



Université Mohamed Khider de Biskra  
Faculté des Sciences et de la Technologie  
Département de génie électrique

# MÉMOIRE DE MASTER

Sciences et Technologies  
Télécommunications  
Réseaux et Télécommunications

Réf. :

---

Présenté et soutenu par :

**Bouzidi adel**

Le : lundi 25 juin 2018

## *Systeme de reconnaissance des empreintes palmaires*

---

### Jury :

<b>Mr</b>	Sbaa salim	<b>MCA</b>	Université de Biskra	<b>Président</b>
<b>Mr</b>	Ouafi abdelkrim	<b>Pr</b>	Université de Biskra	<b>Encadreur</b>
<b>Mr</b>	Barkat aicha	<b>MAA</b>	Université de Biskra	<b>Examineur</b>

Année universitaire : 2017/2018

# *Dédicace*

*Je dédie ce mémoire:*

*À mes chers parents qui m'ont soutenu de tout leur pouvoir pour réaliser ce  
beau moment*

*À mes amis qui m'ont soutenu*

*À ma famille aimable*

*À ceux qui n'ont pas eu la chance de terminer leurs études*

*À tout le personnel universitaire pour ses efforts*

*Et aux professeurs vertueux qui ne leur donnent pas le droit de remercier  
tout ce que nous faisons*

*Adel bouzidi*



# Remerciements

*Nous tenons à remercier tout d'abord dieu qui a aidé à réaliser ce modeste travail, et pour sa grâce toutes au long de notre vie professionnelle et personnelle.*

*Nous remercions chaleureusement notre encadreur Professeur : Ouafi Abdelkrim pour son aide, sa disponibilité, son sérieux ainsi que ses encouragements et ses conseils.*

*Je tiens aussi à remercier :*

- *Tous les enseignants de département de génie électrique.*
- *Messieurs, Azzeddine Benlaamoudi, pour sa disponibilité, sa patience, son suivi constant de ce travail.*
- *Sans oublier qui ont contribué de près ou de loin à la réaffirmation de notre travail.*

*Adel bouzidi*

- *Messieurs. Azzeddine Benlaamoudi. pour sa disponibilité.*

## ملخص :

- ✓ شكلت الخصائص الحيوية للأفراد ميزة تقنية رائدة في أواخر القرن الماضي و أخذت في التطور إلى يومنا هذا و استخدمت كأنظمة أمنية فعالة فيما نسميه بالنظام البيو مترى.
- ✓ تعتمد هذه الأنظمة في عملها على الخصائص المميزة للجسم البشري مثل :بصمة الإصبع و شكل العين و المشي و الصوت و غيرها.
- ✓ و تحجز في هذا النظام بصمة الكف مكانا مهما لما لها من ميزات تؤهلها لذلك كسهولة الاستخدام و الأمانة العالية و بساطة فكرتها .
- ✓ انطلاقا من كلّ هذا قمنا بعمل نظام يحدد انتمائية الشخص لقاعدة بيانات من خلال بصمة الكف .
- ✓ في كل الأنظمة البيو مترية، هناك تقنيات مختلفة لاستخراج مميزات لوصف معلومات الملمس، و قد استخدمنا في هذا العمل تقنية **تكميم المرحلة المحلية LPQ** .
- ✓ طبقنا عملنا هذا على قاعدة بيانات معروفة في هذا المجال و تحصلنا على نتائج مقبولة

## الكلمات المفتاحية :

التقنيات البيو مترية ، بصمة الكف ، استخراج الخصائص ،تكميم المرحلة المحلية،التصنيف .

## Résumé

- Les caractéristiques biologiques des individus ont été un avantage technologique majeur au siècle dernier et ont évolué jusqu'à nos jours et ont été utilisées comme systèmes de sécurité efficaces 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 ce système, les empreintes palmaires sont un lieu important en raison de ses avantages, tels que la facilité d'utilisation, la haute sécurité et la simplicité de la pensée.
- Sur la base de tout cela, nous avons créé un système qui définit le développement d'une base de données à travers un (**palmprint**).
- Dans tous les systèmes biométriques, il existe différentes techniques d'extraction de caractéristiques pour décrire les informations de texture. Dans notre travail nous avons utilisé la méthode de quantification de phase locale **LPQ**.
- Notre travail est appliqué sur une base de données connue dans ce domaine est a donné des résultats acceptables.

Les mots clés : Technique biométrique, empreinte palmaire,Extraction des caractéristiques,LPQ, classification

# *Sommaire*

Dédicace .....	I
Remerciement .....	II
Résumé.....	III
Sommaire .....	IV
Liste des abréviations.....	V
<b><i>Introduction générale</i></b> .....	<b>2</b>

### ***Chapitre I: Généralités sur la biométrie***

<b>I.1 Introduction</b> .....	<b>5</b>
<b>I.2 Définition de la biométrie</b> .....	<b>5</b>
<b>I.3 Principaux modalités biométriques</b> .....	<b>7</b>
I.3.1. Modalités morphologiques (physiologiques).....	8
I.3.2. Modalités comportementale.....	11
I.3.3. Modalités biologiques .....	14
<b>I.4- Représentation comparative entre quelques Techniques Biométriques</b> .....	<b>15</b>
<b>I.5 Système biométrique</b> .....	<b>16</b>
I.5.1 Modes de fonctionnement.....	17
I.5.2 Le mode vérification ou authentification .....	17
I.5.3 Le mode identification .....	18
<b>I.6. Structure d'un système biométrique</b> .....	<b>19</b>
<b>I.6 Evaluation des performances des Systèmes biométriques</b> .....	<b>19</b>
I.6.5 Le FAR (False Acceptance Rate).....	20
I.6.6 Le FRR (False Rejection Rate) .....	20
I.6.7 L'EER (Equal Error Rate) .....	20
I.6.8 courbe ROC .....	22
<b>I.7 Domaine applications des systèmes biométriques</b> .....	<b>23</b>
<b>I.8 Conclusion</b> .....	<b>24</b>

### ***Chapitre II : Système d'identification des personnes à l'empreinte palmaire***

<b>II.1 Introduction</b> .....	<b>26</b>
<b>II.2 Le principe des méthodes d'identification biométrique</b> .....	<b>26</b>
<b>II.3 Empreinte palmaire</b> .....	<b>26</b>
II.3.1 Avantages de l'empreinte palmaire .....	27

<b>II.3.2 Les caractéristiques biométriques d'une empreinte palmaire.....</b>	<b>27</b>
<b>II.4 des méthodes de prétraitement .....</b>	<b>30</b>
II.4.1 - Rehaussement des niveaux de gris .....	30
II.4.2 -Égalisation d'histogramme .....	31
II.3.3 débruitage par Filtre gaussien.....	33
<b>II.5 Méthodes d'Extraction des Caractéristiques .....</b>	<b>33</b>
II.5.1 Extraction basé sur la texture.....	33
II.5.2 Extraction basé sur le filtrage .....	36
<b>II.6. Classification .....</b>	<b>37</b>
II.6.1 Machine à vecteurs de support (SVM) .....	37
II.6.2 Principe de SVM .....	37
II.6.3 Concept des SVM.....	37
II.6.4 Séparation optimale .....	38
II.5.5 Multi-classes.....	38
<b>II.7 Conclusion.....</b>	<b>40</b>

*Chapitre III :Simulation et résultats*

<b>III.1 Introduction .....</b>	<b>42</b>
<b>III.2 Base de données de l'empreinte palmaire multi-spectrale (PolyU -MSP).....</b>	<b>42</b>
<b>III.3 Séparation des bases de données.....</b>	<b>43</b>
III.3.1 Images d'apprentissages .....	43
III.3.2 Images de Tests .....	43
<b>III.4 Environnement du travail .....</b>	<b>43</b>
III .4.1 Environnement matériel .....	43
III .4.2 Outils de développement .....	43
<b>III.5. Architecture globale du système .....</b>	<b>44</b>
III.5.1 Prétraitement .....	44
III.5.2 Extraction de caractéristiques.....	45
III.5.3 classification : .....	46
<b>III.6 Résultats et discussion .....</b>	<b>47</b>
<b>III.7 Conclusion:.....</b>	<b>48</b>
<b><i>Conclusion générale .....</i></b>	<b>50</b>
<b><i>Bibliographie.....</i></b>	<b>51</b>

## ***Liste des abréviations***

**ADN:** Acide DésoxyriboseNucléique

**BDD:** Base de données

**CCD:** Charged Coupled Device

**CMC:** Cumulative Match Curve

**EER:** Equal Error Rate

**FAR:** False Accept Rate

**FFT:** Fast Fourier Transform

**FRR:** False Rejection Rate

**IBG:** International Biometric Group

**LBP:** Local Binary Pattern

**LPQ:** Local Phase Quantization

**MSP:** Multi-Spectral Palm print

**NIR:** Near Infra-Red

**PLM:** Palm print

**RGB:** Red Green Blue

**ROC:** Receiver Operating Characteristic

**ROI:** Region Of Interest

**ROR:** Rank One Recognition

**SVM:** Support Vector Machine



***Introduction***

***Générale***

## *Introduction générale*

L'être humain a connu avec le temps plusieurs mutations radicales dans tous les aspects de sa vie surtout avec l'avènement de l'informatique qui a bouleversé le monde c'était vraiment ou une révolution technologique spécialement au domaine de communication ou même temps ont constaté l'augmentation de taux de criminalisation, le piratage, ce dernier touche même nos renseignements privés. A cet effet, il est nécessaire d'établir une nouvelle méthode pour mettre fin à ce problème, cette méthode est dénommée "système de reconnaissance".

La reconnaissance des individus a connu plus d'importance dans la vie humaine quotidienne. Elle assure les transactions des personnes en différents domaines afin d'assurer une sécurité pertinente. Dans les dernières années, la pratique des systèmes de reconnaissance est limitée aux grands secteurs tels que le secteur militaire et d'autres secteurs nécessitant un besoin de sécurité important.

De nos jours, la reconnaissance biométrique est utilisée dans de nombreuses applications telles que la protection de l'accès à un ordinateur, un téléphone portable, une clé USB, un établissement, des cartes bancaires.... De nombreuses technologies biométriques ont été développées, toutes basées sur les identificateurs biométriques physiologiques et comportementales telles que : l'iris, la voix, les empreintes digitales, le visage, la signature.... Ces derniers sont plus fiables que les systèmes classiques (clé, mot de passe...) dans la reconnaissance d'une personne car ils sont difficilement falsifiables. C'est la raison pour laquelle les systèmes biométriques sont actuellement de plus en plus sollicités.

La reconnaissance d'empreintes palmaires dans le cas usuel, civil ou commercial, n'est autre qu'un processus de comparaison de deux images d'empreintes complètes de qualité contrôlée. La nature de l'empreinte palmaire similaire à celle digitale a incité les chercheurs à exploiter les concepts et les approches conçues pour la reconnaissance digitale.

Dans cette étude, on a choisi un système de reconnaissance par les empreintes palmaires. Ce système utilise la forme de la partie intérieure de la main pour l'extraction des caractéristiques biométriques d'identification des individus.

Ces caractéristiques sont permanentes et stables durant toute la vie, aussi uniques pour chacun. Ce travail a pour objectif la réalisation des systèmes biométriques uni-modal basés sur les méthodes : LPQ, LBP pour l'identification des empreintes palmaires. Dans ce mémoire, nous allons essayer d'atteindre cet objectif à travers quatre chapitres, plusieurs notions et concepts de la biométrie et réalisation des systèmes de reconnaissance vont être abordés:

➤ **Le premier chapitre** : Dans ce chapitre, nous allons suivre l'évolution de la reconnaissance biométrique, mettre le point sur le concept et les bases de la reconnaissance automatique ainsi que sur les différentes modalités. Une étude détaillée d'un système biométrique sera dressée et ses domaines d'application.

➤ **Le deuxième chapitre** : On exposera dans ce chapitre, les méthodes utilisées pour le prétraitement, et l'extraction des caractéristiques, et la classification.

➤ Dans **La troisième chapitre**: Nous présentons l'empreinte palmaire comme modalité biométrique, et ses caractéristiques exploitées dans les différents types de reconnaissance ainsi que le processus général de sa reconnaissance. Puis les résultats expérimentaux obtenus par chaque méthode en analysent leurs performances, suivies d'une discussion avec interprétation des résultats. Enfin, nous terminerons ce mémoire par une conclusion générale où nous tracerons des perspectives et des propositions en vue que ce travail servira d'une introduction pour une recherche plus approfondie dans ce domaine.

**Chapitre I:**  
***Généralités sur la***  
***biométrie***

## I.1 Introduction

Au fil de temps, l'être humain a essayé toujours et à chaque fois d'améliorer sa vie sur plusieurs domaines, surtout de vivre en sécurité (d'être sécurisé dans les lieux publics, sécurisé de toute sorte de vol...).

Avec le développement technologique rapide, la sécurité devient l'un des sujets les plus préoccupants au sein de notre société et qui pose un délicat problème pour les citoyens, les entreprises et le gouvernement au niveau de la protection des informations et des données sensibles contre le vol. Pour toutes ces raisons, il est obligatoire de créer une nouvelle technique de contrôle, il s'agit du système biométrique qui constitue une solution efficace. Dans ce chapitre, on donne quelques notions et définitions de base liées à la biométrie.

