République Algérienne Démocratique et Populaire
Ministère de l'enseignement supérieur et de la recherche scientifique
Université 8Mai 1945 – Guelma
Faculté des sciences et de la Technologie
Département d'Electronique et Télécommunications

Mémoire de fin d'étude
Pour l'obtention du diplôme de Master Académique

Domaine : **Sciences et Technologie**
Filière : **Electronique**
Spécialité : **Instrumentation**

La reconnaissance des individus par leur empreinte des articulations des doigts

---

Présenté par :

Berredjem Achref

Sous la direction de :

Dr. Bourouba Hocine

Juillet 2019

Dédicaces

Je dédie ce modeste travail à celle qui m'a donné la vie, le symbole de tendresse, qui s'est sacrifiée pour mon bonheur et ma réussite, à ***ma mère****.*

A ***mon père****, école de mon enfance, qui a été mon ombre durant toutes les années des études, et qui a veillé tout au long de ma vie à m'encourager, à me donner l'aide et à me protéger.*

Que dieu les gardes et les protège ;

Je dédie toutes la famille berredjem ;

*A mes adorables sœurs (****yosra*** *et* ***sara****) ;*

A mes frères (oussama et ***ayoub****);*

A tous mes amis ;

A tous ceux qui me sont chères ;

A tous ceux qui m'aiment ;

A tous ceux que j'aime ; Je dédie ce travail ;

Remerciements

Mon remerciement et mon profonde gratitude vont à mon promoteur Monsieur Bourouba Hocine pour son encadrement, son suivi et ses conseils tout au long de cette période.

Nos remerciements et notre gratitude vont aux professeurs et enseignants de département d'électronique ainsi que ses étudiants et son personnel côtoyés tout au long de notre cursus universitaire.

Je tiens aussi à remercier mesdames et messieurs les membres du jury pour leur précieux temps accordé à l'étude de mon mémoire.

Que toute personne ayant œuvré de près ou de loin à la réalisation de ce projet par une quelconque forme de contribution, trouve ici le témoignage de mon plus profonde reconnaissance.

RESUME

L'authentification personnelle des individus trouve des applications dans différents domaines importants, allant de la criminalistique aux services commerciaux et gouvernementaux. Les caractéristiques biologiques des individus ont été utilisé comme système de sécurité efficace dans ce que nous appelons le système biométrique. Ces systèmes dépendent des caractéristiques particulières du corps humain telles que les empreintes digitales, la forme des yeux, la marche, le son, etc.

Dans ces systèmes, les empreintes FKP sont importantes en raison de leurs avantages, tels que la facilité d'utilisation, la haute sécurité et la simplicité. Sur la base de tout cela, nous avons développé un système d'identification par le biais des empreintes des articulations des doigts (finger knuckle print (FKP)). Dans tous les systèmes biométriques, il existe différentes techniques d'extraction des caractéristiques pour décrire les informations de texture. Dans notre travail, nous avons utilisé la méthode de quantification de phase locale LPQ, et la méthode de motif binaire locale LBP. Notre travail est appliqué à une base de données connue dans ce domaine et a donné des résultats acceptables.

Mots-clés : Technique biométrique, empreinte FKP, , extraction de caractéristiques, LBP.

Abstract

Personal authentication of individuals has applications in a variety of important areas, ranging from forensic science to commercial and government services. The biological characteristics of individuals have been used as an effective security system in what we call the biometric system. These systems depend on the particular characteristics of the human body such as fingerprints, eye shape, walking, sound, etc.

In these systems, FKP fingerprints are important because of their advantages, such as ease of use, high security and simplicity. On the basis of all this, we have developed an identification system using finger knuckle print (FKP). In all biometric systems, there are different techniques for extracting characteristics to describe texture information. In our work, we used the LPQ local phase quantization method,

and the LBP local binary pattern method. Our work is applied to a database known in this field and has produced acceptable results.

ملخص

تجد عملية تحديد الهوية الأفراد تطبيقات في مجموعة متنوعة من المجالات المهمة، من الطب الشرعي إلى الخدمات التجارية والحكومية. تم استخدام الخصائص البيولوجية للأفراد كنظام أمان فعال في ما نسميه النظام البيومتري. تعتمد هذه الأنظمة على خصائص معينة للجسم البشري مثل بصمات الأصابع وشكل العين والمشي والصوت ، إلخ.

في هذه الأنظمة، تعتبر بصمات أصابع FKP مهمة بسبب مزاياها، مثل سهولة الاستخدام والأمان العالي والبساطة. على هذا الأساس ، قمنا بتطوير نظام تحديد الهوية من خلال بصمة إصبع المفصل.(FKP)

في جميع النظم الحيوية ، هناك تقنيات مختلفة لاستخراج الميزات لوصف معلومات النسيج. في عملنا ، استخدمنا طريقة تقدير حجم المرحلة المحلية LPQ وطريقة النمط الثنائي المحلي .LBP. يتم تطبيق عملنا على قاعدة بيانات معروفة في هذا المجال وقد حقق نتائج مقبولة .

Liste des figures

Liste des tableaux

Liste des Abréviation

CCD : Charged Coupled Device

CMC : Cumulative Match Curve

DB : Data Base

DET : Detection Error Trade-off curve

DOG : Difference of Gaussians

EER : Equal Error Rate

FAR : False Acceptance Rate

FRR : False Rejection Rate

FKP : Finger Knuckle Print

IBG : International Biometric Group

ICA : Independent Component Analysis

HTER : Half Total Error Rate

LBP : Local Binary Pattern

HTER : Taux d'erreur moyenne ("Half Total Error Rate ")

LED : Light-Emitting Diode

LIF : Left Index Fingers

LMF : Left Middle Fingers

LPQ : Local Phase Quantization

PCA : Principal Component Analysis

PIN : Personal Identification Number

RIF : Right Index Fingers

RMF : Right Middle Fingers

ROI : Region Of Interest

ROR : Rank One Recognition

RPR : Rank of Perfect Recognition

ROC : Receiver Operating Curve

TER : Total Error Rate

Introduction générale

Introduction générale

Les technologies biométriques couvrent un large ensemble de techniques permettant d'identifier les personnes et d'automatiser l'authentification de l'identité en utilisant les caractéristiques physiques ou comportementales des personnes concernées. Parmi les nombreuses techniques biométriques, la biométrie à base des traits de la main a été la plus reconnue et suscité beaucoup d'intérêt. Non seulement en raison de ses performances supérieures qui est nécessaire pour les applications de haute sécurité, mais aussi pour leur caractère distinctif, leur confort d'utilisation et leur acceptation.

En générale, la biométrie à base des traits de la main peut être divisée en deux grandes catégories : la partie palmaire et la partie dorsale. La première recouvre les zones proches de la paume. Les attributs biométriques largement utilisés extraits de cette partie de la main sont : L'empreinte digitale, palmaire, des veines du doigt, des veines de la paume, et des articulations du doigt palmaire. Par contre, la partie dorsale de la main occupe la zone située derrière la partie palmaire et la plupart des modalités biométriques utilisables de cette partie sont les suivantes : la géométrie de la main, les veines des mains et l'empreinte des articulations des doigts dorsal. En plus, les combinaisons des traits ci-dessus ont été aussi utilisées comme traits biométriques liés à une main.

La région palmaire est supposée contenir plus de détails informatifs que la partie dorsale et plusieurs systèmes biométriques uni modaux multimodaux ont été développés utilisant la biométrie par empreinte digitale et l'empreinte de la paume.

Cependant, les personnes laissent leur traits biométriques lie a la partie palmaire tel que l'empreinte digitale inconsciemment partout où elles se touchent, ce qui augmente les possibilités d'attaques par des imposteurs sur ces systèmes de sécurité. En outre, cette zone est également plus exposée aux accidents, ce qui entraîne la perte de certaines de ces caractéristiques. Les modalités biométriques de la partie dorsale de la main gagnent donc en popularité. Par conséquent, les modalités biométriques de la partie dorsale de la main deviennent de plus en plus populaires. En raison de l'acquisition sans contact, ils ont moins de chance d'attaques d'imposteurs. Et comme il s'agit d'une zone inactive de la main, le risque de dégradation de l'information est réduit. Bien que les caractéristiques biométriques extraites de la partie dorsale ont montré qu'il est moins utile par rapport aux caractéristiques biométriques appartient à la palmaire

En tant que membres important de la famille de la biométrie liée à la main, l'authentification de personnes par l'empreinte des articulations des doigts et les

veines de la partie dorsale sont devenue de plus en plus importante dans le domaine des informations biométriques en raison des détails texturaux élevés qu'ils possèdent. Mais l'acquisition des veines dans l'environnement externe est un challenge qui nécessite des capteurs thermiques infrarouges coûteux avec de nombreux algorithmes complexes pour le prétraitement. Par contre, les empreinte des articulations des doigts sont acquises par un simple appareil photo numérique et sont largement acceptées par les utilisateurs. Incontestablement, FKP fait référence aux motifs de peau de la surface externe autour de l'articulation phalangienne du doigt et contient des caractéristiques structurelles distinctives, telles que les des motifs de texture. En général, ces caractéristiques possèdent des aptitudes potentiellement discriminatoires et conviennent relativement bien à l'identification d'une personne par rapport aux autres.

Le premier chapitre est destiné à la présentation générale de la biométrie. Il présente les définitions liées à la biométrie, les principales modalités physiques, comportementales et biologiques, leurs avantages et inconvénients. Une petite comparaison a été faite pour ces modalités. Enfin, les applications de la biométrie dans les domaines public et juridique ont été déclarées.

Le deuxième chapitre est consacré à la présentation générale de la biométrie liée à la main, et en particulier FKP et ça place parmi les autres techniques. Il décrit le principe de fonctionnement des systèmes biométriques et définit ensuite les outils utilisés pour évaluer leur performance. En plus, nous faisons un état de l'art de la reconnaissance en prenant les empreintes digitales des articulations des doigts.

Dans le troisième chapitre, nous avons présenté notre système global de reconnaissance FKP et les méthodes que nous avons utilisées pour extraire les textures. Nous présenterons les approches LBP (Local Binary Pattern) et LPQ (Local Phase Quantization). Ce sont les méthodes mathématiques basées sur la caractérisation de la texture de l'image par le calcul des valeurs LBP et LPQ pour chaque pixel de l'image et l'algorithme LDA pour la réduction dimensionnelle. Enfin, nous présentons les résultats expérimentaux obtenus par chaque méthode en analysant leur performance, suivie d'une discussion avec interprétation des résultats.

En termine par une conclusion générale qui résumera les résultats obtenus par les différentes approches et donnera quelques perspectives sur les travaux futurs.

Chapitre I : généralités sur la biométrie

Chapitre I : généralités sur la biométrie

I.1 Introduction

Traditionnellement, l'utilisation de caractéristiques personnelles comme les marques traditionnelle (permis de conduire, carte d'identité ou des connaissances (mot de passe) utilisés pour valider l'identité d'une personne n'est pas une solution fiable d'authentification. Les limites de ces approches traditionnelles sont qu'elles ne sont pas sûres et ne conviennent pas à l'authentification personnelle dans le monde moderne. Il est donc recommandé de développer des méthodes d'authentification personnelle plus cohérentes et plus réalistes pour contrôler la criminalisation et la fraude quotidiennes dans diverses activités sociales et commerciales. La biométrie est la science qui étudiée les méthodes de vérification ou l'identification d'identité, qu'on utilise pour différencier des personnes entre elles en se basant sur la reconnaissance des caractéristiques biologiques (physiologiques ou comportementales) de l'individu.

Nous introduirons dans ce chapitre quelques notions et définitions de base liées à la biométrie. Après définition, nous allons présenter les conditions nécessaire pour être qualifier de la biométrie, les modalités et les technologies biométriques telle que leurs définition leurs avantages, les inconvénients, leurs capteurs utilisés et les applications de chacun nous avons discuté un peu à l'identification et l'authentification, Et on fait une petite comparaison entre les modalités les plus utilisées.

I.2 Définition de la biométrie :

La biométrie est une mesure des caractéristiques biologiques pour l'identification ou l'authentification d'un individu à partir de certaines de ses caractéristiques: comportementales (exemple de la dynamique de frappe au clavier), physiques ou physiologiques (exemple de l'ADN) .Cette technique est utilisée de plus en plus aujourd'hui pour établir la reconnaissance des personnes dans un grand nombre d'applications diverses.

Le mot biométrie est une traduction du mot anglais « biométrics » qui correspond en français à l'anthropométrie. Il désigne dans un sens très large l'étude quantitative des êtres vivants, mais dans le contexte de la reconnaissance d'individus il est défini par :

- Selon le CLUSIF (Club de la Sécurité des systèmes d'Information Français), la biométrie est la science qui étudie à l'aide des mathématiques, les variations biologiques à l'intérieur d'un groupe déterminé.
- Selon la RAND (Public Safety and Justice), la biométrie est définie comme toute caractéristique physique ou trait personnel automatiquement mesurable, robuste et distinctif qui peut être employé pour identifier un individu ou pour vérifier son identité **[1].**

I.3 Propriétés souhaitées dans une caractéristique biométrique

Un certain nombre de caractéristiques biométriques peut être capturé dans la première phase du traitement. Toutefois, la capture automatique et la comparaison automatisée des données précédemment stockées nécessitent que les caractéristiques biométriques répondent aux caractéristiques suivantes :

- **Universalité :** la caractéristique biométrique doit exister, naturellement, chez toutes personnes (ex. empreinte).
- **Invariance** : les caractéristiques doivent être constantes sur une longue période de temps. Elles ne doivent être soumises à des différences significatives liées à l'âge.
- **Mesurabilité** : les propriétés biométriques doivent être mesurables. Les données doivent être facilement et passivement recueillies.
- **Singularité** : les caractéristiques biométriques doivent être uniques à chaque individu. Elles doivent être suffisantes pour distinguer une personne d'une autre.
- **Acceptatio*n*** : la saisie doit être possible d'une manière acceptable pour un grand pourcentage de la population.
- **Fiabilité et inviolabilité** : l'attribut doit être impossible de masquer ou de manipuler. Le processus doit garantir un niveau élevé de fiabilité et de reproductibilité.
- **Confidentialité** : le processus ne doit pas violer la vie privée de la personne.
- **Inimitabilité** : pour une précision sans faille, l'attribut ne doit pas être reproductible par d'autres moyens **[23].**

I.4 L'identification et l'authentification :

I.4.1 Identification :

L'identification d'une personne à plusieurs (1:N) : La biométrie peut être utilisée pour déterminer l'identité d'une personne, même sans son consentement. Par exemple, la numérisation d'une foule avec une caméra et l'utilisation de la technologie de reconnaissance du visage peuvent contribuer dans la détermination du sujet traité, en comparaison avec des profils stockés dans une ou plusieurs bases de données de référence.

I.4.2 Authentification / Vérification :

L'authentification d'une à une personne (1:1) : dans cette configuration, la biométrie est utilisée pour vérifier l'identité d'une personne. Par exemple, on peut assurer un accès physique à un espace sécurisé dans un bâtiment, par empreinte digitale ou on peut garantir l'accès à un compte bancaire ou à un guichet automatique par reconnaissance de l'iris.

L'authentification biométrique nécessite de comparer un échantillon biométrique préalablement enregistré (Modèle biométrique) à un autre échantillon biométrique nouvellement capturé (par exemple, celui capturé lors d'une connexion) **[23].**

I.5 Les principales modalités biométriques :

Il existe un très grand nombre de modalités biométriques, qui peuvent se diviser en trois catégories :

- **La biométrie physiologique ou morphologique**: elle est basée sur l'identification des traits physiques particuliers, tel que la reconnaissance de la forme du visage, de la rétine, de l'empreinte digitale, la géométrie de la main les articulations des doigts,… etc.
- **La biométrie comportementale**: elle se base sur l'analyse de certains traits personnels du comportement de l'individu comme sa façon de taper sur un clavier, le tracé de sa signature, sa démarche, etc…. **[2].**
- **L'analyse des traces biologiques:** utilise les caractéristiques biologiques des individus (ADN, salive, odeur etc.) qui sont très complexes à mettre en œuvre dans un système de reconnaissance

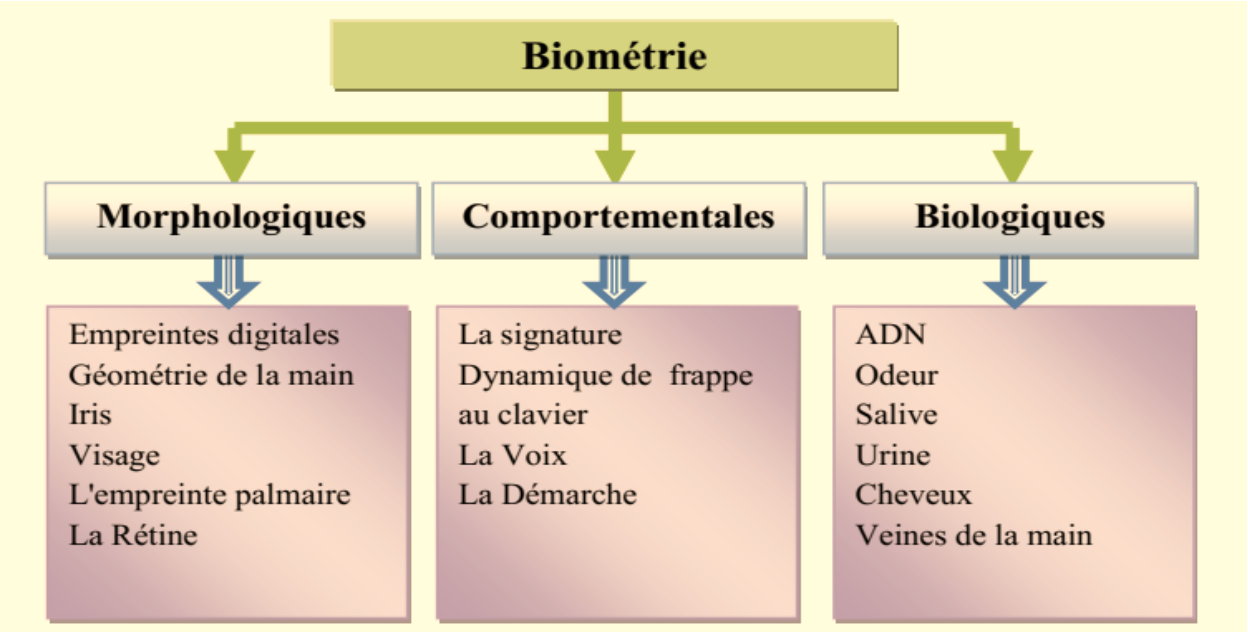


Figure I.1 : Classification des biométries morphologiques et comportementales **[6].**

I.5.1 la biométrie physiologique ou morphologique

i. La géométrie de la main :

❖ **Comment ça fonctionne**

La technique de reconnaissance biométrique qui utilise la mesure de la main (*handscan*) en est une des plus répandus à ce jour. La « mesure » de la main est en fait constituée de plusieurs mesures telles que les dimensions des doigts, les caractéristiques des articulations, la paume et la forme de la main.

