

Ministère de l'Enseignement Supérieur et de Recherche Scientifique

Université Kasdi Merbah Ouargla

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

Département d'électronique et de télécommunication



## Mémoire Master Académique

**Domaine :** Electronique et de télécommunication

**Filière :** Télécommunication

**Spécialité :** Système des télécommunications

**Présenté par :** BASSIMANE Reyane, REZZOUG Balkis

&SLAOUI Abderrahim

### Thème

**Identification des individus par l'empreinte de  
l'articulation de doigt (FKP)**

**Devant les jurys :**

**Président :** SAMAI Djamel

**Examinatrice :** CHARIF Fella

**Encadreur :** CHAA Mourad.

**Année Universitaire :** 2019/2020



# Remerciements

*Tout d'abord, nous tenons à remercier " Dieu " le tout puissant, qui nous a donné la force, la patience et la volonté d'accomplir ce modeste travail.*

*Sans oublier nos parents et nos familles pour leur contribution, leur soutien, leur patience et leurs encouragements.*

*Nous tenons à remercier **Mr. CHAA Mourad**, notre encadreur et enseignant au département d'électronique et communication.*

*Nos remerciements vont aussi aux membres de jury d'avoir accepté de juger et d'évaluer ce travail.*

*Nous tenons à remercier en cette occasion tout le corps professoral et administratif de département d'informatique de l'université Kasdi Merbah de Ouargla pour la richesse et la qualité de leurs enseignements et qui déploient de grands efforts pour assurer à leurs étudiants une formation actualisée.*

*Nous adressons nos plus sincères remerciements à tous nos proches amis, qui nous ont toujours encouragés au cours de la réalisation de ce mémoire.*

*Enfin, nous tenons également à remercier toute personne qui ont participé de près ou de loin à la réalisation de ce travail.*



## *Dédicace*

*J'ai le grand plaisir de dédier ce modeste travail  
A mes chères parents ma mère, qui me donne toujours  
l'espoir de vivre et qui n'a jamais cessé de prier pour moi  
A mon père pour sa patience, son soutien et son sacrifice  
afin que rien n'entrave le déroulement de mes études*

*A mes chères sœurs*

*A toute la famille Bassimane*

*A mes meilleures amies, à mes camarades*

*Sans oublier tous les professeurs que ce soit du primaire, du  
moyen, du secondaire.*

*En fin je remercie tout qui a contribué à la réalisation de ce  
modeste travail.*

BASSIMANE Reyane



# *Dédicace*

*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.*

*À 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.*

*À toute la famille Rezzoug.*

*À mes adorables sœurs: Houyame, Wissam, Soumia, Mayas, Tasnim.*

*À mes chers frères: Mohammed Seghir, Yasser, Ahmed Monib.*

*À mes nièces: Chahd, Amina, Roudina.*

*À mes neveux: Adnane, El-Yaman, Abd-Allah, Abd-El-Hamid.*

*À tous les professeurs et enseignants qui m'ont suivi durant tout mon cursus  
scolaire et qui m'ont permis de réussir dans mes études.*

*À tous mes amis.*

*À chaque personne ayant contribué à ce travail de près ou loin.*

**REZZOUG Balkis**



# *Dédicace*

**Avec l'expression de ma reconnaissance, je dédie ce modeste travail à ceux qui, quels que soient les termes embrassés, je n'arriverais jamais à leur exprimer mon amour sincère.**

- **A mon père qui m'a soutenu et encouragé durant ces années d'études.**
- **Sans oublier mes collègues pour son soutien moral, sa patience et sa compréhension tout au long de ce projet.**
- **A tous mes amis qui m'ont toujours encouragé, et à qui je souhaite plus de succès.**
- **A toute ma famille.**

**SLAOUI Abderrahim**



## ملخص

التحقق من هوية الأفراد وتحديد هويتهم هو إحدى الوسائل لضمان الأمن، من بين هذه الطرق نذكر كلمة المرور أو بطاقة الهوية. ولكن هذه الأنظمة أقل موثوقية. اليوم، تم إنشاء نظام للتعرف على الأفراد، يسمى البيومترية، مما يجعل من الممكن التحقق من أن المستخدم هو بالفعل الشخص الذي يدعي أنه هو. وهي تكنولوجيا تستخدم الخصائص الفسيولوجية، البيولوجية أو السلوكية خاصة لكل فرد لتحديد هويته بأكبر قدر ممكن من الموثوقية لمعالجة هذه المشكلة، نقدم طريقة جديدة وهي: التعرف من خلال بصمات وصلات الأصبع، (الرئيسية والثانوية)

تعد هذه البصمات سهلة الاستخدام ومهمة بسبب مزاياها مثل الأمان العالي والبساطة. وبناءً على كل هذا، قمنا بتطوير نظام لتحديد الهوية من خلال بصمات وصلات الأصبع، في جميع أنظمة القياسات الحيوية، توجد تقنيات مختلفة لاستخراج الخصائص. فبعملنا، استخدمنا طريقة LPQ, RI-LPQ, و طريقة SVM للتصنيف. بعد هذه الخطوة، سيتمكن نظامنا من تحديد ما إذا كان شخص جديد ينتمي إلى القاعدة أم لا.

**الكلمات الرئيسية:** البيومترية، تحديد الهوية، بصمة مفصل الإصبع (FKP)، التصنيف، SVM، RI-LPQ، LPQ.

## Résumé

Pour résoudre les problèmes des méthodes traditionnelles comme l'utilisation des mots de passe, de la carte d'identité, du code PIN ou des cartes à puces qui peuvent être volées ou falsifiées, on a proposé un système biométrique pour l'identification des individus.

La biométrie est une technologie qui utilise les caractéristiques physiologiques, biologiques ou comportementales propres à chaque individu pour établir de façon aussi fiable que possible son identité. Nous avons développé un système d'identification par les empreintes des articulations de doigts (FKP) (Majeur et Mineur).

Dans tous les systèmes biométriques, il existe différentes techniques d'extraction des caractéristiques. Dans notre travail, nous avons utilisé la méthode LPQ (Local Phase Quantization), RI-LPQ (Rotation invariant Local Phase Quantization), et la méthode SVM (Support Vector Machine) pour la classification. Après cette étape notre système sera capable de décider est ce qu'une nouvelle personne appartient à la base ou non.

**Mots clés :** biométrie, identification, l'empreinte de l'articulation du doigt (FKP), classification, LPO, RI-LPO, SVM.

**Abstract:**

To solve the problems of traditional methods such as the use of passwords, identity cards, PIN or smart cards that can be stolen or falsified, a biometric system has been proposed for the identification of individuals.

Biometrics is a technology that uses the physiological, biological or behavioral characteristics of each individual to establish as reliably as possible their identity. We have developed a Finger knuckle print (FKP) identification system (Major and Minor).

In all biometric systems, there are different techniques for extracting characteristics. In our work, we used the LPQ (Local Phase Quantization), RI-LPQ (Rotation invariant Local Phase Quantization) method, and the SVM (Support Vector Machine) method for classification. After this step our system will be able to decide what a new person belongs to the base or not.

**Keywords:** biometrics, identification, «Finger knuckle print (FKP), classification, LPQ, RI-LPQ, SVM.

# Sommaire

Sommaire .....	I
Liste des figures .....	VI
Liste des tableaux.....	IX
Liste des abréviations.....	X
Introduction générale .....	- 1 -

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

I.1.Introduction : .....	- 3 -
I.2. Définition de la biométrie :.....	- 3 -
I.3. Caractéristiques de la biométrie : .....	- 4 -
I.4. Principales modalités biométriques : .....	- 5 -
I.4.1. Les modalités physiologiques (morphologique) : .....	- 5 -
I.4.1.1. L’empreinte digitale : .....	- 6 -
I.4.1.2. Géométrie de main : .....	- 7 -
I.4.1.3. Visage : .....	- 7 -
I.4.1.4. l’iris :.....	- 8 -
I.4.1.5. La rétine : .....	- 9 -
I.4.1.6. Empreinte des articulations des doigts : .....	- 10 -
I.4.2. Les modalités comportementales : .....	- 11 -
I.4.2.1. La signature : .....	- 11 -
I.4.2.2. La voix : .....	- 12 -
I.4.2.3. La dynamique de la frappe : .....	- 13 -
I.4.2.4. La Démarche : .....	- 14 -
I.4.3. Modalités biologiques : .....	- 15 -



# Sommaire

I.4.3.1. Le thermo gramme facial :.....	- 15 -
I.4.3.2. L'ADN :.....	- 15 -
I.4.3.3. Veines des mains :.....	- 17 -
I.5. Architecture d'un système biométrique :.....	- 18 -
I.5.1. Phase d'entraînement :.....	- 19 -
I.5.2. Phase de reconnaissance (phase de test) :.....	- 19 -
I.5.2.1. Mode vérification (authentification) :.....	- 19 -
I.5.2.2. Mode identification :.....	- 20 -
I.6. Principaux modules du système biométrique .....	- 20 -
I.6.1. Module d'acquisition biométrique : .....	- 20 -
I.6.2. Module d'extraction de la région d'intérêt (ROI) :.....	- 21 -
I.6.3. Module base de données :.....	- 21 -
I.6.4. Module d'extraction des caractéristiques : .....	- 21 -
I.6.5. Module comparaison : .....	- 21 -
I.6.6. Module de décision :.....	- 21 -
I.7. Les limitations des systèmes biométriques monomodaux :.....	- 22 -
I.8. La multi modalité : .....	- 22 -
I.8.1. Définition de la biométrie de multi modalité : .....	- 22 -
I.8.2. Les différents multi-possibles :.....	- 22 -
I.8.2.1. Multi-capteurs :.....	- 22 -
I.8.2.2. Multi-instances : .....	- 22 -
I.8.2.3. Multi-algorithmes :.....	- 23 -
I.8.2.4. Multi-échantillons :.....	- 23 -

# Sommaire

I.8.2.5. Multi-biométries :	- 23 -
I.8.3. Les avantages de la multi-modalité :	- 24 -
I.9. Les applications de la biométrie :	- 24 -
I.9.1. Applications commerciales :	- 24 -
I.9.2. Applications de gouvernement :	- 24 -
I.9.3. Applications juridiques (légales) :	- 24 -
I.10. Evaluation des performances des Systèmes biométrique :	- 25 -
I.10.1. Evaluation de la vérification (les mesures des taux d'erreur) :	- 25 -
I.10.1. 1. Le FAR (False Acceptance Rate) :	- 25 -
I.10.1. 2. Le FRR (False Reject Rate):	- 25 -
I.10.1.3. Taux d'égalité erreur (ErrorEqualRateEER) :	- 25 -
I.11. Conclusion :	- 28 -

## **Chapitre II : L'empreinte de l'articulation du doigt (FKP)**

II.1. Introduction :	- 29 -
II.2. Les modalités biométriques liées à la main :	- 29 -
II.2.1. La biométrie FKP :	- 30 -
II.3. Les algorithmes utilisés dans le système biométrique :	- 31 -
II.3.1. Les méthodes de prétraitement :	- 31 -
II.3.1.1. Algorithme du Self-Quotient Image (SQI) :	- 31 -
II.3.1.2. Algorithme de l'adaptive single scale retinex (ASSR) :	- 32 -
II.3.1.3. Le filter Dog (Difference of Gaussians):	- 33 -
II.3.2. Extraction des caractéristiques :	- 34 -

# Sommaire

II.3.2.1. L'analyse en Composantes Principales (PCA) : .....	- 34 -
II.3.2.2. L'analyse Discriminante Linéaire (LDA) : .....	- 35 -
II.3.2.3. Filtre de log-Gabor : .....	- 36 -
II.3.2.4. Caractéristique d'image statistique binarisées (BSIF): .....	- 37 -
II.3.2.5. Quantification de phase locale (LPQ) : .....	- 39 -
II.3.2.6. Quantification de phase locale invariante de rotation (RI-LPQ) : .....	- 41 -
II.3.3. Classifications : .....	- 43 -
II.3.3.1. Les étapes d'une classification : .....	- 44 -
II.3.3.2. Classification par SVM : .....	- 44 -
II.3.3.3. Méthode des K plus proches voisins (KNN) : .....	- 46 -
II.4 Conclusion : .....	- 49 -
<b>Chapitre III : Résultats expérimentaux et discussions</b>	
III.1. Introduction : .....	- 50 -
III.2. Que signifie MATLAB (MATrix LA Boratory) : .....	- 50 -
III.3. Expérience sur les images FKP : .....	- 51 -
III.3.1. Base de données : .....	- 51 -
III.3.2. Protocole de test : .....	- 51 -
III.3.3. Acquisition des données : .....	- 52 -
III.3.4. Taux de reconnaissance : .....	- 53 -
III.3.5. Présentation du système : .....	- 53 -
III.4. Résultats et discussion : .....	- 55 -
III.4.1. Les résultats obtenus par la méthode LPQ : .....	- 55 -
III.4.1.1. La taille de fenêtre (winsize) : .....	- 56 -

# Sommaire

III.4.1.2. Décorrélation (decorr):.....	- 56 -
III.4.1.3. L'estimation de fréquence locale (freqestim):.....	- 57 -
III.4.2. Les résultats obtenus par la méthode RI-LPQ : .....	- 57 -
III.4.2.1. La taille de fenêtre (winsize) : .....	- 58 -
III.4.2.2. Le nombre d'angle (numAngl) : .....	- 58 -
III.4.3.3. La taille de bloc (nombre de pixels) : .....	- 59 -
III.5. Comparaison entre les méthodes LPQ et RI-LPQ dans le système de La reconnaissance des individus par leur FKPs : .....	- 60 -
III.6. Conclusion : .....	- 61 -
Conclusion générale :.....	- 62 -
Bibliographie :.....	- 63 -

# Liste des figures

## Liste des figures

Figure	Titre	Page
<b>Figure I.1</b>	Exemples de modalités biométriques.	4
<b>Figure I.2</b>	Principales modalités biométriques.	5
<b>Figure I.3</b>	a) Dispositif de reconnaissance d'une empreintes digitales b) les caractéristiques principales d'une empreinte digitale	6
<b>Figure I.4</b>	a) Dispositif de reconnaissance par géométrie de la main b) Image de la géométrie de main	7
<b>Figure I.5</b>	La reconnaissance de visage.	8
<b>Figure. I.6</b>	La reconnaissance d'iris	9
<b>Figure I.7</b>	a) Image de la rétine b) Dispositif de reconnaissance par la rétine	10
<b>Figure I.8</b>	Image des empreintes des articulations des doigts (FKP)	11
<b>Figure I.9</b>	La reconnaissance de la signature	12
<b>Figure I.10</b>	Image de la reconnaissance vocale	13
<b>Figure I.11</b>	Dynamique de frappe au clavier	14
<b>Figure I.12</b>	La Démarche	15
<b>Figure I.13</b>	Le thermo gramme facial	16
<b>Figure I.14</b>	Acide Désoxyribonucléique ADN	17
<b>Figure I.15</b>	a) Dispositif de reconnaissance par veines des mains b) Image de la veine des mains	18
<b>Figure I.16</b>	Architecture du mode d'entraînement d'un système biométrique.	19
<b>Figure I.17</b>	Architecture du mode vérification d'un système biométrique	20
<b>Figure I.18</b>	Architecture du mode identification d'un système biométrique.	21



