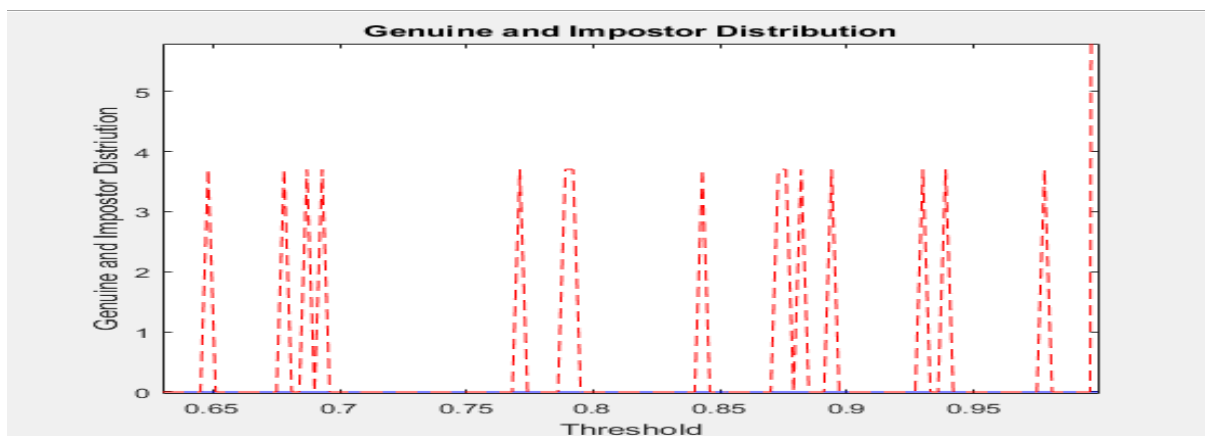


Figure IX.6:Genuine and Impostor Distribution of LBP Method

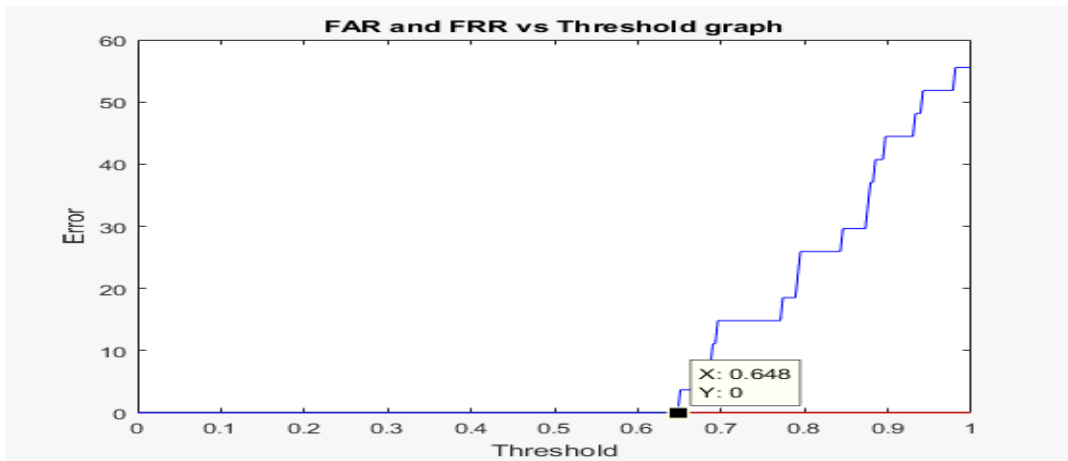


Figure IX.7: FAR and FRR vs Threshold graph of LBP Method

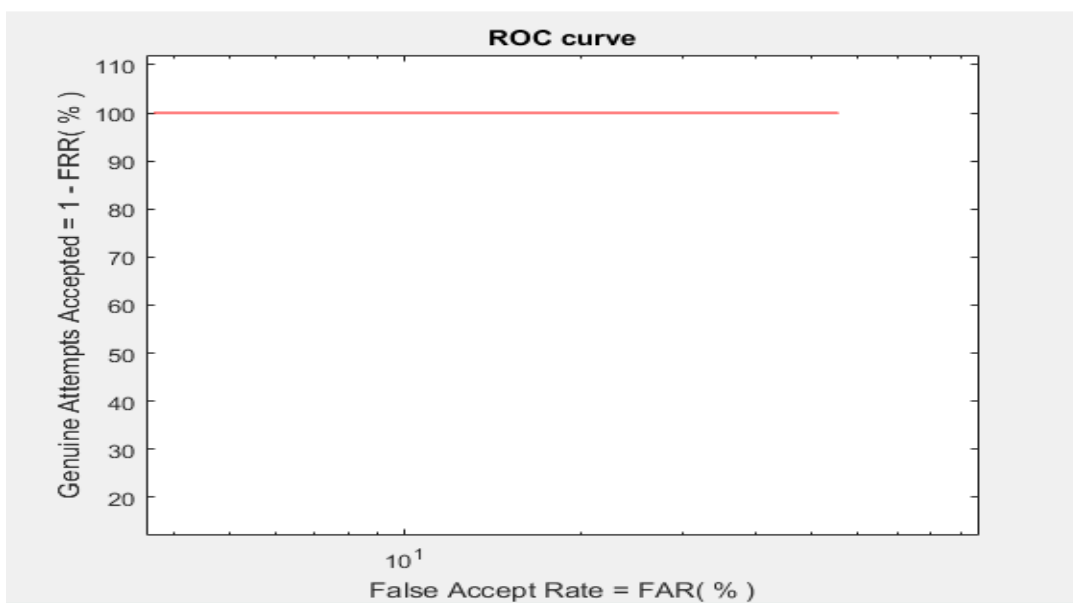


Figure IX.8: ROC curve_1 of LBP Method

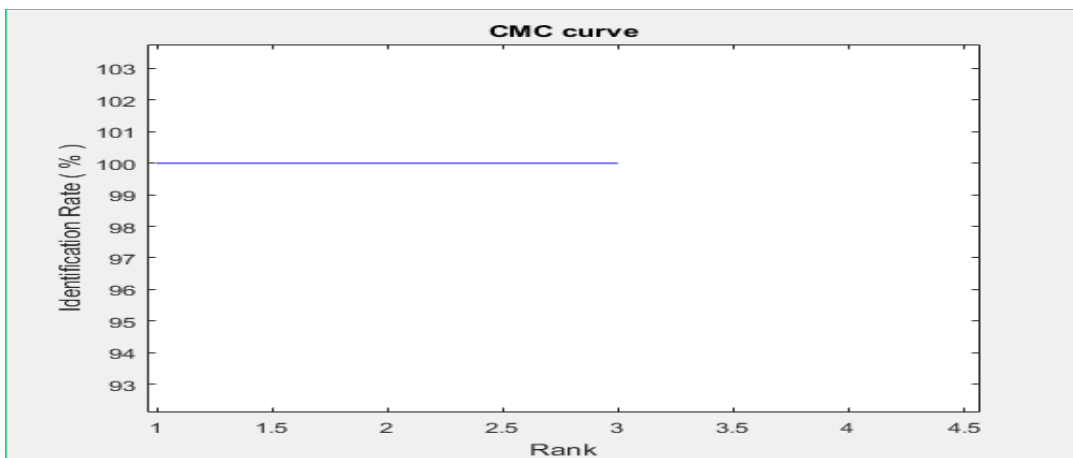


Figure IX.10: CMC curve of LBP Method

Ces résultats du doigt Left-middle, pour les paramètres des autres doigts sont dans le tableau suivant :

| Modalité | Ensemble ouvert | | Ensemble fermé | |
|----------|-----------------|-------|----------------|-----|
| | EER | TO | ROR | RPR |
| LIF | 3.33 | 0.111 | 92.59% | 1 |
| LMF | 0 | 0.648 | 100% | 1 |
| RIF | 0 | 0.573 | 100% | 1 |
| RMF | 3.704 | 0.003 | 96.3% | 1 |