La première étape de l'authentification est celle du scan, la personne doit poser sa main sur une platine. Les doigts doivent être correctement placés. Une caméra à infrarouge prend alors une image sous deux angles différents pour obtenir a une reproduction en 3D, là l'opération ne prend pas que de 3 seconde.

Le duplicata obtenu est alors numérisé et associé à un code. . Lors du scan du *badge* de l'employé (*hand punch*), le système vérifie la concordance des deux codes. Si l'employé n'utilise pas de *badge*, il doit entrer son code d'accès personnel (*hand key*). Comme avec les empreintes digitales, les technologies employant la géométrie de la main vont également vérifier la température et la pression sanguine du corps scanné pour en augmenter la validité.

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

- **Les points positifs**

L'analyse des caractéristiques de la main semble être mieux perçue dans le monde de l'éthique. En effet, elle serait moins pernicieuse et intrusive.

La technique requiert la rétention de fichiers moins volumineux, Par exemple, la numérisation d'une image d'une main ne représente qu'un espace d'environ 15 octets.

Les facteurs externes tels que l'humidité de la peau et la saleté sur la main n'empêchent pas une bonne prise de la mesure. Il en est de même pour les brûlures et les coupures mineures.

- **Les points négatifs**

Les taux de faux positifs sont malheureusement plus élevés. En d'autres mots, il est plus facile pour les membres d'une même famille présentant des ressemblances physiques importantes, notamment au niveau des mains, de tromper le système.

Des maladies associées à la vieillesse, telle que l'arthrite, peuvent occasionner des déformations au niveau des doigts, lesquelles empêchent la reconnaissance de la main.

La géométrie de la main nécessite un *scanner* qui est plus gros que celui utilisé pour le *fingerscan*. Se faisant, son emploi devient embarrassant lorsqu'il est question de sécuriser un objet de petite taille telle qu'une clé USB ou un système GPS.

- **Usage**

Étant mieux acceptée socialement, l'utilisation de la main comme identifiant est davantage répandue que l'emploi des empreintes. Les milieux qui y ont recours sont très diversifiés. Par exemple, le Collège public Salagou de Clermont-L'Hérault

(France) utilise la reconnaissance des contours de la main pour permettre l'accès à sa cantine. Le géant *Coca-Cola* l'utilise afin de facilité la gestion du personnel. Ainsi, au lieu de sortir sa carte de punch à toute heure du jour, l'employé enregistre son arrivée, ses pauses et sa sortie simplement à l'aide de sa main. Le personnel à l'entretien du Musée du Louvre doit lui aussi s'identifier avec la paume de sa main pour accéder à certaines salles.

Malgré que plusieurs entreprises et entités l'utilisent, cette technologie ne semble pas très populaire auprès des compagnies qui protègent des données sensibles ou qui nécessitent une sécurité accrue **[5].**

ii. L'empreinte digitale :

L'empreinte digitale : est une signature que nous laissons derrière nous à chaque fois que nous touchons un objet. Les motifs dessinés par les crêtes et plis de la peau sont différents pour chaque individu ; c'est ce qui motive leur utilisation par la police criminelle depuis le 19è siècle.

Une empreinte digitale est une marque laissée par les crêtes des doigts, des mains, des orteils ou des pieds lorsqu'elles touchent un objet. Il en existe deux types : l'empreinte directe (qui laisse une marque visible) et l'empreinte latente (saleté, sueur ou autre résidu déposé sur un objet). Les empreintes digitales sont regroupées en trois catégories principales : l'arche, le tourbillon et la boucle. À l'intérieur de chacune de ces catégories, il y a un très grand nombre d'éléments qui nous différencient les uns des autres. En plus des cicatrices, il y a les fourches, les îlots et les espaces qui donnent un caractère unique aux empreintes latentes.

L'utilisation de l'empreinte digitale comme moyen d'identification d'une personne n'est pas nouvelle. En fait, les corps policiers utilisent cette technique depuis plus de 100 ans. Aujourd'hui, les empreintes digitales sont recueillies sur une scène de crime et sont ensuite comparées à celles contenues dans un serveur central

Figure I.3 : l'empreinte digitale

❖ **Avantage et inconvénient de l'empreinte digitale**

Les avantages sont:

- Le prix de l'identification digital est faible (cela reste accessible).
- La taille du lecteur biométrique d'empreinte digital n'est pas volumineuse et le système reste très simple à mettre en place.
- L'utilisation est facile, il suffit de poser son doigt dessus.

Les inconvénients sont:

- Cette technologie est ressentie comme intrusive.
- Certaines personnes peuvent créer de "faux doigt" en utilisant l'empreinte digitale d'une autre personne (sachant que l'empreinte est stockée dans la base de données du lecteur d'empreinte digitale).
- Le gros inconvénient est le manque d'hygiène, les traces de doigts se succèdent sur ce lecteur et ainsi les microbes se dispersent sur tout le lecteur ce qui rend celui-ci très sale **[8].**

❖ **Capture de l'image d'une empreinte digitale**

Obtenir des images numériques d'empreintes digitales n'est pas une chose simple, car la surface à capturer est de faible dimension par rapport au contenu des informations. De plus, certaines ethnies ont de très fines empreintes digitales par rapport à d'autres populations (la population asiatique par exemple), de même que pour les enfants. Il est donc important de faire le bon choix de capteur par rapport à la population d'utilisateurs.

Le point commun à toutes les technologies utilisées pour la prise d'image d'une empreinte, est que l'image est constituée à partir des points de contact du doigt sur le capteur

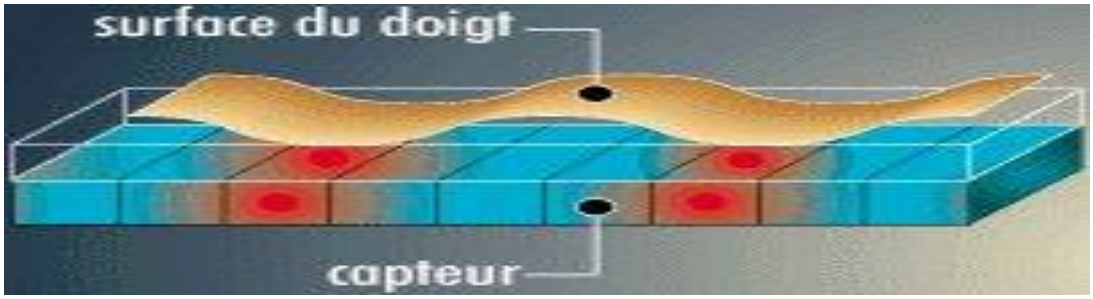


Figure I.4 : Capture de l'image d'une empreinte digitale

Les techniques utilisées pour la mesure sont diverses : capteurs optiques (caméras CCD/CMOS), capteurs ultrasoniques, capteurs de champ électrique, de capacité, de température...

Ces capteurs sont souvent doublés d'une mesure visant à établir la validité de l'échantillon soumis (autrement dit, qu'il s'agit bien d'un doigt) : mesure du constant diélectrique relatif de l'échantillon, sa conductivité, les battements de cœur, la pression sanguine, voire une mesure de l'empreinte sous l'épiderme...**[5].**

- **Capteur optique :**

Il s'assimile à une mini caméra. Le doigt est apposé sur une platine en plastique dur ou en quartz, qui est en vis-à-vis de la mini caméra. Il résiste très bien aux fluctuations de température, mais est gêné par une lumière ambiante trop forte.

- **Capteur en silicium :**

Il utilise l'un de quatre effets observables sur les semi-conducteurs : l'effet piézo-électrique, l'effet capacitif, l'effet thermoélectrique et l'effet photo-électrique.

Il est en général de très petite taille, d'une durée de vie assez longue, et son coût est très intéressant.

- **Capteur ultra sonique**

Il utilise une onde ultra sonore qu'il envoie vers le doigt, puis calcule le temps mis par l'onde pour faire un aller-retour et, point par point, fournit l'image de l'empreinte

Il est très précis, et hérite des propriétés des ultrasons de traverser certains matériaux (gants en latex, saletés, etc.).

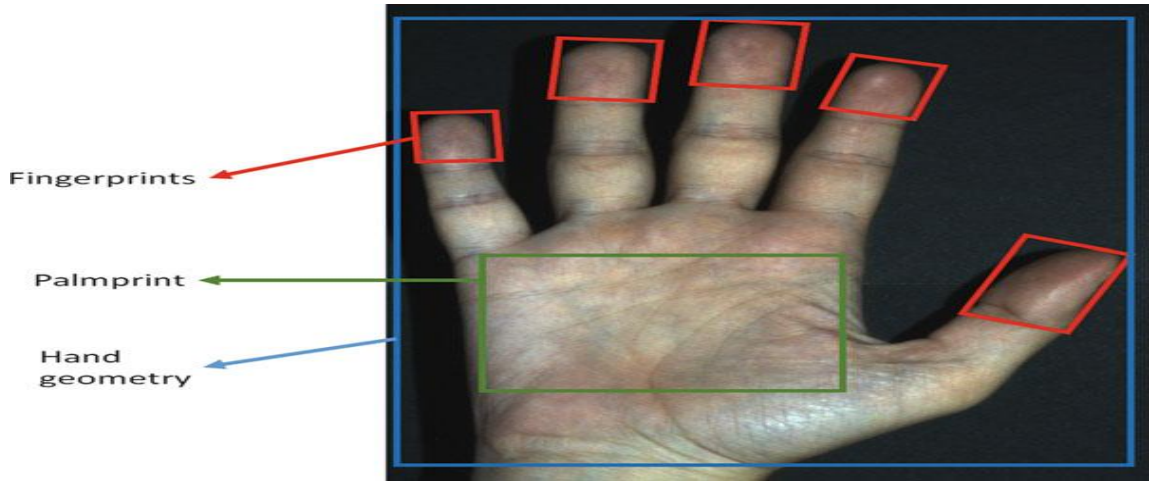
- **Capteur thermique**

La technique de capture thermique est utilisée par le FingerChip d'Atmel. Le capteur mesure une différence de température obtenue selon que la peau touche (dans le cas d'une crête de l'empreinte) ou ne touche pas (pour une vallée) le capteur.

iii. L'empreinte palmaire :

Les systèmes de reconnaissance d'empreintes palmaires sont une catégorie spécifique de systèmes biométriques manuels qui effectuent la reconnaissance en se concentrant sur la zone de la main, du poignet à la base des doigts. Plus précisément, les systèmes à base d'empreintes palmaires analysent la peau qui recouvre la surface interne de la main, qui est le même type de peau qui recouvre les empreintes digitales. Un aperçu schématique de l'empreinte palmaire et d'autres caractéristiques

biométriques de la main, en fonction de la taille de la zone analysée, est présenté sur la figure.



FigureI.5 : Aperçu schématique de l'empreinte palmaire ainsi que des autres traits biométriques de la main, en fonction de la taille de la zone analysée

iv. L'iris :

Le balayage de l'iris est l'une des techniques biométriques les plus intéressantes. Il est tentant de penser que l'iris est un mécanisme simple pour contrôler la quantité de lumière qui traverse le " cristallin " de l'œil et se concentre sur la rétine, mais l'iris est en fait une structure intéressante et complexe qui nous sert bien comme caractéristique d'identification individuelle.

Une étude plus poussée des photographies cliniques sur plusieurs décennies a permis de confirmer ce fait et l'idée que l'iris est au moins aussi unique qu'une empreinte digitale a été établie. Il a en outre découvert que non seulement le motif de l'iris était unique à l'individu, mais que les iris.

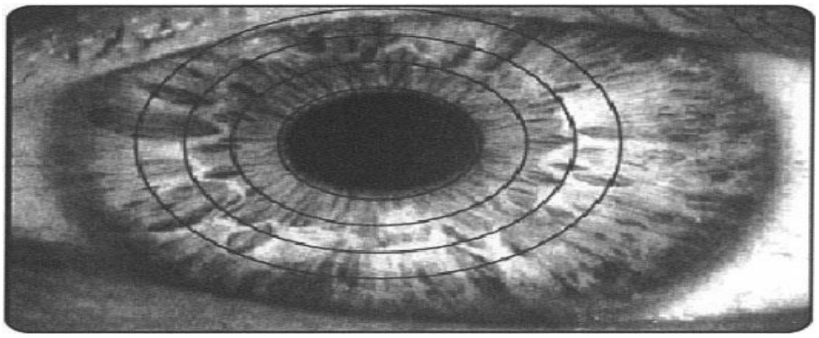


Figure I.6 : Texture de l'iris

L'unicité est une chose, mais capturer cette unicité à des fins de vérification automatisée de l'identité en est une autre. Il y a des avantages théoriques en ce que l'iris a tendance à avoir une géométrie polaire assez régulière, ce qui facilite la mise au point d'un système de coordonnées pour la reconnaissance des entités **[11].**

- **Avantage :**

La texture de l'iris est parfaitement stable au cours du temps et les derniers progrès de l'optique ont permis d'alléger les procédures. Selon Sagem, la vérification de l'identité prend aujourd'hui moins de 4 secondes. La technique reste extrêmement fiable même à travers des lunettes ou des lentilles **[12],** On a d'abord pensé que l'iris était unique lorsque les ophtalmologistes ont remarqué que les modèles d'iris étaient non seulement très individuels mais ne semblaient pas changer avec l'âge **[11].**

- **Inconvénients** :

La prise de vue n'est pas très simple : la taille de l'iris est très variable suivant la lumière ambiante ou l'état de fatigue, et les utilisateurs ont tendance à bouger. D'autre part, la fiabilité diminue proportionnellement à la distance entre l'œil et la caméra. L'infrastructure est plus lourde que pour les empreintes digitales (compter 12 000 euros pour un équipement de base) **[12].**

- **Capteur :**

La prise de vue de l'iris est effectuée le plus souvent par une caméra (caméra CCD monochrome 640 × 480) employée avec une source de lumière de longueur d'onde comprise entre 700 et 900 nm, invisible pour les humains.

- **Usage :**

Les applications potentielles de la biométrie à balayage de l'iris sont très répandues et des installations ont été réalisées dans le secteur financier pour les distributeurs automatiques de billets, pour un contrôle d'accès plus général dans plusieurs secteurs et pour diverses applications de haute sécurité **[11].**

v. La rétine :

La rétine est la couche sensorielle de l'œil qui permet la vision. Cette zone est parcourue par des vaisseaux sanguins qui émergent au niveau de la papille optique où l'on distingue l'artère et la veine centrale qui se divisent elle-même en artères et veines de diamètre plus faible pour vasculariser les cellules qui permettent la vision.

❖ **Avantage :**

- La rétine vérifie donc les quatre conditions pour être qualifiée de biométrique. Elle est unique d'après les observations des ophtalmologistes, elle est universelle puisqu'elle existe chez toute personne, elle est accessible puisqu'on peut acquérir son image grâce à un scanner externe et elle est permanente puisque le réseau vasculaire ne change pas durant toute la vie.
- La biométrie par la rétine est une technologie très ancienne, elle est la plus fiable et la plus dure à contrefaire

❖ **Inconvénients :**

- Cette technologie est très efficace mais assez contraignante pour les gens qui ont du mal à accepter de se faire examiner le fond de l'œil tant que l'œil est un organe très sensible à la lumière. Ce procédé est donc invasif et difficile à mettre en œuvre. C'est ce qui explique la réticence de cette technologie **[13].**
- Cette technique consiste tout bêtement à "reconnaître" quelqu'un par sa photo. Une webcam capture l'image du visage présenté, et l'envoie à un logiciel pour la numériser.
- Le logiciel repère d'abord la position des yeux pour procéder à un "alignement". En fonction de cet alignement, un relevé de différents points caractéristiques du visage est effectué (ailes du nez, forme du menton, écartement des yeux…). Un tracé géométrique personnel est alors enregistré comme gabarit (chaque visage est codé sous forme de fichier de 84 octets), et c'est sur ce dernier que s'effectueront ensuite les recherches.

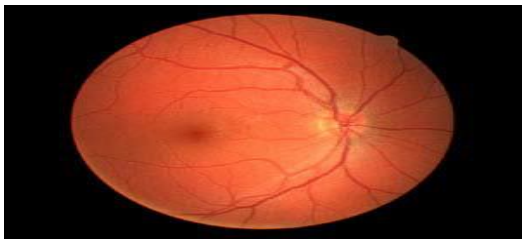


Figure I.7 : Image de fond de l'œil.

❖ **Applications**

La technique, issue du milieu médical, est connue depuis longtemps : dès les années 70, elle a été utilisée par l'armée américaine. Du fait de son utilisation peu aisée, elle reste aujourd'hui réservée aux domaines de haute sécurité. La CIA (Central

Intelligence Agency) et le FBI (Federal Bureau of Investigation) ont par exemple adopté l'identification rétinienne, et aussi certaines prisons américaines **[21].**

vi. La reconnaissance faciale :

Une des technologies les plus utilisées est celle de "Eigen face", développée par le MIT à partir d'analyses statistiques de milliers de visages. Elle consiste à décomposer le visage en plusieurs images faites de nuances de gris, chacune mettant en évidence une caractéristique particulière. Le système des "réseaux de neurones" sont encore plus performants, surtout dans des conditions difficiles de capture. Ils emploient un autre algorithme pour déterminer la similitude entre des captures d'images de visage et des gabarits.

Figure I.8 : La reconnaissance faciale

- **Avantages**
  - Le principal avantage, c'est que cette technologie est non intrusive, et peut même se dérouler à l'insu de l'utilisateur pour la vidéo.
  - Les progrès accomplis ces dernières années sont considérables. Au point que les systèmes sont aujourd'hui capables de reconnaître des individus même avec des artifices (fausses moustaches, barbe, lunettes…). "Seule une chirurgie importante du cartilage du visage pourrait tromper le système" affirme ainsi la société Zalix, qui vend une solution de reconnaissance faciale.
- **Inconvénients**

En position fixe et éclairée, les taux de reconnaissance sont effectivement très élevés, mais en vidéo la technique n'est pas encore au point. Même en imaginant que

la technique s'améliore, le visage est trop changeant pour être un repère biométrique suffisamment fiable.