# Liste des figures

<b>Figure I.19</b>	Multi-capteurs : capteur optique et capteur thermique	22
<b>Figure I.20</b>	La biométrie de multi-instances	23
<b>Figure I.21</b>	Multi-échantillons : Iris droit et Iris gauche	23
<b>Figure I.22</b>	Multi-biométries : L'iris et L'empreinte digitale	24
<b>Figure1.23</b>	Illustration du FRR et du FAR	26
<b>Figure1.24</b>	Courbe du point d'équivalence des erreurs dans un système biométrique	27
<b>Figure1.25</b>	Courbe DET.	27
<b>Figure1.26</b>	Courbe ROC	28
<b>Figure II .1</b>	La main : face dorsale et face palmaire	30
<b>Figure II.2</b>	La surface externe d'un doigt a trois jointures	31
<b>Figure II.3</b>	(a) Images de FKPs. (b) Leur réflectances images en utilisant algorithme de SQI	32
<b>Figure II.4</b>	(a) images de FKPs. (b) Leur réflectances images en utilisant algorithme de ASSR	32
<b>Figure II.5</b>	(a) images de FKPs. (b) Leur images filtrées par un filtre DoG	34
<b>Figure II.6</b>	Méthode globale : PCA et LDA	36
<b>Figure II .7</b>	Différence dans le domaine fréquentiel entre les filtres Gabor et Log-Gabor	37
<b>Figure II .8</b>	Les 13 images naturelles utilisées par J. Kannala et E Rahtu pour l'apprentissage des filtres dans le descripteur BSIF	38

# Liste des figures

<b>Figure II.9</b>	(a) Exemple d'image FKP. (b) Filtre BSIF de taille 11x11 et de longueur 12. (c) Les résultats de la convolution de l'image FKP avec un filtre BSIF. (d) Image finale FKP filtrée par BSIF filtre	39
<b>Figure II.10</b>	Organigramme de l'ensemble des étapes nécessaires du descripteur LPQ	41
<b>Figure II.11</b>	Rotation Invariant Local Phase Quantization (RI-LPQ)	43
<b>Figure II.12</b>	Classification SVM ; (A) SVM linéaire séparation par une ligne droite, (B) SVM non linéaire séparation par une courbe	46
<b>Figure II.13</b>	Méthode des K plus proches voisins (KNN)	48
<b>Figure III.1</b>	Le logiciel MATLAB	50
<b>Figure III.2</b>	Quelques images de la base de données Poly U-FKP((a) Majeur et (b) Mineur)	51
<b>Figure III.3</b>	Dispositif d'acquisition de FKP	52
<b>Figure III.4</b>	Schéma proposé du système de reconnaissance de FKP	54
<b>Figure III.5</b>	(a) Images FKPs , (b) leur images LPQs	55
<b>Figure III.6</b>	Exemple de l'histogramme d'une image FKP.	60

# Liste des tableaux

## Liste des tableaux

Tableau	Titre	Page
<b>Tableau II.1</b>	Comparaison entre les méthodes d'extraction des caractéristiques	<b>43</b>
<b>Tableau III.1</b>	TR en utilisant les différentes tailles de fenêtre.	<b>56</b>
<b>Tableau III.2</b>	TR en utilisant les différentes décorrélation.	<b>56</b>
<b>Tableau III.3</b>	TR en utilisant les différentes estimations de fréquence locale	<b>57</b>
<b>Tableau III.4</b>	TR en utilisant les différentes tailles de fenêtre.	<b>58</b>
<b>Tableau III.5</b>	TR en utilisant les différents nombres d'angle.	<b>58</b>
<b>Tableau III.6</b>	TR en utilisant les différentes tailles de bloc $N \times N$ .	<b>59</b>

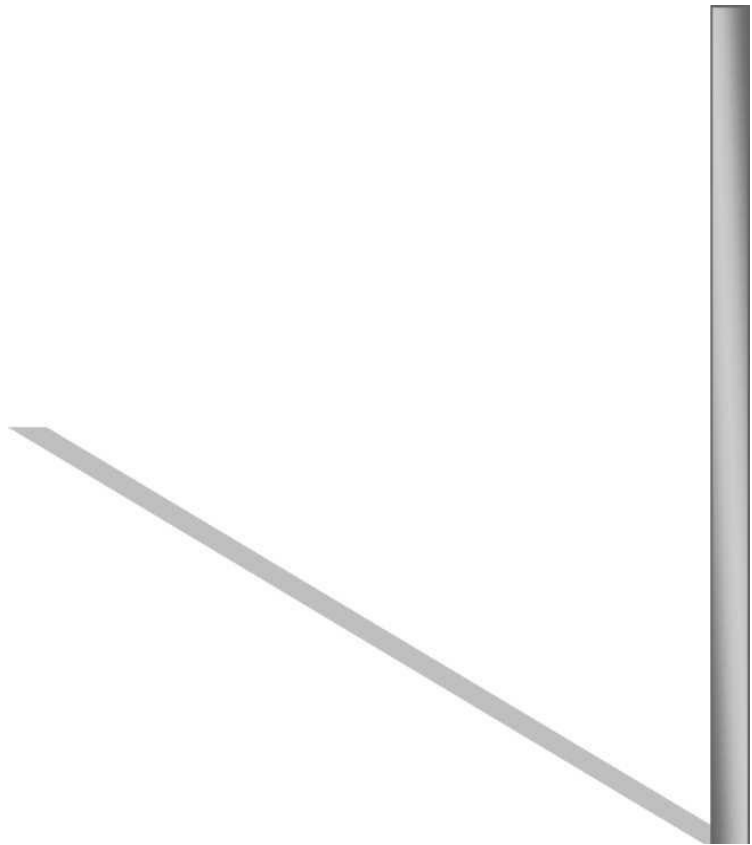
# Liste des abréviations

## Liste des abréviations

Abréviations	Designations
<b>ADN</b>	Acide désoxyribose nucléique
<b>ASSR</b>	Adaptative Single Scale Retinex
<b>BSIF</b>	Binarized Statistical Image Features
<b>DET</b>	Courbes représentant les taux d'erreurs en échelle logarithmique (Détection Error Trade-off curve)
<b>DOG</b>	Difference of Gaussians
<b>EER</b>	Taux d'erreurs égales (Equal Error Rate)
<b>FAR</b>	Taux de Fausses Acceptations (False Acceptance Rate)
<b>FKP</b>	Finger Knuckle Print ( Empreintes des articulations des doigts )
<b>FRR</b>	Le taux de Faux Rejets (False Rejection Rate)
<b>KNN</b>	Nearest-Neighbor
<b>LDA</b>	Linear Discriminant Analysis
<b>LED</b>	Light-emitting diode
<b>LPQ</b>	Local Phase Quantization
<b>PCA</b>	Principal Component Analysais
<b>PIN</b>	Numéro d'Identification Personnel (Personnel Identification Numbers)
<b>RDF</b>	Reconnaissance Des Formes
<b>RI-LPO</b>	Rotation invariant Local Phase Quantization
<b>ROC</b>	Courbe représentant les taux d'erreur (Receiver Operating Characteristic)
<b>ROI</b>	Région d'intérêt (Region Of Interest)
<b>SQI</b>	Self Quotient Image
<b>STFT</b>	Transformée de Fourier à court terme
<b>SVM</b>	Support Vector Machine
<b>TF</b>	Transformée de Fourier
<b>TFA</b>	Taux de fausses acceptations



# **Introduction générale**





# Introduction générale

## Introduction générale :

Pour le moment on parle de plus en plus de l'insécurité dans divers secteurs ainsi que des moyens informatiques à mettre en œuvre pour contrer cette tendance. La vérification et l'identification des individus est l'un des moyens permettant d'assurer cette sécurité. L'être humain se sert quotidiennement de son système visuel pour identifier les personnes de façon automatique, bien que le processus mis en jeu soit complexe.

L'homme a établi des méthodes de validation d'identité qui sont liés, soit à ce que possède une individu telle qu'un passeport ou une carte d'identité, soit à ce que sait cet individu, c'est le cas du mot de passe ou un code PIN., ces éléments peuvent être volés, falsifiés ou oublié. Pour contourner ces limitations, un système a été créé pour la reconnaissance des individus, appelé la biométrie. La biométrie permet de vérifier que l'utilisateur est bien la personne qu'il prétend être. Qui permet d'utiliser, non pas l'information qu'un individu possède ou connaît, mais une information intrinsèque à cette personne.

De plusieurs technologies biométriques ont été évolués, toutes basées sur les identificateurs biométriques physiologiques et comportementales comme : l'iris, la voix, Empreinte des articulations de doigts (FKP), le visage et la signature...etc. 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. [01]

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

Les empreintes des articulations des doigts sont acquises par un simple appareil photo numérique et sont largement acceptées par les usagers.

Indubitablement, FKP fait référence aux motifs de peau de la surface externe autour de l'articulation phalangienne de doigt et comporte des caractéristiques structurelles distinctives, telles que les motifs de texture. Généralement, ces caractéristiques possèdent des aptitudes potentiellement discriminatoires conviennent comparativement bien à l'identification d'un individu par rapport aux autres.[02]

# Introduction générale

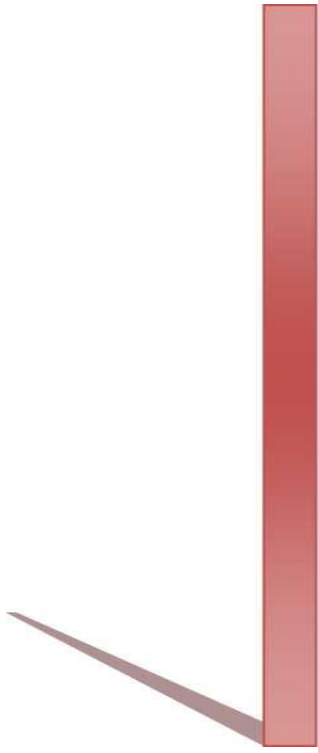
Le travail présenté dans cette mémoire se compose de trois chapitres, plusieurs notions et concepts de la biométrie et réalisation des systèmes de reconnaissance vont être abordés, les trois chapitres vont être comme suite :

Le premier chapitre présente les concepts de base sur la biométrie ainsi que ses caractéristique et ses principales modalités. Nous présentons aussi l'architecture et principale module d'un système biométrique, ensuite on va parler sur les limitations des systèmes biométriques monomodaux, la multi modalité et les applications de la biométrie. Ce chapitre est finalisé par l'évaluation des performances des systèmes biométrique.

Le deuxième chapitre sera dévoué à la présentation de la biométrie de l'empreinte de l'articulation de doigt (FKP), les méthodes de prétraitement et l'extraction des caractéristiques et la classification.

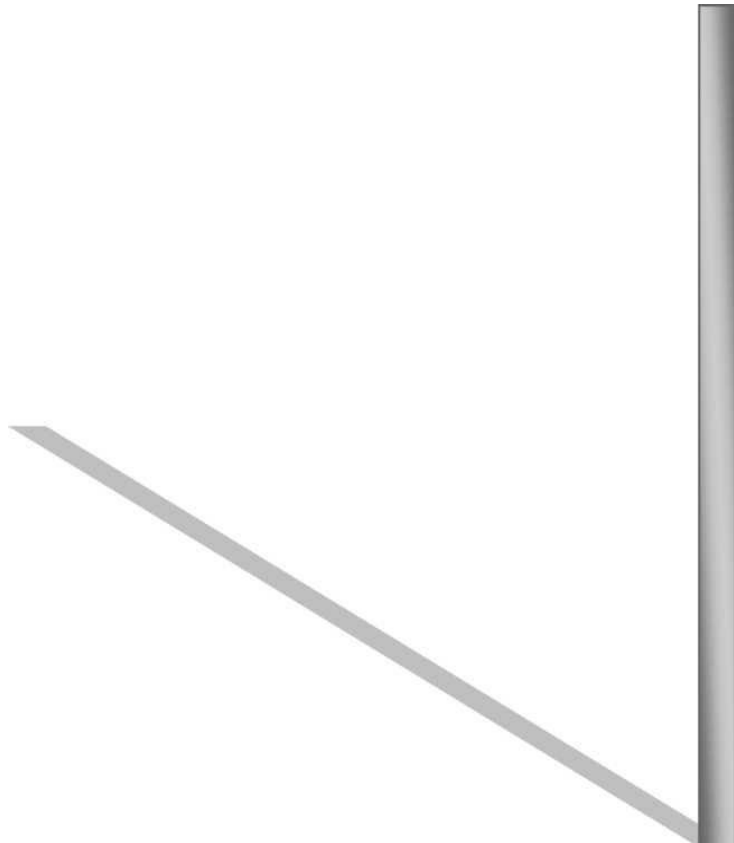
Le dernier chapitre est consacré pour les résultats expérimentaux. La première partie on parlera de la base de données, protocole de test ensuite l'extraction de la région d'intérêt que nous avons appliqué à l'empreinte des articulations de doigts (FKP), deuxième partie de ce chapitre discute les résultats expérimentaux obtenus par les méthodes LPQ et RI\_LPQ et enfin on a fait une comparaison entre ces deux méthodes utilisées.

En termine par une conclusion générale qui résumera les résultats obtenus par les différentes approches.



# *Chapitre I*

## *Généralité sur la biométrie*



## I.1.Introduction :

Dans tous les domaines de sécurité et de contrôle d'accès, on utilise des mots de passe ou des clés qui se composent des chiffres ou des lettres. Mais, dans ces derniers temps avec l'avancement de la technologie ces mots de passe sont devenus facilement falsifiables. C'est pour ça, que les chercheurs de différents domaines ont orientés leurs travaux sur des clés et mots de passe impossible à falsifier, sûr et surtout efficace. [03]

Dans ce chapitre, nous allons mettre en relation quelques notions de base sur la biométrie. Nous donnerons ses principales modalités et l'évaluation des performances des systèmes biométrique ainsi que les domaines d'applications.

## I.2. Définition de la biométrie :

L'expression « biométrie » est originaire d'une contraction des deux anciens termes grecs : « **bios** » qui signifie : la vie et « **metron** » qui se traduit par: mesure.

La biométrie est La reconnaissance automatique d'une personne selon ses caractéristiques physiologiques, biologiques ou comportementales.

La biométrie comprend l'ensemble des processus permettant de déterminer une personne à partir de la mesure de l'une ou de plusieurs de ses caractéristiques physiologiques, comportementales ou biologique. La biométrie est la science d'établir l'identité d'une personne basée sur les attributs physiologique comme empreintes digitales, visage, géométrie de la main, iris, rétine...etc. Comportementaux comme démarche, signature, dynamique de clavier...etc. ou biologique comme ADN, Odeur et cheveux.... etc. liés à un individu. [04]

# Chapitre I : Généralité sur la biométrie



Figure I.1 : Exemples de modalités biométriques

## I.3. Caractéristiques de la biométrie :

Les modalités biométriques doivent être déterminées par quelques caractéristiques en but d'assurer leurs fiabilités. Chaque modalité possède ses propres avantages et inconvénients, le choix d'une modalité biométrique pour une application donnée dépend d'une variété de paramètres liés à la nature et les exigences de l'application et aux propriétés de la modalité, ont identifié quelques paramètres généralement employés dans une application biométrique, qui sont :

- **Universalité** : la caractéristique biométrique doit exister, naturellement, chez toutes personnes.
- **Invariance** : les caractéristiques doivent être constantes sur une longue période de temps.
- **Mesurabilité** : les propriétés biométriques doivent être mesurables.
- **Singularité** : les caractéristiques biométriques doivent être uniques à chaque individu. Elles doivent être suffisantes pour distinguer une personne d'une autre.
- **Acceptabilité** : 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.



# Chapitre I : Généralité sur la biométrie

- **Inimitabilité:** pour une précision sans faille, l'attribut ne doit pas être reproductible par d'autres moyens.
- **Unicité:** Le trait biométrique doit être suffisamment différent d'une personne aux autres.
- **Enregistrables:** collecter les caractéristiques d'un individu avec son accord.