Nous introduirons aussi le principe de fonctionnement d'un système biométrique et ses performances ainsi que les différentes modalités utilisées [1]

## I.2 Définition de la biométrie

Étymologiquement, le terme biométrie se compose du terme « bio » (du grec ancien βίος qui signifie « vie ») et du terme « métrie » (du grec ancien μέτρον, qui signifie « mesure »). Ainsi, dans son sens premier, biométrie signifie « mesure du vivant » et fait référence à l'étude scientifique et quantitative du monde vivant et des êtres vivants. La biométrie fait maintenant surtout référence à l'ensemble des techniques utilisées pour identifier un individu grâce à certaines de ses caractéristiques physiques, biologiques, et comportementales [2]

Pour que les caractéristiques, propre à chaque individu, puissent être qualifiées de modalités biométriques, elles doivent être :

- **universelles** (existent chez tous les individus),
- **uniques** (possibilité de différencier un individu par rapport à un autre),
- **permanentes** (Fixé dans le temps),
- **enregistrables** (possibilité d'enregistrer les caractéristiques d'un individu avec son accord),
- **mesurables**

Le tableau suivant compare les systèmes biométriques existants en fonction des paramètres précédents :

**Tableau I.1** : Comparaison des Technologies Biométriques

Comparison of various biometric technologies, modified from Jain et al., 2004 (H=High, M=Medium, L=Low)							
Biometrics	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention
Face	H	L	M	H	L	H	L
Fingerprint	M	H	H	M	H	M	H
Hand geometry	M	M	M	H	M	M	M
Keystrokes	L	L	L	M	L	M	M
Hand veins	M	M	M	M	M	M	H
Iris	H	H	H	M	H	L	H
Retinal scan	H	H	M	L	H	L	H
Signature	L	L	L	H	L	H	L
Voice	M	L	L	M	L	H	L
Facial thermograph	H	H	L	H	M	H	H
Odor	H	H	H	L	L	M	L
DNA	H	H	H	L	H	L	L
Gait	M	L	L	H	L	H	M
Ear Canal	M	M	H	M	M	H	M

L'empreinte digitale, la géométrie de la main, l'iris, la rétine, le visage, l'empreinte palmaire, la géométrie de l'oreille, l'ADN, la voix, la démarche, la signature ou encore la dynamique de frappe au clavier sont autant de modalités biométriques différentes (**Fig.I.1**)

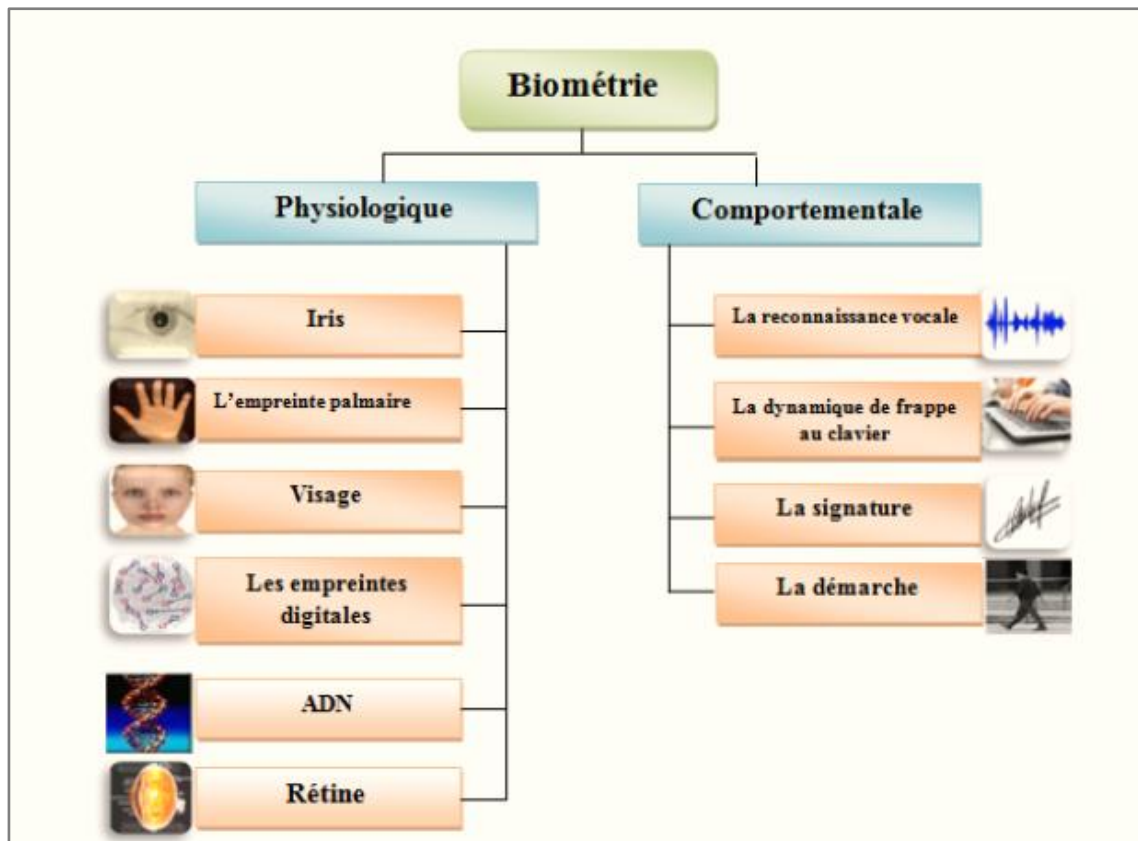


Figure I.1 : Catégories technologique de la biométrie.

### I.3 Principaux modalités biométriques

Il existe plusieurs modalités biométriques utilisées dans divers secteurs, On peut distinguer trois catégories :

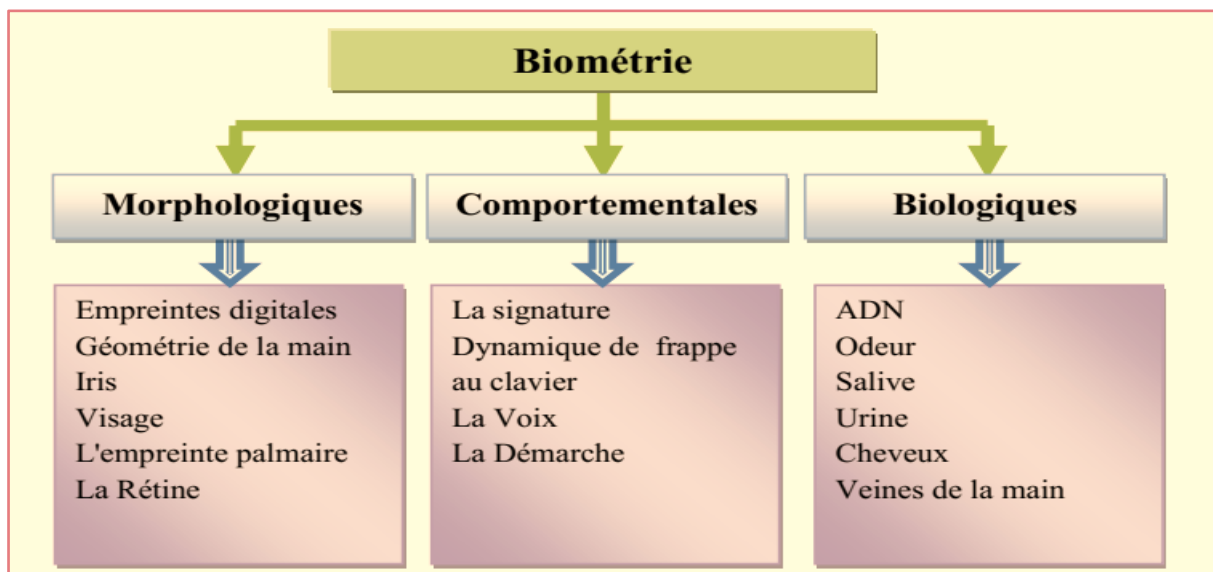


Figure I.2: Classification d'un certain nombre de modalités biométriques[1]

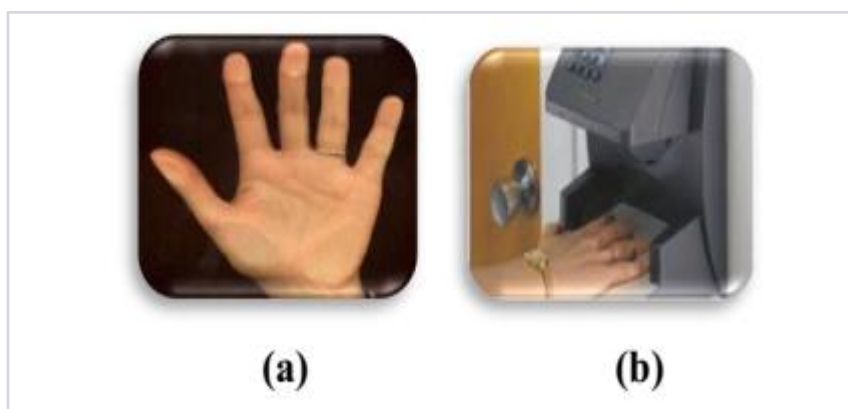
### I.3.1. Modalités morphologiques (physiologiques)

Elle est basée sur l'identification de traits physiologique particuliers qui, pour toute personne, sont uniques et permanents.

Cette catégorie regroupe l'iris de l'œil, la forme de la main, les empreintes digitales, les traits du visage, etc. [2]

#### a- La géométrie de main ;

Cette modalité consiste à analyser, la forme de la main, sa longueur, sa largeur, son hauteur, la courbure des doigts...etc. Cette technique est récente, simple, et bien acceptée par les utilisateurs qui suivent des guides des capteurs (LED infrarouge, des appareils photos numériques) pour qu'ils bien positionner leurs doigts, ce qui rend ainsi la détection / la segmentation plus aisée, cependant ce genre de système peut être trompé par de vrais jumeaux ou même par des personnes ayant des formes de la main proches.



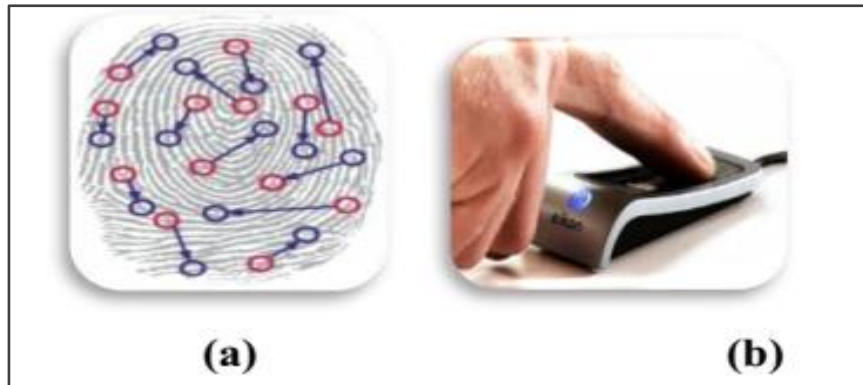
**Figure I.3** :a) Image de la géométrie de main ;b) Dispositif de reconnaissance de la géométrie de main

#### b- Empreinte digitale ;

L'empreinte digitale est la caractéristique d'un doigt, on le croit que chaque empreinte digitale est unique. Chaque personne a ses propres empreintes digitales avec l'unicité permanente, ainsi les empreintes digitales sont utilisées depuis longtemps pour l'identification et l'investigation juridique.

Une empreinte digitale se compose de beaucoup des rides et sillons. Ces rides et sillons présentent de bonnes similitudes dans chaque petite fenêtre locale [2]





**Figure I.4:** a) Image d'une empreinte digitale ;b) Dispositif de reconnaissance d'empreintes digitales.

### c- Visage ;

Les systèmes actuels de reconnaissance du visage sont composés d'un module d'acquisition d'images avec une caméra.

Il procède d'abord à une détection du visage dans l'image acquise. Ensuite, on va la traiter en utilisant des algorithmes afin d'extraire une signature du visage.

Finalement, cette signature est comparée, à l'aide d'un classificateur, avec les signatures déjà existantes dans une base de données locale, afin d'identifier l'individu [3]



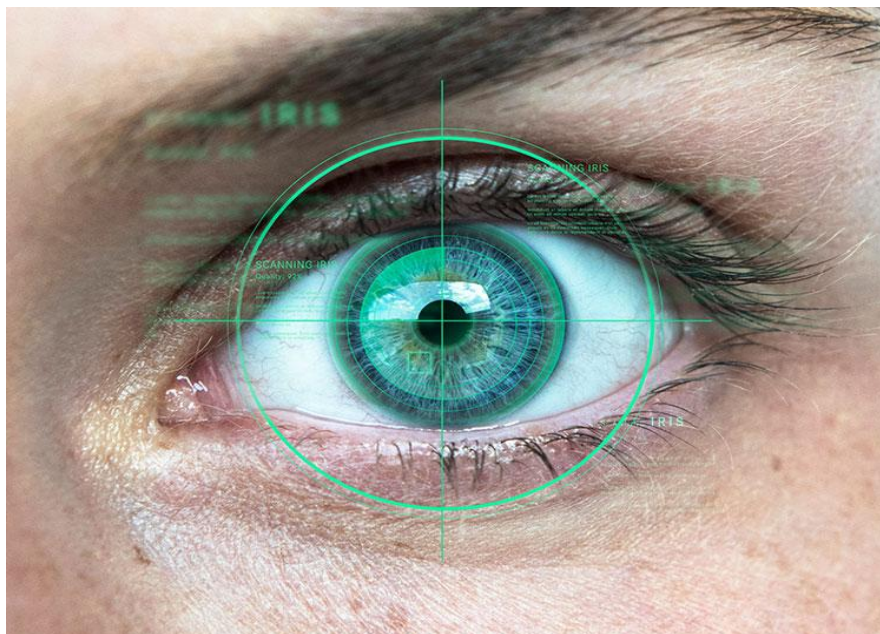
**Figure I.5 :** la reconnaissance de visage

**d- l'iris ;**

Est la membrane colorée de l'Œil, Une caméra proche des infrarouges photographie une tranche de l'iris, elle relève les caractéristiques particulières du relief, C'est une technologie fiable ; et semble être beaucoup plus précise que certains autres moyens biométriques, Ceci s'explique par le fait que notre iris comporte énormément de caractéristiques pouvant varier d'un individu à l'autre.