Une étude américaine a par exemple montré qu'un changement d'angle de 45° de la caméra rendait le système quasi inutilisable. Du coup, plusieurs aéroports ont abandonné la technique.

- **Applications**

La technologie de reconnaissance faciale est aujourd'hui en pratique dans plusieurs casinos aux Etats Unis et en France (identification des joueurs interdits ou individus fichés), aéroports, stades (refoulement de supporters connus et dangereux), centres commerciaux ou grands magasins.

Mais pour des usages à grande échelle, la reconnaissance faciale est le plus souvent associée à une autre technique biométrique. Le gouvernement israëlien utilise un système combiné forme de la main / reconnaissance faciale pour filtrer les palestiniens en provenance de la bande de Gaza, et en Ouganda, les élections se déroulent à partir d'un fichier de "visages" d'électeurs **[14].**

I.5.2 La biométrie comportementale :

a. La reconnaissance vocale :

La biométrie est une science qui n'est pas encore au point. En effet, la reconnaissance vocale fait partie des domaines qu'il faut encore développer. Cette reconnaissance a des failles car elle dépend de plusieurs paramètres comme la qualité du micro, le fait qu'il ne doit pas y avoir de sons parasites lors de l'analyse ou des bruits de fond. Celle-ci est souvent utilisée pour les transactions par téléphone pour minimiser les fraudes mais elle n'est pas très efficace. L'un de ses avantages réside dans le fait que l'utilisateur n'est pas en contact direct avec l'appareil :son cerveau ne la perçoit pas comme intrusive.

Selon certains sondages elle reste quand même une des méthodes les plus utilisées. La reconnaissance vocale serait utilisé à 32% par les utilisateurs ensuite en second viendrait la reconnaissance par empreintes digitale à 27% puis la reconnaissance faciale à 20% et enfin les reconnaissances de la main et de l'iris à respectivement 12 et 10%.

❖ **Fonctionnement de la reconnaissance vocale :**

La reconnaissance vocale est simple d'utilisation car il n'y a que deux méthodes de reconnaissance vocale qui ne sont cependant pas très différentes. L'utilisateur peut enregistrer un mot de passe dans le système grâce à sa voix et il ne peut alors avoir accès à ce système uniquement si une voix exprime le bon mot de passe, l'accès sera donc autorisé et ce avec n'importe quelle voix. Selon la seconde méthode, l'utilisateur peut associer une sorte de voix (grave ou aigu...) à ce mot de passe afin que la machine sache qui est la personne qui parle. Par exemple, si une personne dit le bon mot de passe mais que sa voix ne correspond pas à la base de données du système, l'accès lui sera refusé. En revanche si le mot de passe et la voix correspondent, il sera autorisé. Cette méthode est donc un système avec deux conditions à remplir pour valider l'accès **[18].**

Figure I.9 : La reconnaissance vocale

❖ **Applications de reconnaissance vocale : quelle utilité ?**

Les applications de reconnaissance vocale sont aujourd'hui déclinées sur différentes plateforme (iOS et Android, BlackBerry, Nokia, etc.), et répondent à différents besoins pratiques liés aux usages nomades, plus particulièrement dans la vie professionnelle

- Utilisation en configuration mains-libres pour les commandes vocales standard (recherche dans le répertoire, appels)
- Traduction
- Recherche web
- Recherche d'adresses et d'itinéraires (ex : avec Google Maps)
- Mettre à jour ses statuts sur les réseaux sociaux (Facebook, Twitter) **[15].**

b. Signature dynamique

Chaque personne a un style d'écriture unique. On peut donc définir, à partir de la signature d'une personne, un modèle qui pourra être employé pour effectuer une identification. De plus, la signature est utilisée dans beaucoup de pays comme élément juridique ou administratif. Elle permet de justifier de la bonne foi d'une personne ou de la confondre devant des documents signés.

Figure I.10 : Capture d'une signature

❖ **Capture d'une signature :**

On distingue deux façons de capturer une signature, soit avec des capteurs qui s'assimilent à de simples scanners, soit par l'usage d'une tablette graphique et d'un stylet sensible à la pression.

- ✓ Scanner **:** son fonctionnement est à tout point identique aux scanners de bureau. Très simple à mettre en œuvre, cette méthode est utile pour des applications où le travail est répétitif mais trouve sa limite pour l'authentification de documents électroniques où une signature préalablement numérisée a été apposée.
- ✓ Tablette graphique : utilisée à la base dans les sociétés de design, on la retrouve aussi sur les assistants personnels (Palm, etc.). Elle permet d'obtenir les informations de variations de pression et de vitesse au moment où la personne signe. Elle est très simple à mettre en œuvre.

❖ **Les applications**

- ✓ Validation par la signature électronique de l'identité de l'acheteur en ligne.
- ✓ Gestion des chèques, opérations au comptoir, sécurisation des retraits… Vérification de l'identité des opérations en ligne ou par e-mail.

- ✓ Permet également de protéger les ordinateurs des personnes non autorisées, empêchant l'ouverture d'une cession NT à travers l'écran de veille sécurisé garantissant ainsi l'accès au réseau.
- ✓ Protection des documents par intégration du système dans MS Word, Adobe et les autres traitements de texte.
- ✓ Le verrouillage et déverrouillage des fichiers se fait de manière très aisée par une simple signature. Les documents, bases de données et images peuvent être verrouillés et envoyés par e-mail partout dans le monde et en toute sécurité **[17].**

c. La dynamique de la frappe (au clavier) :

La dynamique de la frappe est propre à chaque individu. Il s'agit en quelque sorte de la graphologie des temps modernes car nous écrivons plus souvent avec un clavier qu'avec un stylo. Les éléments analysés sont : vitesse de frappe, suite de lettre, temps de frappe, pauses...

L'objectif est de développer une solution biométrique à bas coût afin de renforcer la sécurité des mots de passe qui ne cessent de se multiplier dans la vie quotidienne. En associant la fourniture d'un mot de passe à la signature spécifique de la personne qui le tape sur un clavier, nous introduisons un deuxième facteur d'authentification peu onéreux et plus facilement accepté par les utilisateurs **[22].**

Figure I.11: La dynamique de la frappe (au clavier) :

❖ **Avantage :**

Elle est non intrusif, geste naturel pour un individu

❖ **Inconvénients :**

Elle dépend de l'état (physique, émotion, fatigue...)

❖ **Applications**

Documents administratif, bancaire, assurance **[20].**

I.5.3 La biométrie biologique :

i. La biométrie des gènes :

Figure I.12 : La biométrie des gènes

Une **empreinte génétique**, ou **profil génétique**, est le résultat d'une analyse génétique, rendant possible l'identification d'une personne à partir d'une petite quantité de ses tissus biologiques (bulbe de cheveux, sang, salive, sécrétion vaginale, sperme).

❖ **Les Avantages de la reconnaissance par l'ADN**

Au royaume de la biométrie, l'identification par ADN devrait être reine. Impossible à berner et valable de la naissance à la mort, la signature génétique d'un individu est la plus fiable pour identifier un individu!

❖ **Les inconvénients de la reconnaissance par l'ADN**

Mais cette technique présente d'importants défauts: elle coûte cher (600 $ à 1 500 $ par test), nécessite des analyses qui prennent plusieurs heures ainsi qu'un prélèvement de cellules (sang, salive, peau).

❖ **Applications**

- Pour l'instant, elle est donc réservée à l'identification à partir de prélèvements effectués sur des scènes de crime
- Cette technique est utilisée pour vérifier la parenté des réfugiés et des demandeurs d'asile, ou dans le cadre du regroupement familial **[19].**

I.6 Une représentation comparative entre les techniques biométriques :

Chaque technologie possédant des avantages et des inconvénients, acceptables Ou inacceptables suivant les applications.

Ces solutions ne sont pas concurrentes, elles n'offrent ni les mêmes niveaux de sécurité ni les mêmes facilités d'emploi. Le **tableau** résume une comparaison des traits biométriques.

TECHNIQUE	AVANTAGE	INCONVINIENT
EMPREINTE DIGITALE	➢ Cout ➢ Ergonomie moyenne	➢ Acceptabilité moyenne ➢ Possible d'attaque
Forme de la main	➢ Très ergonomique ➢ Bon acceptabilité	➢ Système encombrant et couteux ➢ Perturbation possible par des blessures
Visage	➢ Cout ➢ Bon acceptabilité	➢ Jumeaux, déguisement, ➢ Vulnérabilité à l'attaque.
Rétine	➢ Fiabilité ➢ Pérennité	➢ Acceptabilité très faible ➢ Contrainte d'éclairage
Iris	➢ Fiabilité	➢ Acceptabilité très faible ➢ Contrainte d'éclairage
Voix	➢ Facilite	➢ Vulnérable à l'attaque
Signature	➢ Ergonomie	➢ Dépond de l'état émotionnel de la personne ➢ Peu fable
Frappe de clavier	➢ Ergonomie	➢ Dépond de l'état physique de la personne ➢ Peu fiable

Tableau I.1: comparaison des traits biométrique **[10].**

I.7 Les applications de la biométrie :

Aujourd'hui, les principales applications sont la production de titres d'identité, le contrôle d'accès à des sites sécurisés, le contrôle des frontières, l'accès aux réseaux, systèmes d'information et stations de travail, le paiement électronique, la signature

électronique et même le chiffrement de données. Cette liste n'est pas exhaustive, et de nouvelles applications vont très certainement voir rapidement le jour.

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

I.7.1 Application commerciales :

Telles que l'accès au réseau informatique, la sécurité de données électroniques, le commerce électronique, l'accès d'internet, l'ATM, la carte de crédit, le contrôle d'accès physique, le téléphone portable, le PDA, la gestion des registres médicales, l'étude de distances, etc.…

I.7.2 Applications de gouvernement :

Telles que la carte nationale d'identifications, le permis de conduite, la sécurité sociale, le contrôle de passeport, etc.…

I.7.3 Applications juridiques :

Telles que l'identification de cadavre, la recherche criminelle, l'identification de terroriste, les enfants disparus, etc.**[1].**

I.8 Conclusion

Dans ce chapitre nous avons décrit les technologies utilisées dans les systèmes biométriques pour l'identification des personnes, leurs architectures et leurs différentes applications, ainsi nous avons montré les différentes modalités biométriques tout en soulignant les avantages et les inconvénients de chacune.et leur applications, Nous avons constaté aussi que pour être qualifier a la biométrie ca dépendent de plusieurs facteurs et qu'elles varient d'un système à un autre.

Parmi les modalités utilisées dans la reconnaissance biométrique, nous avons trouvé que la texture de l'iris et les minuties de l'empreinte digitale sont les traits les plus intéressants à cause de leurs précisions et leurs stabilités. De même, l'utilisation de l'iris et de l'empreinte digitale suscite de plus en plus l'intérêt de la communauté scientifique car elle présente plusieurs challenges et verrous technologiques.

CHAPITRE II : Les systèmes biométriques d’empreinte FKP

CHAPITRE II : Les systèmes biométriques d’empreinte FKP

II.1 Introduction :

Dans ce chapitre, nous avons commencé par une brève introduction sur les modalités biométriques liées à la main, puis nous avons discuté sur les systèmes biométriques, de leur architecture et du module principal qui sont le module de capture, le module d'extraction, le module de comparaison et le module de décision, nous allons également discuter l'évaluation des systèmes biométriques, en particulier l'évaluation des performances des systèmes biométriques, comme les mesures du taux d'erreur, les courbes et les benchmarks. Les méthodes d'extraction des caractéristiques biométriques telles que LBP et LPQ et l'état de l'art de FKP seront également présentées..

II.2 Les modalités biométriques liées à la main :

Parmi les traits biométriques existants, les empreintes digitales, la voix, la signature, l'iris et les caractéristiques faciales sont couramment utilisés pour diverses applications de sécurité. Ceci est dû à leurs caractéristiques optimales comme la praticabilité, le caractère unique, la permanence, la précision et la fiabilité. Il a été constaté qu'aucune caractéristique biométrique n'est supérieure aux autres ou ne peut remplacer l'autre caractéristique, parce que chacune a ses propres avantages et inconvénients.

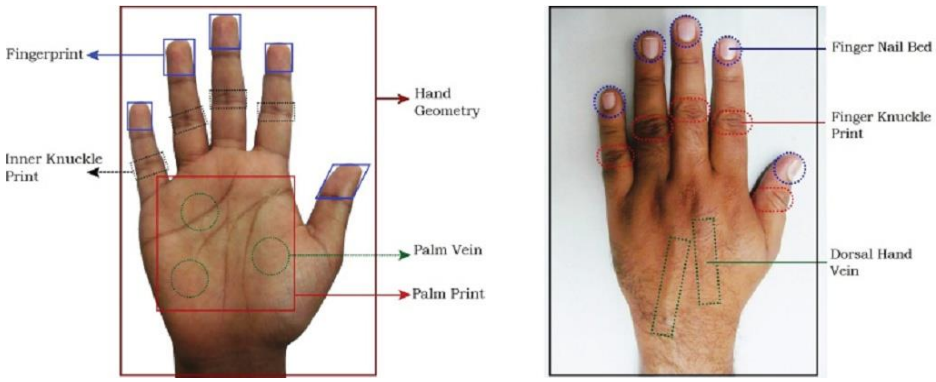


Figure II.1 : Vue avant et arrière de la main

Dans ces dernières années seulement, un intérêt considérable a été accordé aux caractéristiques biométriques liées à la main en raison de sa grande acceptation par les utilisateurs **[5].** Ils ont une anatomie très particulière et fournissent donc des informations très distinctes pour reconnaître les individus. De plus, ils peuvent être capturés avec des équipements de capture d'image de petite taille et à faible coût sans nécessiter de matériel

supplémentaire, ce qui conduit à des modèles de plus petite taille, et sont appropriés pour les pratiques de grande population.

La main est la partie du corps à l'extrémité de votre bras qui comprend vos doigts et votre pouce, elle est composée de parties contenant des informations riches en texture qui ont fourni les bases des systèmes de reconnaissance rapide. La main est une région particulièrement riche en informations pouvant être utilisées pour l'authentification ou pour l'identification des individus. Parmi les divers types d'identifiants biométriques, la biométrie de la main a suscité une attention considérable et disponible l'empreinte digitale est certainement une des modalités les plus utilisés dans les systèmes biométrique notamment grâce à son invariance dans le temps.

Hormis l'empreinte digitale, d'autres caractéristiques plus ou moins robuste mais aussi plus moins acceptable pour l'utilisation peuvent être considérée, nous peuvent citer par exemple :

Les traits biométriques basés sur la main peuvent être divisés en deux grandes catégories: les unes appartenant à la partie palmée et les autres à la partie dorsale de la main. La partie palmée est la partie interne et saisissante de la main. Les attributs biométriques largement utilisés extraits de cette partie sont:

- Empreinte digitale (fingerprint)
- Empreinte palmaire (palmprint)
- Les réseaux veineux (palm vein, fingervein)

La partie dorsale de la main occupe la zone située derrière la partie palmée. Les traits biométriques appartenant à la partie dorsale de la main n'ont pas été explorés autant que leurs contreparties palmées. Les traits utilisés dans cette partie sont:

- La morphologie de la main (hand geometry or shape)
- Géométrie des doigts (fingergeometry)
- Les réseaux veineux (dorsal hand vein)
- Les motifs d'articulation du doigt sur la face dorsal de la main (Finger dorsal knuckle print FKP)
- Les motifs d'articulation du doigt sur la face de la paume de la main (fingerinner-knuckle print IKP)
- Finger Nail Bed

Les caractéristiques biométriques propres aux surfaces avant et arrière de la région de la main sont illustrées à la figure …….

II.3 La biométrie FKP

II.3.1 Anatomie des doigts :

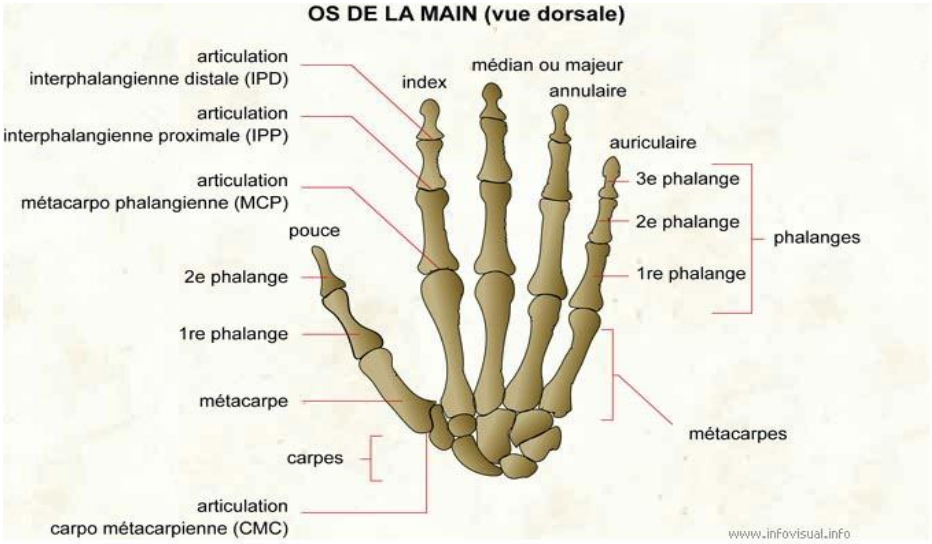


Figure II.2 : OS de la main (vue dorsale) **[70].**

La main est constituée d'une face palmaire (ou antérieure) et d'une face dorsale (ou postérieure). Elle comporte sur sa face palmaire la paume, trois plis de flexion et les lignes de la main.

La main est constituée d'une face palmaire (ou antérieure) et d'une face dorsale (ou postérieure), ainsi que d'une extrémité proximale (ou supérieure) et d'une extrémité distale (ou inférieure). La main comporte sur sa face palmaire la paume, trois plis de flexion et les lignes de la main. Sur cette même face, les doigts possèdent deux plis de flexion à l'exception du pouce qui n'en a qu'un seul. La partie dorsale de la main se caractérise par la présence de l'ongle sur l'extrémité distale des doigts. Les cinq doigts de la main sont raccrochés à sa partie proximale et forment son extrémité distale. Ils sont appelés le pouce, l'index, le majeur, l'annulaire et l'auriculaire (également appelé petit doigt), en partant du côté latéral (côté de l'éminence thénar) pour se diriger vers le médial (celui de l'éminence hypothénar). Les quatorze os formant le squelette des doigts sont longs et appelés les phalanges. Les doigts comportent trois phalanges, l'une proximale, l'autre intermédiaire (ou médiane) et enfin une dernière distale, qui forme l'extrémité des doigts. Hormis le

pouce, qui n'a pas de phalange intermédiaire, tous les doigts sont concernés. Ces phalanges sont reliées entre elles par des articulations. Il existe deux types d'articulations ; les métacarpo-phalangiennes, qui se situent entre les métacarpiens et les phalanges proximales correspondantes, soit au niveau de la jonction entre les doigts et la main et l'inter phalangiennes, entourées de chaque côté par une phalange. Pour tous les doigts sauf le pouce, on décrit les articulations inter phalangiennes proximale et distale. En plus des os vus précédemment, il existe également de petits os présents dans les articulations ou les tendons, les os sésamoïdes.