## I.4. Principales modalités biométriques :

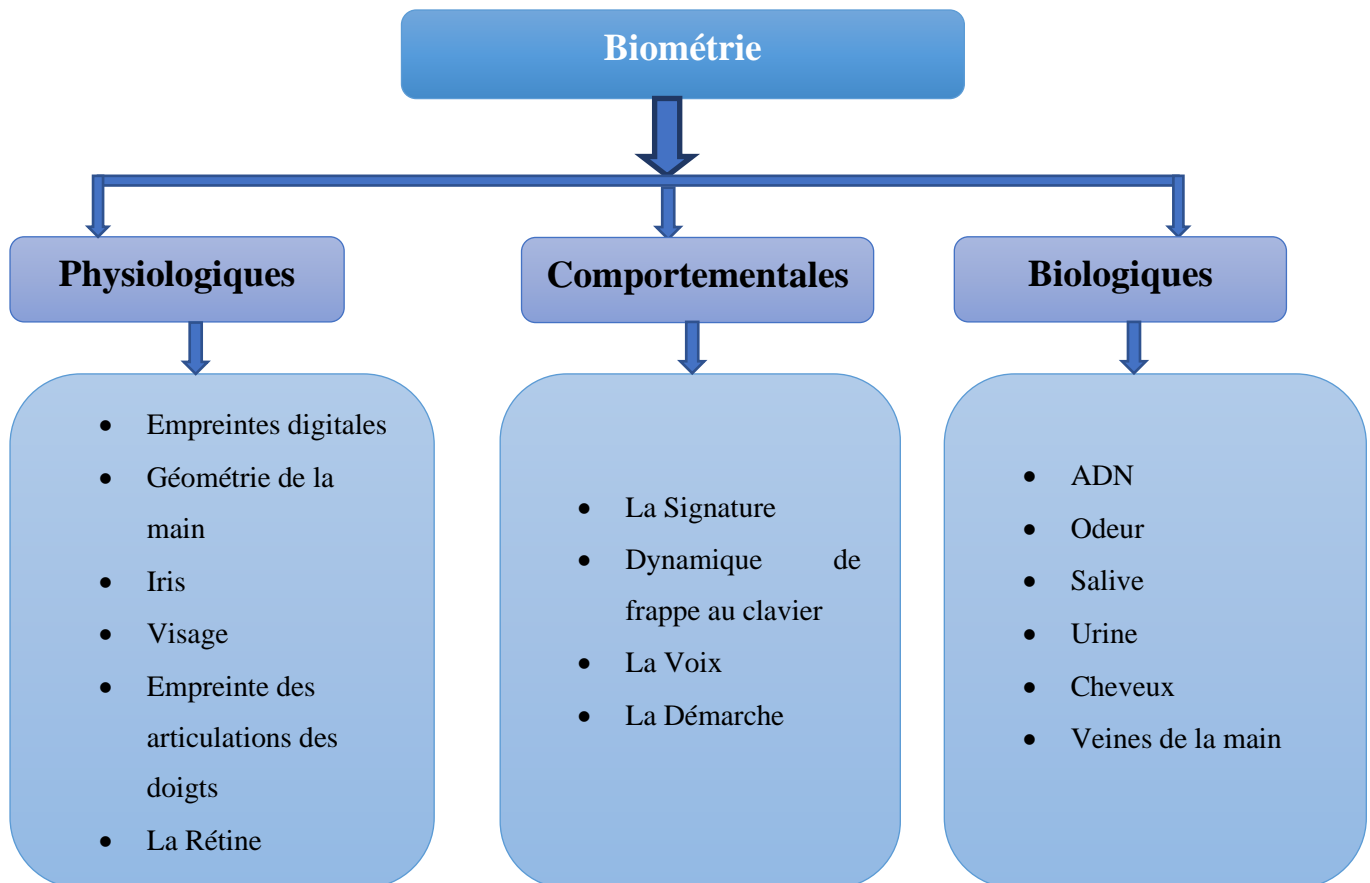


Figure1.2 : Principales modalités biométriques.

### I.4.1. Les modalités physiologiques (morphologique) :

Elle basée sur l'identification de traits physique particuliers qui pour toute personne, sont uniques et permanents. Les modalités physiologiques regroupent les empreintes digitales, géométrie de la main, l'iris de l'œil, les traits du visage, empreint des articulations des doigts, le réseau veineux de la rétine la forme de la main etc. [05]

# Chapitre I : Généralité sur la biométrie

## I.4.1.1. L'empreinte digitale :

L'empreinte digitale La plus ancienne et la plus utilisé des technologies d'identification. Elle représente plus de cinquante pour cent des applications. Ce dessin est unique et différent pour chaque personne. En pratique, les informations fournies par ce dessin (la figure I.3) sont tellement nombreuses qu'il est quasiment impossible de toutes les utiliser. On choisira donc en extraire les traits fondamentaux comme les bifurcations de crêtes, les "îles", les lignes qui disparaissent.

Cette empreinte contient environ une centaine de ces points caractéristiques encore appelés "minuties". La loi impose un minimum de douze pour identifier avec certitude une personne car il est statistiquement impossible de trouver deux individus présentant les mêmes douze points caractéristiques, même en considérant une population de plusieurs dizaines de millions de personnes.[06]



**Figure I.3 :** a) Dispositif de reconnaissance d'empreintes digitales ; b) Les caractéristiques principales d'une empreinte digitale.

### Les avantages :

- ✓ Traitement rapide.
- ✓ Ergonomie moyenne.

### Les inconvénients :

- ✓ Acceptabilité moyenne.
- ✓ Difficulté de lecture (cicatrice, égratignure).

## I.4.1.2. Géométrie de main :

Est une technologie biométrique récente, elle consiste à analyser et à mesurer la forme de la main, qui signifie mesurer la longueur, la largeur et la hauteur de la main d'un utilisateur et de créer une image 3D (la figure I.4). Des LED infrarouges et un appareil - photo numérique sont utilisés pour acquérir les données de la main.

Géométrie de la main offre un niveau raisonnable de précision et est relativement facile à utiliser. Cependant, elle peut être facilement trompée par des jumeaux ou par des personnes ayant des formes des mains proches. [01]



**Figure I.4 :** a) Dispositif de reconnaissance par géométrie de la main ; b) Image de la géométrie de la main

### Les avantages :

- ✓ Très simple à utiliser.
- ✓ Bonne acceptation des usagers.

### Les inconvénients :

- ✓ Système encombrant et coûteux.
- ✓ Perturbation possible par des blessures.

## I.4.1.3. Visage :

La reconnaissance de visages qui est classée parmi les techniques principales de la biométrie est facilement tolérée par les utilisateurs, peu intrusive et moins coûteuse la plus facile à utiliser car elle

# Chapitre I : Généralité sur la biométrie

est non contraignante. En effet, elle n'exige pas beaucoup d'effort de la part de l'utilisateur lors de la saisie de mesures. Certains systèmes employant cette technique fonctionnent même sans que l'utilisateur en soit conscient. [07]



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

## **Les avantages :**

- ✓ Technique acceptable par le public.
- ✓ Fonctionnement simple et capable.

## **Les inconvénients :**

- ✓ La technique est trop sensible au changement d'éclairage ou l'angle de l'appareil-photo...etc.
- ✓ La distance pour la capture de l'image du visage n'est pas inconfortable.

### **I.4.1.4. L'iris :**

La technologie de reconnaissance de l'iris est très intéressante pour la biométrie, car elle permet de différencier même des jumeaux ou l'œil gauche de l'œil droit d'une même personne et très difficilement falsifiable.[06]

L'iris est considérée la membrane colorée située entre le blanc de l'œil et la pupille, elle est composée d'une multitude de tubes très fins qui s'entrecroisent, procurant à elle une forme particulière et unique qui ne varie que très peu au cours d'une vie. La capture de l'iris se fait à l'aide d'une caméra un premier temps positionné l'iris par rapport à l'ensemble de l'œil. Ensuite, la caméra scanne l'image de l'iris pour

# Chapitre I : Généralité sur la biométrie

en analyser les points caractéristiques. Le dispositif analyse notamment la position, la longueur et le relief des tubes qui composent l'iris. Enfin, en ayant retenu au-dessus de 200 points distinctifs, l'ordinateur relié à la caméra procède à la comparaison de l'iris avec la banque de données des identifiants possibles. Le processus d'identification ne prend que quelques secondes. [08]



**Figure. I.6 :** La reconnaissance d'iris

## Les avantages :

- ✓ Les structures de l'iris restent stables durant toute la vie.
- ✓ Grande quantité d'information contenue dans l'iris.
- ✓ L'iris pas modifiable même par intervention chirurgical.

## Les inconvénients :

- ✓ Les gens ont du mal à accepter cette biométrie.
- ✓ L'acquisition des images exige une certaine formation et de la pratique.
- ✓ Des problèmes peuvent survenir lors de la mesure.

## I.4.1.5. La rétine :

La rétine est la pellicule photographique de l'œil. Elle est composée de 4 couches de cellules et est située on fond de l'œil.

Les éléments qui permettent de distinguer Photographie des deux rétines d'un individu eux rétines sont les veines qui les tapissent. La disposition de ces veines est stable et unique d'un individu à l'autre (d'un œil à l'autre). De plus, pour un fraudeur, il est impossible de pouvoir reproduire ce motif. D'où un très haut niveau de sécurité. [09]



# Chapitre I : Généralité sur la biométrie

Pour obtenir une image d'une rétine, il est nécessaire d'éclairer le fond de l'œil à l'aide d'un faisceau lumineux ; à travers la pupille et le corps vitreux. Ce faisceau est de négligeable intensité pour ne pas déranger l'utilisateur, il est sans danger et d'intensité que sur les dispositifs ophtalmologiques. Un système de caméra très précis vient ensuite recouvrir l'image de la rétine. Des lecteurs de rétine sont en disposition, et permettent d'acquérir un haut niveau de sécurité. Ils autorisent l'accès à un poste informatique.



(a)

(b)

**Figure I.7 :** a) Image de la rétine ; b) Dispositif de reconnaissance par la rétine

## Les avantages :

- ✓ La rétine est stable durant la vie d'un individu.
- ✓ Très efficace, haut sécurité.
- ✓ Carte vasculaire propre à chaque individu et différent, même entre jumeaux.

## Les inconvénients :

- ✓ Mauvaise acceptation du public (l'œil est un organe sensible).
- ✓ Cout plus important que d'autres technologies.

### I.4.1.6. Empreinte des articulations de doigts :

Récemment on constate que l'empreinte d'articulation de doigt, qui se révèle aux formes inhérentes de la surface externe autour de doigt et spécialement la partie haute de doigt, est fortement unique et peut servir à une modalité biométrique distinctive. L'articulation de doigt est encore à la phase de développement et peut être considérée comme nouvelle tendance dans la biométrie. [10]



**Figure I.8 :** Image des empreintes des articulations de doigts (FKP)

## **Les avantages :**

- ✓ Technique acceptable.
- ✓ Utilisation simple.

## **Les inconvénients :**

- ✓ Très similaire pour les jumeaux.
- ✓ Problème dans le cas de couper un doigt.
- ✓ Pose incorrecte de doigt sur le lecteur provoque une grande erreur.

## **I.4.2. Les modalités comportementales :**

Dans ces techniques de reconnaissance, on s'intéresse aux caractéristiques physiques en activité des individus qui peuvent être typiques et permettent de distinguer une personne d'une autre. Dans la suite, nous présenterons quelques modalités de ce type avec leurs modes d'utilisations :

### **I.4.2.1. La signature :**

La vérification par la signature est l'une des premières méthodes utilisées dans le domaine de la biométrie. Les systèmes de reconnaissance de l'écriture analysent soit la géométrie de la signature (mode statique), soit ses caractéristiques spécifiques comme la vitesse, la pression sur le crayon, ce mode qui s'appelle le mode dynamique est le plus discriminant. La capture se fait à l'aide d'une tablette graphique. Bien que la signature soit bien acceptée par les utilisateurs, sa variabilité (à cause de l'état de santé ou l'état émotionnel de l'individu) pose un grand problème. [11]

Ces données sont enregistrées pour comparaison ultérieure. Certains systèmes ne font qu'enregistrer l'image statique de la signature pour comparaison.



**Figure I.9 :** La reconnaissance de la signature

## **Les avantages :**

- ✓ Plus confortable.
- ✓ Utilisé dans le document administratif.
- ✓ Accepter par les personnes.
- ✓ Rapide et efficace.

## **Les inconvénients :**

- ✓ Besoin d'une tablette graphique.
- ✓ On ne peut pas utiliser à contrôle d'accès extérieur.
- ✓ Les signatures falsifiées (imitation).
- ✓ Dépendant de l'état émotionnel de la personne peu fiable.

### **I.4.2.2. La voix :**

La première application en sécurité de la reconnaissance d'un individu par sa voix remonte aux années 1970 et à son utilisation par les pilotes de chasse de l'armée américaine. Les caractéristiques composant le gabarit sont une combinaison de facteurs comportementaux (vitesse, rythme...) et physiologiques (âge, fréquence, sexe, accent, tonalité et harmoniques...). La reconnaissance de l'identité se fait soit sur la base de la lecture d'un texte prédéterminé, aléatoire ou d'un message défini librement par un individu. Une phrase fixe expose cependant au risque que l'authentification soit contournée par un enregistrement vocal.[12]

Le contrôle d'accès par la voix peut pâtir de faux rejets et de fausses acceptations en nombre haut, notamment en raison de l'état émotionnel, d'une maladie tel un simple rhume etc.





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

## **Les avantages :**

- ✓ Efficaces au téléphone.
- ✓ Rapide et efficace.
- ✓ Acceptées par les personnes.
- ✓ La dynamique des ondes produites est unique.

## **Les inconvénients :**

- ✓ Sensible au bruit ambiant.
- ✓ Sensible à l'état physique et émotionnel et médical de l'individu.
- ✓ Vulnérable aux attaques (faciles à falsifier).

### **I.4.2.3. 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.... [02]



**Figure I.11** : Dynamique de frappe au clavier

## **Les avantages :**

- ✓ Peu onéreux.
- ✓ Plus facilement accepté par les utilisateurs.
- ✓ Sécurité bien précise.
- ✓ Elle est non intrusive, geste naturel pour un individu.

## **Les inconvénients :**

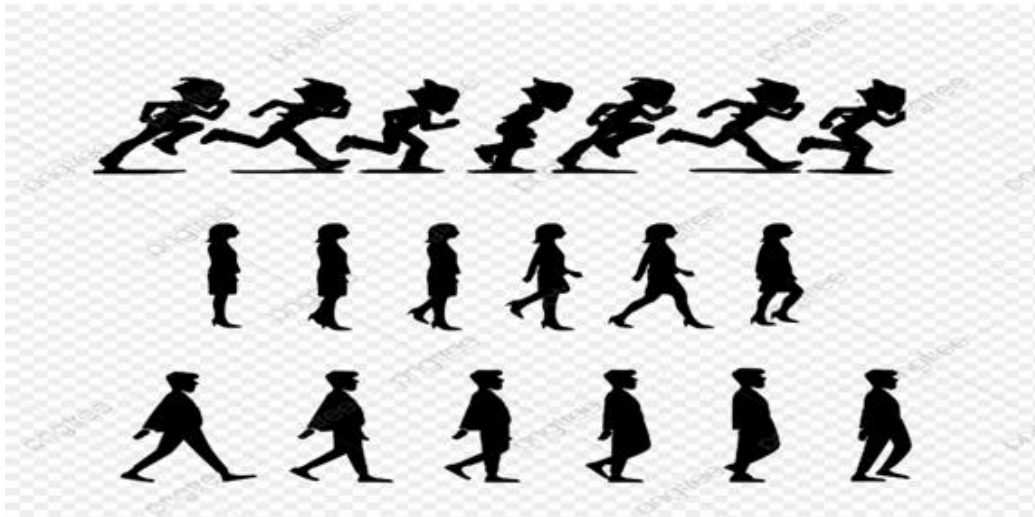
- ✓ N'est pas unique pour chaque individu.
- ✓ Elle dépend de l'état (physique, émotion, fatigue...).