L'iris se compose d vaisseaux sanguins et ceux-ci sont disposés différemment d'un individu à un autre. Chaque œil est unique, il est prouvé que la probabilité de trouver deux iris identiques est inférieure à l'inverse du nombre d'humains ayant vécu sur terre. Une fois que l'image de la configuration des vaisseaux sanguins est obtenue par le système biométrique, le fonctionnement est quasi identique à celui du système analysant l'empreinte digitale. La grosseur des vaisseaux, leur positionnement et les bifurcations qui les caractérisent font partie des éléments, les minuties, qui seront étudiés par le système dans le but d'en dégager un algorithme particulier.

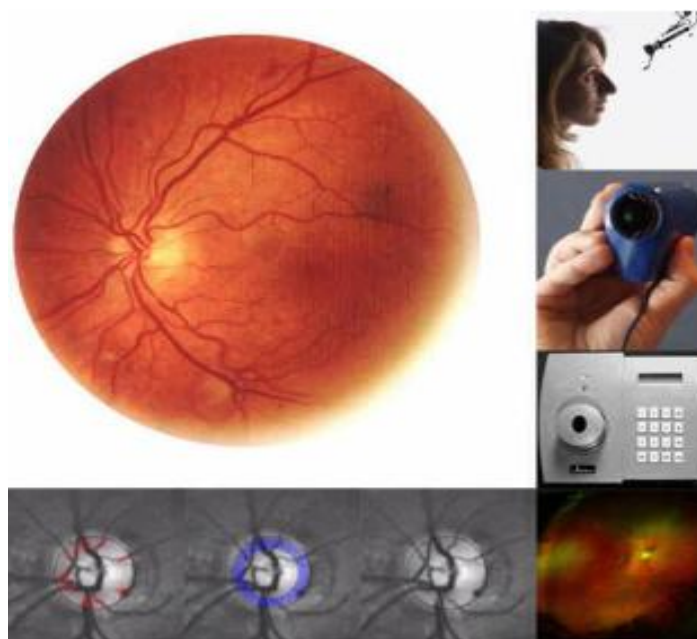
La comparaison avec le fichier référence pourra s'ensuivre. Le point faible de ce type de système utilisant l'œil à des fins d'identification ou de vérification est qu'il éprouve beaucoup de difficultés à lire l'image de l'œil d'une personne aveugle ou d'un individu ayant un problème de cataracte [4]



**Figure I.6 : image iris**

**e- La rétine :**

Cette mesure biométrique se base sur le fait que les vaisseaux sanguins d'une rétine sont différents d'une personne à une autre et stable durant la vie, Cette technologie est la plus complexe à falsifier, mais probablement à cause de son coût élevé, elle n'est pas utilisée que dans les cas où la sécurité est primordiale. L'analyse biométrique de la rétine est la technologie la plus difficile à mettre en œuvre[5]



**Figure I.7 :** Système de reconnaissance de la rétine

**I.3.2. Modalités comportementale**

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

**a- L'écriture** (la signature) :

Les systèmes de reconnaissance de l'écriture consistent à analyser les caractéristiques spécifiques d'une signature comme la vitesse, la pression sur le crayon, le mouvement, les points et les intervalles de temps où le crayon est levé. Elle se base généralement sur le fait que l'utilisateur signe avec un stylo électronique sur une palette graphique et au même temps elle examine l'ensemble de dynamique comme la vitesse, la direction, et la pression de l'écriture, le temps pendant laquelle le stylo est en contact avec le papier, le temps pris pour faire la signature et les positions où le stylo est relevé et abaissé sur le papier [1]



**Figure I.8** : Système de reconnaissance de signature

### **b - La dynamique de frappe au clavier :**

La dynamique de frappe au clavier est une caractéristique de l'individu, quelque soit la transposition de la graphologie aux moyens électroniques.

les paramètres suivants sont généralement pris en compte : [6]

- Vitesse de frappe.
- Suite des lettres.
- Mesure de temps de frappe.
- Pause entre chaque mot.
- Reconnaissance de mot(s) précis.



**Figure I.9** : Système de reconnaissance de frappe au clavier

**c- La voix (Reconnaissance vocale) :**

La reconnaissance par voix utilise les caractéristiques vocales pour identifier les personnes en utilisant des phrases mot de passe. Un téléphone ou un microphone peut être utilisé comme dispositif d'acquisition ce qui rend cette technologie relativement économique et facilement réalisable, cependant elle peut être perturbée par des facteurs extérieurs comme le bruit de fond ou la maladie ou l'état émotionnel de la personne [2]



**Figure I.10:** Image de la Reconnaissance vocale

**d- la démarche :**

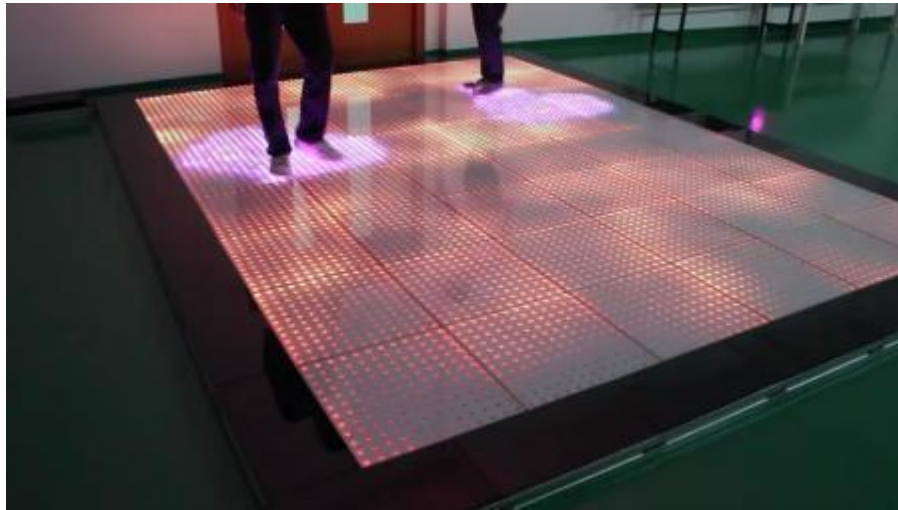
On peut aussi modéliser la démarche d'une personne à travers plusieurs techniques, mais le problème c'est qu'on peut tromper ce système facilement. La biométrie de la marche est une biométrie basée sur la marche de la personne. Ça devrait être mentionné que la marche n'est pas affectée par la vitesse de la marche de la personne.

Certains scientifiques distinguent la démarche de la reconnaissance de la démarche, soulignant que la démarche peut être considérée comme une combinaison cyclique de mouvements qui entraîne la locomotion humaine et la reconnaissance de la démarche est la reconnaissance de certain style de propriété de la marche, la pathologie, etc.

Les paramètres communs de l'analyse de la marche sont [7]:

- Paramètres cinématiques tels que le genou, les mouvements de la cheville et les angles.
- Paramètres spatiotemporels tels que la longueur et la largeur des marches, la vitesse de marche.





**Figure I.11** : Capteur de solde marche

### I.3.3. Modalités biologiques

Elle est basée sur l'identification de traits biologique particuliers.

**L'ADN :** L'analyse des empreintes génétiques est une méthode extrêmement précisée'identification, issue directement de l'évolution de la biologie moléculaire.

L'information génétique d'un individu est unique car aucun membre de l'espèce ne possède la même combinaison de gènes codés dans l'acideDésoxyribonucléique (ADN).

L'ADN est l'outil d'identification par excellence.

L'analyse des empreintes génétiques est devenue en quelquesannées l'un des outils majeurs de la criminalistique, la science del'identification des indices matériels.

L'analyse de l'ADN est courammentutilisée en criminologie pour identifier une personne à partir d'un morceau depeau d'un cheveu ou d'une goutte de sang [8]



**Figure I.12** : image d'ADN

**b-Veines de la main :**

On a longtemps considéré que le modèle des veines dans l'anatomie humaine peut être unique aux individus. En conséquence, il y a eu diverses réalisations du balayage de veines au cours des années, du balayage de main, au balayage de poignet et, plus récemment, au balayage de doigt. La plupart de ces techniques ont été utilisées sur terrain et ont pu certainement former la base d'un système biométrique viable de vérification d'identité. Le problème auquel elles font face n'est pas un problème de possibilités ou d'efficacité technique, mais plutôt un problème de réalité du marché. La prépondérance de systèmes d'empreinte digitale, de visage et d'iris, facilement disponibles à une large gamme de coûts, ne permet pas à une technique distincte de gagner la part de marché sans avantage clair et irrésistible. Même les techniques primaires, telles que la géométrie de main, ont une base qui est peu susceptible d'être réalisée par une technique plus récente de performance comparable. En conséquence, peu importe quelle nouvelle technique biométrique prenant place dans le marché, elle doit gagner le terrain et offrir des avantages clairs qui ne peuvent pas être réalisés par des méthodes contemporaines. Les diverses réalisations de balayage des veines. Bien qu'assurément intéressantes, ne peuvent lutter que peu dans ce contexte. Cependant, le temps peut s'avérer un niveau intéressant dans ces contextes et les demandes de la technique de balayage de veines peuvent s'accroître [9]



Figure I.13 : Image de système configuration des veines

#### I.4- Représentation comparative entre quelques 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 I.2** résume une comparaison des traits biométriques.

**Tableau I.2** : comparaison des traits biométriques(2)

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

## I.5 Système biométrique

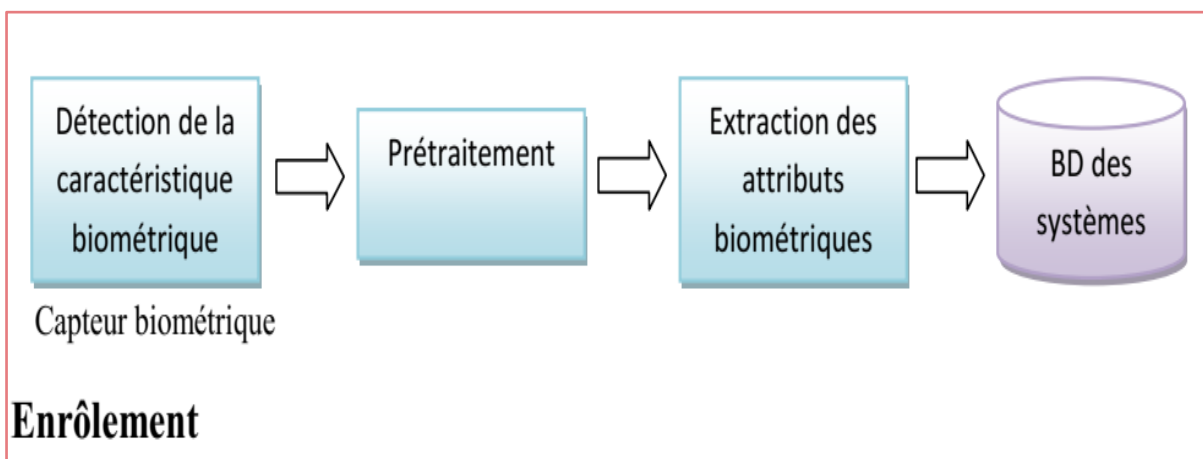


Les systèmes biométriques peuvent fournir trois modes de fonctionnement à savoir mode d'enrôlement, mode vérification et le mode identification.

### I.5.1 Modes de fonctionnement

#### Le mode d'enrôlement :

C'est une phase d'apprentissage qui a pour but de recueillir des informations biométriques sur les personnes à identifier. Plusieurs campagnes d'acquisitions de données peuvent être réalisées afin d'assurer une certaine robustesse au système de reconnaissance aux variations temporelles des données. Pendant cette phase, les caractéristiques biométriques des individus sont saisies par un capteur biométrique, puis représentées sous forme numérique et enfin stockées dans une base de données [10]



**Figure I.14** : Mode d'enrôlement d'un système biométrique

### I.5.2 Le mode vérification ou authentification

C'est la comparaison 1-à-1, entre les données biométriques capturées (model test) et les données stockées dans sa propre base (les modèles d'apprentissage). Dans un tel système, un individu qui désire être identifié réclame une identité, habituellement par l'intermédiaire d'un PIN (numéro d'identification personnelle), d'un nom d'utilisateur, d'une carte d'identité, etc.