II.3.2 FKP

Dans un système biométrique FKP, un individu est vérifié par l'extraction des lignes, des plis et de la texture sur l'impression de jointure qui se trouvent à proximité des trois articulations.

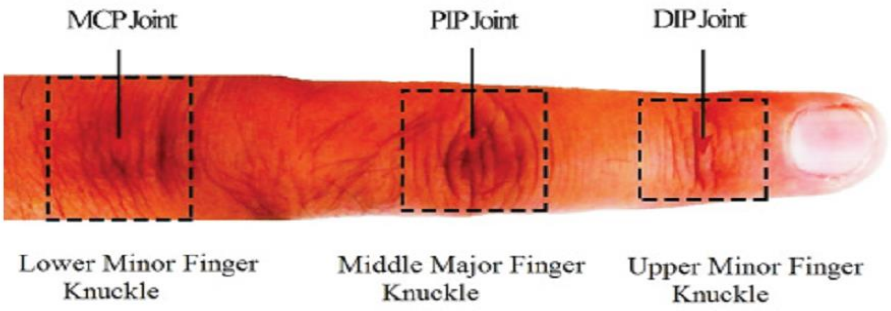


Figure II.3 : La surface externe d'un doigt a trois jointures

La surface externe d'un doigt a trois jointures comme illustré à la Fig. II 2 classé en articulations majeure et mineure :

- une articulation inter phalangienne distale (DIP) (première FKP mineure)
- une articulation inter phalangienne proximale (PIP) (FKP majeur)
- une articulation métacarpo phalangienne (MCP) (deuxième FKP mineure)

La plupart des recherches se sont concentrées sur des algorithmes de reconnaissance des motifs de texture des articulations PIP et ont évalué ses performances à l'aide d'une base de données d'images publique.

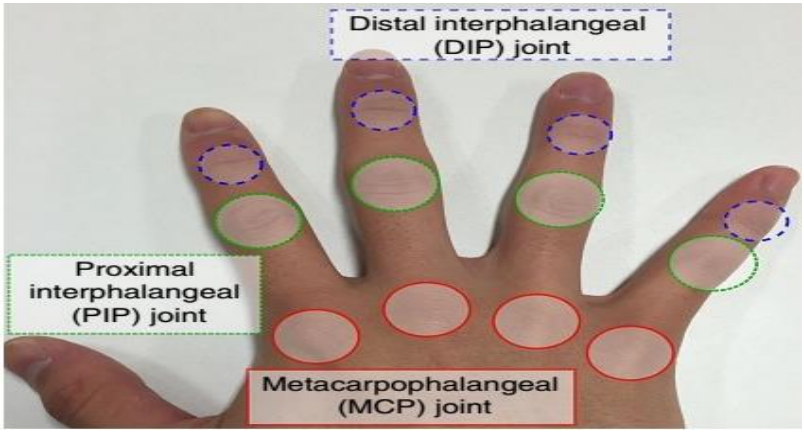


Figure II.4 : La surface externe de la main

II.3.3 FKP, IKP comparaison avec d'autres traits des mains

Récemment, les chercheurs en biométrie ont découvert que l'empreinte de l'articulation du doigt (FKP et IKP), qui fait référence aux motifs inhérents à la surface externe (interne) autour de l'articulation phalangienne du doigt, est très unique et peut servir d'identificateur biométrique distinctif. Une image FKP (ou IKP) contient de nombreuses textures semblables à celles d'une ligne.

La technologie des empreintes digitales nécessite des images haute résolution (>400 dpi) pour un meilleur résultat de reconnaissance par contre, l'IKP peut être facilement capturé à l'aide d'un dispositif d'imagerie sans contact. En plus Les rides et les ridules peuvent également être clairement visibles à l'FKP dans les images de de faible résolution. En plus, des traces apparaissent sur la surface externe des doigts (FKP) à un stade peu avancé de la vie et durent plus longtemps que les empreintes digitales, qui sont particulièrement difficiles à obtenir chez les agriculteurs et les travailleurs.

En termes d'acquisition d'images, l'empreinte FKP et la biométrie veineuse peuvent être captées au moyen d'une configuration sans contact. Il est à noter qu'une source de lumière infrarouge (NIR) supplémentaire est nécessaire pour l'acquisition veineuse, ce qui rend ces dispositifs d'imagerie veineuse légèrement coûteux et complexes pour un usage en grand nombre.

Malgré que, la région de la paume de la main fournit plus de détails que la région dorsal car elle considère les lignes principales, les rides, la géométrie de la paume et les points de référence pour l'identification d'individu mais dans une grand région. En comparaison avec l'empreinte de la paume, l'FKP contient des lignes appropriées

et des plis dans une petite région. Aussi les l'empreintes de la paume sont plus vulnérable aux attaques par imposteur car les personnes laissent leur empreinte digitale/palmaire par inadvertance lorsqu'elles touchent un objet.

En plus, les caractéristiques biométriques qui se trouvent sur la surface dorsal de la main, telles que FKP, FNP, Etc. ne peuvent pas être facilement reproduites et le risque de perte d'informations de cette région est également moindre

II.4Les systèmes biométriques

II.4.1 Définition

Les systèmes biométriques sont : des applications de technologies biométriques, qui permettent l'identification et/ou vérification automatiques d'une personne. Des applications d'authentification/vérification sont fréquemment utilisées pour l'exécution de diverses tâches relevant de domaines totalement différents et sous la responsabilité d'un vaste éventail d'entités différentes**[29].**

II.4.2 Architecture d'un système biométrique :

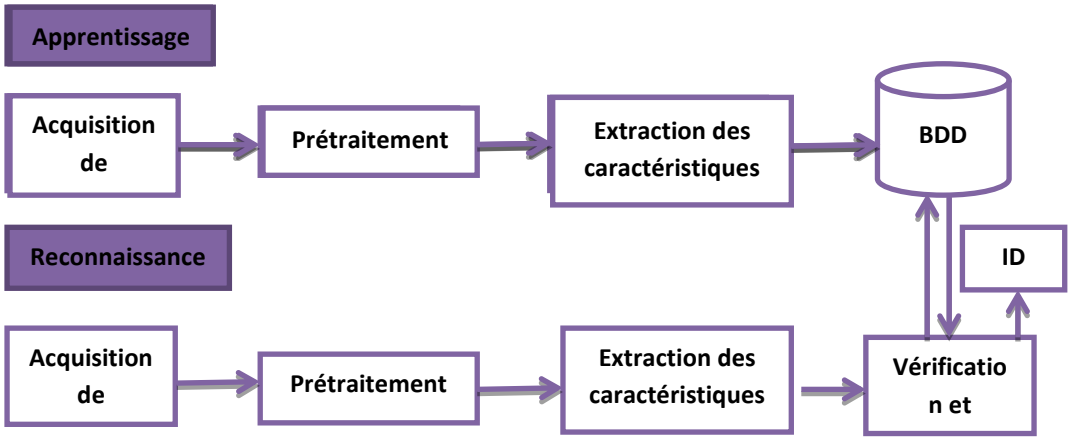


Figure II.5 : Architecture d'un système biométrique

II.4.2.1Etape d'acquisition des données :

C'est le processus par lequel un échantillon physique ou comportemental est entré dans le système. Différents systèmes utilisent différents dispositifs pour obtenir les échantillons. Les signaux originaux de l'appareil sont ensuite traduits en codes numériques avec ou sans prétraitement.

En général, les données biométriques physiques sont capturées par certains types de caméras et l'échantillon est sauvegardé sous forme d'image numérique pour

traitement. Les caméras vidéo sont utilisées pour capturer l'iris et le visage tandis que les caméras thermiques sont utilisées pour obtenir des images du visage et des mains en arrière. Un type de lecteur d'empreintes digitales est composé d'une petite caméra et un autre type utilise la technique du capteur thermique.

Le dispositif de capture de la rétine est un type spécial d'appareil photo avec une lumière vive. Les dispositifs de capture des traits comportementaux sont différents les uns des autres. Le système basé sur la voix fait uniquement appel à un haut-parleur PC et le système basé sur la signature utilise un tableau écrit en ligne **[34].**

La capture est la première étape de l'identification automatique des personnes, donc la qualité des données collectées est très importante et moins il y a de bruit, mieux c'est.

II.4.2.2 Etape d'extraction des caractéristiques :

Acquisition et extraction d'entités : s'effectue lors de l'enregistrement et de la vérification de l'identité. L'extraction des caractéristiques est une figuration des données (p. ex. image ou signal temporel acquis) sous la forme d'un vecteur qui se veut à la fois représentatif des données et discriminatoire par rapport à d'autres données (d'autres personnes). Lors de l'enregistrement, le vecteur caractéristique extrait de l'échantillon biométrique est appelé une référence et est stocké sur le support personnel ou dans une base de données selon les applications. Pendant la phase d'authentification, les modules d'acquisition et d'extraction d'entités fournissent une représentation des données biométriques à tester dans l'espace de la caractéristique **[35].**

L'extraction de caractéristiques est le processus par lequel des données uniques sont obtenues à partir de l'échantillon et un modèle est créé. Les modèles pour deux personnes doivent être différents et pour des échantillons différents de la même personne doivent être suffisamment identiques **[34].**

II.4.2.3 Etape de la comparaison :

Dans cette étape les données biométriques extraites par le module d'extraction des caractéristiques sont comparées à un ou plusieurs modèles précédemment stockés ? Ce module détermine donc le degré de similitude (ou de divergence) entre deux vecteurs biométriques **[53].**

Ce module fonctionne soit en mode vérification (pour une identité proclamée), soit en mode identification (pour une identité recherchée).

II.4.2.4 Etape de la Décision :

Cette phase est le processus par lequel le système décide si le modèle extrait du nouvel échantillon correspond au modèle enregistré. Au cours de cette étape, une note de correspondance est obtenue pour montrer le degré similaire entre le nouveau modèle et les données stockées dans le système. Afin de donner une réponse précise de "oui" ou de "non", un seuil est fixé. Lorsque le résultat de l'appariement est supérieur au seuil, la réponse est " oui ", sinon " non " est un output **[34].**

II.5 Les taches d'un système biométrique :

Les systèmes biométriques fonctionne selon trois modes que sont l'enrôlement, l'identification et l'authentification**.**

II.5.1 L'enrôlement :

L'enrôlement est la première phase de tout système biométrique, il s'agit de l'étape pendant laquelle un utilisateur est enregistré dans le système pour la première fois, elle commune a l'authentification et a l'identification, pendant l'enrôlement la caractéristique biométrique est mesurée en utilisant un capteur biométrique afin d'extraire une représentation numérique.

Par exemple les minuits sont le mode de représentation de l'empreinte digitale le modèle biométrique retenu est stocké soit dans une base de données soit sur un élément personnel propre à chaque personne **[25].**

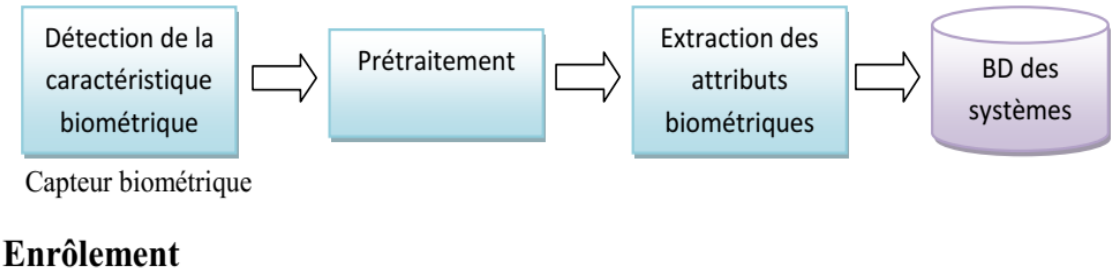


Figure II.6 : le mode enrôlement

II.5.2 L'identification :

L'identification permet de vérifier que l'identité d'un individu qui se présente existe bien dans la base de référence. Le système doit deviner l'identité de la personne. Il répond donc a une question de type "Qui suis-je ? ". À partir de l'échantillon biométrique fourni, le dispositif cherche le gabarit correspondant dans sa base de données **[33].**

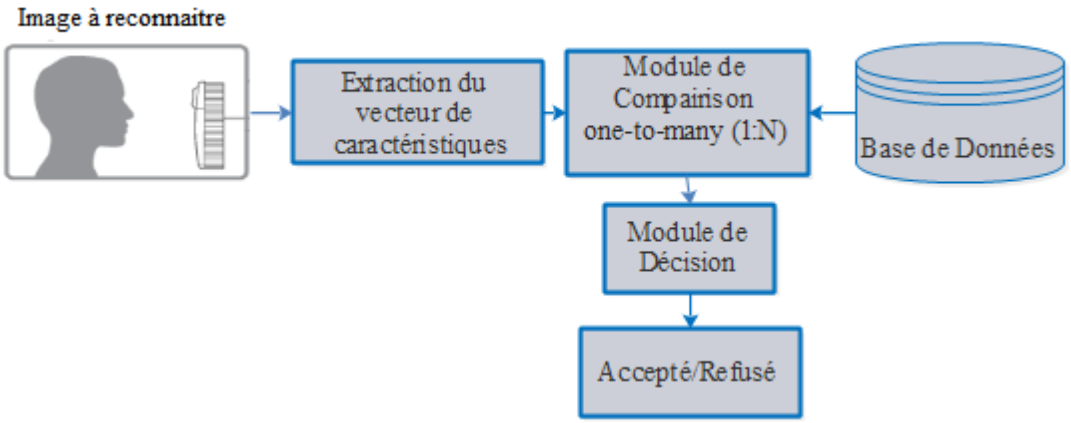


Figure II.7 : Architecture du mode identification

II.5.3 L'authentification :

En mode vérification, le système valide l'identité d'une personne en comparant les données biométriques saisies à sa ou ses propres modèles biométriques stockés dans la base de données du système. Dans un tel système, une personne qui désire être reconnue revendique une identité, habituellement au moyen d'un NIP (numéro d'identification personnel), d'un nom d'utilisateur, d'une carte à puce, etc., et le système effectue une comparaison individuelle pour déterminer si la demande est vraie ou fausse. La vérification de l'identité est généralement utilisée pour la reconnaissance positive, lorsque l'objectif est d'éviter que plusieurs personnes utilisent la même identité **[30].**

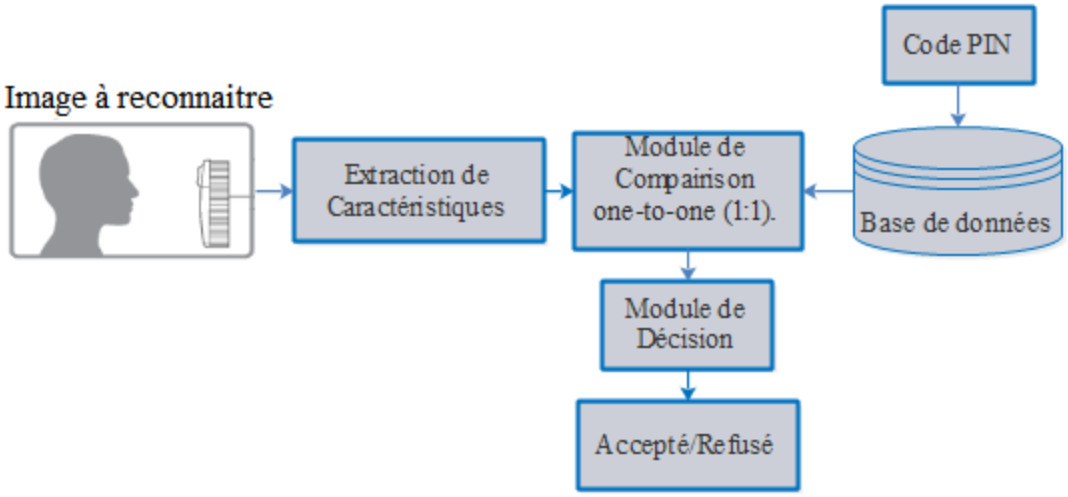


Figure II .8 : Architecture du mode vérification

II.6Evaluation des systèmes biométriques

En biométrie, chaque système est face à deux catégories de population

- Les clients qui appartiennent au système, ceux qui sont autorisés à entrer dans la zone protégée.
- Les imposteurs qui n'appartiennent pas au système, mais qui essaient généralement de le pénétrer.

La biométrie est une technologie émergente pour la vérification ou l'identification d'individu, de façon générale. L'évaluation d'un système biométrique se réalise suivant les trois approches :

- **La performance :** qui mesure l'efficacité d'un système biométrique en termes d'erreur tel que le taux d'´échec `a l'acquisition (FTA) **[26].**
- **L'usage qui mesure :** l'acceptabilité et la satisfaction des utilisateurs lors de l'utilisation de systèmes biométriques **[28].**
- **La sécurité :** qui mesure la robustesse d'un système biométrique (capteur et algorithmes) contre la fraude **[27].**

Les systèmes basés sur des mots de passe nécessitent une correspondance parfaite entre deux chaînes alphanumériques pour valider l'identité d'un utilisateur, un système biométrique rencontre rarement deux échantillons de caractéristiques biométriques d'un utilisateur qui donnent exactement le même ensemble de caractéristiques. Ceci est dû à :

- Des conditions de détection imparfaites.
- Des altérations des caractéristiques biométriques de l'utilisateur.

- Des changements des conditions ambiantes.
- Des variations dans l'interaction de l'utilisateur avec le capteur **[25].**

La performance mesure l'efficacité et la fiabilité d'un système biométrique dans un contexte d'utilisation donné.

Il existe dans la littérature plusieurs métriques de diverses natures que sont les mesures des taux d'erreur, les mesures liées au temps de traitement et occupation mémoire, les courbes de performance ainsi que les points de fonctionnement associent.

Selon l'Organisation Internationale de Normalisation ISO/IEC 19795-1, les mesures des taux d'erreur sont divisées en trois classes que sont :

- Les taux d'erreurs fondamentales
- Les taux d'erreurs de systèmes d'authentification
- Les taux d'erreurs de systèmes d'identification.