### **I.4.2.4. La Démarche :**

La biométrie de la marche est une biométrie basée sur la marche d'être humain. Ça devrait être mentionné que la marche n'est pas affectée par la rapidité de la personne. Certains scientifiques distinguent la démarche de la reconnaissance de la démarche, soulignant que la démarche peut être observée comme une combinaison cyclique de mouvements qui entraîne la locomotion humaine et la reconnaissance de la démarche est de certain style de propriété de la marche, la pathologie, etc.

Les paramètres communs de l'analyse de la marche sont [08] :

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



**Figure I.12 :** La Démarche

## **Les avantages :**

- ✓ Très acceptable par les individus.

## **Les inconvénients :**

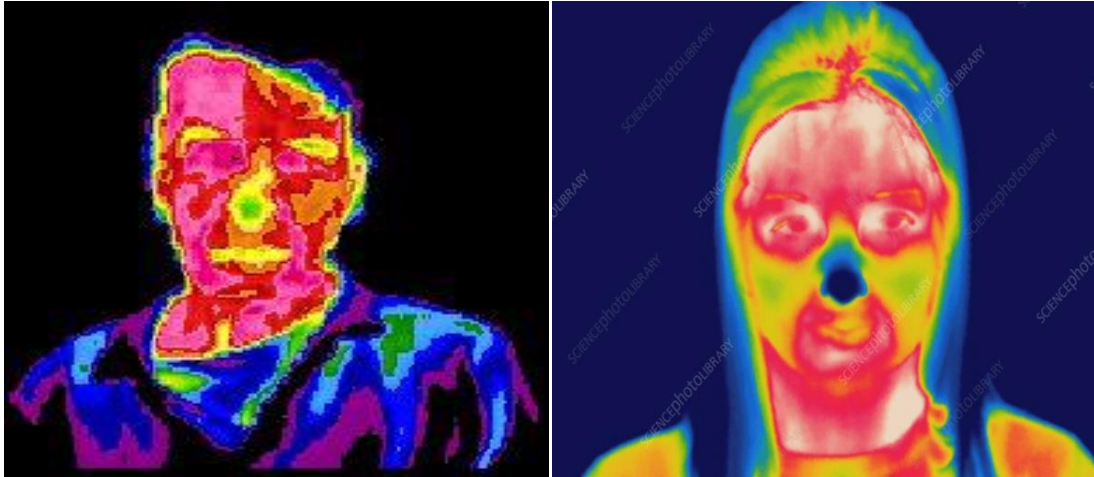
- ✓ Des vêtements amples, peuvent compromettre une bonne identification.
- ✓ On peut tromper ce système facilement.
- ✓ N'est pas permanente (âge, fatigue, maladie).
- ✓ Affectées par le changement de l'environnement.

## **I.4.3. Modalités biologiques :**

Cette catégorie s'appuie sur l'analyse de caractéristiques biologiques de l'individu. La prémisse à ce type d'analyse est que la donnée biologique de chaque individu constitue une signature personnelle.

### **I.4.3.1. Le thermo gramme facial :**

La quantité de chaleur émise par les différentes parties du visage caractérise chaque individu. Elle dépend de la localisation des veines mais aussi de l'épaisseur du squelette, la quantité de tissus, de muscles, de graisses, etc. Pour capturer l'image, il est possible d'utiliser un appareil photo ou une caméra numérique dans le domaine de l'infrarouge, la capture peut se faire dans des conditions d'éclairage différentes même dans le noir complet.[13]



**Figure I.13** : Le thermo gramme facial

## Les avantages :

- ✓ Cette technologie est non intrusive, et peut même se dérouler à l'insu de l'utilisateur pour la vidéo.
- ✓ 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.
- ✓ Possibilité de distinguer des jumeaux.

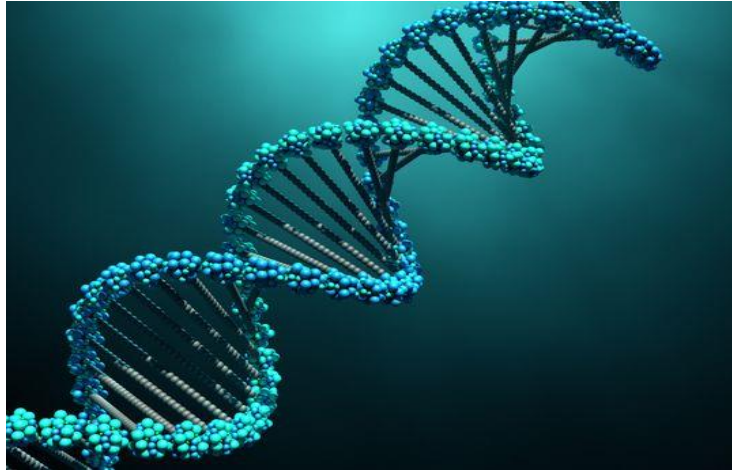
## Les inconvénients :

- ✓ Une étude américaine montrée qu'un changement d'angle de 45° de la caméra rendait le système quasi inutilisable. Du coup, plusieurs aéroports ont abandonné la technique.
- ✓ Influencée par des facteurs tels que la température du corps et l'état émotionnel.

### I.4.3.2. L'ADN :

L'analyse des empreintes génétiques est devenue en quelques années l'un des outils majeurs de la criminalistique, la science de l'identification des indices matériels. L'analyse de l'ADN est couramment utilisée en criminologie pour identifier une personne à partir d'un morceau de peau d'un cheveu ou d'une goutte de sang. [08]

La génétique a permis de démontrer que l'ADN (acide désoxyribonucléique) est la particularité la plus fiable pour identifier une personne.



**Figure I.14** : Acide Désoxyribonucléique ADN

## **Les avantages :**

- ✓ Cette modalité est unique et permanente durant toute la durée de vie.
- ✓ Distinguer les individus avec une grande précision.
- ✓ Il facilite la détection des délinquants.
- ✓ Il est impossible de trouver deux personnes qui ont le même ADN.

## **Inconvénients :**

- ✓ Lente pour obtenir les résultats.
- ✓ Avoir un coût élevé.

### **I.4.3.3. Veines des mains :**

Avec la biométrie du réseau veineux, la reconnaissance de l'identité est réalisée avec la paume de la main, et plus précisément le motif et le flux veineux. Le motif et le flux restent identiques de la petite enfance à la mort, et sont clairement identifiables. Grâce à un scanner infrarouge et une caméra grand angle intégrée, le système capte, en quelques millisecondes, la structure veineuse et donc l'identité univoque d'une personne enregistrée.[11]



**Figure I.15 :** a) Dispositif de reconnaissance par veines des mains ; b) Image de la veine des mains

## Les avantages :

- ✓ Il n'existe aucun moyen de frauder, car on ne peut pas "photographier" les veines de la main. Parce que Le réseau vasculaire est propre à chaque individu (même les vrais jumeaux en ont un différent).
- ✓ Il n'y a aucun contact lors de l'authentification comme avec les empreintes digitales, donc pas de problème d'hygiène.
- ✓ Le TFA - taux de fausses acceptations est de moins de 0,00008% Selon Fujitsu, qui a comparé 140 000 paumes de main.

## Les inconvénients :

- ✓ Le scanner est relativement encombrant comparé aux capteurs d'empreintes digitales.
- ✓ Très coûteuse.

## I.5. Architecture d'un système biométrique :

Dans ces jours les systèmes biométriques sont de plus en plus utilisés aux dernières années. En général, un système de reconnaissance des personnes basé sur leurs descripteurs biométriques peut se décomposer en deux phases, phase d'enrôlement (création de la base de données) et phase de reconnaissance (phase de test).[13]

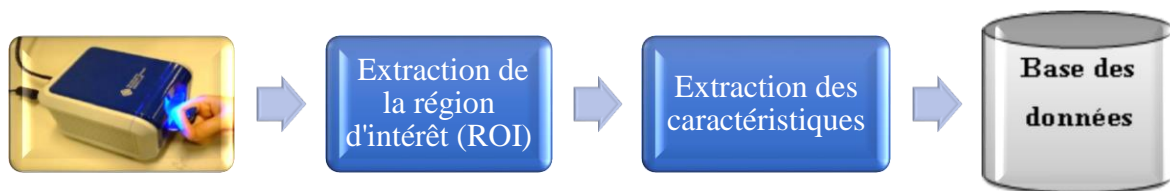
En effet, il existe deux phases : la phase d'entraînement (la phase d'enrôlement) et la phase de test (la phase de reconnaissance).



## I.5.1. Phase d'entraînement :

La phase d'entraînement est une phase d'apprentissage qui a pour but de recueillir des informations biométriques sur les personnes à identifier. Typiquement, les données biométriques acquises par module de capture (une caméra de sécurité, un lecteur d'empreintes digitales, etc.) sont traitées par le module d'extraction de caractéristiques afin d'extraire des traits saillants et distinctifs pour chaque individu. [14]

A travers cette phase, les caractéristiques biométriques des personnes sont saisies par un capteur biométrique, puis représentées sous forme numérique (signatures), et enfin stockées dans la base de données.[04]



**Figure I.16 :** Architecture du mode d'entraînement d'un système biométrique.

## I.5.2. Phase de reconnaissance (phase de test) :

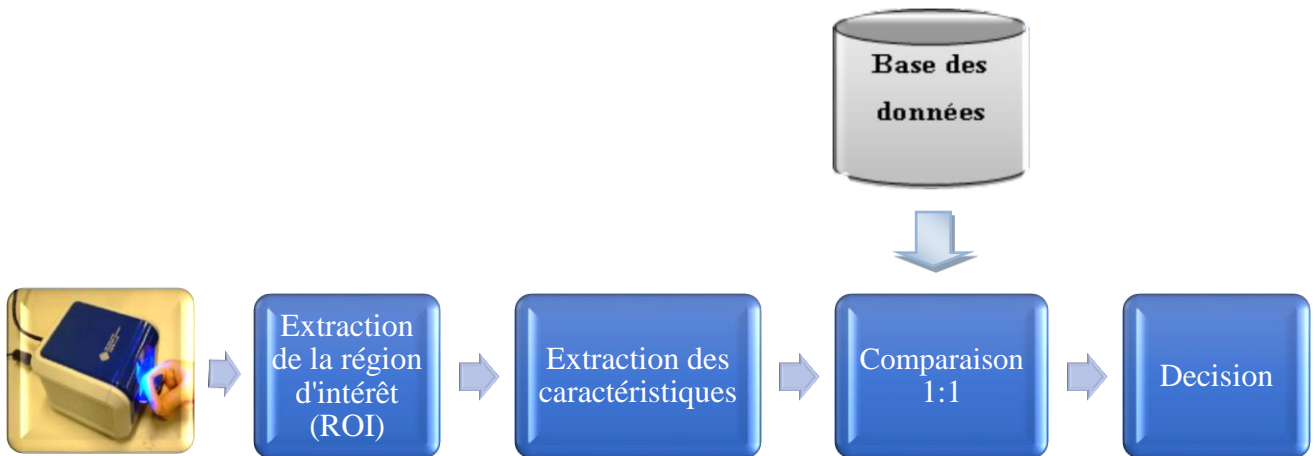
La donnée biométrique acquise par personne de test est comparée avec les données stockées par le module de comparaison. La détermination de l'identité de l'utilisateur se fait par le module de décision [14]. Cette phase peut être décomposée en deux modes :

### I.5.2.1. Mode vérification (authentification) :

Dans ce cas, le système compare la donnée de test (de la personne de test) avec la donnée biométrique stockée dans la base de données pour vérifier l'identité déclarée. [13]

Dans ce système une personne qui désire être identifié réclame une identité, en général par l'intermédiaire d'un PIN, d'un nom d'utilisateur, d'une carte d'identité etc. [10]

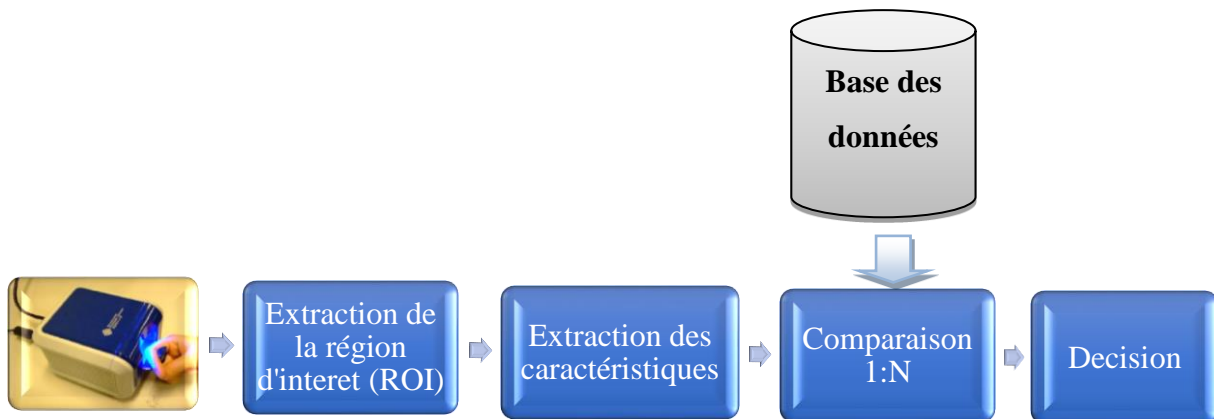
Dans ce type de système, la comparaison n'est faite qu'une fois, il effectue alors une comparaison on appariement (1 : 1) afin de déterminer si la déclaration est vraie ou non.



**Figure I.17 :** Architecture du mode vérification d'un système biométrique.

## I.5.2.2. Mode identification :

Dans ce cas, le système compare la donnée de test avec toutes les références stockées dans la base de données et sert ensuite à prendre une décision à partir de la sortie du module de comparaison (voir **Figure 1.18**), appelée aussi one-to-many (1:N). [14]



**Figure I.18 :** Architecture du mode identification d'un système biométrique.

## I.6. Principaux modules du système biométrique

### I.6.1. Module d'acquisition biométrique :

La capture est la première étape dans le processus. Il faut réussir à capter l'information pertinente sans bruit. Dans une application, l'acquisition des données biométriques : certaines caractéristiques



physiologiques, comportementales ou biologiques peuvent être de type et de nature différente et dépendent de ce que l'on recherche. Dans la partie de l'acquisition des données, suivant la nature de donnée, un capteur est nécessaire (un appareil de photo, un lecteur d'empreintes digitales, une caméra de sécurité...etc.) pour acquérir le signal puis faire la conversion en un format numérique pour qu'il soit traitable par un système informatique. Le but de cette étape est d'obtenir une représentation des formes à traiter qui soit manipulable en machine.[06] [02]

## **I.6.2. Module d'extraction de la région d'intérêt (ROI) :**

C'est la deuxième étape du processus. A ce stade, les points les plus importants et les plus basiques sont identifiés (ces points sont considérés comme des points de connexion) et extraits des données biométriques.

## **I.6.3. Module base de données :**

Le module du stockage qui contient les modèles biométriques des utilisateurs enrôlés du système.

## **I.6.4. Module 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. [08]

Le module d'extraction des caractéristiques Crée un paradigme numérique afin de représenter la donnée biométrique acquise. Ce paradigme, sera conservé sur la base de données.

## **I.6.5. Module comparaison :**

Dans ce module, les caractéristiques biométriques extraites sont comparées les caractéristiques biométriques d'un individu soumise à contrôle avec les modèles biométrique enrôlés du système par conséquent détermine le degré de similitude (ou la différence). [13]

## **I.6.6. Module de décision :**

Dans cette étape finale, on doit aboutir à une décision sur l'identité de la personne à reconnaître. Pour le faire dans le mode vérification d'identité, le score de similarité entre les caractéristiques extraites et les modèles stockés, est comparé à un seuil de décision fixé en avance pour répondre à la question : acceptée comme " utilisateur légitime" ou rejetée comme un "imposteur".

## I.7. Les limitations des systèmes biométriques monomodaux :

Les systèmes biométriques qui fonctionnent en utilisant n'importe qu'elle caractéristique seule (systèmes biométriques monomodale) ont les limites suivantes :

- ✓ Bruit introduit par le capteur.
- ✓ Les variations d'intra-classe.
- ✓ Non-universalité.
- ✓ Les attaques.
- ✓ Manque d'individualité.