Le système doit alors répondre à la question suivante "*Suis-je réellement la personne que suis-je entrain de proclamer?*" [11]

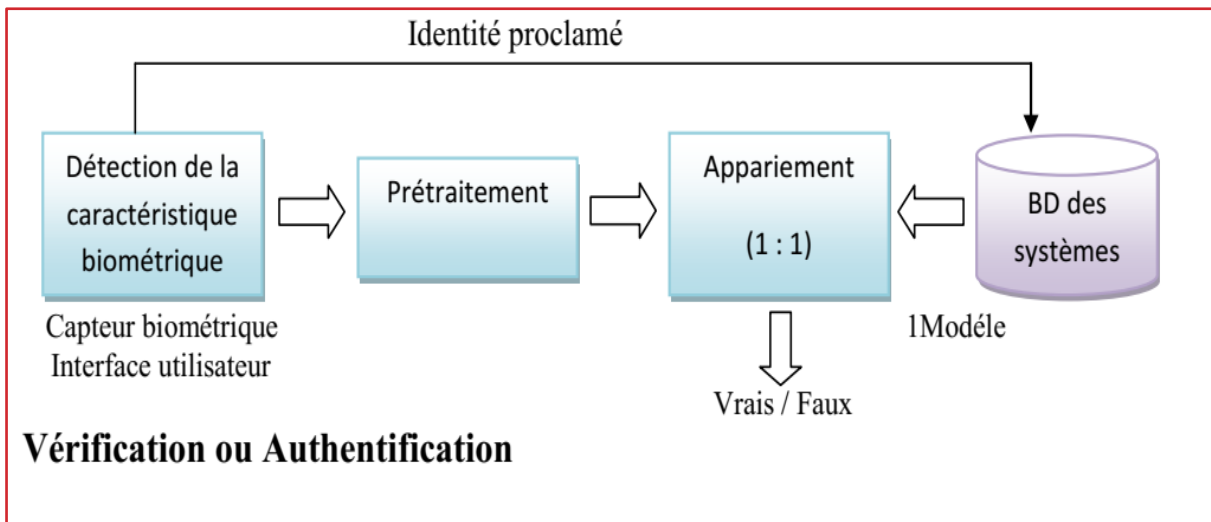


Figure I.15 : Mode de vérification d'un système biométrique. [2]

### I.5.3 Le mode identification :

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

Le système effectue un appariement (1 : N) pour identifier la personne en question comme illustré à la Figure I.16 [2]

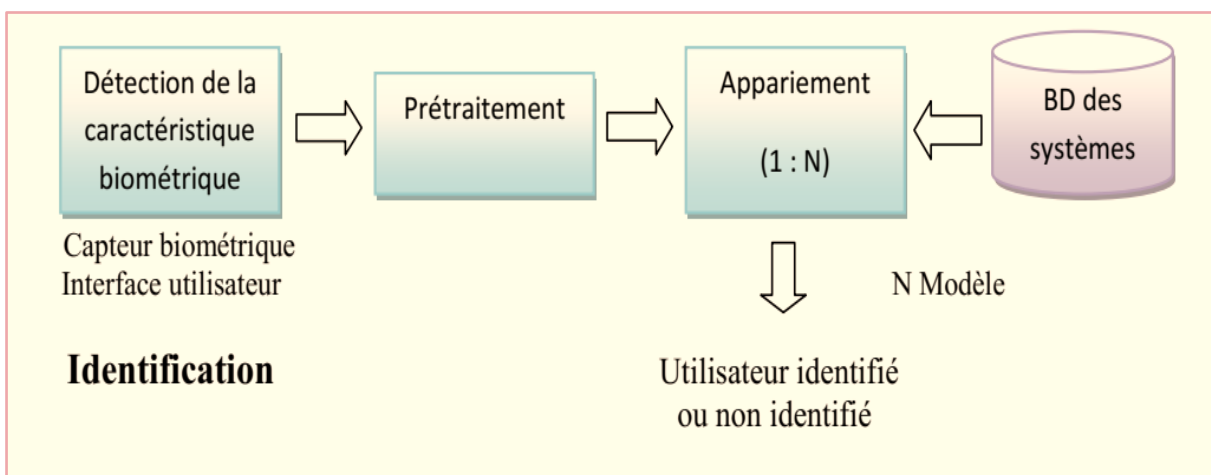


Figure I.16 : Mode d'identification d'un système biométrique

## I.6. Structure d'un système biométrique

Un système biométrique typique peut être représenté par quatre modules principaux :

### 1-Module capteur biométrique:

C'est le responsable de l'acquisition des données biométriques d'un individu (cela peut être un appareil photo, un lecteur d'empreintes digitales, une caméra de sécurité, ...etc.) [12]

### 2. Module d'extraction des caractéristiques :

Prend en entrée les données biométriques acquises par le module de capture et extrait seulement l'information pertinente afin de former une nouvelle représentation des données (modèle extrait). Idéalement, cette nouvelle représentation est censée être unique pour chaque personne et relativement invariante aux variations intra-classe. [2]

### 3-Le module de correspondance :

Compare l'ensemble des caractéristiques extraites avec le modèle enregistré dans la base de données du système et détermine le degré de similitude (ou de divergence) entre les deux.

### 4. Le module de décision :

Vérifie l'identité affirmée par un utilisateur ou détermine l'identité d'une personne basée sur le degré de similitude entre les caractéristiques extraites et le(s) modèle(s) stocké(s). [12]

## I.6 Evaluation des performances des Systèmes biométriques

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

On ne s'attend à ce qu'aucune modalité biométrique ne réponde efficacement aux exigences de toutes les applications.

Plusieurs études ont été menées afin d'évaluer les performances des systèmes biométriques [10]

Ces études sont basées sur quatre critères d'évaluation :

### I.6.1 Intrus vite :

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

### I.6.2 Fiabilité :

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

**I.6.3 Coût :**

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

**I.6.4 Effort :**

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

Un système biométrique peut faire deux types d'erreurs. Il peut rejeter un utilisateur légitime et dans ce premier cas on parle de faux rejet (false rejection). Il peut aussi accepter un imposteur et on parle dans ce second cas de fausse acceptation (false acceptante). La performance d'un système se mesure donc à son taux de faux rejet (False Rejection Rate ou FRR) et à son taux de fausse acceptation (False Acceptance Rate ou FAR). [13]

**I.6.5 Le FAR (False Acceptance Rate)**

Ce taux représente le pourcentage d'individus reconnus par le système biométrique. Le système classe alors deux caractéristiques provenant de deux personnes différentes comme appartenant à la même personne. [2]

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

**I.6.6 Le FRR (False Rejection Rate)**

La fréquence des rejets par rapport aux personnes qui doivent être correctement vérifiées. Quand un utilisateur autorisé est rejeté il ou elle doit représenter leurs caractéristiques biométriques au système [14]

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

**I.6.7 L'EER (Equal Error Rate)**

Le point d'équivalence des erreurs est le taux d'exactitude croisée EER, il est déterminé par le point d'intersection entre la courbe du taux de fausses acceptations et la courbe du taux

defaux rejets, on peut aussi définir le taux d'erreur égal (EqualError Rate ou EER) commesuit :

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

La Figure I.17 illustre l'EER à partir des courbes FAR

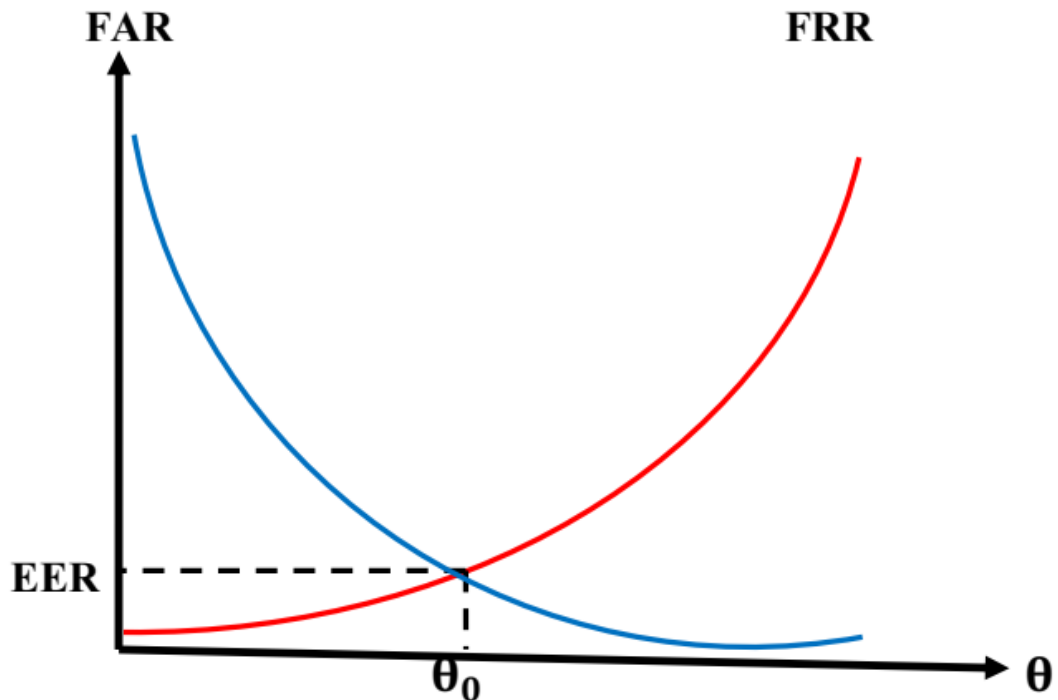


Figure I.17 : Graphe démonstratif de l'EER

$\theta_0 =$  Seuil correspondant au point d'équivalence des erreurs [2]

Les performances d'un système biométrique peuvent être présentées graphiquement à l'aide de la courbe ROC (Receiver Operating Characteristic), illustrée par à la (Figure I.18).

Cette courbe permet de représenter graphiquement la performance d'un système de vérification pour les différentes valeurs de  $\theta$ . Le taux d'erreur égal (EqualErrorRate ou EER) correspond au point FAR=FRR, c'est-à-dire graphiquement à l'intersection de la courbe ROC avec la première bissectrice.

## I.6.8 courbe ROC

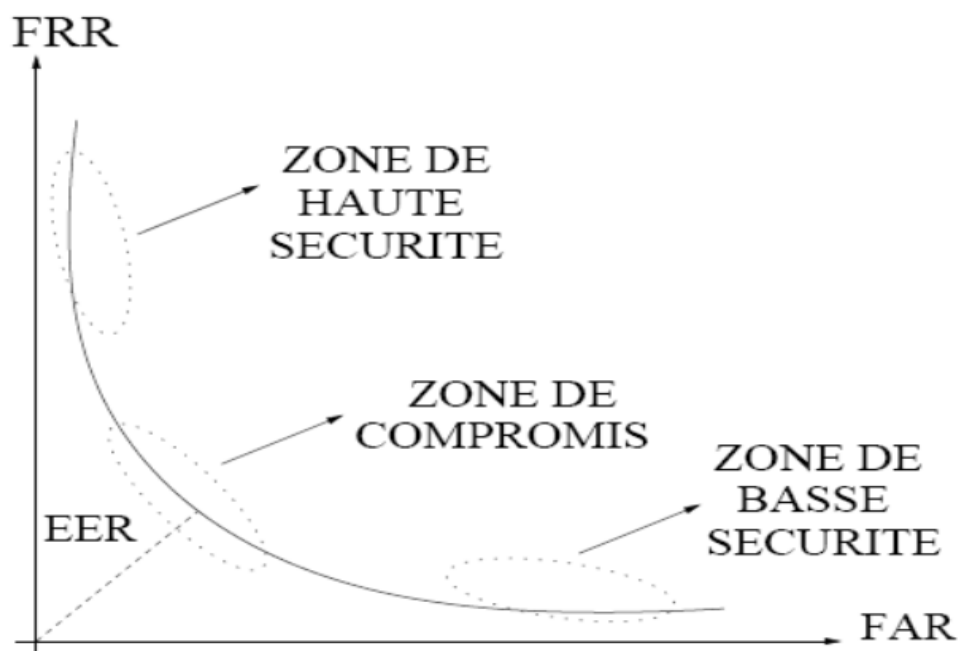


Figure I.18 : Courbe ROC

Il est fréquemment utilisé pour donner un aperçu de la performance d'un système biométrique.

Cependant, il est important de souligner que l'EER ne résume en aucun cas toutes les caractéristiques d'un système biométrique. Le seuil doit donc être ajusté en fonction de l'application ciblée : haute sécurité, basse sécurité ou compromis entre les deux. [15]

Le but fondamental de tout système biométrique opérant au niveau score, est de pouvoir séparer au maximum les distributions de score des imposteurs et des authentiques (Figure I.19).

En minimisant la zone de recouvrement entre ces deux distributions, on améliore la performance globale du système en augmentant le taux de reconnaissance [12]

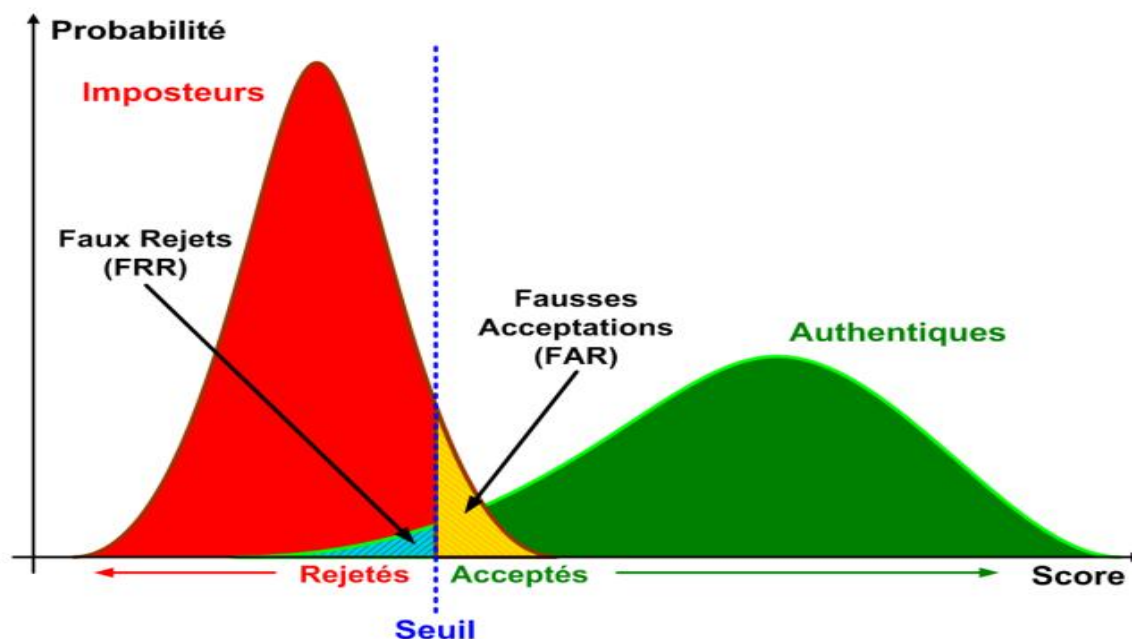


Figure I.19 : Illustration du FRR et du FAR.

## I.7 Domaine applications des systèmes biométriques :

La biométrie répond aux exigences de sécurité par les secteurs particuliers et les entreprises dans tous les pays. La sécurité biométrique couvre presque tous les domaines.