II.6.1 Les taux d'erreurs fondamentales

- **Taux d'échec à l'acquisition (failure-to-acquire rate, FTA)**

Le FTA est la probabilité qu'un système biométrique identifie de manière incorrecte une personne ou ne réussisse pas à rejeter un imposteur. Il mesure le pourcentage d'intrants non valides qui sont acceptés à tort. Il est également connu sous le nom de «taux de faux positifs» **[29].**

- **Taux d'´échec à l'enrôlement (failure-to-enroll rate, FTE)**

Le FTE proportion de la population d'utilisateurs pour laquelle le système biométrique ne parvient pas à saisir ou à extraire des informations utilisables à partir d'un échantillon biométrique. Cette défaillance peut être due à des conditions comportementales ou physiques du sujet qui entravent sa capacité à présenter correctement les informations biométriques requises **[31].**

- **Taux de fausse non-correspondance (false non-matche rate, FNMR)**

Le taux de fausse non-correspondance est la probabilité qu'un échantillon soit faussement déclaré comme ne correspondant pas à un modèle de la même mesure du même utilisateur qui fournit l'échantillon. (Une fausse non-correspondance est parfois appelé "faux négatif" dans la littérature.)

- **Taux de fausse correspondance (false matche rate, FMR)**

Le taux de fausse concordance est la probabilité attendue qu'un échantillon soit faussement déclaré comme correspondant à un seul échantillon non auto-généré

sélectionné au hasard. (Une fausse correspondance est parfois appelée "faux positif" dans la littérature.)

II.6.2 Taux d'erreur de système d'authentification

- **Taux de faux rejets (false rejection rate, FRR)**

  La probabilité qu'un système produise un faux rejet. Un faut rejet se produit lorsqu'aucune correspondance n'est établie entre une personne et son modèle biométrique. Il est également connu sous le nom de taux de faux négatifs **[29].**

  Exemple : pour une transaction de vérification `a une seule tentative et unseuil fixé t le taux de faux rejets est calculé par :

$$FRR(t) = FTA + FNMR(t) * (1 - FTA)$$

- **Taux de fausses acceptations (False Acceptance rate, FAR)**

  La probabilité qu'un système biométrique identifie de manière incorrecte une personne ou ne réussisse pas à rejeter un imposteur. Il mesure le pourcentage d'intrants non valides qui sont acceptés à tort. Il est également connu sous le nom de taux de faux positifs **[4]**

  Exemple : pour une transaction de vérification `a une seule tentative et un seuil fixé t le taux de fausses acceptations est calculé par :

$$FAR(t) = FMR(t) * (1 - FTA)$$

La figure suivante représente la distribution théorique des taux de vraisemblance des utilisateurs l´légitimes et des imposteurs. Les deux taux d'erreurs, FAR et FRR, sont liés et d´dépendent d'un seuil de d´décision qui doit être ajustée en fonction caractéristique ciblé du système biométrique haute ou basse sécurité.

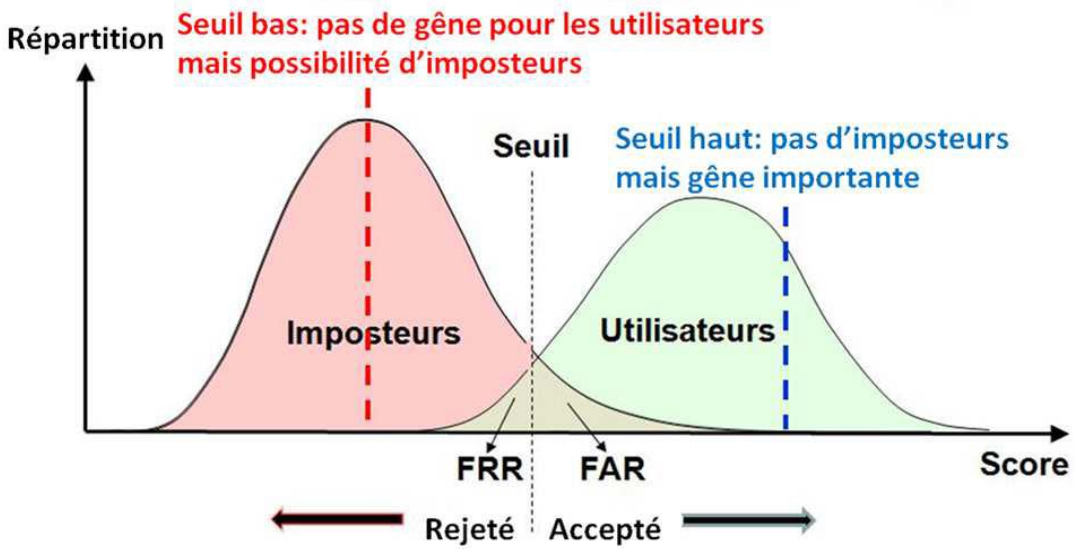


Figure II.9 : Taux de vraisemblance des utilisateurs légitimes et des imposteurs d'un système d'authentification biométrique **[29].**

II.6.3 Taux d'erreur de système d'identification:

- **Le taux d'identification (IR : Identification Rate) :**

  La proportion de tentatives d'identification authentiques pour lesquelles l'inscription correcte est indiquée dans la liste des identifiants.

- **Le taux de faux-négative d'identification (FNIR : False Negative Identification Error rate) :**

  La proportion des tentatives d'identification dans lesquelles un membre inscrit dans un système n'a pas au moins un de ses modèles retourné parmi la liste des identifiants.

  Pour une transaction d'identification a une seule tentative contre une base de données contenant N modèles, le taux de faux-négatif d'identification est calculé par:

$$FNIR(t) = FTA + (1 - FTA) * FNRT(t).$$

- **Le taux de pénétration (PR : Penetration Rate) :**

  Mesure, en moyenne, le nombre de modèles biométriques présélectionnés par rapport au nombre total de modèles.

- **L'erreur de l'algorithme présélection (Preselection error):**

  L'algorithme d'erreur de présélection réduit le nombre de modèles biométriques à comparer avec l'image acquise lors de la phase d'identification. L'erreur se produit

lorsque le modèle qui correspond aux données biométriques obtenues ne se trouve pas dans la liste des modèles retournés **[37].**

Les performances de l'identification sont étroitement liées à la taille de la base de données. Par conséquent, lorsqu'on communique un résultat d'identification, il est important d'indiquer explicitement la taille de la base de données utilisée pour l'expérience **[36].**

II.6.4 Les mesure de taux de traitement et d'occupation mémoire :

Le temps de traitement de l'information par le system est un facteur très important pour l'évaluation de system biométrique il est généralement mesure en :

- **Temps moyen d'enrôlement**

  Indique le temps moyen pour la création de modèles biométriques des individus.

- **Temps moyen de vérification :**

  Se réfère au temps moyen nécessaire pour acquérir les données biométriques requises et les comparer avec le modèle correspondant. Ce temps ne dépend pas du nombre de personnes dans la base de données **[39].**

- **Temps moyen d'identification**

  Décrit le temps moyen que prennent l'acquisition des données biométriques nécessaires et la comparaison de ces données avec les modèles existants dans la base de données. Le nombre d'utilisateurs du système a un effet très important sur cette information. Il peut être recommandé pour les grandes bases.

- **L'espace mémoire :**

  Un autre facteur important à prendre en considération lors de l'évaluation des systèmes biométriques est l'espace mémoire requis par le système. Il est principalement mesuré en taille moyenne et maximale d'un modèle biométrique mais aussi en espace mémoire maximal alloue pendant les phases d'enrôlement, de vérification et d'identification. Il faut aussi prendre en compte, par exemple, le temps de vérification d'empreintes digitales sur un SE qui est limite a 500 ms **[37].**

II.6.5 Les courbe de performance :

Une grande variété de graphiques peut être utilisée pour comparer les systèmes biométriques et représenter la précision. De nombreux graphiques sont simplement

des façons différentes d'afficher les mêmes données pour illustrer un aspect particulier de la performance.

- **La courbe ROC (Receiver Operating Characteristic Curve) :**

Cette courbe permet de représenter graphiquement les performances d'un système de vérification pour les diverses valeurs de θ. Le taux d'erreur égal (EER) est celui correspondant au point FAR=FRR, c'est-à-dire à l'intersection graphique de la courbe ROC et de la première bissectrice **[38].**

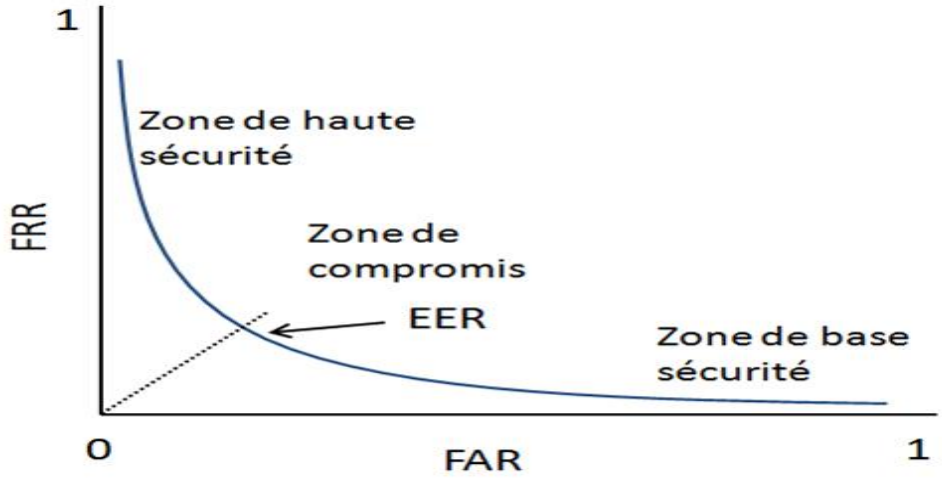


Figure II.10 : Exemple de la courbe ROC : Variation du FRR en fonction de FAR lorsque le seuil de d´décision varie.

- **La courbe CMC (Cumulative Match Characteristic Curve) :**

Cette courbe présente les valeurs du rang d'identification et les probabilités d'une identification correcte inférieure ou égale à ces valeurs, respectivement sur l'abscisse et sur l'ordonnée. Cette courbe est utilisée pour comparer les performances des systèmes d'identification biométriques **[39].**

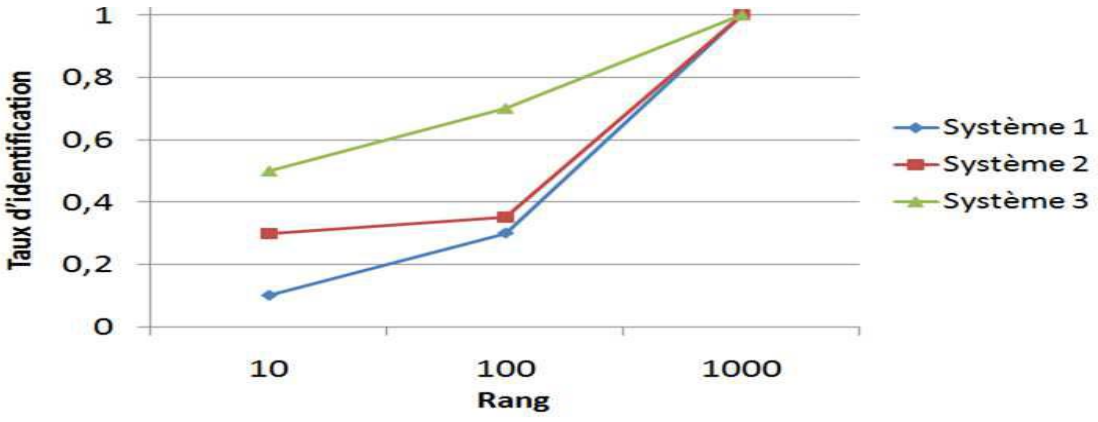


Figure II .11 : Exemple de courbes CMC pour différents systèmes biométriques.

- **La courbe RC (Robustness Curve) :**

  cette courbe illustre la robustesse du système en terme de performance contre les déférentes type d'altérations (c'est à dire altération due au bruit pendant l'acquisition de donnée biométrique) la performance du système est illustrer par le point de fonction taux d'égale erreur (EER)**,** Un exemple de cette courbe est présenter dans la figure suivante :

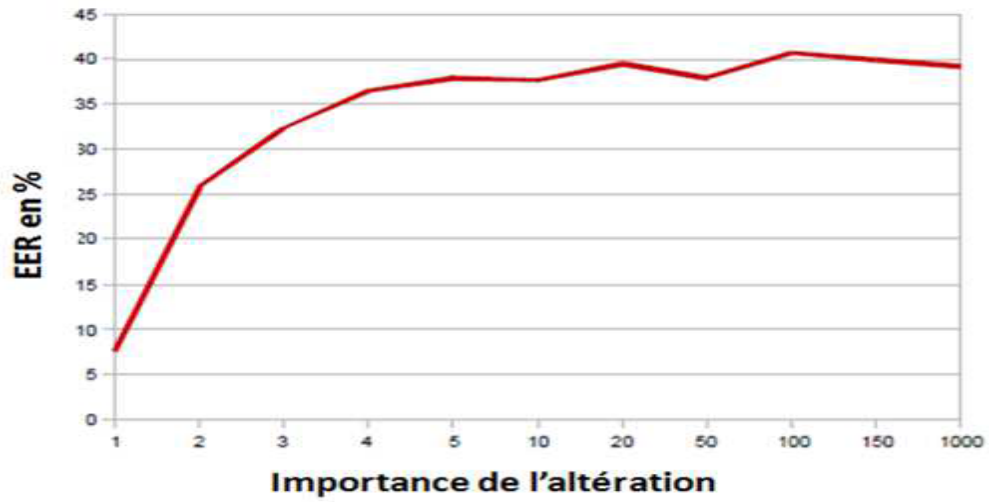


Figure II.12 : Evolution des valeurs de l'EER en fonction de la quantité des altérations [**39].**

- **Les points de performance :**

  Les points de performance sont utilisés pour illustrer la performance des systèmes biométriques. Il existe dans la littérature plusieurs métriques.

- **Taux d'égale erreur (Equal Error Rate, EER) :**

  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 faux rejeté [38]. Dans cette figure $\boldsymbol{\theta_0}$ représente le Seuil correspondant au point d'équivalence des erreurs

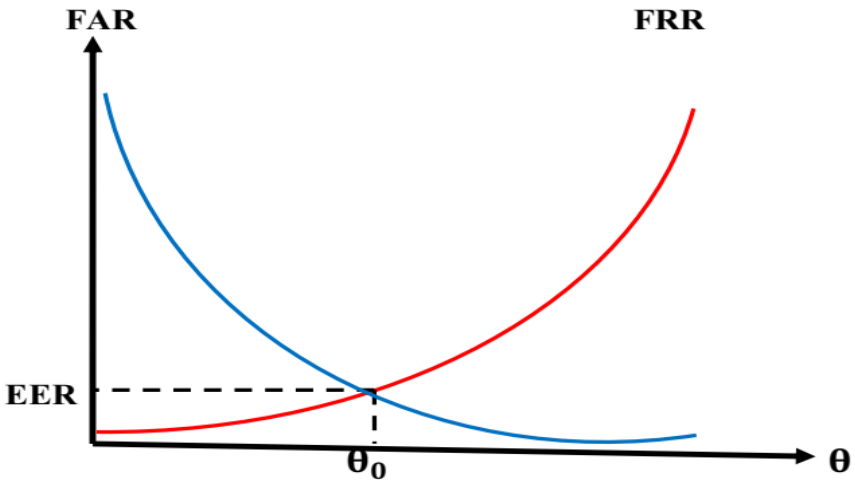


Figure II.13 : Courbe démonstratif de l'ERR

- **HTER : « Half Total Error Rate »**

  C'est le taux d'erreur moyenne d'un système biométrique. Cette métrique est la moyenne entre le FRR et le FAR

- **Taux d'erreur pondéré: (Weighted Error Rate, WER)**

  Ce taux d'erreur correspond au seuil tel que le FRR soit proportionnel au FAR avec un coefficient qui dépend de l'application. Pour un coefficient égal à 1, le seuil du WER est égal au seuil de l'EER;

- **Intervalle de confiance :**

  En biométrie, les bases de données recueillies sont utilisées pour jauger la performance des systèmes biométriques. Toutefois, ces bases ne sont pas représentatives de l'ensemble de la population pour deux raisons principales. Premièrement, ces bases de données ne contiennent pas suffisamment de personnes et il y a généralement peu de données par personne. Deuxièmement, il y a souvent une différence entre le nombre de scores des utilisateurs légitime et frauduleux, ce qui n'est pas non plus représentatif de la réalité. Enfin, les taux d'erreur (EER, WER, HTER et AUC) utilisés pour illustrer la performance globale du système dépendent du revêtement - test de décapage. Pour toutes ces raisons, il est nécessaire de calculer un intervalle de confiance à l'EER pour comparer les systèmes biométriques. Cet intervalle de confiance est particulièrement important lorsque l'on compare des systèmes biométriques présentant des taux d'erreur similaires **[37].**

II.6.6 Benchmarks

Afin d'évaluer les systèmes biométriques, nous avons besoin d'une base de données pour cette évaluation. Cette base de données assure que les systèmes seront testés selon les mêmes conditions d'acquisition. Les bases de données biométriques peuvent également être utilisées pour régler les paramètres d'un système monomode (réglage du seuil de décision) et multimodale (réglage du poids pour la fusion). Les bases de données biométriques collectées sont généralement divisées en deux types : les bases réelles et les bases synthétiques**.**

- **base de données réelle :**

  Ces bases de données comportent des données biométriques réelles acquises par la participation de volontaires. Dans la littérature, il y a deux catégories de bases, les bases unimodales et les bases multimodales. Par exemple les bases monomodales sont : AR **[41],** FERET **[42, 43],** FVC2002 DB2 **[44],** FRGC (Face Recognition Grand Challenge) **[45],** USF Human ID Gait Baseline **[46],** ENSIB **[47],** GREYC-Keystroke **[51],** FACES94 **[40].** Un exemple des bases multimodales est XM2VTSDB **[48],** BANCA **[49],** BIOSECURE **[50].**

- **base de données synthétique**

  Ces bases de données contiennent des données synthétiques simulant des données biométriques réelles. Une base synthétique doit avoir deux propriétés. Tout d'abord, la performance d'une base de données synthétique doit être proche de celle qui est obtenue avec une base de données réelle. Deuxièmement, les données contenues dans la base de données synthétique ne doivent pas représenter les données biométriques réelles d'une personne**,** La base SFinGe générée par le logiciel SFinGe **[52]**, développé par le laboratoire italien BioLab 1, est un exemple de base synthétique.