## I.8. La multi modalité :

Pour améliorer les performances de reconnaissance devraient diminuer les limitations vues au précédemment par la multi modalité.

### I.8.1. Définition de la biométrie de multi modalité :

La multi modalité est la combinaison de plusieurs modalités biométriques différentes ce qui implique l'utilisation d'information complémentaires. En augmentant la quantité d'information discriminante de chaque personne, on souhaite augmenter le pouvoir de reconnaissance.

### I.8.2. Les différents multi-possibles :

#### I.8.2.1. Multi-capteurs :

Lorsqu'ils associent plusieurs capteurs pour acquérir la même modalité.



Figure I.19 : Multi-capteurs : capteur optique et capteur thermique

#### I.8.2.2. Multi-instances :

Lorsqu'ils associent plusieurs instances de la même biométrie.



Figure I.20 : La biométrie de multi-instances

### I.8.2.3. Multi-algorithmes :

Lorsque plusieurs algorithmes traitent la même image acquise, cette multiplicité des algorithmes peut intervenir dans le module d'extraction en considérant plusieurs ensembles de caractéristiques et/ou dans le module de comparaison en utilisant plusieurs algorithmes de comparaison.

### I.8.2.4. Multi-échantillons :

Lorsqu'ils associent plusieurs échantillons différents de la même modalité, dans ce cas les données sont traitées par le même algorithme mais nécessitent des références différentes à l'enregistrement contrairement aux systèmes multi-instances qui ne nécessitent qu'une seule référence.



Figure I.21 : Multi-échantillons : Iris droit et iris gauche

### I.8.2.5. Multi-biométries :

Lorsque l'on considère plusieurs biométries différentes.



**Figure I.22** : Multi-biométries : L'iris et l'empreinte digitale

### **I.8.3. Les avantages de la Multimodalité :**

- ✓ Précision.
- ✓ Non-universalité.
- ✓ La flexibilité.
- ✓ Données bruyantes.
- ✓ Sécurité.

### **I.9. Les applications de la biométrie :**

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 [02] :

#### **I.9.1. Applications commerciales :**

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

#### **I.9.2. Applications de gouvernement :**

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

#### **I.9.3. Applications juridiques (légal) :**

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

## I.10. Evaluation des performances des Systèmes biométrique :

Les systèmes biométriques ne donnent pas une réponse précise sur l'image à reconnaître mais une réponse relative qui s'exprime par un taux de similitude qui n'atteint jamais 100%. Donc il est impossible d'obtenir une coïncidence absolue entre l'image de référence stocké dans la base des données créé lors de l'apprentissage et celle créé lors de la reconnaissance. Pour cela la mesure de la performance d'un système de RDF est une étape importante dans la conception de ce type de système.[06]

### I.10.1. Evaluation de la vérification (les mesures des taux d'erreur) :

Alors le système biométrique doit déterminer si l'identité par l'utilisateur est acceptée ou rejetée.

Deux taux sont alors calculés :

#### I.10.1.1. Le FAR (False Acceptance Rate) :

C'est le taux en pourcentage de personnes non autorisées (imposteurs) qui sont acceptées par erreur.

Si l'accès d'imposteurs doit absolument être évité [06], Il est exprimé par la relation suivante :

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

#### I.10.1.2. Le FRR (False Reject Rate):

Ce taux détermine la probabilité pour qu'un système ne reconnaisse pas une personne qui normalement aurait dû être reconnue [04], Il est exprimé par la relation suivante :

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

Le taux le plus simple pour mesurer la performance d'un algorithme dans le contexte de la Vérification est de calculer le point d'équivalence des erreurs (Equal Error Rate ou EER).

#### I.10.1.3. Taux d'égale erreur (Error Equal Rate EER) :

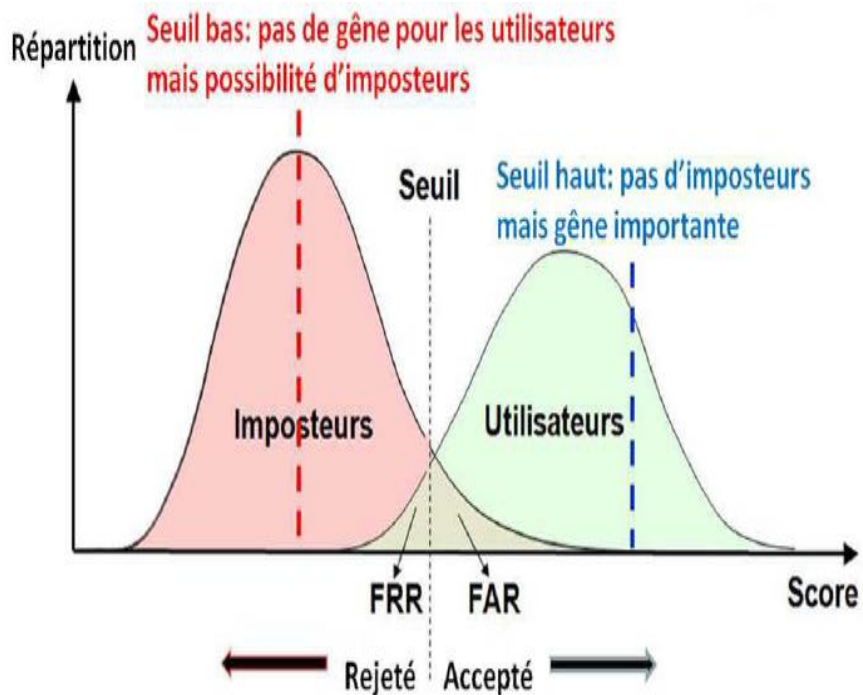
Ce taux est calculé à partir de FAR et FRR et constitue un point de mesure de performance courant.

[16]

# Chapitre I : Généralité sur la biométrie

$$\text{EER} = \frac{\text{nombre de fausses acceptations} + \text{nombre de faux rejets}}{\text{nombr totale d'accès}} \quad (\text{I.3})$$

La figure suivante représente la distribution théorique des taux de vraisemblance des utilisateurs légitimes et des imposteurs. Les deux taux d'erreurs, FAR et FRR, sont liés et dépendent d'un seuil de décision qui doit être ajustée en fonction caractéristique ciblée du système biométrique haute ou basse sécurité. [15]



**Figure1.23** : Illustration du FRR et du FAR [15]

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. Dans cette figure, le point  $\bullet$  représente le Seuil correspondant au point d'équivalence des erreurs. [10]

# Chapitre I : Généralité sur la biométrie

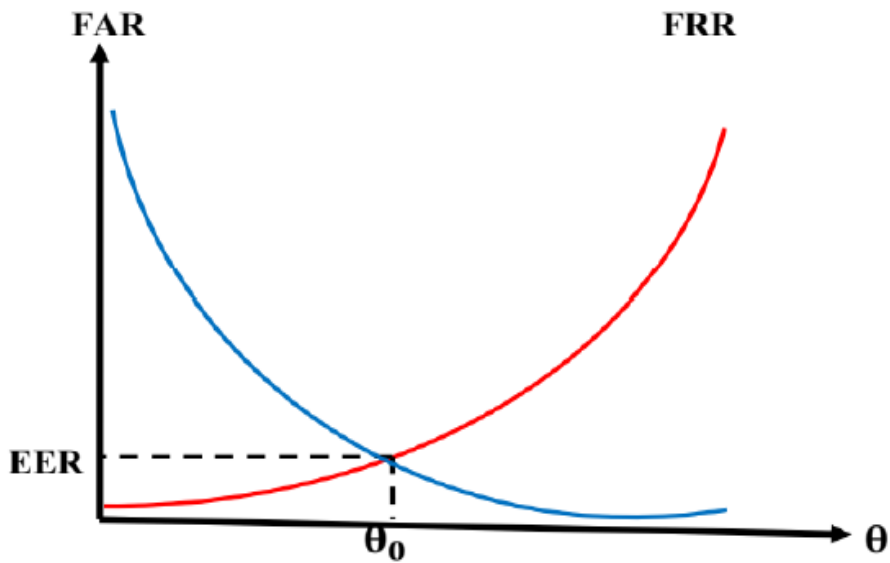


Figure1.24 : Courbe du point d'équivalence des erreurs dans un système biométrique [02]

Cette courbe illustre la relation entre le FRR et le FAR. Elle est obtenue en faisant varier le seuil de décision et en calculant à chaque fois les deux valeurs FRR et FAR. La Figure I.25 illustre un exemple de la courbe DET.[16]

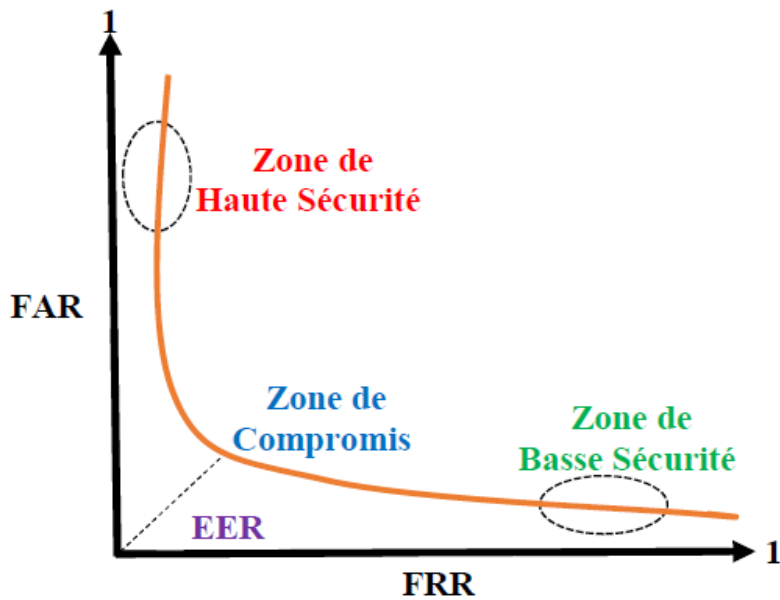
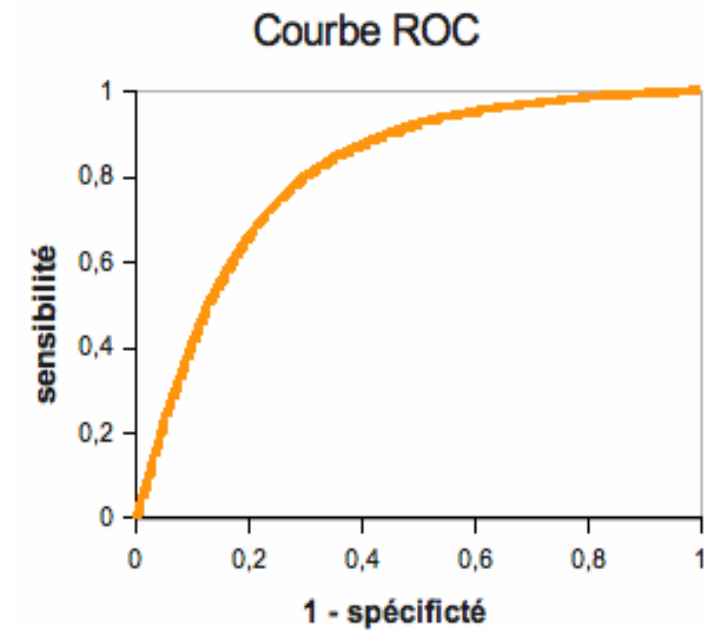


Figure1.25 : Courbe DET.[16]

# Chapitre I : Généralité sur la biométrie

Cette courbe permet de représenter graphiquement les performances d'un système de vérification pour les diverses valeurs de  $\theta$ . 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.[10]



**Figure1.26** : Courbe ROC [14]

## I.11.Conclusion :

Dans ce chapitre, nous avons présenté les différents concepts de la biométrie, en donnant quelques définitions élémentaires portant sur ce sujet, et qui seront sûrement des points essentiels dans la suite de notre travail. Nous avons également présenté quelques aspects de l'architecteur, principale module et évaluation des performances des systèmes biométrique.





# *Chapitre II*

*L'empreinte de l'articulation de doigt  
(FKP)*



### II.1. Introduction :

Nous parlons dans ce chapitre sur l'empreinte de l'articulation du doigt (FKP). Nous allons également discuter sur les méthodes de prétraitement telles que SQL, ASSR et DOG. Les méthodes d'extraction des caractéristiques biométriques telles que PCA, LDA, Log Gabor, BSIF, LPQ et RI LPQ. Et enfin les méthodes de classification telles que KNN et SVM.

### II.2. Les modalités biométriques liées à la main :

Les traits biométriques basés sur la main peuvent être divisés en deux grandes catégories [02] :

Les unes appartenant à la partie palmée et les autres à la partie dorsale de la main.

- ✓ **La partie palmée** : est la partie intérieure et saisissante de la main. Les attributs biométriques largement utilisés extraits de cette partie sont :
  - ✓ Empreinte digitale (finger print).
  - ✓ Empreinte palmaire (palmprint).
  - ✓ Les réseaux veineux (palm vein, finger vein).
  - ✓ Les motifs d'articulation de doigt sur la face de la paume de la main (finger inner knuckle print IKP).
- **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 de doigts (finger geometry).
- ✓ Les réseaux veineux (dorsal hand vein).
- ✓ Les motifs d'articulation du doigt sur la partie dorsale de la main (Finger dorsal knuckle print FKP).



Figure II .1 : La main : face dorsale et face palmaire

### II.2.1. La biométrie FKP :

Récemment, les chercheurs en biométrie ont découvert que l'empreinte de l'articulation de doigt (FKP), qui fait référence aux motifs inhérents à la surface externe autour de l'articulation phalangienne de doigt, est très unique et peut servir d'identificateur biométrique distinctif.

La technologie des empreintes digitales nécessite des images haute résolution (>400 dpi) pour un meilleur résultat de reconnaissance, En plus Les rides et les ridules peuvent également être clairement visibles à l'FKP dans les images de faible résolution.[02]

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. La surface externe d'un doigt a trois jointures classées en articulations majeure et mineure [02] :

- ✓ Première FKP mineure
- ✓ FKP majeur
- ✓ Deuxième FKP mineure

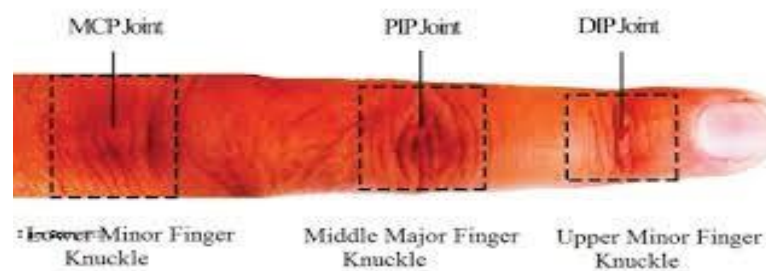


Figure II.2 : Les trois jointures d'un doigt [02]

### II.3. Les algorithmes utilisés dans le système biométrique :

#### II.3.1. Les méthodes de prétraitement :

Dans l'étape de prétraitement, nous évitons les informations inutiles par la correction des erreurs, l'homogénéisation des données, la normalisation de la taille et la segmentation, la localisation et l'extraction de la région d'intérêt.

Les algorithmes les plus utilisés pour le prétraitement sont :

- ✓ SQI (Self-Quotient Image).
- ✓ ASSR (adaptive single scale retinex).
- ✓ DOG (Difference of Gaussians).