Aujourd'hui, La sécurité biométrique est utilisée dans l'accès aux réseaux et aux systèmes d'information, paiement électronique et cryptage des données. Généralement, les applications de la sécurité biométrique peuvent être classées en quatre sections principales.

[16]

### I.7.1- Service public

- Le contrôle et la sécurité des bâtiments gouvernementaux frontière.
- Contrôle les immigrants qui entrent et sortent du pays.
- les aéroports et la santé.

### I.7.2- Pouvoir judiciaire

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

### **I.7.3-Secteurs des banques**

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

### **I.7.4-Accès physique et logique**

Ceci se rapporte au contrôle d'accès physique comme la sécurisation des lieux (bâtiment ou une pièce) ou le contrôle d'accès logique comme la sécurisation d'une session informatique (ordinateur ou base de données) [16]

## **I.8 Conclusion**

Dans ce chapitre, nous avons introduit le concept de des systèmes biométriques, leur architecture et leurs différentes applications. Nous avons aussi constaté que les performances des systèmes biométriques dépendent de plusieurs facteurs et qu'elles varient d'un système à un autre.

Parmi les critères d'évaluation de la qualité du système biométrique, nous avons présenté les taux des erreurs (FAR, FRR et ERR) ainsi que les courbes ROC selon qu'on est en mode identification ou vérification.



**Chapitre II :**  
***Systeme***  
***d'identification des***  
***personnes à***  
***l'empreinte palmaire***

### II.1 Introduction

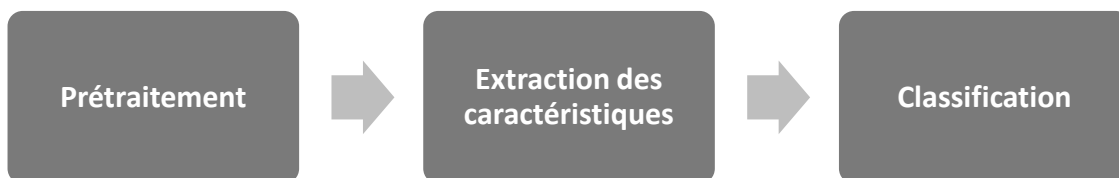
Le système de reconnaissance des empreintes palmaires, comme tous les systèmes biométriques est constitué de trois étapes primordiales : Le prétraitement, l'extraction des caractéristiques et la classification.

Dans l'étape de prétraitement, les images sont traitées pour faciliter l'extraction des caractéristiques. Ce processus sert à éviter les informations inutiles.

Le deuxième module sert à traiter l'image afin d'extraire uniquement les caractéristiques biométriques, sous forme d'un vecteur ou Template, qui ensuite peuvent être utilisées pour reconnaître les personnes. Ces caractéristiques sont uniques à chaque personne et stable. La reconnaissance est faite par la comparaison (classification) du vecteur de caractéristique avec une base de données.

### II.2 Le principe des méthodes d'identification biométrique

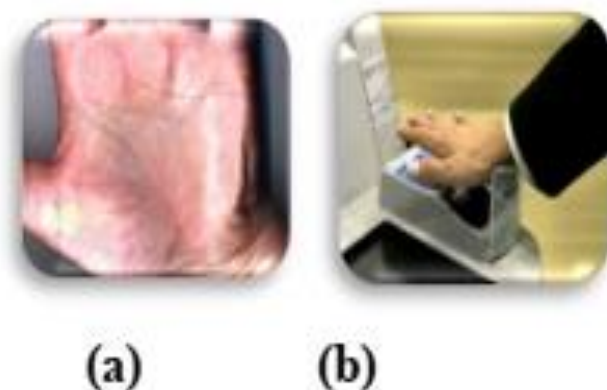
En général, Les méthodes d'identification biométrique des personnes sont en plusieurs étapes, comme le montre la figure suivante ;



**Figure II.1:** Le principe des méthodes d'identification biométrique

### II.3 Empreinte palmaire

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



**Figure II.2:**a) Image d'une empreinte palmaire ; b) Dispositif de reconnaissance de l'empreinte palmaire.

### II.3.1 Avantages de l'empreinte palmaire [3]

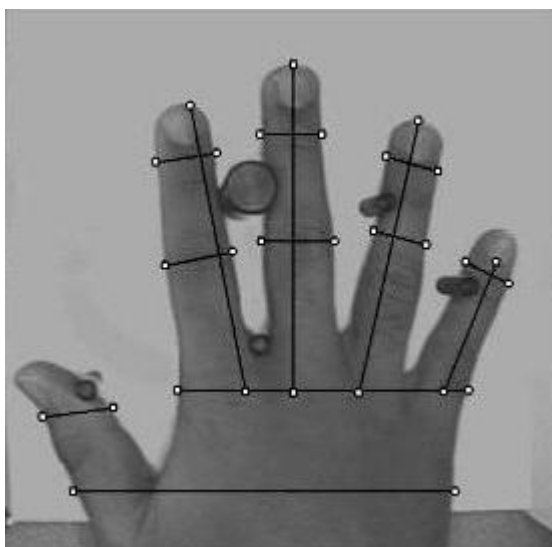
- Les empreintes palmaires contiennent plus d'information que les empreintes digitales
- Elles sont plus discriminantes.
- Les sources de capture d'empreintes palmaires sont beaucoup moins chères que celles des empreintes digitales.
- Les empreintes palmaires contiennent des caractéristiques distinctives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

### II.3.2 Les caractéristiques biométriques d'une empreinte palmaire

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

#### a) Les caractéristiques géométriques

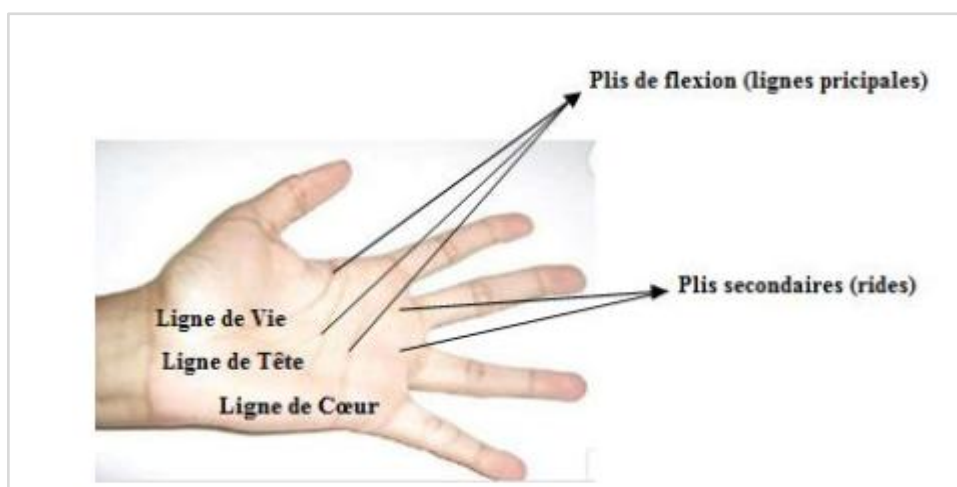
Comme toute image, l'empreinte palmaire présente des caractéristiques géométriques telles que : la longueur, la largeur, et la surface. Ces caractéristiques ne sont pas distinctives mais peuvent tout de même être utiles pour une première vérification.



**Figure II.3 :** Les caractéristiques géométriques de main

### b) Les lignes principales (Plis de flexion)

L'empreinte palmaire est caractérisée par trois plis de flexion, dites lignes principales : la ligne de tête, la ligne de vie et celle du cœur. La Figure II.4 montre les différents plis de la paume.

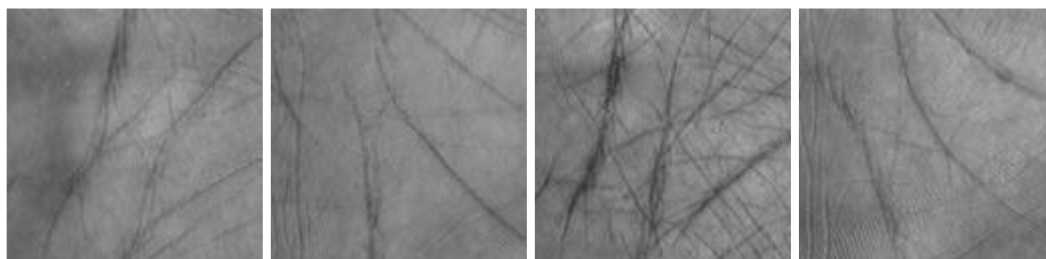


**Figure II.4:** La paume de main et ses plis

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

### c) Les rides (Plis secondaires)

L'empreinte palmaire contient de nombreux autres plis qui diffèrent de ceux de flexion du fait qu'ils sont plus minces et plus irréguliers. Certains d'entre eux sont congénitaux, d'autres sont dus aux activités musculaires. Les lignes principales et les rides peuvent être observées facilement sur les images capturées à basse résolution (figure II.5). Comme les lignes principales seules ne fournissent pas une information distinctive suffisante, les rides jouent un rôle important dans la reconnaissance palmaire. Combinées aux lignes principales, elles fournissent une information distinctive pour la reconnaissance.



**Figure II.5:** Empreintes différentes avec des lignes principales similaires

### d) Les points de référence (Datum points)

Les points représentant les deux extrémités de la paume de la main sont appelés points de références. Ce sont les points a et b dans la **Figure II.6**



**Figure II.6:** Points de référence de l'empreinte palmaire (a et b)

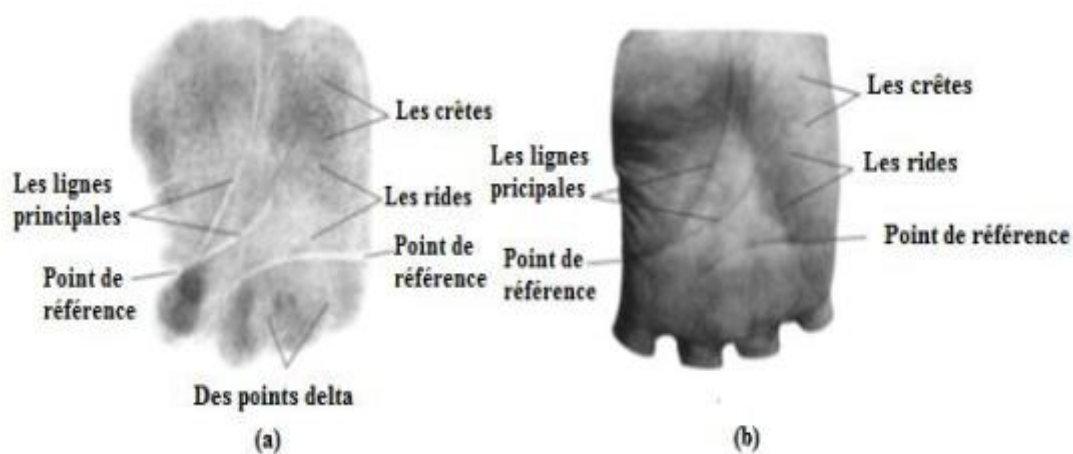
Ils servent de points de repère lors de l'alignement et l'extraction des caractéristiques de l'empreinte palmaire. La taille de cette dernière peut être aussi estimée grâce à ces deux points

### e) Les crêtes papillaires

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

- Les minuties
- Les points singuliers

Comme le montre la **Figure II.7**, selon la résolution utilisée dans l'acquisition de l'empreinte, une ou plusieurs de ces caractéristiques peuvent être observées et par conséquent exploitées dans la reconnaissance palmaire des individus. Cela a permis de classer les approches de reconnaissance en deux grandes catégories principales : approches haute résolution et approches basse résolution.



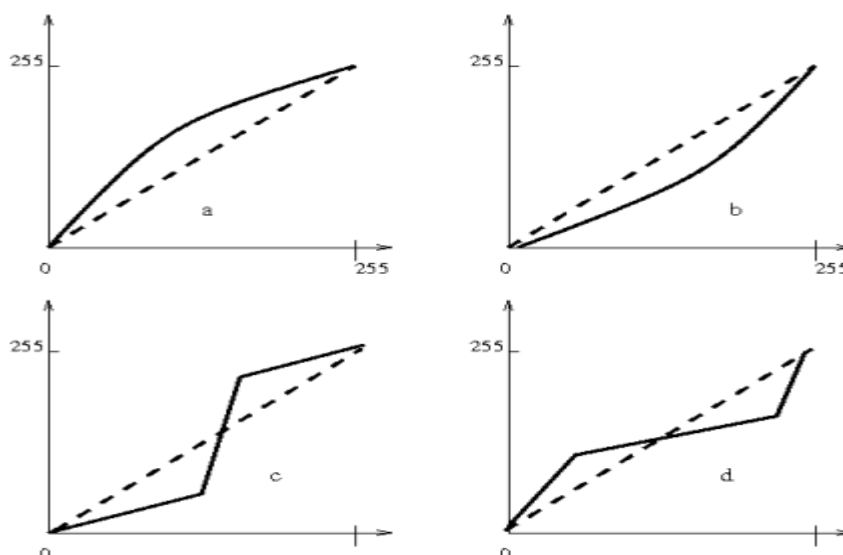
**Figure II.7:** Caractéristiques d'une empreinte palmaire : a) Image basse résolution, b) Image haute résolution.