II.7 Etat de l'Art de l'empreinte des articulations des doigts :

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 du 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) **[53],** ont tout d'abord étudié la surface du doigt pour l'authentification individuelle. Ils ont utilisé un capteur Minolta 900/910 pour acquérir la surface du dos du doigt 3D. Leur étude valide le caractère unique de la surface arrière du doigt en tant que caractéristique biométrique pouvant être utilisée. Cependant, leur travail n'est pas totalement centré sur les points d'articulation et ils ont utilisé toute la surface du dos des doigts pour l'authentification. De plus, le prétraitement de la surface du doigt en 3D et augmente le temps et la complexité du système ce qui limite son utilisation pour les applications biométriques en ligne.

En 2009, Kumar et Ravikanth **[54],** a présenté une description plus détaillée de l'acquisition et de l'extraction des points d'articulation de la partie dorsale de la main. Ils utilisent un appareil photo numérique à moindre coût (Canon Powershot A620-) pour capter le dos de la main. L'image de la main captée 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 traits extraits de points d'articulation. Ce travail a mis beaucoup d'efforts pour valider le caractère unique de la surface externe supérieure du doigt, mais il n'a pas apporté de solution pratique.

De plus, la méthode **[55],** utilise principalement l'information de la forme 3D du dos du doigt mais n'utilise pas toutes les informations de texture. Alors que les méthodes d'analyse sous-espace utilisées dans **[56]**, ne peuvent extraire efficacement les lignes et les caractéristiques distinctes du dos de la surface du doigt. D'autre part, dans l'article **[57]**, ils ont élaboré un système de reconnaissance d'empreinte d'articulation incluant plus spécifiquement le dispositif d'acquisition, puis une détection de la région qui les intéresse a été réalisée et ensuite un filtre de Gabor 2D a servi pour extraire les informations de l'orientation locale. Pour la comparaison, ils ont utilisé la distance angulaire pour mesurer la similitude entre deux codes qui correspondent aux images.

Malgré le développement d'un nouvel appareil d'acquisition, le temps d'exécution reste un problème et ce problème est dû au ***matching*** et à la mesure de similarité (le temps total d'exécution pour une seule vérification prend environ une seconde), comme résultat ils ont trouvé un taux de reconnaissance de 97% et un FAR de 0.02% et un EER de 1.09%.

Le centre biométrique de recherches 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 la construction d'une base de données à grande échelle.

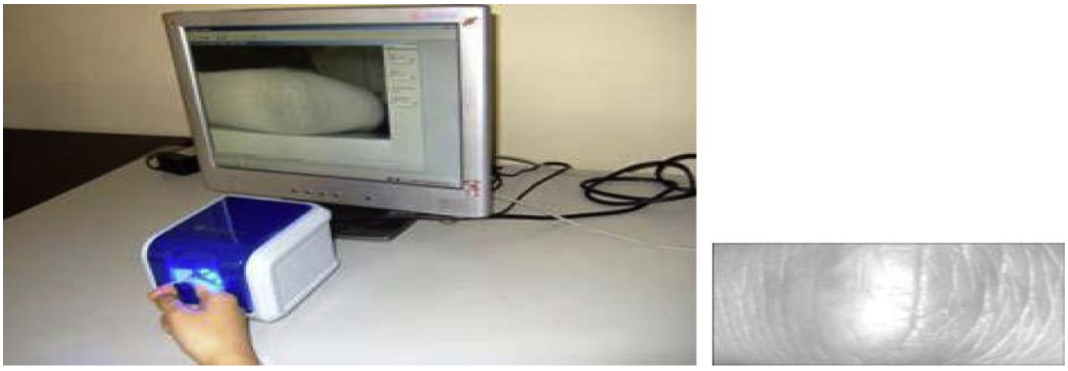


Figure II.14 : Dispositif d'acquisition d'images FKP et son ROI **[54].**

Dans **[58],** les images de l'empreinte de l'articulation contiennent plus de bruit que les empreintes de la paume. Dans ce cas, ils ont proposé deux étapes : l'application du filtre 2D de Gabor pour améliorer les lignes de l'empreinte de l'articulation et les descripteurs SIFT (Scale-Invariant Feature Transform). Après le filtre de Gabor, l'algorithme CLAHE (Contrast Limited Adaptive Histogram Equalization) est appliqué pour corriger le contraste des lignes de l'articulation.

ZHU. Le **[59],** utilise la base de données *PolyU.* Dans un premier temps, une normalisation du ROI FKP a été utilisée, après l'application de l'algorithme SURF (Speeded Up Robust Features) pour l'extraction des caractéristiques en vue d'une comparaison ultérieure avec RANDOM SAMPLE Consensus (RANSAC). Ils ont obtenu 90,63 % comme pourcentage de vérification et 96,91 % pour l'identification.

Yang Wankou **[60],** propose une autre méthode qui consiste à utiliser le filtre de Gabor et l'analyse discriminante linéaire orthogonale (OLDA) pour identifier les individus à partir de leurs empreintes articulaires. Tout d'abord, la représentation des caractéristiques obtenues à partir du filtre de Gabor est calculée après l'utilisation d'une ACP, et après le calcul d'une OLDA de transformation. Ce travail également basé sur la base de données PolyU, les résultats montrent que cette méthode est plus performante que les algorithmes qui utilisent uniquement LDA ou PCA.

Zahra S. et al. **[61],** utilisent une banque de filtre de Gabor pour l'extraction des caractéristiques, la combinaison des PCA et LDA pour la fragmentation de la dimension de l'espace et la distance euclidienne pour la classification. Ce travail

regroupe quatre empreintes d'articulation du même individu au niveau des caractéristiques. La base de données PolyU a été utilisée pour examiner la performance de la méthode proposée. Les résultats obtenus sont 98.79% pour l'identification et 91.8% pour la vérification.

Guangwei Gao et al **[62],** développent le code compétitif pondéré (W-CompCode) pour une extraction des caractéristiques effective. En premier lieu, ils proposent une matrice pondérée pour chaque ROI des images de FKP basée sur le filtre de Gabor. Pour le matching des W-CompCode, la distance de Hamming normalisée est utilisée en se basant sur la distance angulaire. L'EER obtenu est 1.203 pour la base de données PolyU FKP.

Chetana Hegde et al **[63],** proposent trois algorithmes différents pour la reconnaissance des empreintes d'articulation. La première approche utilise la transformée de Radon pour l'extraction des caractéristiques et pour la phase de prétraitement, la détection du contour et le filtre médian ont été utilisé. Après l'application de la morphologie mathématique et la dilatation, un taux FAR de 1.55% est obtenu et 1.02% pour le FRR. Dans la deuxième méthode, les ondelettes de Gabor sont utilisées pour l'extraction des caractéristiques. Dans la première étape, ils éliminent le bruit et incrémentent l'intensité avec les coefficients de corrélation. Les résultats obtenus sont le FAR : 1.24% et le FRR : 1.11%. Pour le dernier algorithme, celui-ci reconnait les parties endommagées des FKP. Ils ont créé 450 FKP endommagés pour introduire le bruit et aléatoirement éliminer quelques valeurs des pixels de l'image des FKP. Un taux de reconnaissance de 95.33% est obtenu.

Dans **[64],** une méthode par la fusion de plusieurs algorithmes pour l'extraction des caractéristiques est présentée. Ils utilisent LG (Log Gabor), LPQ (Local Phase Quantization), PCA et LPP (Locality Preserving Projections) pour l'extraction des caractéristiques. Dans la première expérience, ils utilisent un seul algorithme pour extraire les caractéristiques. Les résultats de cette étude montrent que l'algorithme de LG est d'une grande précision par rapport aux 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%. Dans cet article, ils se concentrent uniquement sur la phase d'extraction des caractéristiques.

II.8 Conclusion :

Dans ce chapitre nous avons étudié le principe de base d’un système biométrique, Au module d’extraction des caractéristiques, les systèmes de reconnaissances faits des étapes plus importantes avant le stockage des informations dans ces bases de données. Ces étapes sont basées sur des algorithmes spécifiques comme : L'extraction de caractéristiques : pour obtenir les caractéristiques de chaque image acquise sous forme de vecteur. Il-y-a plusieurs méthodes pour faire cette opération comme LPQ, LBP et le filtre de Gabor. Nous avons présenté les deux méthodes d'extraction des caractéristiques qui ont été utilisées pour représentés les caractéristiques de l’empreinte. Nous avons donné des détails sur l’application de ces méthodes sur l’image de l’empreinte.

Chapitre III : Résultats et Discutions

Chapitre III : Résultats et Discutions

III.1 Introduction :

L'étude expérimentale de cette mémoire est basée sur la reconnaissance de personnes par leurs empreintes des articulations des doigts en utilisant les méthodes LBP et LPQ. Elle est réalisée sur la base de données de PolyU. Afin d'évaluer l'efficacité des méthodes étudiées et les performances de notre système biométrique proposé, et vue l'importance affectée à la modalité de l'empreinte FKP dans les dernières années, nous allons présenter brièvement les méthodes d'extraction des caractéristiques telle que le LPQ et LBP.

III.2 Présentation du système :

Cette section présente notre système de reconnaissance basé sur l'FKP qui est conçu en base sur les fonctions LBP et LPQ au niveau de la phase d'extraction des paramètres. Au cours de cette phase, diverses techniques d'extraction de caractéristiques locales sont mises en œuvre pour extraire les structures locales d'images FKP et leur fréquence d'apparition sur l'ensemble de l'image (histogramme). Le descripteur de texture (LBP d'origine et plusieurs de ses variantes mentionnées dans la section suivante permettent de coder la texture des images FKP et d'obtenir un vecteur de caractéristiques basé sur un histogramme représentant chaque image. Il faut noter que les FKPs sont également sensibles à plusieurs variations en raison de la qualité de la peau différente, comme la peau sèche ou sale. Ce problème doit donc être pris en compte à l'étape de l'extraction des caractéristiques. En fait, dans **[71],** il est montré que l'histogramme LBP est très robuste pour les variations d'échelle de gris puisqu'il est par définition invariant contre toute transformation monotone de l'échelle de gris. De plus, il est possible d'obtenir l'invariance de rotation en incorporant simplement un ensemble de motifs invariants de rotation. Pour cette raison l'histogramme est utiliser comme un vecteur caractéristique calculé sur l'image LBP ou LPQ entière ou sur blocks.

Pendant la reconnaissance, les vecteurs de caractéristiques correspondants de l'interrogation et les FKP inscrits sont appariés à l'aide de la méthode la plus proche voisin **[71],** pour obtenir les scores d'appariement respectifs. Le schéma fonctionnel du système de reconnaissance basé sur le FKP proposé est illustré à la **Figure** suivante.

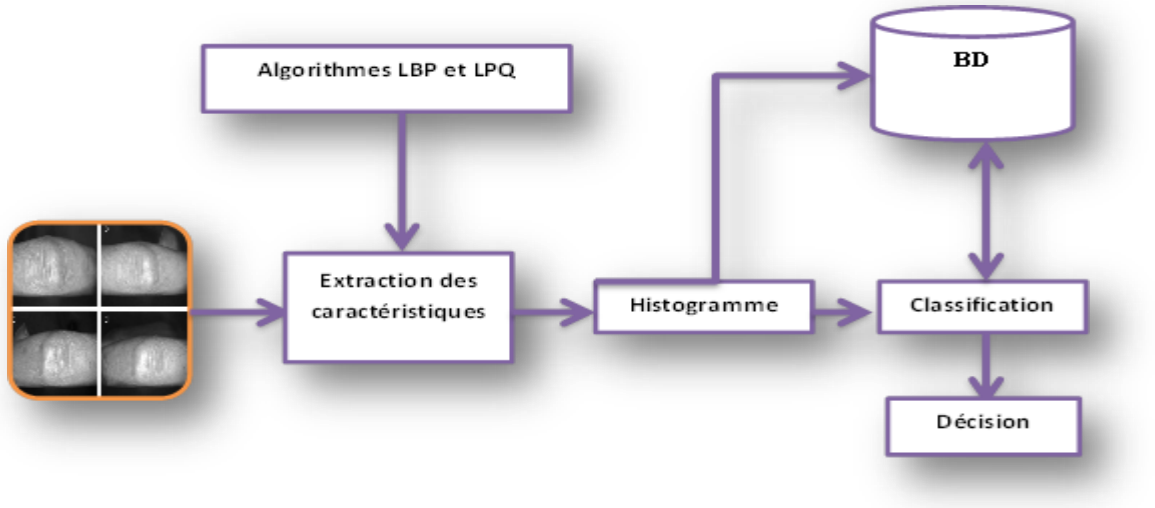


Figure III.1 : Architecture globale du système biométrique d'identification FKP.

III.2.1 Acquisition d'image :

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. La source de lumière LED et la caméra CCD sont enfermés dans une boîte de sorte que l'éclairage soit presque constant. Un bloc basal et un bloc triangulaire sont utilisés pour fixer la position de l'articulation du doigt

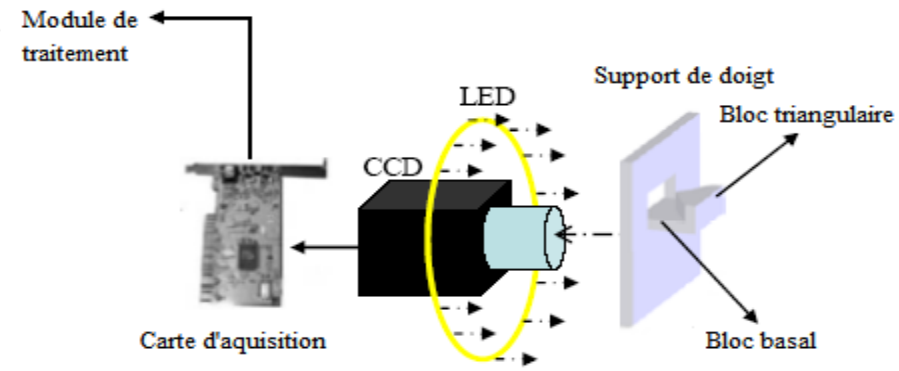


Figure III.2: Structure du module d'acquisition**.**

Dans acquisition de données, l'utilisateur peut facilement mettre son doigt sur le bloc basal en touchant les deux pentes du bloc triangulaire (voir **Figure suivante)**. Une telle conception vise à réduire les variations de position du doigt dans différentes sessions de capture.

Figure III.3 : Dispositif d'acquisition de FKP.

Dès que, l'image est capturée elle est envoyée au module de traitement de données pour le prétraitement et l'extraction de caractéristiques. La taille des images FKPs acquises est de taille 768 × 576 sous une résolution d'environ 400 dpi.

III.2.2 Détection de ROI :

La base de données utilisée dans notre test, la base (PolyU), est une base qui a subi déjà des prétraitements, donc ne nécessite aucun prétraitement supplémentaire. La figure suivante donne des exemples des images de cette base.

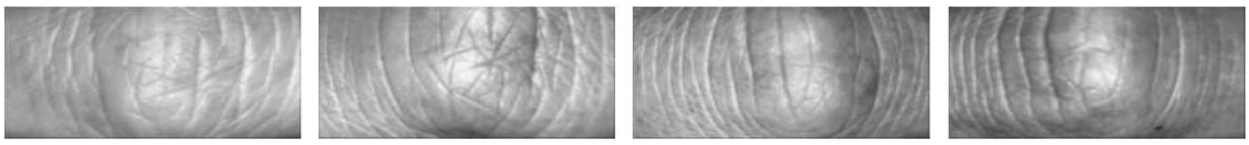


Figure III.4: Quelque image de la base de données PolyU

III.2.3 Extraction des paramètres

L'extraction des caractéristiques est au cœur de tout système de reconnaissance et représente une phase très importante dans la construction d'un système efficace d'identification. Toutefois, le choix de la méthode d'extraction des caractères est basé sur trois informations essentielles : ***texture***, lignes et apparence de l'impression. Plusieurs techniques d'extraction ont été introduites pour capturer des structures locales intrinsèques et discriminatives à partir d'images.

Les images FKP, similaires à d'autres images biométriques, contiennent de nombreuses informations sur la ***texture***. Par conséquent, une bonne méthode d'extraction de caractéristiques de texture est nécessaire. Parmi ces techniques on trouve les descripteurs de texture, qui codent et caractérisent les informations de texture des images.

Les motifs binaires locaux représentent un descripteur de texture important qui a donné des résultats efficaces dans certaines applications de vision par ordinateur comme la reconnaissance faciale et la détection d'objets. Le succès par exemple de la méthode LBP (local binary patten) dans ces applications nous a motivé à l'utiliser dans notre système biométrique FKP. Dans notre cas nous avons choisis les algorithmes :

- Quantification de la phase locale (LPQ).
- Motifs binaires locaux (LBP).

❖ **Motif binaire local (LBP) :**

L'opérateur d'analyse de la texture LBP, introduite par Ojala et al **[66]**, D'où le principe général est de comparer le niveau de gris d'un pixel avec les niveaux de ses voisins. Tous les voisins prendront une valeur 1 si leur valeur est supérieure ou égale au pixel courant et 0 si leur valeur est inférieure.