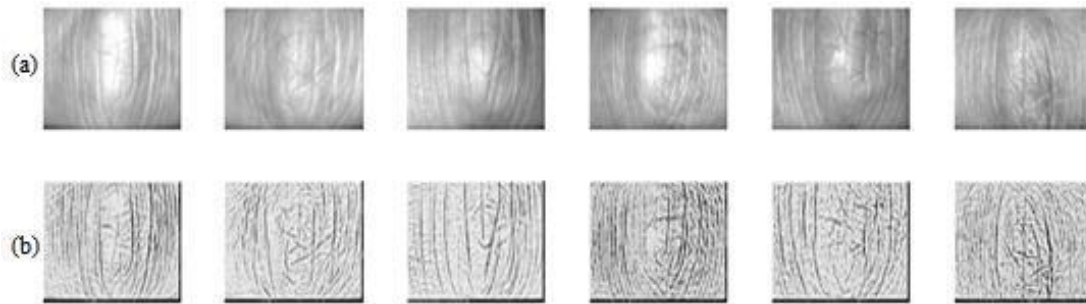
##### II.3.1.1. Algorithme du d'image auto-quotient (SQI) :

L'algorithme SQI a été introduit par Wang dans le domaine de la reconnaissance faciale. En général, l'image  $Q$  d'auto-quotient de l'image  $I$  est définie par :

$$Q = \frac{I}{\hat{I}} = \frac{I}{F * I} \quad (\text{II.1})$$

Où  $\hat{I}$  est la version lissée de  $I$ .  $F$  est les noyaux de lissage, et la division n'est point-sage comme dans l'image de quotient d'origine.

Nous appelons  $Q$  l'image du quotient dérivée de l'image que je lui-même plutôt que des images d'une personne différente comme dans  $Q$ . [17]



**Figure II.3 :** (a) Images de FKPs.

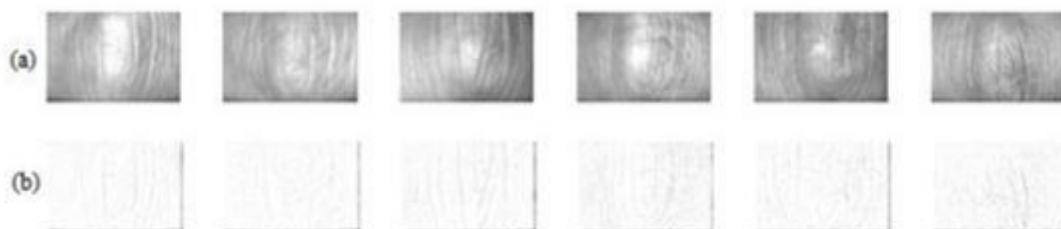
(b) Leur réflectances images en utilisant algorithme de SQR [14]

### II.3.1.2. Algorithme de retinex adaptatif à échelle unique (ASSR) :

L'algorithme adaptatif de retinex à échelle unique (ASSR) est l'un des plus récents ajouts aux techniques de retinex et a été proposé par Park et al. La technique ASSR est implémentée dans la boîte à outils avec une fonction qui possède le prototype suivant :

$[R, L] = \text{adaptive\_single\_scale\_retinex}(X, T, S, h, \text{normalise})$

Où :  $X$  désigne l'image à l'échelle grise d'entrée à traiter,  $T$  représente le nombre d'itérations effectuées pendant le traitement, et  $S$  et  $h$  représentent les paramètres nécessaires à la technique. L'argument d'entrée  $\text{normalise} \in \{1,0\}$  signifie un paramètre contrôlant si une procédure de post traitement est appliquée à l'image normalisée ou non. Le lecteur est renvoyé au document original pour plus d'informations sur les paramètres.[18]



**Figure II.4 :** (a) images de FKPs, (b) Leur réflectances images en utilisant algorithme de ASSR [14]

### II.3.1.3. Le filter Dog (Difference of Gaussians):

En science de l'imagerie, la différence des gaussiens (DoG) est un algorithme d'amélioration des fonctionnalités qui implique la soustraction d'une version floue d'une image originale d'une autre version moins floue de l'original. Et c'est un filtre passe-bande qui rejette presque toutes les fréquences spatiales présentes dans l'image d'origine en niveaux de gris. Les images floues sont obtenues en convoluant les images en niveaux de gris d'origine avec des noyaux gaussiens ayant des écarts types différents. Le flou d'une image à l'aide d'un noyau gaussien supprime uniquement l'espace à haute fréquence information. La soustraction d'une image de l'autre préserve les informations spatiales situées entre la plage de fréquences conservée dans les deux images floues. [19]

À la première ; l'image est lissée par convolution avec un noyau gaussien d'une certaine largeur  $\sigma_1$ :

$$G_{\sigma_1}(x, y) = \frac{1}{\sqrt{2\pi\sigma_1^2}} \exp\left(-\frac{x^2+y^2}{2\sigma_1^2}\right) \quad (\text{II.2})$$

Obtenir :  $\mathbf{g}_1(x, y) = G_{\sigma_1}(x, y) * f(x, y) \quad (\text{II.3})$

Avec une largeur différente  $\sigma_2$ , une seconde image lissée peut être obtenue :

$$\mathbf{g}_2(x, y) = G_{\sigma_2}(x, y) * f(x, y) \quad (\text{II.4})$$

Où :  $G$  : convolution avec un noyau gaussien d'une certaine largeur.

$g$  : une image lissée gaussienne.

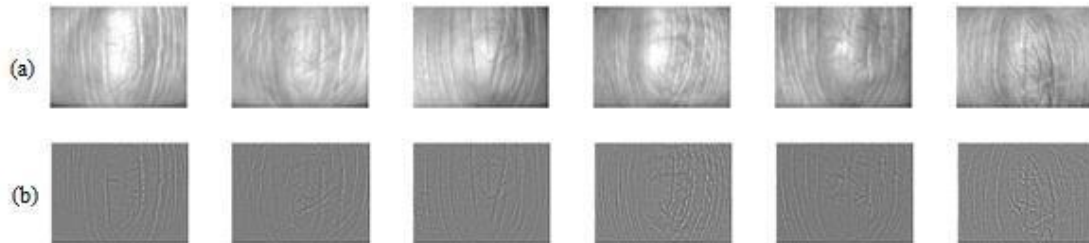
Nous pouvons montrer que la différence de ces deux images lissées gaussiennes, appelée différence de gaussienne (DoG), peut être utilisée pour détecter les contours de l'image.

$$\begin{aligned} \mathbf{DOG} &= g_1(x, y) - g_2(x, y) = G_{\sigma_1} * f(x, y) - G_{\sigma_2} * f(x, y) \\ &= (G_{\sigma_1} - G_{\sigma_2}) * f(x, y) = \mathbf{DoG} * f(x, y) \quad (\text{II.5}) \end{aligned}$$

Le DoG en tant qu'opérateur ou noyau de convolution est défini comme :

$$\mathbf{DoG} \triangleq G_{\sigma_1} - G_{\sigma_2} = \frac{1}{\sqrt{2\pi}} \left( \frac{1}{\sigma_1} e^{-\frac{(x^2+y^2)}{2\sigma_1^2}} - \frac{1}{\sigma_2} e^{-\frac{(x^2+y^2)}{2\sigma_2^2}} \right) \quad (\text{II.6})$$

En tant que différence entre deux images filtrées passe-bas différemment, le DoG est en fait un filtre passe-bande, qui supprime les composants hauts fréquence représentant le bruit, ainsi que certaine composante basse fréquence représentant les zones homogènes de l'image. On suppose que les composantes de fréquence dans la bande passante sont associées aux bords des images.



**Figure II.5 :** (a) Images de FKPs. (b) Leur images filtrées par un filtre DoG[14]

### II.3.2. Extraction des caractéristiques :

L'étape de l'extraction des paramètres représente le cœur du système de reconnaissance des formes. Ayant une image ou une voix en entrée, une étape de segmentation permet d'extraire la caractéristique dont le processus d'authentification a besoin, elle consiste à effectuer le traitement de l'image dans un autre espace de travail plus simple et qui assure une meilleure exploitation de données, et donc permettre l'utilisation, seulement, des informations utiles, discriminantes et non redondantes.[20]

Il existe trois grandes méthodes dans l'extraction des caractéristiques, sont : méthode globale, local et hybride.

- Méthode globale :** dans laquelle on analyse l'image dans son entier ; les algorithmes : PCA, LDA...

#### II.3.2.1. L'analyse en Composantes Principales (PCA) :

PCA est une méthode de baisse de dimensionnalité qui est souvent utilisée pour concision la dimensionnalité de gros ensembles de données, en transformant un grand ensemble de changeables en un plus petit qui contient encore la plupart des informations du grand ensemble.

Concision le nombre de variables d'un ensemble de données se fait naturellement au détriment de la précision, mais l'astuce dans la réduction de la dimensionnalité est de troquer un peu de précision pour la simplicité. Parce que les ensembles de données plus petits sont plus faciles à explorer et à visualiser et que l'analyse des données est beaucoup plus simple et plus rapide pour les algorithmes d'apprentissage automatique sans variables étrangères à traiter.

## Chapitre II : L'empreinte de l'articulation de doigt (FKP)

Donc, pour résumer, l'idée de l'ACP est simple : réduire le nombre de variables d'un ensemble de données, tout en préservant autant d'informations que possible. [21]

### II.3.2.2. L'analyse Discriminante Linéaire (LDA) :

La LDA est une méthode d'analyse numérique qui autoriser de chercher la combinaison linéaire des variables qui représentent au mieux les données, elle est très utilisée dans le domaine de la reconnaissance des formes à savoir la reconnaissance de visage. Elle permet de maximiser la dispersion inter-classes (the between-class scatter) et de réduire l'éparpillement intra classes (the within-class scatter).

L'Analyse Discriminante Linéaire (LDA) est utilisée pour trouver la combinaison linéaire des caractéristiques qui séparent le mieux les classes d'objet ou d'événement. Les combinaisons résultantes peuvent être utilisées comme classificateur linéaire, ou généralement dans la réduction de caractéristiques avant la classification postérieure.

LDA essaie explicitement de modéliser la différence entre les classes de données contrairement à l'ACP qui ne tient pas compte des différences entre les classes.

Par exemple : Chaque visage, qui se compose d'un grand nombre de pixel, est réduit à un plus petit ensemble de combinaisons linéaires avant la classification. Chacune des nouvelles dimensions est une combinaison linéaire des valeurs de pixel, qui forment un Template. Les combinaisons obtenues en utilisant LDA s'appellent les fisherfaces. [22]

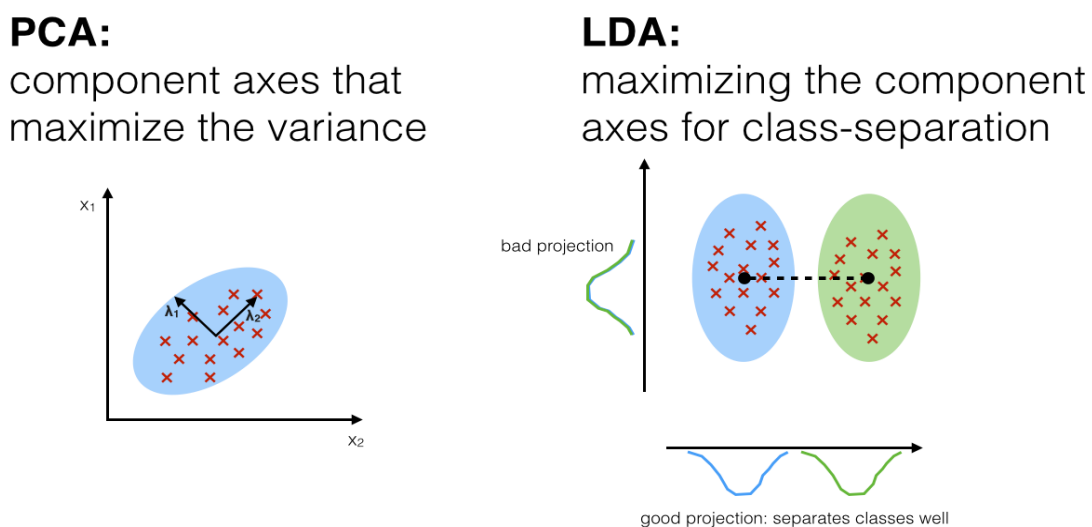


Figure II.6 : Méthode globale : PCA et LDA



- **Méthode locale** : basé sur un modèle, dans laquelle le système essaie de détecter, regrouper et reconnaître les différents éléments constitutifs de l'image, les algorithmes : Gabor, log-Gabor, LBP, LPQ, TPLBP, BSIF, HOG....

### II.3.2.3. Filtre de log-Gabor :

Les filtres de Gabor sont un choix traditionnel pour obtenir des informations de fréquence localisées. Ils offrent la meilleure localisation simultanée des informations spatiales et fréquentielles. Cependant, ils ont deux limitations principales. La bande passante maximale d'un filtre de Gabor est limitée à environ une octave et les filtres de Gabor ne sont pas optimaux si l'on recherche des informations spectrales larges avec une localisation spatiale maximale.

Bien que le filtre de Gabor réalise un sentiment d'optimalité en termes de compromis espace-fréquence, dans certaines applications, il peut ne pas être un filtre idéal. À certaines bandes passantes, le filtre Gabor a un composant DC non nul. Cela signifie que la réponse du filtre dépend de la valeur moyenne du signal. Si la sortie du filtre doit être utilisée pour une application telle que la reconnaissance de formes, ce composant DC n'est pas souhaitable car il donne une fonctionnalité qui change avec la valeur moyenne. [23]

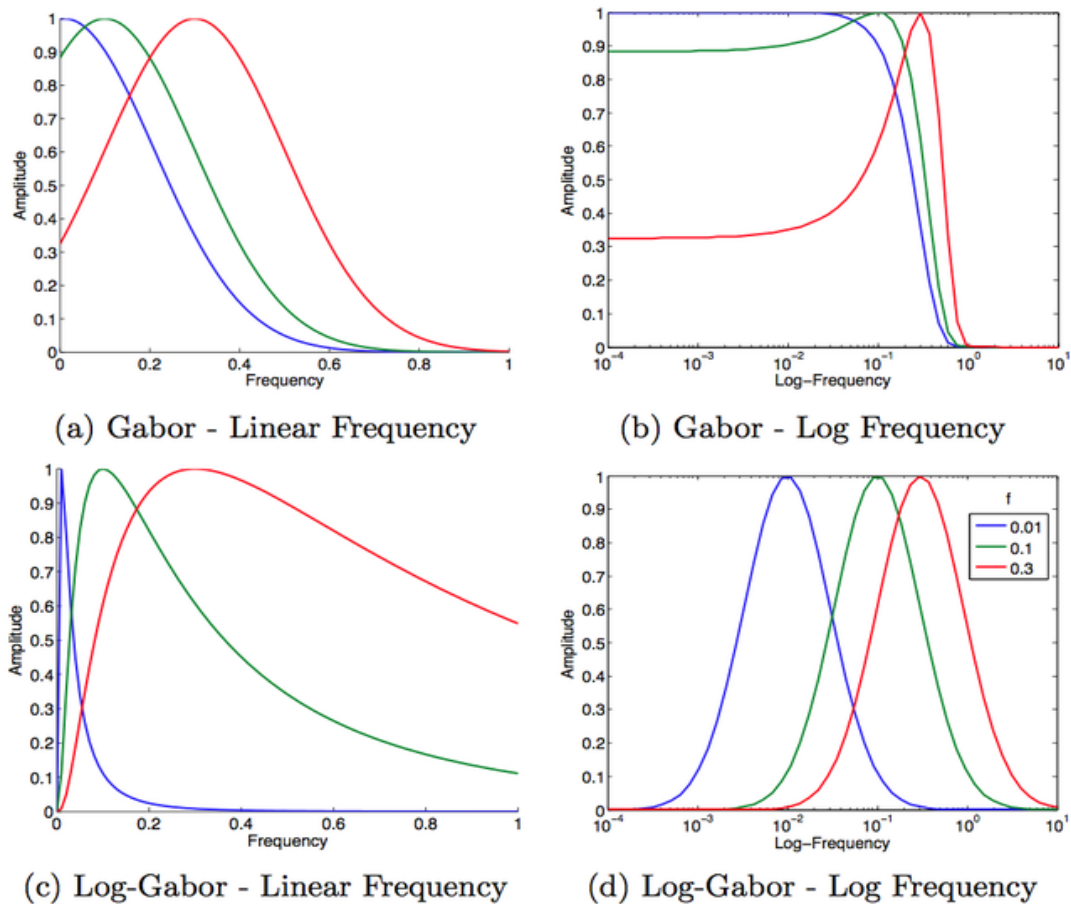
Une alternative à la fonction de Gabor est la fonction log-Gabor proposée par Field [1987]. Field suggère que les images naturelles sont mieux codées par des filtres qui ont des fonctions de transfert gaussiennes lorsqu'elles sont visualisées sur l'échelle de fréquence logarithmique. (Les fonctions de Gabor a des fonctions de transfert gaussiennes lorsqu'elles sont visualisées sur l'échelle de fréquence linéaire). Sur l'échelle de fréquence linéaire.[24]

La fonction log-Gabor a une fonction de transfert de la forme :

$$\mathbf{G}(\mathbf{f}) = \exp \left\{ \frac{-[\log(f/f_0)]^2}{2[\log(\sigma/f_0)]^2} \right\} \quad (\text{II.7})$$

Où  $f_0$  représente la fréquence centrale et  $\sigma$  donne la bande passante du filtre et le rapport  $\sigma/f_0$  devrait rester constant.