## II.4 des méthodes de prétraitement

### II.4.1 - Rehaussement des niveaux de gris

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

Soient  $h_{max}$  et  $h_{min}$  les niveaux de gris maximum et minimum de l'image I. Le rehaussement des niveaux de gris consiste à appliquer aux niveaux de gris de l'image I une fonction croissante  $f$  telle que  $f(h_{min}) = h_{min}$  et  $f(h_{max}) = h_{max}$ . Les courbes de la **figure II.8** décrivent ce type de transformation.[17]



**Figure II.8** :(- Rehaussement des niveaux de gris)

- a. Courbe représentant un rehaussement des bas niveaux de gris (zones foncées)
- b. Courbe représentant un rehaussement des hauts niveaux de gris (zones claires)
- c. Courbe représentant un rehaussement des niveaux de gris moyens
- d. Courbe représentant un rehaussement des niveaux de gris extrêmes

#### **II.4.2 -Égalisation d'histogramme**

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

Cette transformation se définit à l'aide de l'histogramme cumulé de l'image. L'histogramme cumulé de l'image I est un vecteur de dimension 256. Chaque élément  $hc(i)$  représente le nombre de pixels de l'image dont le niveau de gris est inférieur ou égal à  $i$ . À un facteur de normalisation près, l'histogramme cumulé représente la fonction de répartition des niveaux de gris.

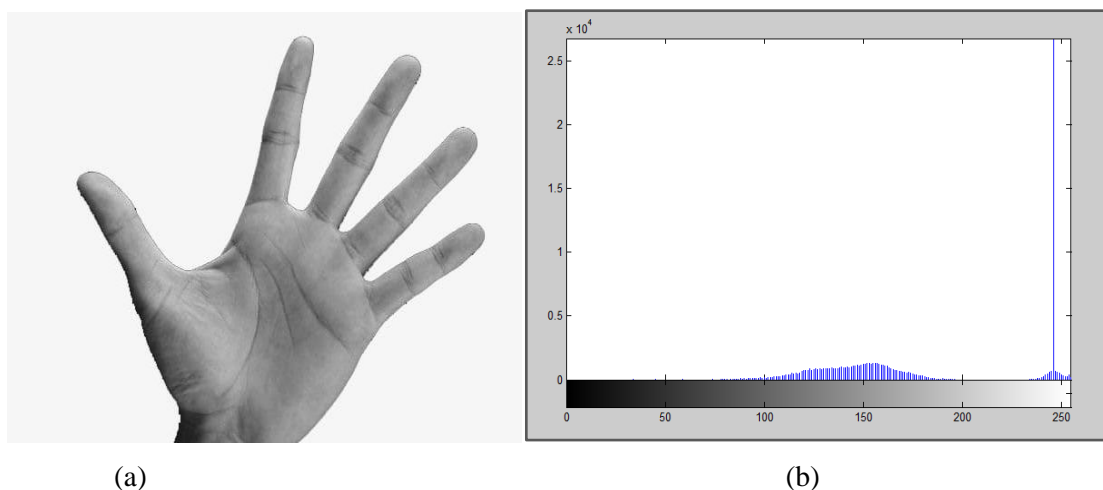
$$hc(i) = \sum_{j=0}^i h(j) \quad (\text{II.1})$$

On peut définir la transformation d'égalisation d'histogramme de la manière suivante. Soit  $G$  le niveau de gris d'un pixel de départ, le niveau de gris de l'image d'arrivée sera :

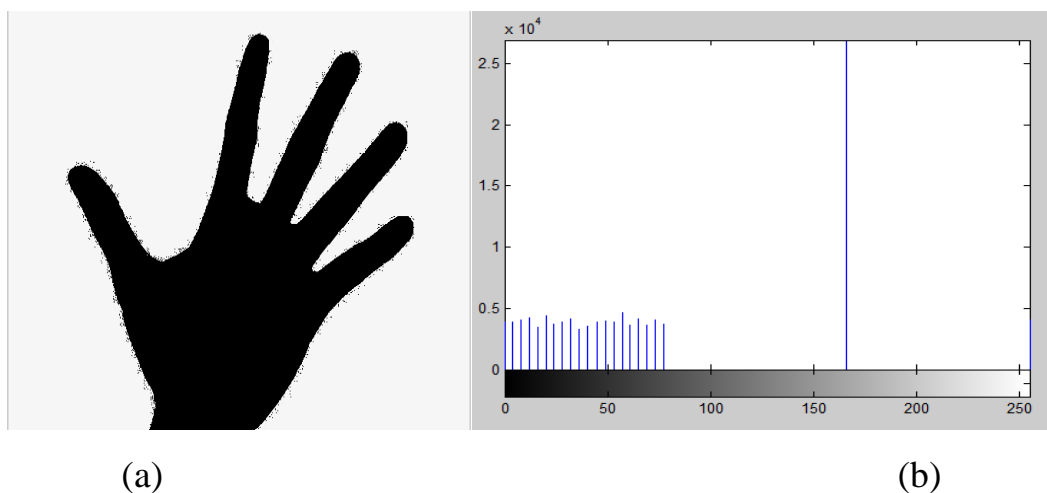
$$G' = \frac{255}{\text{Nombre de pixels}} hc(G) \quad (\text{II.2})$$

L'outil Image : Calque  $\Rightarrow$  Couleurs  $\Rightarrow$  Auto  $\Rightarrow$  Égaliser permet de réaliser cette opération.

Il ne s'applique qu'à une image en niveaux de gris, telle que celle de la figure II.9(a), dont l'histogramme apparaît figure II.9(b). Le résultat apparaît figure II.10 (a), et l'histogramme transformé figure II.10 (b). [17]



**Figure II.9 :** (a) Image de départ, (b) Histogramme de l'image (a)



**(b) Figure II.10 :** (a) image égalisation de l'histogramme, (b) Histogramme après égalisation



### II.3.3 débruitage par Filtre gaussien

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

$$g(x, y) = \frac{1}{2\pi\sigma} e^{-\frac{(x^2+y^2)}{2\sigma^2}} \quad (\text{II.3})$$

Le paramètre  $\sigma$  permet de régler facilement le degré de filtrage. Comparé au filtre moyenneur, ce filtre accorde une grande importance aux pixels proches du pixel central, et diminue cette importance au fur et à mesure que l'on s'éloigne de lui. Le masque suivant permet une pondération gaussienne : [18]

$$\frac{1}{16} * \begin{pmatrix} 1 & 2 & 1 \\ 2 & 4 & 2 \\ 1 & 2 & 1 \end{pmatrix} \quad (\text{II.4})$$



**Figure II.11 :** (a) Flou gaussien de rayon 2, (b) Flou gaussien de rayon 3

## II.5 Méthodes d'Extraction des Caractéristiques

Cette étape représente le cœur du système de reconnaissance, on extrait de l'image les informations qui seront sauvegardées en mémoire pour être utilisées plus tard dans la phase de décision.

### II.5.1 Extraction basé sur la texture

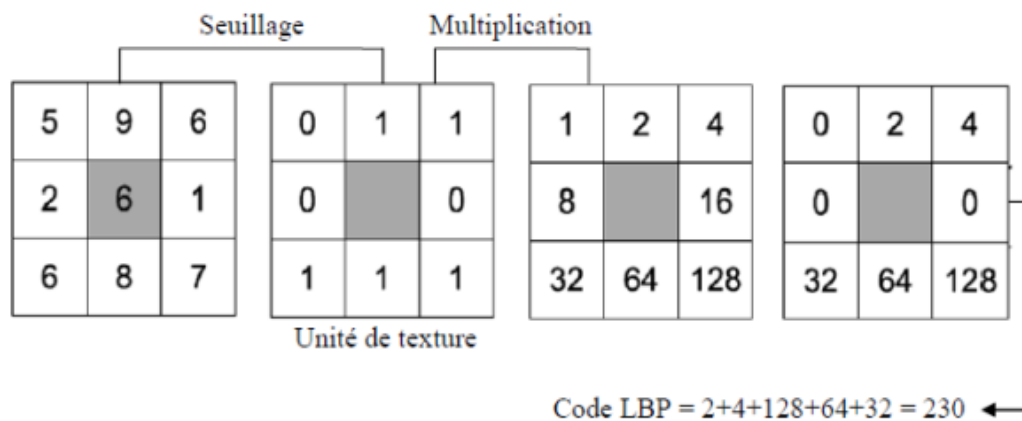
**a)-Méthode du Motif Binaire Local**

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

Ces valeurs sont calculées en comparant le niveau de gris du pixel central P aux valeurs des niveaux de gris des pixels voisins. [3]

Le concept du LBP est simple, il propose d'assigner un code binaire à un pixel en fonction de son voisinage. Ce code décrivant la texture locale d'une région est calculé par seuillage d'un voisinage avec le niveau de gris du pixel central. Afin de générer un motif binaire, tous les voisins prendront alors une valeur "1" si leur valeur est supérieure ou égale au pixel courant et "0" autrement (**Figure II.12**). Les pixels de ce motif binaire sont alors multipliés par des poids et sommés afin d'obtenir un code LBP du pixel courant.

On obtient donc pour toute l'image, des pixels dont l'intensité se situe entre 0 et 255 comme dans une image à 8 bits ordinaire. Plutôt que de décrire l'image par la séquence des motifs LBP, on peut choisir comme descripteur de texture un histogramme de dimension 255.[3]



**Figure II.12:** Construction d'un motif binaire et calcul du code LBP.

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

$$LBP(X_c, Y_c) = \sum_{n=0}^{p-1} U(g_i - g_c) * 2^n \quad (II.5)$$

Où  $x_c$  et  $y_c$  les coordonnées du pixel central,  $u()$  est la fonction signe et où  $g_i$  et  $g_c$  sont respectivement les niveaux de gris d'un pixel voisin et du pixel central.(3)

$$U(x) = \begin{cases} 1 & \text{si } x \geq 0 \\ 0 & \text{autrement} \end{cases} \quad (II.6)$$

**b) Descripteur de base LPQ (Local phase quantization) :**

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

$$F_u(x) = \sum_{m \in N_x} h(m-x) f(m) e^{-j2\pi u^T m} = E_u^T f_x \quad (\text{II.7}) \quad \text{Où } E_u, \text{ de taille } = 1$$

$\times M^2$ , est un vecteur de base de 2DWFT avec la fréquence  $u$ , et  $f_x$ , taille =  $M^2 \times N$ , est un

vecteur contenant les valeurs des pixels d'image dans  $N_x$  à chaque position  $x$ . La

fonction fenêtre,  $h(x)$  est une fonction rectangulaire.

La transformation est calculée à quatre valeurs de la fréquence,  $u = [u_0, u_1, u_2, u_3]$  où

$u_0 = [a, 0]^T$ ,  $u_1 = [0, a]^T$ ,  $u_2 = [a, a]^T$  et  $u_3 = [a, -a]^T$ . La valeur  $a$  est la plus haute fréquence

scalaire pour laquelle  $H_{ui} > 0$ . Ainsi, seuls quatre fonctions complexes comme un banc de

filtres sont nécessaires pour produire huit images résultantes, composées de 4 images de

la partie réelle et 4 images de la partie imaginaire de la transformée. Chaque pixel de l'image

complexe résultant peut être codé en une valeur binaire représentée dans l'équation (II.4) en

appliquant (the quadrant bit coding). [19]

$$B_{u_i}^{Re}(x) = \begin{cases} 1 & \text{si } F_{u_i}^{Re}(x) > 0 \\ 0 & \text{si } F_{u_i}^{Re}(x) \leq 0 \end{cases} \quad B_{u_i}^{Im}(x) = \begin{cases} 1 & \text{si } F_{u_i}^{Im}(x) > 0 \\ 0 & \text{si } F_{u_i}^{Im}(x) \leq 0 \end{cases} \quad (\text{II.8})$$

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

En fait, il fournit également la quantification de la fonction de phase de *Fourier*.

En général, LPQ est une chaîne binaire, présentée dans l'expression (II.5), obtenue pour

chaque pixel par la concaténation des codes quadrant bits réelles et imaginaires des

huit coefficients de *Fourier* de  $u_i$

$$LPQ(x) = [B_{u_0}^{Re}(x), B_{u_0}^{Im}(x), \dots, B_{u_3}^{Re}(x), B_{u_3}^{Im}(x)] \quad (\text{II.9})$$

La chaîne binaire est convertie en nombre décimal par l'expression (II.6) pour produire une étiquette de LPQ. La figure II.3 résume l'ensemble de ces étapes.

$$LPQ(x) = B_{u_0}^{Re}(x) + B_{u_0}^{Im}(x) \times 2^1 + \dots + B_{u_3}^{Re}(x) \times 2^{k-1} + B_{u_3}^{Im}(x) \times 2^k \quad (\text{II.10})$$

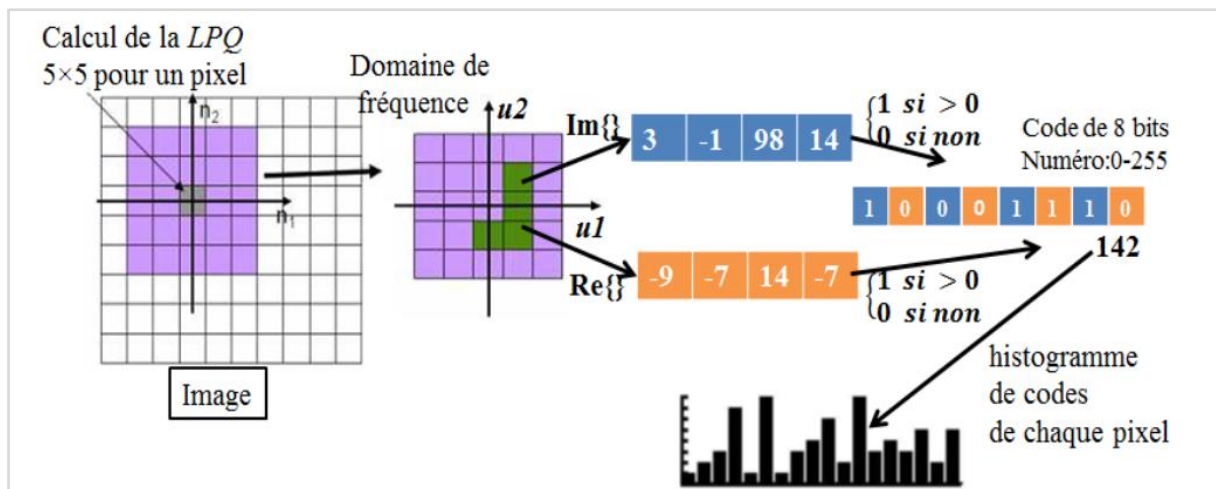


Figure II.13 : Organigramme de l'ensemble des étapes nécessaires à la construction du descripteur LPQ

## II.5.2 Extraction basé sur le filtrage

### a)-Filtre de Gabor

Pour les applications nécessitant une analyse par orientations, les fonctions de Gabor qui produisent une décomposition en ondelettes est très utilisée. De nombreuses applications d'images font appel à l'utilisation de ces types de fonctions, comme par exemple l'analyse de textures ou d'objets par attributs fréquentiels. En effet, les lignes de l'empreinte sont caractérisées par leur fréquence locale et leur orientation. En utilisant des filtres de Log Gabor, bien choisis, il est possible d'en extraire les caractéristiques biométriques. Cependant, lorsque ceux-ci sont correctement paramétrés, ils permettent de préserver les lignes et fournissent des informations sur l'orientation locale de la texture. Dans le domaine fréquentiel, la réponse ( $f_{Gb}$ ) de filtre log-Gabor 1D se définit comme [20] :

$$f_{Gb} = \exp \left[ \frac{-(\log(\frac{f}{f_0}))^2}{2(\log(\frac{\sigma}{f_0}))^2} \right] \quad (\text{II.11})$$

Où  $f_0$  est la fréquence centrale et  $\sigma$  dénote la variance.