La technique LBP a été étendu par la suite en utilisant des quartiers de taille respectueuse. Dans ce cas, un cercle de rayon R autour du pixel central et les valeurs des P points échantillonnés sur le bord de ce cercle sont prises et comparées avec la valeur du pixel central. Pour obtenir les valeurs des points P échantillonnés à proximité pour n'importe quel rayon R, une interpolation est nécessaire. On adopte la notation (P, R) pour définir le voisinage de P points de rayon R d'un pixel. La figure III.5 illustre trois quartiers pour des valeurs R et P différentes **[71].**

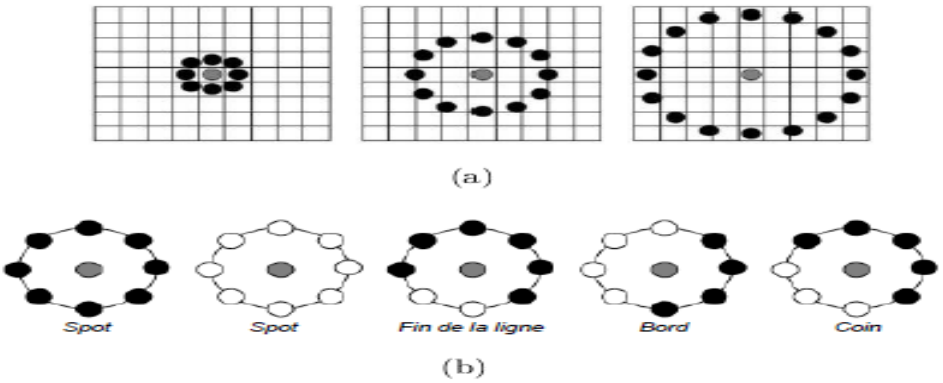


Figure III.5 : (a): Trois voisinages pour des R et P différents, (b) : Textures particulières détectées par *LBP*

Les pixels de ce motif binaire sont alors multipliés par des poids et sommés afin d'obtenir un code LBP du pixel courant. LBP est un moyen puissant de description de texture et parmi ses propriétés dans des applications réelles sont ses discriminatives puissances, simplicité de calcul **[66].**

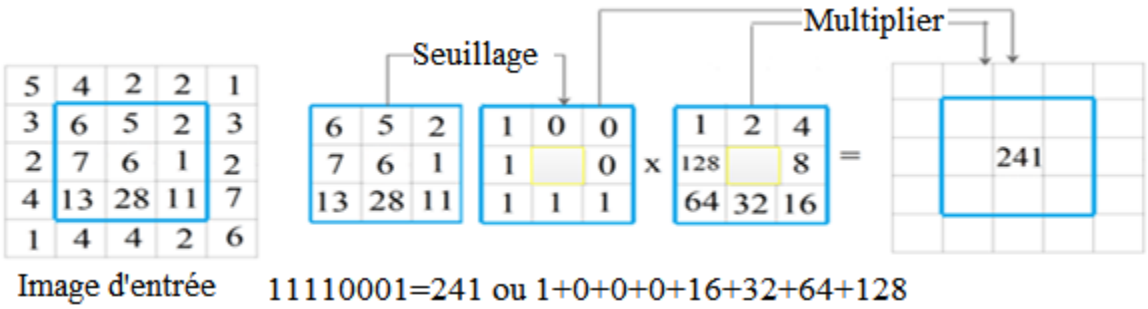


Figure III.6 : Exemple de traitement de l'opérateur LBP

Soit $g_c$un pixel dans l'image d'entrée, ses p pixels voisins sont (g_0,g_1,…,g_{P-1}). La réponse *LBP* du pixel $g_c$est calculée comme suit :

$$LBP(xc\ ,\ yc\ ) = \sum_{i=0}^{p-1} f(x)(g_i - g_c)\ 2^i$$

Où *f(x)* est la fonction de seuillage, donnée par :

$$f(x) = \begin{cases} 1, & x \geq 0 \\ 0, & x < 0 \end{cases}$$

La **figure suivante**. Montre un exemple des étapes nécessaire à la génération du vecteur des caractéristiques en utilisant l'operateur LBP basique.

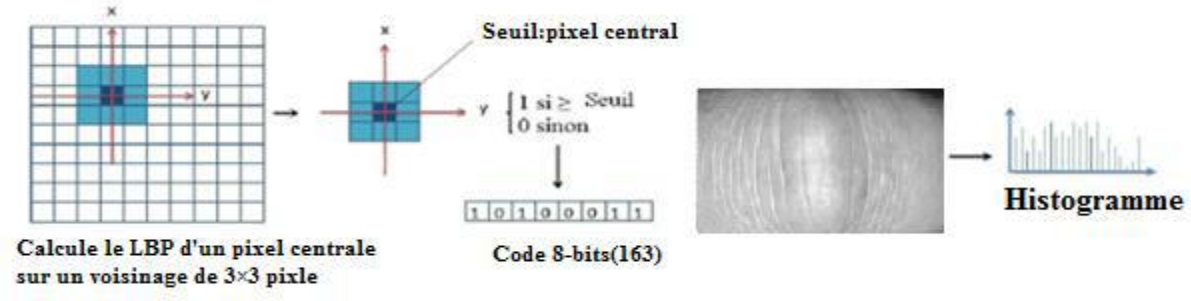


Figure III.7 : Organigramme de l'ensemble des étapes nécessaire à la génération du vecteur des caractéristiques par la méthode LBP.

❖ **Descripteur de base LPQ (Local phase Quantization) :**

La quantification de phase locale (LPQ) est un algorithme largement utilisé pour extraire les caractéristiques de plusieurs technologies biométriques telles que le visage, l'empreinte palmaire, l'iris et FKP. Cette méthode a d'abord été introduite par Ojansivu et al **[67]**, ils divisent l'image en petites zones égales N*N, dans chaque zone, des informations locales et utiles de l'image sont extraites.

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

$$Fu(x) = \sum_{m \in Nx} h(m-x) f(m) e^{-2j\pi u^T m} = Eu^T f(x)$$

Où *Eu*, de taille = $1 \times M^2$, est un vecteur de base de 2DWFT avec la fréquence *u*, et *fx*, taille = $M^2 \times N$, 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 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 fréquence scalaire la plus élevée pour laquelle Hui>0. Ainsi, seules quatre fonctions complexes telles qu'une banque 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 transformation. Chaque pixel de l'image complexe résultante peut être codé en une valeur binaire représentée dans l'équation suivante en appliquant (le codage binaire par quadrant) **[73].**

$$B_{ui}^{\mathrm{Re}}(x) = \begin{cases} 1 & si\ \mathrm{F}_{ui}^{\mathrm{Re}}(x) > 0 \\ 0 & \mathrm{si}\ \mathrm{F}_{\mathrm{ui}}^{\mathrm{Re}}(x) \leq 0 \end{cases} \quad B_{ui}^{\mathrm{Im}}(x) = \begin{cases} 1 & si\ \mathrm{F}_{ui}^{\mathrm{Im}}(x) > 0 \\ 0 & \mathrm{si}\ \mathrm{F}_{\mathrm{ui}}^{\mathrm{Im}}(x) \leq 0 \end{cases}$$

La technique LPQ peut être résumée en quatre étapes principales **[68].** Tout d'abord, nous appliquons l'opérateur (LPQ) à l'image d'entrée pour obtenir l'image étiquetée. Ensuite, l'image résultante est divisée en petites régions. Pour chacun d'eux, un histogramme des étiquettes est construit afin d'obtenir des vecteurs des caractéristiques des articulations locales des doigts (FKP) (Templates).

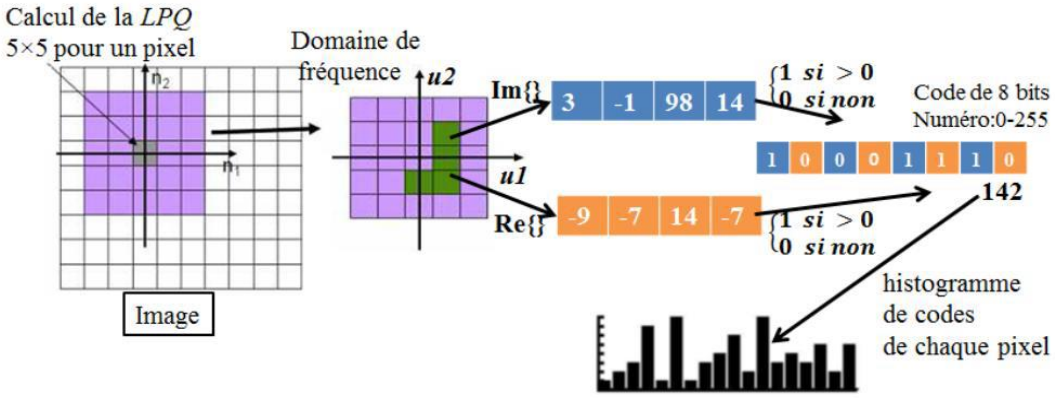


Figure III.8: Organigramme de l'ensemble des étapes nécessaire à la construction du descripteur LPQ

La représentation globale (vecteur des caractéristiques globales qui représente l'image entière) de l'articulation du doigt (FKP) est obtenue en combinant tous les vecteurs. La partie (c) de la figure suivante résume toutes les étapes nécessaires pour générer ce vecteur **[69].**

- **Réduction de la dimensionnalité :**

Dans notre travail on a utilisé l'algorithme LDA (*Linear Discriminant Analysis*), ce L'algorithme a été développé par *Belhumeur* de l'Université de Yale (USA) en 1997 **[72]**, Contrairement à l'algorithme PCA, l'algorithme LDA effectue une séparation de classe réelle. Le LDA analyse les vecteurs propres de la matrice de dispersion des données, dans le but de maximiser les variations entre les images d'individus différents (interclasses) tout en minimisant les variations entre les images d'un même individu (intra-classe).
Cependant, lorsque le nombre d'individus à traiter est inférieur à la résolution de l'image, il est difficile d'appliquer le LDA, qui peut alors révéler des matrices de dispersion singulières (non invariables).

Comme l'ACP ne tient pas compte de la discrimination de classe, mais que l'LDA résout ce problème, et que la méthode *Fisher faces,* appliquent d'abord l'ACP pour la réduction de taille et ensuite l'analyse discriminante. Les questions appropriées au sujet de l'ACP sont habituellement liées au nombre de composantes principales (CP) utilisées et à leur incidence sur le rendement.

En pratique, pour tous les échantillons de toutes les classes, il y a deux mesures. La première mesure est la matrice de dispersion à l'intérieur de la classe S_w qui est notée :

$$S_w = \sum_{j=1}^{c} \sum_{i=1}^{N_j} (x_i^j - \mu_j)(x_i^j - \mu_j)^T$$

Avec x_i^j le *i*ème échantillon de la classe *j*, μ_j la moyenne de la classe *j*, *c* le nombre de classes et N_j le nombre d'échantillons de la classe *j*. La deuxième mesure est la matrice d'éparpillement interclasses S_b ("between-class scatter matrix") qui est définie par :

$$S_b = \sum_{j=1}^{c} (\mu_j - \mu)(\mu_j - \mu)^T$$

Avec μ la moyenne de tous les échantillons. Le but est de maximiser les distances interclasses tout en minimisant les distances intra-classes, ce qui revient à retrouver la

matrice de transformation W qui maximise le critère $J(W) = \frac{W^T S_b W}{W^T S_w W}$ donc W est optimale pour :

$$W_{opt} = \arg\max_{w}\left(\frac{\left|W^T S_b W\right|}{\left|W^T S_b W\right|}\right) = (w_1, w_2, w_3, ..., w_m)$$

Ce problème est ramené à un problème de recherche des vecteurs propres de la matrice $S_w^{-1} S_b$ **[74].**

III.2.4 Phase de comparaison

Le résultat de la phase d'extraction des paramètres est un vecteur de caractéristiques représentant chaque image qui sera évaluée à l'aide d'une comparaison basé sur une métrique de distance.

La phase de comparaison des caractéristiques dans le système de reconnaissance peut être réalisée en utilisant n'importe quelle mesure de distance ou de similarité telle que Euclidienne, cosinus, corrélation, Minkowski et autres. Cependant, en raison de la spécificité des descripteurs de caractéristiques basés sur des histogrammes, on utilise des mesures de similarité plus spécialisées. La mesure de distance la plus fréquente pour l'appariement des histogrammes utilisés dans les tâches de vision par ordinateur est la statistique du Chi-square qui sert de mesure de dissimilarité et plus la valeur est faible, plus les deux histogrammes sont semblables.

La distance Chi-square entre deux vecteurs de caractéristiques.

Les vecteur $V_1 = [x_0, x_2, ..., x_n]$ et $V_2 = [y_0, y_2, ..., y_n]$ est défini comme :

$$dist^{chi}(V_1, V_2) = \sum_{i=0}^{n} \frac{(x_i - y_i)}{x_i + y_i}$$

Pour les expériences d'identification, les vecteurs de caractéristiques sont comparés d'une manière références -à-test et les scores résultants sont triés et classés pour trouver le rang auquel une correspondance réelle se produit.

III.3 Résultats expérimentaux

Dans cette section, nous conduisons des expériences sur la base de données PolyU FKP largement utilisée **[65],** pour évaluer la méthode proposée pour une tache d'identification seulement.

Ensuite, nous présentons les résultats expérimentaux des expériences d'identification de la FKP pour toutes les caractéristiques évaluées basées sur la LBP et LPQ.

III.3.1 Description de la base de données

La base de données PolyU FKP contient 7 920 images FKP collectées par 165 personnes volontaires dont 125 mâles et 40 femelles. Ces images sont obtenues à au moyen d'un dispositif de capture FKP en temps réel élaboré par le Centre de recherche biométrique (UGC / CRC) de l'Université polytechnique de Hong Kong. Chaque personne est invitée de fournir 48 images en deux sessions séparées par un intervalle de temps d'environ 25 jours à partir de 4 doigts. Pour chaque session, la personne fournit 24 images pour chaque index gauche, majeur gauche, index droit et majeur droit. Par conséquent, la base de données PolyU FKP se compose de 7 920 (165*48) échantillons de 660 (165x4) doigts différents.

III.3.2 Structure da la base de données

La base de données contienne plusieurs dossiers. Chaque dossier est nommé XXX-finger type représente l'identité de la personne. Par exemple « 001_left index ».

Dans chaque dossier, les 6 premières images (01~06) ont été capturées lors de la première session et les 6 dernières images (07~12) lors de la seconde session.

La base de données contient toutes les images FKP originales collectées avec le dispositif de capture FKP. En plus elle contient également les images ROI extraites en utilisant l'algorithme d'extraction de ROI décrit dans **[65].**

III.3.3 Protocole d'évaluation

L'identification par l'empreinte FKP est une procédure de comparaison un contre plusieurs pour identifier une image FKP de test. Dans cette étude, nous avons sélectionné les premières n (n=2,....,6) images pour chaque doigt comme un ensemble d'apprentissage et nous avons utilisé le reste comme des images de test. Le Taux l'identification de rang a été calculé afin d'évaluer la performance d'identification de la méthode proposée.

III.3.4 Expérience de reconnaissance sur chaque type de doigt

Dans cette expérience, la performance de chaque doigt est évaluée en utilisant la technique proposée. Le taux de reconnaissance est calculé et présenté dans les tableaux.

III.3.4.1 les résultats obtenus par la méthode LPQ :

III.3.4.1.1 Pour le doigt index gauche :

MxM K	3x3	5x5	7x7	9x9	11x11	13x13	15x15	17x17	19x19
1	29.73	42.91	52.70	58.56	59.57	58.56	63.18	61.37	67.91
2	51.01	84.57	93.13	94.59	94.26	94.14	94.14	94.59	92.79
3	88.51	95.95	97.64	98.20	98.09	96.96	97.07	96.96	96.73
4	92.45	96.17	97.41	97.86	97.86	97.64	96.96	97.18	97.07
5	93.24	96.62	96.06	96.85	96.73	97.30	96.62	96.51	96.62

Tableau III.1 : les résultats obtenus par la méthode LPQ de LIF.

Meilleur résultat de taux de reconnaissance pour le LIF sans chevauchement est de : T=98.20.

Et avec chevauchement pour 0.5 : T = 98.31 et pour 0.75 : T = 98.42.

III.3.4.1.2 Pour le doigt majeur gauche :

MxM K	3x3	5x5	7x7	9x9	11x11	13x13	15x15	17x17	19x19
1	35.25	53.28	55.52	59.80	62.50	61.60	62.61	64.19	64.41
2	54.73	87.16	92.79	94.71	95.95	94.03	94.26	94.26	93.02
3	89.53	96.73	98.42	97.97	98.42	98.09	97.86	97.07	97.46
4	93.36	97.52	98.09	97.97	97.75	97.64	98.42	97.52	97.07
5	94.93	98.09	98.20	98.20	97.30	96.51	97.07	96.73	96.85

Tableau III.2 : les résultats obtenus par la méthode LPQ de LMF.

Meilleur résultat de taux de reconnaissance pour le LMF sans chevauchement est de : T= 98.42.

Et avec chevauchement pour : 0.5 : T = 98.87 et pour 0.75 : T = 98.87.

III.3.4.1.3 Pour le doigt index droit:

MxM K	3x3	5x5	7x7	9x9	11x11	13x13	15x15	17x17	19x19
1	32.32	55.86	64.75	63.74	67.12	65.32	67.23	64.86	66.10
2	55.52	87.27	91.22	93.47	92.91	91.67	92.45	92.00	92.12
3	89.86	95.61	95.83	97.18	97.52	96.62	96.51	95.72	94.93
4	92.45	95.95	95.83	95.61	96.17	96.40	95.83	95.16	95.50
5	92.45	94.82	94.82	95.38	95.05	94.48	95.05	94.93	93.81

Tableau III.3 : les résultats obtenus par la méthode LPQ de RIF.

Meilleur résultat de taux de reconnaissance pour le RIF sans chevauchement est de : T= 97.52.

Et avec chevauchement pour : 0.5 : T = 98.08 et pour 0.75 : T = 97.64.

III.3.4.1.4 Pour le doigt majeur droit:

MxM / K	3x3	5x5	7x7	9x9	11x11	13x13	15x15	17x17	19x19
1	33.56	52.04	62.93	64.85	67.12	67.35	69.84	71.66	69.95
2	62.02	88.78	92.74	94.67	94.10	93.88	94.90	94.22	91.84
3	89.80	96.71	97.28	97.51	97.39	97.51	96.15	97.05	95.35
4	94.10	96.6	96.60	96.71	97.62	96.15	95.92	95.69	95.35
5	91.95	94.90	96.15	95.80	96.71	96.26	95.80	95.12	95.46

Tableau III.4 : les résultats obtenus par la méthode LPQ de RMF

Meilleur résultat de taux de reconnaissance pour le RMF sans chevauchement est de : T= 97.62.

Et avec chevauchement pour : 0.5 : T = 97.85.

III.3.4.2 Les résultats obtenus par la méthode LBP :

III.3.4.2.1 Pour le doigt index gauche :

R / K	2	4	6	8	10	12	14	16	18
1	34.80	41.89	47.86	44.48	49.66	50.45	51.80	49.89	49.89
2	64.86	87.39	94.03	95.38	93.13	92.57	91.55	88.85	85.25
3	90.99	96.62	96.17	96.40	96.85	95.61	94.37	93.36	91.87
4	93.24	96.51	96.40	96.17	95.95	94.82	94.26	92.68	91.33
5	93.85	95.61	95.38	95.61	95.50	94.93	93.24	91.55	90.65

Tableau III.5 : les résultats obtenus par la méthode LBP de LIF.

Meilleur résultat de taux de reconnaissance pour le LIF sans chevauchement est de : T= 96.62.

Et avec chevauchement pour : 0.5 : T = 97.07.