La figure suivante montre la réponse en fréquence du Gabor par rapport au Log-Gabor :



**Figure II.7 :** Différence dans le domaine fréquentiel entre les filtres Gabor et Log-Gabor

### II.3.2.4. Caractéristique d'image statistique binarisées (BSIF):

BSIF est un descripteur local récent pour reconnaître des textures. BSIF descripteur a été mentionné pour la première fois par J. Kannala et E. Rahtu en 2012.

Cette méthode représente une chaîne de code binaire pour les pixels d'une image donnée, lorsque la valeur de code d'un pixel est considérée un descripteur local de l'image entourant le pixel. Donnée une image  $I_p$  et un filtre linéaire  $W_i$  de la même taille, la réponse de filtre  $R_i$  est trouvée comme :

$$R_i = \sum_{m,n} I_p(m,n)W_i(m,n) \quad (\text{II.8})$$

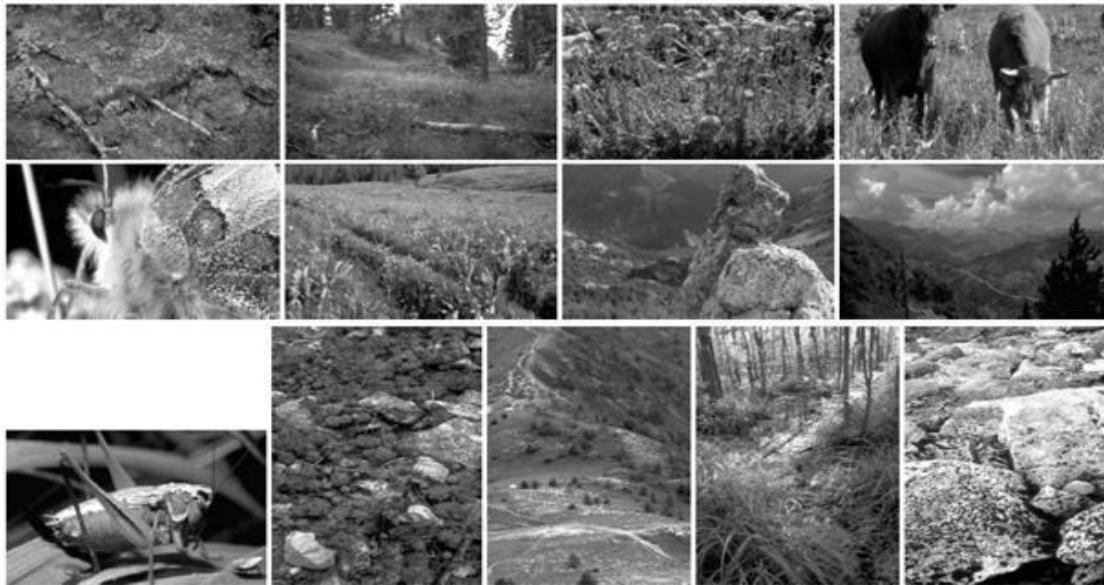
Où  $m$  et  $n$  dénotent la taille du patch PPI et  $W_i$  indique le nombre de filtres linéaires pour tous les

$i = \{1, 2, \dots, n\}$  dont la réponse peut être calculée et binarisée pour obtenir la chaîne binaire suivante :

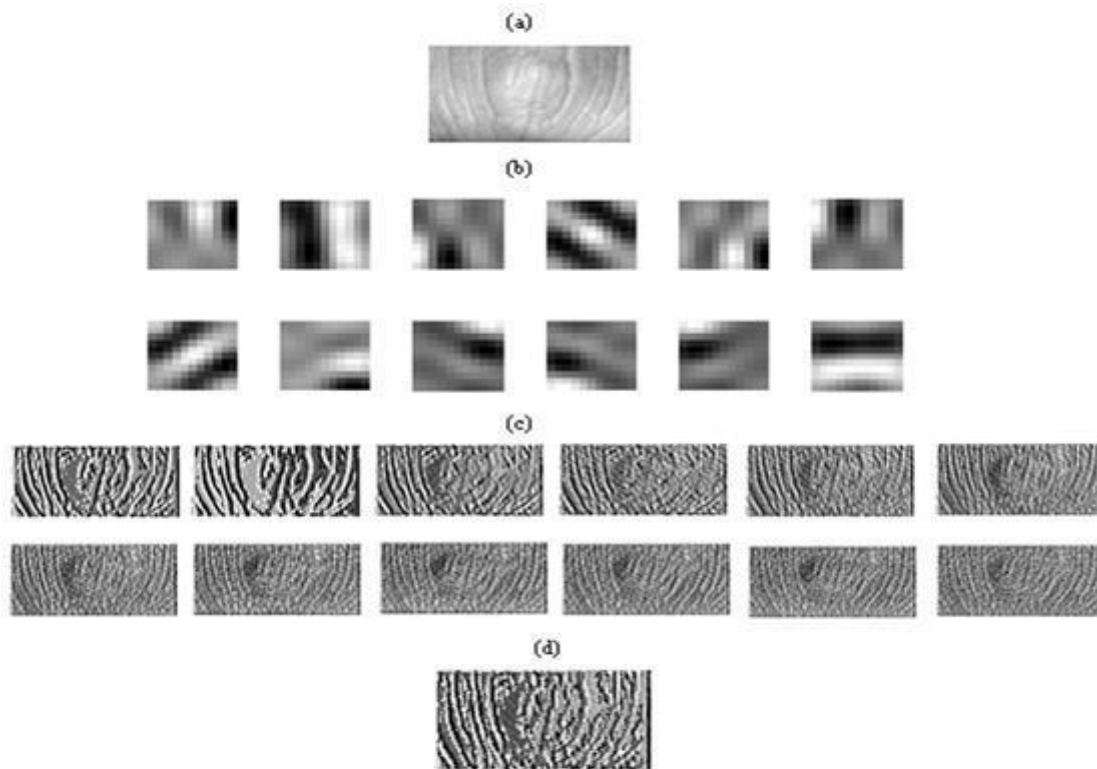
$$b_i = \begin{cases} 1 & , \text{ si } R_i > 0 \\ 0 & , \text{ si } R_i < 0 \end{cases} \quad (\text{II.9})$$

## Chapitre II : L'empreinte de l'articulation de doigt (FKP)

Les codes BSIF sont présentés sous la forme d'un histogramme de pixels codes binaires, qui peuvent effectivement distinguer la texture caractéristique de l'IPP. Taille de filtre et longueur des chaînes de bits sont importants pour évaluer efficacement le descripteur BSIF pour la vérification de l'empreinte de la paume. Dans cette étude, huit tailles de filtre ( $3 \times 3$ ,  $5 \times 5$ ,  $7 \times 7$ ,  $9 \times 9$ ,  $11 \times 11$ ,  $13 \times 13$ ,  $15 \times 15$ , et  $17 \times 17$ ) avec quatre longueurs de bits (6, 7, 9 et 11) ont été évalués.[25]



**Figure II .8 :** Les 13 images naturelles utilisées par J. Kannala et E Rahtu pour l'apprentissage des filtres dans le descripteur BSIF [26]



**Figure II.9 :** (a) Exemple d'image FKP. (b) Filtre BSIF de taille 11x11 et de longueur 12. (c) Les résultats de la convolution de l'image FKP avec un filtre BSIF. (d) Image finale FKP filtrée par BSIF filtre

### II.3.2.5. Quantification de phase locale (LPQ) :

La quantification de la phase locale ou le descripteur LPQ a été désigné pour la première fois par Ojansivu et Heikkilä pour l'utiliser dans la classification de textures pour les images floues. Il permet d'améliorer la classification de textures pour être robuste aux artefacts générés par le flou présent dans une image. Le descripteur LPQ est construit de façon à ne retenir dans une image que l'information locale invariante à un certain type de flou. Il est insensible au flou central symétrique, tel que celui causé par le mouvement linéaire et hors du foyer du capteur.

L'opérateur LPQ est basé sur TF de la phase (TF : transformée de Fourier). L'extraction de l'information de la phase locale est utilisée par l'application de STFT (la transformée de Fourier à court terme) calculée sur un rectangle  $N_x$  de  $M \times M$  voisins pour chaque pixel  $x$  dans l'image  $f(x)$  définie par l'équation suivante [27] :

## Chapitre II : L'empreinte de l'articulation de doigt (FKP)

$$\mathbf{F}(\mathbf{u}, \mathbf{x}) = \sum_{v \in \mathbf{x}} f(x - y) e^{2j\pi \mathbf{u}^T y} = w_{\mathbf{u}} f_x \quad (\text{II.10})$$

Où:  $w_{\mathbf{u}}$  correspond aux vecteurs de base de la décomposition à la fréquence  $\mathbf{u}$ ,  $f_x$  contient toutes les valeurs de l'image appartenant au voisinage  $N_x$ .

La seulement 4 fréquences transformée de Fourier est alors calculée pour :

$$u_i (i = 1, \dots, 4): \mathbf{u}_1 = [a, 0]^T, \mathbf{u}_2 = [0, a]^T, \mathbf{u}_3 = [a, a]^T \text{ et } \mathbf{u}_4 = [a, -a]^T \quad (\text{II.11})$$

Où : représente la fréquence scalaire suffisamment élevée pour  $H_{u_i}$  Supérieur à 0 , alors nous obtenons un vecteurs  $F_x^C$  où :

$$\mathbf{F}_x^C = [F(u_1, x), F(u_2, x), F(u_3, x), F(u_4, x)] \quad (\text{II.12})$$

Par la suite, un quantificateur scalaire simple est utilisé pour l'extraction des informations de la phase dans chaque coefficient de Fourier en observant les signes des parties réelles (*Re*) et imaginaires (*Im*).

Le quantificateur scalaire est donné par l'équation suivante :

$$g_j(x) = \begin{cases} 1 & g_j(x) \geq 0 \\ 0 & \text{ailleurs} \end{cases} \quad (\text{II.13})$$

Où :  $g_j(x)$  représente la  $j^{\text{ième}}$  composante du vecteur  $g_x = [Re \{F_x\}, Im \{F_x\}]$ .

Les huit coefficients binaires obtenus  $q_j(x)$  sont représentés comme des valeurs entières entre 0 et 255 en utilisant un codage binaire simple pour obtenir les étiquettes de LPQ, *FLPQ* qui est définie par :

$$\mathbf{F}_{LPQ}(X) = \sum_{i=1}^8 q_i(x) 2^{i-1} \quad (\text{II.14})$$

En conséquence, nous obtenons l'étiquette d'image, dont les valeurs sont invariantes pour le flou (barbouillage). [27]

La figure suivante présente l'organigramme de l'ensemble des étapes nécessaires à la construction du descripteur LPQ pour une image :

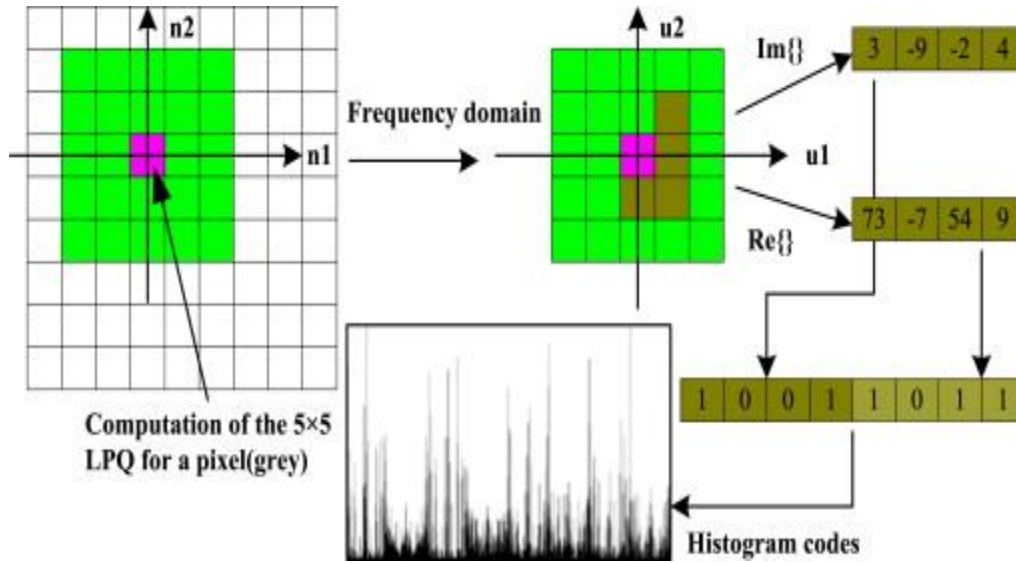


Figure II .10 : Organigramme de l'ensemble des étapes nécessaires du descripteur LPQ [28]

### II.3.2.6. Quantification de phase locale invariante de rotation (RI-LPQ) :

La méthode de quantification locale invariante de phase de rotation (RI\_LPQ) est composée de deux étapes : l'estimation de l'orientation caractéristique et l'extraction de descripteur dirigé.

#### II.3.2.6.a. Estimation de l'orientation caractéristique :

Que  $R_\theta$  soit une matrice de rotation 2D correspondant à angle  $\theta$ , et  $f(x)' = f(R_\theta^{-1}x)$  désignent les Image. Il est un fait connu que la transformation Fourier de  $f'$  est tout simplement la transformation Fourier de  $f$  tourné par  $R_\theta$ . Là s'appliquera aux quartiers circulaires  $N_x$ , dont la position sera en plus de changement à  $x' = R_\theta x$ . Grâce à l'équation (II.10) nous avons :

$$\mathbf{F}(\mathbf{u}, \mathbf{x}) = \sum_y f(y) w_R(x - y) e^{-2j\pi u^T y} \quad (\text{II.15})$$

Où :  $w_R$  est un rectangle  $N_R$ -by- $N_R$ , donné comme :  $w_R(x) = 1$  si  $|x_1|, |x_2| < N_R/2$  et 0 autrement.

Profitant de ce phénomène, nous estimons les coefficients (II.16) sur un cercle de rayon  $r$  aux fréquences :

$$\mathbf{V}_i = r [\cos(\varphi_i) \sin(\varphi_i)]^T \quad (\text{II.16})$$

Où :  $\varphi_i = 2\pi i / M$  et :  $i = 0, \dots, M - 1$

Nous remplaçons en outre la fenêtre rectangulaire  $w_R$  dans (1) par une circulaire gaussienne définie comme :

$$\mathbf{w}_G(\mathbf{x}) = 1/(2\pi\sigma^2) \exp\{-(x_1^2+x_2^2)/(2\sigma^2)\} \quad (\text{II.17})$$

Si :  $|x_1|, |x_2| < N_G/2$  et 0 autrement.