Pour l'application du filtre de Log-Gabor, il faut un choix empirique de paramètres de filtre ( $f_0$  et  $\sigma$ ). Ces paramètres empiriques sont très difficiles à déterminer et c'est l'un des inconvénients des approches basées sur ce filtre [20].

### II.6. Classification

Cette étape consiste à modéliser les paramètres extraits d'une modalité d'un individu en se basant sur leurs caractéristiques communes.

Un modèle est un ensemble d'informations utiles, discriminantes et non redondantes qui caractérise un ou plusieurs individus ayant des similarités. Ces derniers seront regroupés dans la même classe, et ces classes varient selon le type de décision [12].

#### II.6.1 Machine à vecteurs de support (SVM)

Une machine à vecteurs de support ou Support Vector Machine (SVM) est une technique de discrimination. C'est une méthode d'apprentissage supervisé utilisée pour la classification et la régression. Elle consiste à séparer deux ou plusieurs ensembles de points par un hyper plan. Selon les cas et la configuration des points [21].

#### II.6.2 Principe de SVM

Les machines à supports vecteurs ou SVM sont une technique de classification supervisées introduite par Vladimir Vapnik dans les années 1995. L'idée originale des SVMs est basée sur l'utilisation de fonctions noyau kernel, qui permettent une séparation optimale des points du plan en différentes catégories. La méthode fait appel à un ensemble de données d'apprentissage, qui permet d'établir un hyper plan séparant au mieux les points [1].

#### II.6.3 Concept des SVM

La vocation originale des SVM fut la séparation linéaire d'objets appartenant à deux classes différentes par un hyperplan optimal [21][22].

Soit  $\{x_i\}_{i=1}^{i=m} \in \mathbb{R}^k$  l'ensemble d'apprentissage composé d'objets caractérisés par un vecteur de  $k$  composantes chacun, appartenant à deux classes différentes : Une classe positive libellée  $+1$  et une classe négative libellée  $-1$ .

Soit également  $y_i = \{1, -1\}$  la variable représentant les étiquettes des deux classes. Le but des SVM est de déterminer la frontière linéaire définie par l'équation  $wx + b$  entre les objets positifs et les objets négatifs Figure II.14, où  $w$  représente le vecteur normal à ce séparateur linéaire, et  $b$  le biais. Déterminer un hyper plan revient à définir le couple de valeurs  $(w, b)$  qui le caractérise. Dans la mesure où plusieurs solutions sont possibles, quel sera donc le critère qui définira la séparation optimale?

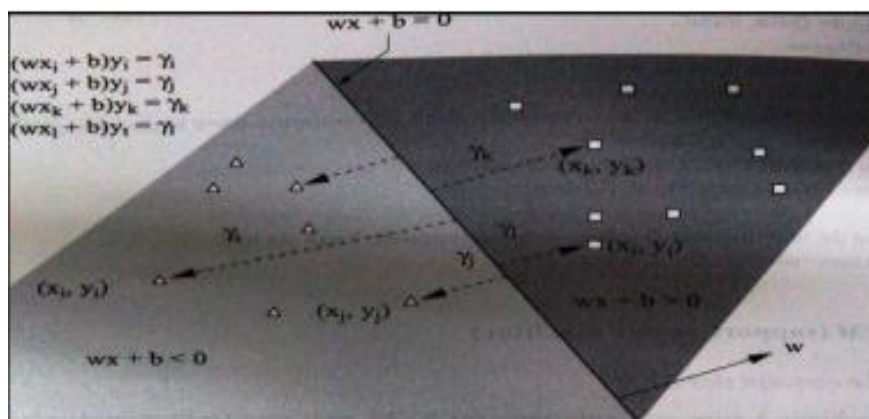


Figure II.14: Séparation linéaire des objets carrés et triangles par un hyperplan

La détermination de l'étiquette de l'exemple  $x$  est faite de la façon suivante :

$l = \text{sign}(y(x))$ . Cette fonction est faite de telle façon à effectuer une séparation linéaire des données d'apprentissages en maximisant la marge.

#### II.6.4 Séparation optimale

Dans un plan à deux dimensions dans lequel sont répartis deux groupes de points associés à deux classes : les points (+) pour  $y > 0$  et les points (-) pour  $y < 0$ , on peut trouver un séparateur linéaire évident, qui est l'axe des abscisses et qui sépare parfaitement les points.

Le problème est dit *linéairement séparable*. Pour des problèmes plus compliqués, la caractérisation d'un séparateur linéaire peut être très compliquée et tout à fait non optimale [23].

#### II.5.5 Multi-classes

A l'origine, les SVM ont été conçus essentiellement pour les problèmes à 2 classes, cependant plusieurs approches permettant d'étendre cet algorithme aux cas à N classes ont été proposées. La généralisation dans le cas multi-classes peut se faire de trois façons différentes. Les deux premières méthodes sont basées sur une multiplication des classifieurs bi-classes tandis que la dernière propose une résolution globale. [22]

#### ✚ Un-contre-tous

L'approche la plus naturelle est d'utiliser cette méthode de discrimination binaire et d'apprendre N fonctions de décision  $\{f_m\}_{m=1 \dots N}$  permettant de faire la discrimination entre chaque classe de toutes les autres (chaque classe est opposée à toutes les autres). Il faut donc

poser N problèmes binaires. L'affectation d'un nouveau point  $x$  à une classe  $C_i$  se fait par la relation

$$i = \operatorname{argmax}_{m=1..N} F_m(x) \quad (\text{II.12})$$

### ✚ Un-contre-un

La deuxième méthode est une méthode dite de *un contre un*. Au lieu d'apprendre N fonctions de décisions, ici chaque classe est discriminée d'une autre. Ainsi, N (N-1)/2 fonctions de décisions sont apprises et chacune d'entre elle effectue un vote pour l'affectation d'un nouveau point  $x$ . La classe de ce point  $x$  devient ensuite la classe majoritaire après le vote.

### ✚ Méthode globale

La dernière méthode est une approche étendant la notion de marge aux cas multi-classes. Le problème fait intervenir N fonctions de décision et il est très gourmand en temps de calcul et en espace mémoire ce qui fait qu'il reste peu utilisé dans les cas réels.

### **II.7 Conclusion**

Dans ce chapitre nous avons étudié le principe de base d'un système de reconnaissance des empreintes palmaires. Ce système comprend trois modules.

Dans le premier module, l'image est soumise à un traitement initial lors de l'entrée dans le canal du système biométrique afin de l'améliorer et d'éliminer les interférences. Il y a plusieurs types d'opérations, par exemple gestion des niveaux de gris, filtrage d'image.

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.

La classification des données : dernière étape fait classer les caractéristiques semblables d'un ou plusieurs individus à la même classe, cette étape est appliquée par des algorithmes comme SVM.



***Chapitre III :***

***Simulation et***

***résultats***

### III.1 Introduction

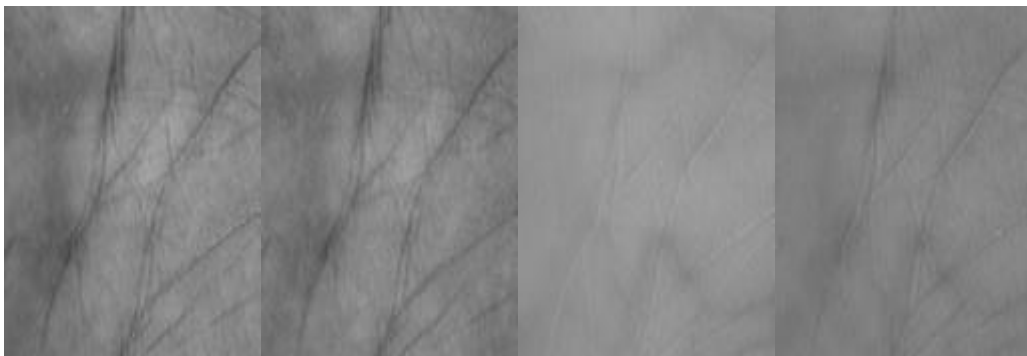
L'étude expérimentale de cette étude est basée sur la reconnaissance de personnes par leurs empreintes palmaires en utilisant les méthodes décrites dans le chapitre précédent. Elle est réalisée sur la base de données de Poly-Multi-spectrale (multi spectral palmprint).

Afin d'évaluer l'efficacité des méthodes étudiées et les performances de notre système biométrique proposé, et vu l'importance affectée à la modalité de l'empreinte palmaire dans les dernières années, nous allons présenter brièvement les caractéristiques de l'empreinte palmaire.

### III.2 Base de données de l'empreinte palmaire multi-spectrale (PolyU - MSP)

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

Le système collecte quatre images depuis quatre bandes (Rouge, Vert, Blue et NIR)



**Figure III.1** : Quelques images de la base de données PolyU-MSP.

### III.3 Séparation des bases de données

Notre base de données est divisée en deux parties: une base pour effectuer l'apprentissage et l'autre pour tester les techniques et déterminer leurs performances. Il n'y a pas de règles pour déterminer ce partage de manière quantitative. Dans les séries de test que nous avons effectuées, la base de données a été scindée de la façon suivante :

#### III.3.1 Images d'apprentissages ;

Les six premières images de chaque personne servent pour la phase d'apprentissage.

#### III.3.2 Images de Tests ;

Les six dernières images par personne restantes de chaque individu nous ont servi pour la réalisation de différents tests.

### III.4 Environnement du travail

Dans cette section, nous allons fournir l'environnement de l'équipement et les caractéristiques et le logiciel adopté dans l'application.

#### III.4.1 Environnement matériel

Afin d'accomplir notre travail nous avons fourni l'équipement suivant avec les caractéristiques suivantes:

- ✓ Un ordinateur : **DELL** avec les caractéristiques suivantes :
- ✓ Processeur : Intel® core(TM) **i3-3217U@180GHZ**
- ✓ RAM: **4.00 Go de RAM.**
- ✓ Disque Dur: **500 Go.**
- ✓ OS: Microsoft **Windows 8.1** 64bits.

#### III.4.2 Outils de développement

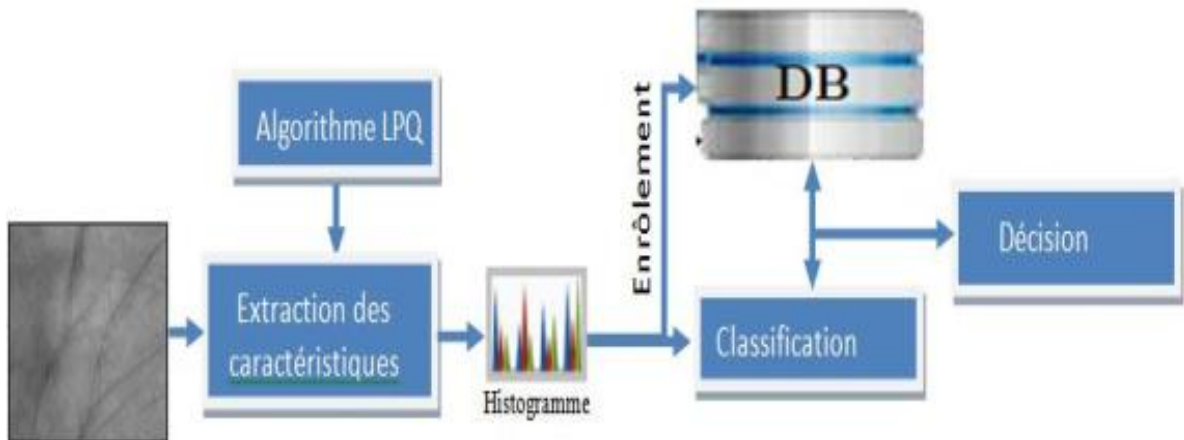
Nous avons eu recours lors de l'élaboration de notre système au logiciel Matlab R2010b(7.11.0) que nous présenterons ci-dessous.

Matlab est un langage informatique technique à haut niveau et environnement interactif pour le développement d'algorithmes; il est utilisé à des fins de calcul numérique.

Matlab permet de manipuler des matrices, d'afficher des courbes et des données, de mettre en œuvre des algorithmes, de créer des interfaces utilisateurs, et peut s'interfacer avec d'autres langages comme le C, C++, Java, et Fortran. Il dispose de plusieurs boîtes à outils en particulier celle du traitement d'images.