Tableau III.2: Résultats obtenus selon la méthode LBP

IX-4 Etude comparative entre les deux méthodes une fois par rapport à l'ensemble fermé et ouvert :

| Ensemble ouvert | | | Ensemble fermé | | |
|-----------------|-----|-------|----------------|-----|------------|
| valeurs | EER | TO | ROR | RPR | |
| Méthode | | | | | |
| LBQ | 0 | 0.28 | LMF 100% | 1 | LMF RIF |
| LBP | 0 | 0.573 | RIF 100% | 1 | LMF RIF |

Tableau III.3: Comparaison entre les deux méthodes

Les critères de comparaison sont le taux d'identification et le temps de calcul. Le but est de sélectionner la meilleure méthode pour concevoir un système d'identification :

Et d'après le tableau précédent (Tableau III.3) on peut en conclure les résultats, Le temps de calcul du système basé sur la méthode LPQ, est moins grand par rapport au système basé sur la méthode LBP, donc LPQ a donné de bon résultat (surtout par l'empreinte LMF) par rapport LBP. Tout dépend de l'application visée, on peut faire un compromis entre ces deux paramètres d'évaluations (taux d'identification et temps de calcul). Cependant, pour une application temps réel, le système basé sur RMF avec la méthode LBP est bien adapté

Finalement, d'après ces résultats, le système d'identification par FKP est un système fiable. Il permet une bonne séparabilité des classes clients et imposteurs.

IX-5 Conclusion

Dans ce chapitre, les résultats expérimentaux présentés ont mené à l'élaboration d'un système d'identification des personnes par reconnaissance d'empreintes des articulations des doigts. Pour entreprendre à cela, Nous avons utilisé deux systèmes biométriques différents pour expérimenter la base de données. Ces systèmes utilisés sont examinés dans le but d'améliorer et évaluer le taux d'identification des modalités dans les deux modes d'identification, ensemble ouvert et ensemble fermé. Après, Les résultats sont pris et discutés

Conclusion générale:

La biométrie est un domaine à la fois passionnant et rigoureux. Elle utilise, des outils mathématiques souvent très développés, pour identifier et reconnaître des individus, nous obligeant à travailler dans un contexte d'immense diversité. Cette diversité se manifeste également dans beaucoup d'algorithmes qui ont été mis pour la reconnaissance par l'empreinte.

Dans ce mémoire, nous nous sommes intéressés au problème de la reconnaissance d'empreinte d'articulation de doigts (FTP). Notre travail consiste à la mise au point d'un algorithme ou programme destiné à reconnaître un individu par ses empreintes d'articulation (FTP), on commence par Le prétraitement optimisation de la chaîne de traitement d'images permettait d'améliorer la qualité du système en utilisant d'autres opérateurs de filtrage, ensuite en utilisant la méthode « LBQ-LBP » qui se base sur une analyse des informations acquise dans la méthode de prétraitement et ensuite l'extraction des caractéristiques des modalités biométriques et puis calculer termes de taux d'égale erreur (EER), de taux de reconnaissance et de séparation globale des distributions des imposteurs et clients et Après avoir les résultats.

En dernier, c'est L'utilisation des méthodes de décision et de comparaison telles que LBQ, LBP,... etc. et Réaliser une hybridation de deux méthodes pour améliorer le taux de reconnaissance. S'orienter vers La multi-modalité qui permet d'améliorer de manière systématique la performance d'un système biométrique.

Bibliographie :

[1] S.Boudjelel " Détection et identification d'individu par méthode biométrique" UMMTO 2014 .

Prise de Thèse: BenaggaAbderahmane "Reconnaissance des personnes basée sur l'empreinte d'articulation de doigt" KasdiMerahOuagala.

[2] thèse de doctorat de Benchennaneibtissem "Etude et mise au point d'un procédé biométrique multimodale pour la reconnaissance des individus"

[3]. FATIHA, SAIDAT DJEMAA-GUEZIZ. "Identification des personnes par l'empreinte de l'articulation des doigts. " OUARGLA : UNIVERSITE KASDI MERBAH OUARGLA, 2016.