III.3.4.2.2 Pour le doigt majeur gauche :

R / K	2	4	6	8	10	12	14	16	18
1	38.74	53.72	55.86	58.45	60.02	52.82	51.13	52.14	48.99
2	68.92	92.68	92.91	94.93	91.89	91.78	90.77	88.18	85.47

3	92.68	97.75	97.52	96.96	95.95	94.59	93.92	93.69	92.12
4	95.50	98.09	97.30	96.62	96.62	94.82	94.93	94.03	91.33
5	94.93	97.75	96.17	96.28	95.05	95.16	93.92	92.57	90.88

Tableau III.6 : les résultats obtenus par la méthode LBP de LMF.

Meilleur résultat de taux de reconnaissance pour le LMF sans chevauchement est de : T= 98.09.

Et avec chevauchement pour : 0.5 : T = 98.09 et pour 0.75 : T=98.20

III.3.4.2.3 Pour le doigt index droit:

R / K	2	4	6	8	10	12	14	16	18
1	39.98	53.72	55.63	55.18	54.39	54.62	53.49	55.41	55.97
2	67.91	91.33	92.34	91.89	90.65	91.33	89.64	86.94	83.45
3	91.44	94.48	96.17	94.37	94.03	93.24	92.57	92.23	89.30
4	93.58	93.69	95.83	93.92	93.36	93.92	92.57	91.33	98.98
5	93.58	94.14	94.93	94.14	93.13	92.34	90.17	89.75	88.74

Tableau III.7 : les résultats obtenus par la méthode LBP de RIF

Meilleur résultat de taux de reconnaissance pour le RIF sans chevauchement est de : T= 96.17.

Et avec chevauchement pour : 0.5 : T = 96.40 et pour 0.75 : T=96.28.

III.3.4.2.4 Pour le doigt majeur droit:

R / K	2	4	6	8	10	12	14	16	18
1	38.66	51.47	59.30	58.28	53.51	56.46	56.01	54.31	50.34
2	69.16	91.27	94.67	91.38	93.54	90.93	89.34	88.10	84.01
3	93.42	96.15	96.49	95.69	95.80	93.65	94.33	92.97	91.84
4	94.44	94.90	96.26	95.24	95.01	93.88	93.20	92.97	91.61
5	92.86	95.46	94.56	95.01	93.88	92.97	92.29	91.61	89.57

Tableau III.8 : les résultats obtenus par la méthode LBP de RIF

Meilleur résultat de taux de reconnaissance pour le RMF sans chevauchement est de : T= 96.49.

Et avec chevauchement pour : 0.5 : T = 96.94 et pour 0.75 : T=97.51.

III.4 Conclusion :

Dans ce chapitre nous avons présenté notre système global de reconnaissance par l'empreinte des articulations des doigts FKP basée sur les algorithmes LPQ et LBP, on a présenté aussi les différents résultats obtenus pour chaque algorithme. Notre système de reconnaissance par l'empreinte des articulations des doigts FKP, est appliquée sur la base de donné de FKP (PolyU). Pour conclure, Nous pouvons noter que les expérimentations ont montré que la méthode de reconnaissance FKP base sur la méthode LPQ est la plus efficace que la méthode LBP. Cependant, nous avons également vu que de nombreux facteurs extérieurs influent sur la qualité de la reconnaissance

CONCLUSION GENERALE

CONCLUSION GENERALE

La reconnaissance biométrique et l'identification des personnes basées sur l'utilisation de ses caractéristiques physiques ou comportementales ou biologies.

Parmi les modalités les plus utilisées dans la reconnaissance biométrique est l'empreinte FKP par ce qu'elle est permanente et unique. Les chercheurs essayent toujours de développer les systèmes de reconnaissance à travers des outils mathématiques habituellement complexes pour faire la discrimination entre les individus.

L'objectif suivis dans ce mémoire propose une démarche qui consiste à améliorer la performance de l'identification biométriques via l'empreinte FKP par plusieurs méthodes avec un ensemble d'opérations. Pour cela, nous avons fait la comparaison entre différentes méthodes d'extraction des caractéristiques, ce qui nous a permis d'en choisir celle qui est la mieux adaptée pour notre problème. Suivant les résultats obtenus, nous avons opté pour le choix des méthodes LPQ et LBP.

Enfin, le système proposé est appliqué sur une base de donnés connue dans le domaine des empreintes FKP et les résultats obtenus, sont intéressants. En effet on est arrivé à un taux de reconnaissance acceptable. Ce taux est intéressant 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] Benchennane Ibtissam « Etude et mise au point d'un procédé biométrique multimodale pour la reconnaissance des individu**s** » THÈSE En vue de l'obtention du Diplôme de Doctorat, Université des Sciences et de la Technologie d'Oran Mohamed Boudiaf

[2] Souilla Benkhaira« Systèmes multimodaux pour l'identification et l'authentification biométrique » mémoire Pour l'obtention du diplôme de Magister en Informatique, Université 20 Août 1955-Skikda

[3] Michèle Gagnon *« La géométrie de la main »* sur (http://biometrics.over-blog.com/pages/La_geometrie_de_la_main-2019729.html) l'École de Criminologie Université de Montréal Intérêt particulier : cybercriminalité, technologies, sciences forensiques consulté le 24 avril 2019.

[4] Moulay Brahim Oussama et Arbaoui Mohamed Ibrahim « *Identification des personnes par les articulations des doigts »* mémoire de Master académique Université Kasdi Merbah Ouargla

[5] Michèle Gagnon *« Les empreintes digitales »* sur (http://biometrics.over-blog.com/pages/Les_empreintes_digitales-2005982.html) consulté le 25 avril 2019.

[6]C. L. Tisse, L. Torres, L. Martin et M. Robert « Systèmes biométriques pour la vérification d'individu, Un exemple: l'iris » Center for Autonomous System, University of Sydney, The Rose Street Building J04, NSW 2006, Australia.

[7] Julian Ashbour « Biometrics: advanced identify verification: the complete guide » Library of Congress Cataloging-in-Publication Data Ashbourn, Julian, 1952

[8] Article de **Secriteinfo**, La sécurité informatique *« la Biométrie »* disponible sur web *(https://www.securiteinfo.com/conseils/biometrie.shtml)* 21 Janvier 2002consulté le 30 avril 2019.

[9]Angelo Genovese, Vincenzo Piuri, Fabio Scotti « Touchless Palmprint Recognition,Systems »

[10] Bouzidi adel « Système de reconnaissance des empreintes Palmaires » mémoire de master Université Mohamed Khider de Biskra

[11] julian ashourn « biometrics advenced identify verification»

[12] Céline delizarche, Linternaute*« L'iris »* disponible sur web http://www.linternaute.com/science/biologie/dossiers/06/0607-biometrie/iris.shtml) consulté le 30 avril 2019

[13] Jlassi Hajer, Hamrouni Kamel « Caractérisation de la rétine en vue de l'élaboration d'une méthode biométrique d'identification de personnes » *Ecole Nationale d'Ingénieurs de Tunis (ENIT)*

[14]Céline delizarche, linternaute, *« la reconnaissance vocale »*disponible sur **(**http://www.linternaute.com/science/bigie/dossiers/06/0607-biometrie/visage.shtml) consulté le 30 avril 2019

[15]Clara L. Clément Duplessis« *Biométrie par reconnaissance vocale »*disponible sur web(https://sites.google.com/site/tpelabiometrie/home/biometrie-par reconnaissance-vocale)cite de Lycée Maurice Genevoixconsulté le 15 avril 2019

[16] Jean-François Pillou,*« les applications de reconnaissance vocale pour android et ios »*disponible sur (https://www.commentcamarche.net/faq/33392-les-applications-dereconnaissance vocale-pour-android-et-ios) consulté le 15 mars 2019

[17] Didier Guillerm *« Signature dynamique »* disponible sur web (https://www.biometrie-online.net/technologies/signature-dynanique) consulté le 3 avril2019

[18] Allano Lorène *« La Biométrie multimodale : stratégies de fusion de scores et mesures de dépendance appliquées aux bases de personnes virtuelles »*. Thèse de doctorat, l'institut national des télécommunications dans le cadre de l'école doctorale SITEVRY de Paris, 2009

[19] Marine Corniou « *Reconnaissance faciale, iris, veines…les nouvelles cartes d'identité »* disponible sur (https://www.quebecscience.qc.ca/technologie/reconnaissance-faciale-iris-veines-les-nouvelles-cartes-didentite/) consulté le 22 avril 2019

[20] ZEMMIT Saad« identification d'un individu par l'EMG » Mémoire présenté pour l'obtention du diplôme de Master Académique UNIVERSITE MOHAMED BOUDIAF - M'SILA

[21] Céline delizarche, L'internaute*« la retine »* magasin de science, disponible sur (http://www.linternaute.com/science/biologie/dossiers/06/0607- Biometrie/retine.shtml) consulté le 22 mai 2019

[22] Marc Zaffagni *« La frappe au clavier, un outil biométrique prometteur » disponible sur* (https://www.futura-sciences.com/tech/actualites/informatique-frappe-clavier-outil-biometrique-prometteur-41010/) consulté le 3 avril 2019

[23] Yeihya KABBARA « Caractérisation des images à Rayon-X de la main par des modèles mathématiques : application à la biométrie »Thèse de doctorat université paris-est université libanaise.

[24] E. GokulaKrishnan(&) and G. Malathi*« A Survey on Multi-feature Hand Biometric Recognition »* School of Computing Science and Engineering, VIT University Chennai Campus, Chennai, India

[25] Anil K. Jain et Patrick Flynn et Arun A. Ross*«Handbook of Biometrics »* p 7

[26] ISO/IEC 19795-1. Information technology « biometric performance testing and reporting – part 1 : Principles and framework, 2006. »

[27] M. Theofanos, B. Stanton, and C. A. Wolfson. *« Usability &Biometrics : Ensuring Successful Biometric Systems. »* National Institute of Standards and Technology (NIST), 2008. [cit´e p. 23]

[28] ISO/IEC FCD 19792. *« Information technology – security techniques – security evaluation of biometrics, 2008 ».*

[29] Timo Ahonen, Abdenour Hadid, and Matti Pietikainen. « *Face Recognition with Local Binary Patterns. 2003 »*

[30] Anil K. Jain, Arun Ross and Salil Prabhakar *« An Introduction to Biometric Recognition »* Appeared in IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics, Vol. 14, No. 1, January 2004.

[31] F. Cherifi, B. Hemery, R. Giot, M. Pasquet, C. Rosenberger*« Performance Evaluation Of Behavioral Biometric Systems »*GREYC Laboratory ENSICAEN–CNRS–University of Caen, France

[32] A. J. Mansfield, NPL J. L. Wayman,*« Practices in Testing and Reporting Performance of Biometric Devices »* Centre for Mathematics and Scientific Computing National Physical Laboratory Queens Road

[33] khellat souad ***«*** *identification biométrique par fusion multimodale de l'empreinte d'articulation l'empreinte digitale et l'empreinte veineuse du doigt* **»**thèse de doctorat de l'Université de science et technologies d'Oran Mohammed Boudiaf

[34] David D. Zhang*« AUTOMATED BIOMETRICS Technologies and Systems »*The Kluwer International Series on ASIAN STUDIES IN COMPUTER AND INFORMATION SCIENCE Hong Kong Polytechnic University

[35] DJILI Abdellah MAHDADI Djamel Eddine *« Reconnaissance de personnes utilisant la multi-représentation de l'iris »* mémoire de master académique UNIVERSITE KASDI MERBAH OUARGLA

[36] Ted Dunston et Neil Yager*« biometric system and data analysis »* design evaluation and data mining *Eveleigh, NSW, Australia springer*

[37] Benoît Vibert*« Contributions à l'évaluation de systèmes biométriques embarqués »*Thèse Pour obtenir le diplôme de doctorat Université Caen Normandie

[38] Bouzidi adel « *Système de reconnaissance des empreintes palmaires »*mémoire de master Université Mohamed Khider de Biskra

[39] Mohamad El-Abed*« Évaluation de système biométrique »* THESE DE Doctorat de l'Université de Caen Basse-Normandie

[40] FR Bach and MI Jordan. *« Kernel independent component analysis. Journal of Machine Learning Research »*, pages 1_48, 2002

[41] A.M. Martinez and R. Benavente.*« The AR face data base. CVC Tech. Report, 1998 ».*

[42] P.J. Phillips, H. Wechsler, J. Huang, and P. Rauss.*« The FERET database and evaluation procedure for face recognition algorithms ».* Journal of Image and Vision Computing, 16 :295–306, 1998.

[43] P.J. Phillips, H. Moon, S.A. Rizvi, and P.J. Rauss. *« The FERET evaluation methodology for face-recognition algorithms ».* IEEE Transactions on Pattern Analysis and Machine Intelligence (PAMI), 22(10) :1094–1104, 2000.

[44] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain.*« Fvc2002 : Second fingerprint verification competition. »*In International Conference on Pattern Recognition (ICPR'02), volume 3, pages 811 – 814, 2002.

[45] P.J. Phillips, P.J. Flynn, T. Scruggs, K.W. Bowyer, J. Chang, K. Hoffman, J. Marques, J. Min, and W. Worek. « *Overview of the face recognition grand challenge ».* In Proceedings of the 2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'05),

[46] S. Sarkar, P. J. Phillips, Z. Liu, I. R. Vega, P. Grother, and K. W. Bowyer. *« The human ID gait challenge problem : data sets, performance, and analysis. »* IEEE Transactions on Pattern Analysis and Machine Intelligence (PAMI), 27(2) :162–177, 2005.

[47] B. Hemery, C. Rosenberger, and H. Laurent. *« The ENSIB database : a benchmark for face recognition ».* In International Symposium on Signal Processing and its Applications (ISSPA), special session "Performance Evaluation and Benchmarking of Image and Video Processing", 2007.

[48] K. Messer, J. Matas, J.V. Kittler, J. Luettin, and G. Maitre. XM2VTSDB : The Extended M2VTS Database. In Proc. Second International Conference on *« Audio- and Video-based Biometric Person Authentication (AVBPA'99) »*, pages 72–77, 1999

[49] V. Popovici, J. Thiran, E. Bailly-Bailliere, « *The BANCA database and evaluation protocol »*. In 4th International Conference on Audio- and Video-Based Biometric Person Authentication, volume 2688, pages 625–638, 2003.

[50] J. Huang, and P. Rauss*« Biosecure Multimodal Biometric Databas »* disponible sur (http ://www.biosecure.info/, 2008).

[51] R. Giot, M. El Abed, and C. Rosenberger. Greyc keystroke*« a benchmark for keystroke dynamics biometric systems »*. In IEEE Third International Conference on Biometrics : Theory, Applications and Systems (BTAS), pages 1–6, 2009.

[52] R. Cappelli, D. Maio, and D. Maltoni.*« Synthetic fingerprint-database generation. In International Conference on Pattern Recognition (ICPR), »* pages 744–747, 2002

[53]*« Etude et mise au point d'un procédé biométrique multimodale pour la reconnaissance des individus »* PHD. dissertation.

[54] L. Zhang, L *Online finger-knuckle-print verification for personal authentication, Pattern Recogn. »* 43 (7) (2010) 2560–2571.

[55] D.L. Woodard and P.J. Flynn, *« Finger surface as a biometric identifier »*.CVIU, vol. 100, pp. 357–384, 2005.

[56] C. Ravikanth and A. Kumar, *« Biometric Authentication using Finger-Back Surface »*, CVPR'07, pp. 1-6, 2007.

[57] L. Zhang,,*« Finger knuckle print : anew biometric identifie »*, IEEE, pp. 1981–1984,Hong-Kong, 2009.

[58] A. Morales et al, *« Improved finger-knuckle-print authentication based on orientation enhancement »*, electronics letters, Vol. 47 No. 6 , 17th March 2011.

[59] ZHU Le-qing, « *Finger knuckle print recognition based on SURF algorithm »* , Eighth International Conference on Fuzzy Systems and Knowledge Discovery (FSKD),IEEE, 2011.

[60] YANG Wankou, *« Finger-Knuckle-Print Recognition Using Gabor Feature and OLDA »* , Proceedings of the 30th Chinese Control Conference, Yantai, China, July 22-24, 2011.

[61] Zahra S. Shariatmadar, Karim Faez, *« A Novel Approach for Finger-Knuckle-Print Recognition Based on Gabor Feature Fusion »* ,4th International Congress on Image and Signal Processing, IEEE, 2011.

[62] Guangwei Gao and Jian Yang, *« Weight Competitive Coding for Finger-Knuckle-Print Verification »* pp. 185–192, Springer International Publishing Switzerland, 2013.

[63] Chetana Hegde et al, *« Authentication using Finger Knuckle Prints »*, Springer-Verlag London, 2013

[64] Harbi AlMahafzah et al, *« Multi-Algorithm Decision-Level Fusion Using Finger-Knuckle-Print Biometric »*.Springer India 2014.

[65] Lei ZHANG,*« the Hong Kong Polytechnic University (PolyU) Finger-Knuckle-Print Database »,disponible*sur**(**https://www4.comp.polyu.edu.hk/~biometrics/FKP.htm) consulté le 22 mai 2019

[66] Ojala, T., Pietikäinen, M., Mäenpää, T.: *« Multiresolution gray-scale and rotation invariant texture classification with local binary patterns »*.IEEE Trans. Pattern Anal. Mai Mach. Intell. 24(7), 971–987 (2002)

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

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

[69] CécileFicher, *« Repousser les limites de l’identification faciale en contexte de vidéo-surveillance »*. GRENOBLE 2012

[70] Docteur Thierry Aimard ***«*** *Anatomie de la Main »*disponible sur web (http://www.thierryaimard.fr/anatomie-main.php) consiulté le 21mai2019

[71] T. Ojala, M. Pietikainen and T. Maenpaa, « *Multi-resolution gray-scale and rotation invariant texture classification with local binary patterns »*, IEEE Trans. Pattern Anal.Mach. Intell.24 (2002) 971987

[72] K. Etemad, R. Chellappa, « *Discriminant Analysis for Recognition of Human Face images »*, Journal of the Optical Society of America A, Vol. 14, No. 8, August 1997, pp. 1724-1733

[73] BETTAHAR Abdessettar ABER Fathi « *Extraction des caractéristiques pour l'analyse biométrique d'un visage* » Mémoire MASTER ACADEMIQUE UNIVERSITE KASDI MERBAH OUARGLA

[74] Anouar Mellakh « *Reconnaissance des visages en conditions dégradées* » THÈSE de doctorat de l'Institut National des Télécommunications l'université d'Evry-Val d'Essonn

Liste des matières