### III.5. Architecture globale du système :

Le schéma du principe d'un système d'identification est donné par la **Figure III.2**:



**Figure III.2** : Architecture globale de notre système.

Notre système est constitué des étapes suivantes :

- **Prétraitement** : la base de données utilisée dans notre travail est déjà traitée.
- **Extraction** : l'extraction des caractéristiques.
- **Classification** : comparer les caractéristiques des images de test par les vecteurs de caractéristiques stockés dans la base de données d'apprentissage.

#### III.5.1 Prétraitement :

La base de données utilisée dans notre test, la base multi-spectrale (PolyU -MSP), est une base qui a subi déjà des prétraitements, donc ne nécessite aucune prétraitement supplémentaire. La figure III.3 donne des exemples de cette base.

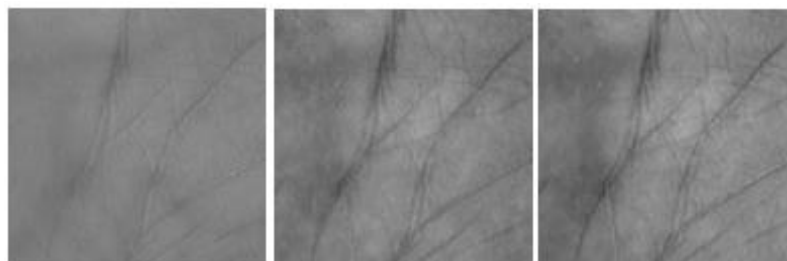


Image Rouge (a)

image Vert (b)

image Bleu (c)

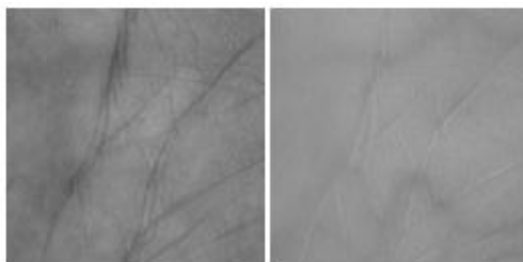


Image RGB (d) image Infrarouge (e)

**Figure III.3** :Exemple d'images de la base de données de test.

### III.5.2 Extraction de caractéristiques :

Dans notre application nous avons utilisé l'extraction des caractéristiques par l'algorithme LPQ.

La figure III.4 suivante représente l'extraction des caractéristiques par LPQ des différents types d'images de test de notre base.

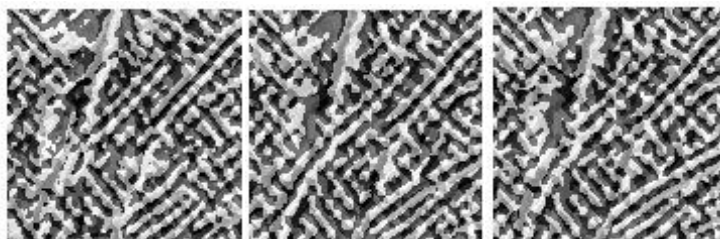


Image LPQ Rouge (a) image LPQ Vert (b) image LPQ Bleu (c)

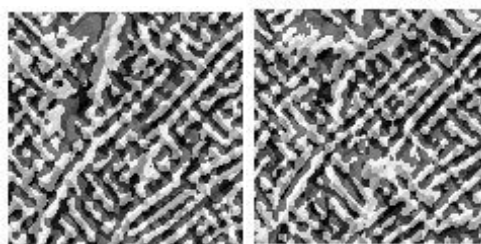


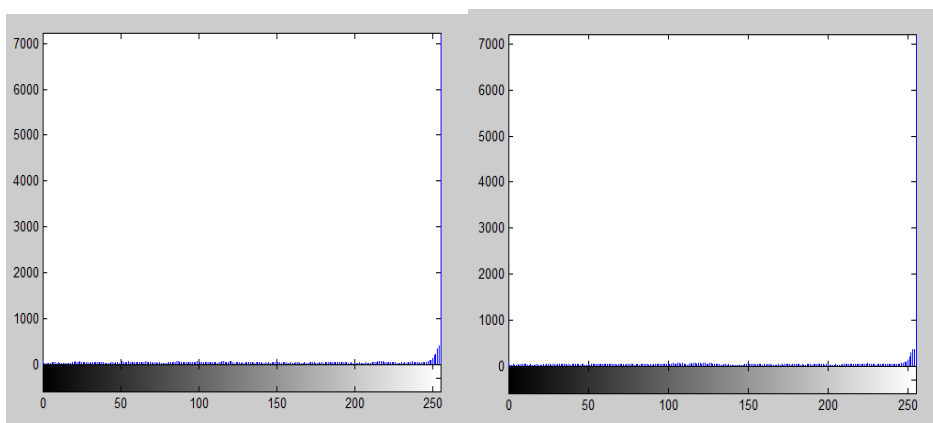
Image LPQ RGB (d) image LPQ Infrarouge (e)

**Figure III.4** :Exemple d'extraction de caractéristique des images  
De la base de données de test.

### III.5.3 classification :

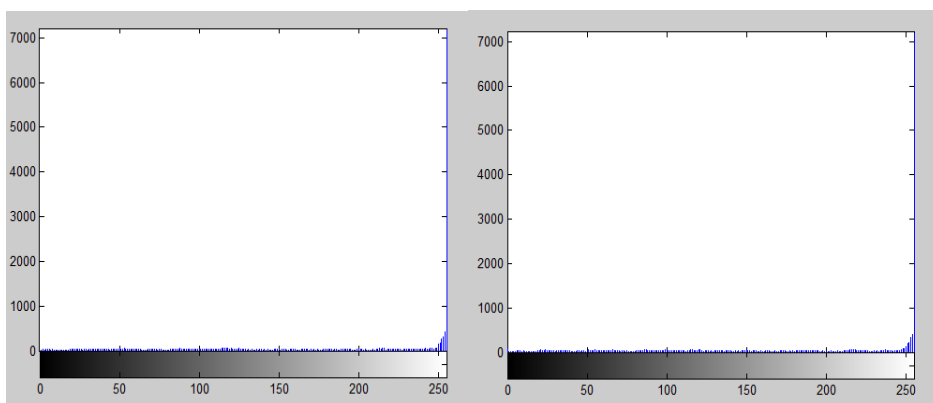
Dans ce travail pour déterminer les résultats, nous classons chaque vecteur en fonction des valeurs de chaque image où nous exécutons un algorithme qui compare la valeur du vecteur de toutes les valeurs des vecteurs enregistrées dans la base de données pour obtenir la personne désirée.

Quelques exemples de valeurs vectorielles :



Histogramme Image LPQ Rouge (a)

Histogramme image LPQ Vert (b)



Histogramme Image LPQ Bleu (c)

Histogramme image LPQ Infrarouge (d)

**Note:** Les Histogrammes sont très proches de l'œil nu et sont si proches des formes d'images.

### III.6 Résultats et discussion

-Nous avons appliqué notre algorithme sur la base de données de test, la base multi-spectrale (PolyU -MSP). Le tableau suivant donne un résumé des résultats de l'erreur EER obtenu.

Nombre de personnes de la BDD	Méthode	Images Rouge	Images Bleu	Images Vert	Images Infrarouges (NIR)	Taux de reconnaissance
500 personnes	LPQ	0.1131	0.1778	0.3878	0.1034	92.02 %

**Tableau III.1 : Résultats obtenus**

À travers les résultats obtenus par notre méthode (tableau III.1), On remarque que :

- La bande Infrarouge donne le meilleur EER par rapport les autres bandes (rouge, bleu et vert). Ceci est dû au fait que la bande NIR capte quelques structures de veine palmaire. Ces informations additionnelles aident au mieux de bien classifier cette bande.
- Les bandes rouge et bleu sont très similaires. Les lignes des empreintes palmaires de ces deux bandes semblent presque les mêmes.
- Les résultats obtenus sont acceptable du point de vue taux de reconnaissance qui est de l'ordre 92%.

**III.7 Conclusion:**

Dans ce chapitre nous avons détaillé notre système de reconnaissance des empreintes palmaire. Ce système est composé de trois étapes : prétraitement, extraction et classification. La base de données utilisées dans notre travail est déjà prête donc, ne nécessite aucun prétraitement supplémentaire. A partir des images de la base de données de test, la deuxième étape permette l'extraction des caractéristiques des empreintes palmaires par la méthode LPQ. Les vecteurs de caractéristiques sont ensuite classifiés par le calcul de la distance minimal entre le vecteur de l'image de test et celles de la base de données.

---



*Conclusion*

*Générale*

## **Conclusion générale**

La reconnaissance biométrique est l'identification des personnes est basée sur l'utilisation de ses caractéristiques physiques ou comportementales ou biologiques. Parmi les modalités les plus utilisées dans la reconnaissance biométrique est l'empreinte palmaire 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.

Les objectifs suivis dans ce mémoire proposent une démarche qui consiste à améliorer la performance de l'identification et vérification biométriques via l'empreinte palmaire 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.

En fin, le système proposé est appliqué sur une base de données connue dans le domaine des empreintes palmaires 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 nous concentrer 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]. **FATIHA, SAIDAT DJEMAA-GUEZIZ.***Identification des personnes par l'empreinte de l'articulation des doigts.* OUARGLA : UNIVERSITE KASDI MERBAH OUARGLA, 2016.
- [2]. **Meriem, Fedias.***Combinaisons de données d'espaces couleurs et de méthodes de vérification d'identité pour l'authentification de visages.* Biskra : Université Mohamed Khider .
- [3]. **Soumia, BENOUAER Aichouche-TAHRINE.***Système biométrique basé sur les motifs locaux binaires orientés (LBP<sup>o</sup>).* OUARGLA : UNIVERSITE KASDI MERBAH OUARGLA, 2016.
- [4]. **Abdelmoumen, ZITOUNI Sif Eddine-SACI.***Authentification et Identification biométrique des personnes par les empreintes palmaires.* OUARGLA : UNIVERSITE KASDI MERBAH OUARGLA, 2016.
- [5]. **LAMARE, François.***OCT en phase pour la reconnaissance biométrique par empreintes digitales et sa sécurisation.* Paris : École doctorale : Informatique, Télécommunications et Électronique de Paris, 2016.
- [6]. **FATIMA, BOUKRAA.***Caractéristiques Biométrique pour l'identification.* ORAN : université d'oran 1, 07-04-2016.
- [7]. **Ibtissam, BENCHENNANE.***Etude et mise au point d'un procédé biométrique multimodale pour la reconnaissance des individus.* Oran : Université des Sciences et de la Technologie d'Oran Mohamed Boudiaf, 2016.
- [8]. **Arbaoui, O. Moulay Brahim et M.***Identification des personnes par les articulations des doigts.* Ouargla : Université Kasdi Merbah , 2015.
- [9]. **Abes, A. Ben Khalif et F.***Identification d'individus par reconnaissance d'empreintes palmaires.* Ouargla : Université Kasdi Merbah, 2008.
- [10]. **Babich, Aleksandra.***Biometric authentication. Types of biometric identifiers.* Helsinki : university of applied sciences, 2012.
- [11]. **ashbourn, Julian.***Guide To Biometrics For Large-Scale Systemes.* springer : s.n., 2011.
- [12]. **Ababsa, Guerfi.***Authentification d'individus par reconnaissance de caractéristiques biométriques liées aux visages 2D/3D .* Evry : Université d'Evry Val d'Essonne, 2008.

- [13]. **MORIZET., Nicolas.***Reconnaissance Biométrique par Fusion Multimodale du Visage et de l'Iris.* Paris : Ecole Nationale Supérieure des, 18 Mars 2009.
- [14]. **Guesmi, H.***Identification de personnes par fusion de différentes modalités biométriques .* French : Université de Rennes, 2014. Thèse de Doctorat.
- [15]. **Akrouf, S.***Une approche multimodale pour l'identification du locuteur .* Setif : Université Ferhat Abbas, 2011. Thèse de Doctorat.
- [16]. **Boudjellal, S.***Détection et identification des personnes par méthode biométrique.* Tizi-Ouzou : Université Mouloud Mammari. Mémoire de Magister.
- [17]. **KAHLAOUI, Abdelatif GHACHOUA-Ibrahim.***Reconnaissance de personnes en utilisant L'empreintes Palmaires multispectral basés sur L'apprentissageapprofondi.* Ouargla : Universite Kasdi Merbah , 2016. MEMOIRE MASTER ACADEMIQUE.
- [18]. [biometrie-online.net/technologies/modalites-comparatif#Adn](https://www.biometrie-online.net/technologies/modalites-comparatif#Adn). *biometrie-online.net*. [En ligne] 10 05 2018. <https://www.biometrie-online.net/technologies/modalites-comparatif#Adn>.
- [19]. **OUAMANE, Abdelmalik.***Reconnaissance Biométrique par Fusion Multimodale du Visage 2D et 3D.* biskra : Université Mohamed Khider, 2015. Doctorat en sciences en Electronique.
- [20]. **Abdelatif GHACHOUA, Ibrahim KAHLAOUI.***Reconnaissance de personnes en utilisant L'empreintes Palmaires multispectral basés sur L'apprentissageapprofondi.* OUARGLA : UNIVERSITE KASDI MERBAH , 2016. MEMOIRE MASTER ACADEMIQUE.
- [21]. **Amine Nait-Ali, Régis Fournier.***Traitement du signal et de l'image pour la biométrie.* L'OUASIR : s.n., 2012.
- [22]. **Vapnik, V.***The Nature of Statistical Learning Theory.* New York : s.n., 1995.
- [23]. **Buysens, Pierre.***Fusion de différents modes de capture pour la reconnaissance du visage appliquée aux e transactions.* Normandie : Université de Caen Basse, 2011.
- [24]. *Option de traitement d'images.* Nice : s.n., Semaine du 19 novembre 2007.
- [25]. **Dubuisson, Séverine.***Bases du traitement des images.* : s.n., 22 octobre 2010.