[4]. Meriem, Fedias. » "Combinaisons de données de "espaces couleurs et de méthodes de Vérification d'identité pour l' authentification de visages." « Biskra : Université Mohamed Khider .mpreinte de l'articulation de doigt" KasdiMerbahOuagala.

[5]. Soumia, BENOUAER Aichouche-TAHRINE. "Système biométrique basé sur les motifs Locaux binaires orientés (LBP^o)". OUARGLA : UNIVERSITE KASDI MERBAH OUARGLA, 2016.

[6]. Abdelmoumen, ZITOUNI Sif Eddine-SACI. "Authentification et Identification biométrique des personnes par les empreintes palmaires. " OUARGLA : UNIVERSITE KASDI MERBAH OUARGLA, 2016.

[7]. LAMARE, François. "OCT en phase pour la reconnaissance biométrique par empreintes digitales et sa sécurisation. "Paris : École doctorale : Informatique, Télécommunications et Électronique de Paris, 2016.

[8]. FATIMA, BOUKRAA. "Caractéristiques Biométrique pour l'identification." ORAN : université d'oran 1, 07-04-2016.

[9]. Ibtissam, BENCHENNANE. "Etude et mise au point d'un procédé biométrique multimodale pour la reconnaissance des individus. " Oran : Université des Sciences et de la Technologie d'Oran Mohamed Boudiaf, 2016.

[10]. Arbaoui, O. Moulay Brahim " Identification des personnes par les articulations des doigts. " Ouargla : Université KasdiMerbah , 2015.

[11]. Abes, A. Ben Khalif, "Identification d'individus par reconnaissance d'empreintes palmaires. " Ouargla : Université KasdiMerbah, 2008.

[12]. Babich, Aleksandra. "Biometric authentication. Types of biometric identifiers " Helsinki : university of applied sciences, 2012.

- [13]. ashbourn, Julian. "Guide To Biometrics For Large-Scale Systèmes." springer :s.n., 2011.
- [14] D.L. Woodard and P.J. Flynn, "Finger surface as a biometric identifier", CVIU, vol. 100, pp. 357-384, 2005.
- [15] C. Ravikanth and A. Kumar, "Biometric Authentication using Finger-Back Surface", CVPR'07, pp. 1-6, 2007.
- [16] L. Zhang,, "Finger knuckle print : anew biometric identifier", IEEE, pp. 1981-1984,Hong-Kong, 2009.
- [17] A. Morales et al, "Improved finger-knuckle-print authentication based on orientation enhancement", electronics letters, Vol. 47 No. 6 , 17th March 2011.
- [18] HarbiAlMahafzah et al, "Multi-Algorithm Decision-Level Fusion Using Finger-Knuckle-Print Biometric». Springer India 2014.
- [19]. Babich, Aleksandra. "Biometric authentication. Types of biometric identifiers." Helsinki : university of applied sciences, 2012.
- [20]. MORIZET., Nicolas. "Reconnaissance Biométrique par Fusion Multimodale du Visage et de l'Iris." Paris : Ecole Nationale Supérieure des, 18 Mars 2009.
- [21]. Meriem, Fedias. "Combinaisons de données d'espaces couleurs et de méthodes de Vérification d'identité pour l'authentification de visages." Biskra : Université Mohamed Khider .
- [22]. Akrouf, S."Une approche multimodale pour l'identification du locuteur" .Setif : Université Ferhat Abbas, 2011. Thèse de Doctorat.
- 23]. Ababsa, Guerfi. "Authentification d'individus par reconnaissance de caractéristiques biométriques liées aux visages 2D/3D. " Evry : Université d'Evry Val d'Essonne, 2008.
- [24]. Guesmi, H. "Identification de personnes par fusion de différentes modalités biométriques." French : Université de Rennes, 2014. Thèse de Doctorat.
- [27] "l'identification des personnes par l'empreinte de l'articulation des doigts " UNIVERSITE KASDI MERBAH OUARGLA.