Sur la base des arguments ci-dessus, dans le cas de rotation du vecteur  $V(\mathbf{x})$  :

$$\mathbf{V}(\mathbf{x}) = [F(V_0, \mathbf{x}), \dots, F(V_{M-1}, \mathbf{x})] \quad (\text{II.18})$$

Seront déplacés vers  $x'$ , et il subit un changement circulaire correspondant à l'angle de rotation  $\theta$ , dans la précision de la discrétion  $2\pi/M$ . Notez également qu'en raison de la séparabilité,  $V(\mathbf{x})$  est évaluation efficace pour toutes les positions d'image  $\mathbf{x}$  à l'aide simplement 1-D convolutions pour les lignes et les colonnes successivement.[29]

### II.3.2.6.b. Calcul de LPQ orienté :

Dans la deuxième étape de la méthode, nous extrayons le vecteur de descripteur binaire. La procédure ici est similaire au LPQ d'origine, mais le quartier à chaque emplacement est tourné vers la direction de l'orientation caractéristique. L'opération peut être formulée en définissant coefficients de fréquence orientés comme :

$$\mathbf{F}_\varepsilon(\mathbf{u}, \mathbf{x}) = \sum_y f(y) w_R(R_{\varepsilon(x)}^{-1}(y - x)) e^{-j2\pi u^T R_{\varepsilon(x)}^{-1} y} \quad (\text{II.19})$$

Pour l'image tournée  $f'$  cela devient :

$$\mathbf{F}_\varepsilon(\mathbf{u}, \mathbf{x})' = \sum_y f(y)' w_R(R_{\varepsilon(x)'}^{-1}(y - x)) e^{-j2\pi u^T R_{\varepsilon(x)'}^{-1} y} \quad (\text{II.20})$$

$$\begin{aligned} &= \sum_t f(y) w_R(R_{\varepsilon(\varepsilon_\theta^{-1}x)}^{-1}(t - R_\theta^{-1}x)) e^{-j2\pi u^T R_{\varepsilon(\varepsilon_\theta^{-1}x)}^{-1} t} \\ &= F_\varepsilon(u, R_\theta^{-1}x) \quad (\text{II.21}) \end{aligned}$$

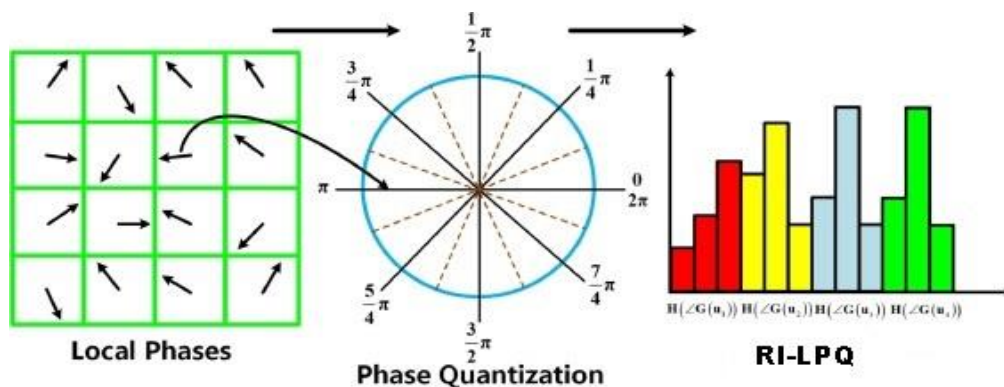
Où nous avons utilisé le fait que :  $R_{\varphi+\gamma} = R_\varphi R_\gamma$  et remplacé  $t = R_\varphi^{-1} y$ . Pour RI-LPQ, nous définissons  $F_\varepsilon(\mathbf{x})$  en remplaçant le  $F_{(u_i, \mathbf{x})}$  dans (II.12) par les coefficients orientés  $F_\varepsilon(u_i, \mathbf{x})$ . Nous procédons ensuite de la même manière à LPQ, uniquement en utilisant  $F_\varepsilon(\mathbf{x})$  au lieu de  $F(\mathbf{x})$ , pour produire Vecteur de descripteur 256 dimensions.



## Chapitre II : L'empreinte de l'articulation de doigt (FKP)

L'équation (II.21) montre que la rotation de  $f$  ne déplace que les coefficients  $F_{\varepsilon}(u, x)$ , ce qui n'affecte pas l'histogramme construit plus tard dans le processus. Donc en raison des mêmes arguments que pour LPQ, les caractéristiques résultantes sont insensibles à la rotation et au flou.

En outre, nous avons quantifié les orientations  $F_{\varepsilon}(u, x)$  à  $K$  valeurs possibles, et précompté l'ensemble correspondant de fonctions de fenêtre et d'exponentiels complexes. De cette façon, la complexité informatique est devenue proche de celui de la LPQ standard.[29]



**Figure II .11** : Rotation Invariant Local Phase Quantization (RI-LPQ)

- **Méthode hybride** : C'est une méthode qui combine les deux approches précédentes.

Le tableau ci-dessous présente une comparaison entre les méthodes d'extraction des caractéristiques :

**Tableau II.1** : Comparaison entre les méthodes d'extraction des caractéristiques

	Vitesse de réponse	Complexité algorithmme	Réponse
<b>Globale</b>	Très bien	Simple	Médiocre
<b>Locale</b>	Moyen	Complexe	Bien
<b>Hybride</b>	Mauvais	Très complexe	Très bien

### II.3.3. Classifications :

La classification automatique des images consiste à attribuer automatiquement une classe à une image à l'aide d'un système de classification. On retrouve ainsi la classification d'objets, de scènes, de textures, la reconnaissance de visages, d'empreintes digitale et de l'empreinte de l'articulation du doigt

(FKP). Classifier une image est une besogne théorie unifiée pour pouvoir utiliser les images pour les diagnostics complémentaires.

Elle consiste à déterminer des transactions autorisées de rassembler l'ensemble des pixels de l'image en un nombre limité de classes correspondant aux grands éléments structuraux de l'image. Donc cette étape de classification 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. [8]

### II.3.3.1. Les étapes d'une classification :

- ✓ Sélection des données.
- ✓ Calcul des similarités entre les n individus à partir des données initiales.
- ✓ Choix d'un algorithme de classification et exécution.
- ✓ L'interprétation des résultats.

### II.3.3.2. Méthode de machine à vecteurs de support (SVM) :

Le SVM est une nouvelle technique d'apprentissage statistique utilisée pour l'analyse des données et la reconnaissance des formes, proposé par Cortes et Vapnik. L'algorithme SVM a été développé au cours des années 1990 à des fins industrielles. Il peut traiter nombreux problèmes tels que la classification, la régression et la fusion. Au début et dans sa forme de base.[18]

Le SVM est par nature un classifieur binaire car il permet de séparer un espace en deux. Néanmoins, en télédétection on cherche rarement à discriminer deux classes uniquement. On peut trouver dans la littérature plusieurs extensions des SVM au cas multi-classes, mais on peut se concentrer sur les deux principales [29] :

1) L'approche dite **“un contre tous”** : Cette méthode compare successivement une classe avec toutes les autres au moyen d'un classifieur binaire. Si on a n classes, n classifieurs binaires sont construits (n hyperplans, soit n problèmes d'optimisation), le nième classifieur étant destiné à distinguer la classe d'indice n. Chaque élément à classifier est donc présenté aux n classifieurs et se voit attribuer l'étiquette du classifieur ayant renvoyé le plus grand pourcentage d'appartenance, en plus d'être simple, permet d'obtenir des performances qui ne sont pas significativement inférieures à celles des autres méthodes des SVM multi classes lorsqu'elle est correctement paramétrée.

2) L'approche “**un contre un**” : Cette approche consiste à chercher toutes les paires de classes possibles et aboutit à un classifieur par paire. Autrement dit, si on a  $n$  classes on aboutit à  $n(n-1)/2$  hyperplans. Le classifieur indicé par le couple  $(k,l)$  est destiné à distinguer la classe d'indice  $k$  de celle d'indice  $l$ . Chaque élément à classifier est présenté à  $n(n-1)/2$  classifieur et obtient le label de la classe ayant eu le plus de vote.

Le SVM binaire cherche à trouver l'hyperplan de séparation optimale entre les deux classes en maximisant la marge entre l'hyperplan et les deux classes qui sont étiquetées avec  $-1$  et  $1$ . Supposons que  $A$  est un ensemble de données,  $x_i$  ( $i = 1, 2, \dots$ ) sont les vecteurs caractéristiques d'apprentissage en  $k$ -dimension et  $y_i$  sont les étiquettes (labels) : [27]

$$A = \{(x_i, y_i) | x_i \in R^K\} \quad (\text{II.22})$$

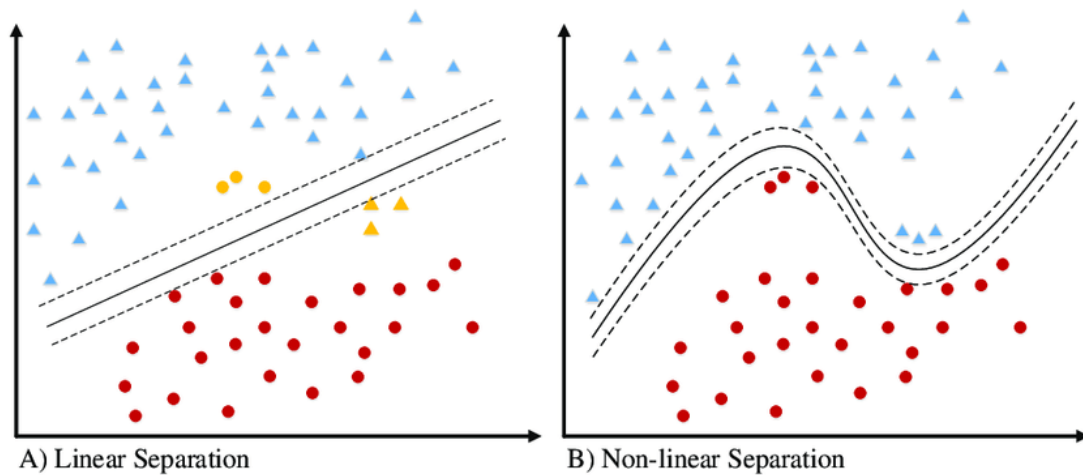
$$y_i \in \{-1, +1\} \quad (\text{II.23})$$

Pour le SVM linéaire, l'hyperplan de séparation optimale peut être exprimé par la fonction suivante :

$$(\mathbf{x}) = (w \cdot \mathbf{x}) + b \quad (\text{II.24})$$

L'élément important du SVM en approche non linéaire est qu'il repose sur l'utilisation d'une fonction noyau. Il existe un nombre très important de noyaux utilisés dans la littérature, dont plusieurs sont proposés pour inclure l'information spatiale. Néanmoins, les quatre noyaux les plus fréquemment utilisés sont [29] :

- ✓ Linéaire.
- ✓ Gaussien (Gaussien Radial Basic Function Kernel, RBF), qui serait d'après le noyau à utiliser préférentiellement.
- ✓ Polynomial.
- ✓ Sigmoidal.



**Figure II.12** : Classification SVM ; (A) SVM linéaire séparation par une ligne droite, (B) SVM non linéaire séparation par une courbe

### II.3.3.3. Méthode des K plus proches voisins (KNN) :

La méthode des k plus proches voisins (noté k-NN pour Nearest-Neighbor) appartient à la famille des algorithmes d'apprendre automatique (machine Learning). L'idée d'apprentissage automatique ne date pas d'hier, parce que l'expression de **machine learning** a été utilisée pour la première fois par l'informaticien américain Arthur Samuel en 1959. Les algorithmes d'apprentissage automatique ont connu un fort regain d'intérêt au début des années 2000 surtout grâce à la quantité de données disponibles sur internet. [30]

La méthode des plus proches voisins consiste à déterminer pour chaque nouvelle personne que l'on veut classer, la liste des KNN parmi les individus déjà classés. L'individu est affecté à la classe qui contient le plus d'individus parmi ces plus proches voisins. Et le nombre de voisins à prendre en compte. Cette méthode est surveillance et non-paramétrique est souvent performante. De plus, son apprentissage est assez simple, car il est de type apprentissage par cœur (on garde tous les exemples d'apprentissage). Cependant, le temps de prévision est très long, car il nécessite le calcul de la distance avec tous les exemples, mais il existe des heuristiques pour réduire le nombre d'exemples à prendre en compte. [31]

Le principe de cet algorithme de classification est très simple. On lui fournit un ensemble des données d'apprentissage  $D$ , une fonction de distance  $d$  et un entier  $k$ . Pour tout nouveau point de test  $x$ , pour lequel il doit prendre une décision, l'algorithme recherche dans  $D$  les  $k$  points les plus proches de  $x$  au sens de la distance  $d$ , et attribue  $x$  à la classe qui est la plus fréquente parmi ces  $k$  voisins. [32]

## Chapitre II : L'empreinte de l'articulation de doigt (FKP)

Cette algorithm est basée sur une fonction distance arbitraire  $d$ , les plus classiques sont :

➤ **Distance euclidienne :**

La distance la plus connue est la distance Euclidienne, qui calcule la racine carrée de la somme des différences carrées entre les coordonnées de deux points :

$$\mathbf{d}(\mathbf{x}, \mathbf{y}) = \sqrt{\sum_{i=1}^n (x_i - y_i)^2} \quad (\text{II.25})$$

➤ **Distance Minkowsky :**

Cette distance est le cas général de la distance euclidienne avec une variable  $P$ , qui nous donne l'équation suivante :

$$\mathbf{d}(\mathbf{x}, \mathbf{y}) = (\sum_{i=1}^n |x_i - y_i|^p)^{1/p} \quad (\text{II.26})$$

➤ **Distance Manhattan (Cityblock) :**

La distance de Manhattan (aussi appelée distance « city-block » ou métrique absolue), calcule la somme des valeurs absolues des différences entre les coordonnées de deux points :

$$\mathbf{d}(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^n |x_i - y_i| \quad (\text{II.27})$$

✓ **Distance Hamming :**

La distance entre deux points donnés est la différence maximale entre leurs coordonnées sur une dimension.

$$\mathbf{d}_h(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^k |x_i - y_i| \quad (\text{II.28})$$

Avec :  $x = y \implies d=0$  et  $x \neq y \implies d=1$

✓ **Distance Chebychev :**

Pour  $p = \infty$ , on obtient la distance de Chebychev (aussi appelée : **Distance Queen-wise** ou encore métrique maximum) qui est donné par l'équation :

$$\mathbf{d}(\mathbf{x}, \mathbf{y}) = \max |x_i - y_i| \quad (\text{II.29})$$

✓ **Distance de Mahalanobis :**

## Chapitre II : L'empreinte de l'articulation de doigt (FKP)

La distance de Mahalanobis serait égale à la distance Euclidienne. La boule associée à une distance de Mahalanobis est de forme elliptique, alors que la boule d'une distance Euclidienne est un cercle (en deux dimensions).

La distance de Mahalanobis Donnée par l'équation suivante :

$$d(\mathbf{x}, \mathbf{y}) = \sqrt{(\mathbf{x} - \mathbf{y}) * \text{cov}(d)' * (\mathbf{x} - \mathbf{y})'} \quad (\text{II.30})$$

Où :  $\text{cov}(d)$  est la matrice de covariance.

### II.3.3.3.a. Choix de k :

- K est grand** : Moins sensible au bruit, une grande base d'apprentissage permet une plus grande plus grande valeur de k.
- K est petit** : Rend mieux compte de structure fine, nécessaire pour les petites bases d'apprentissage.

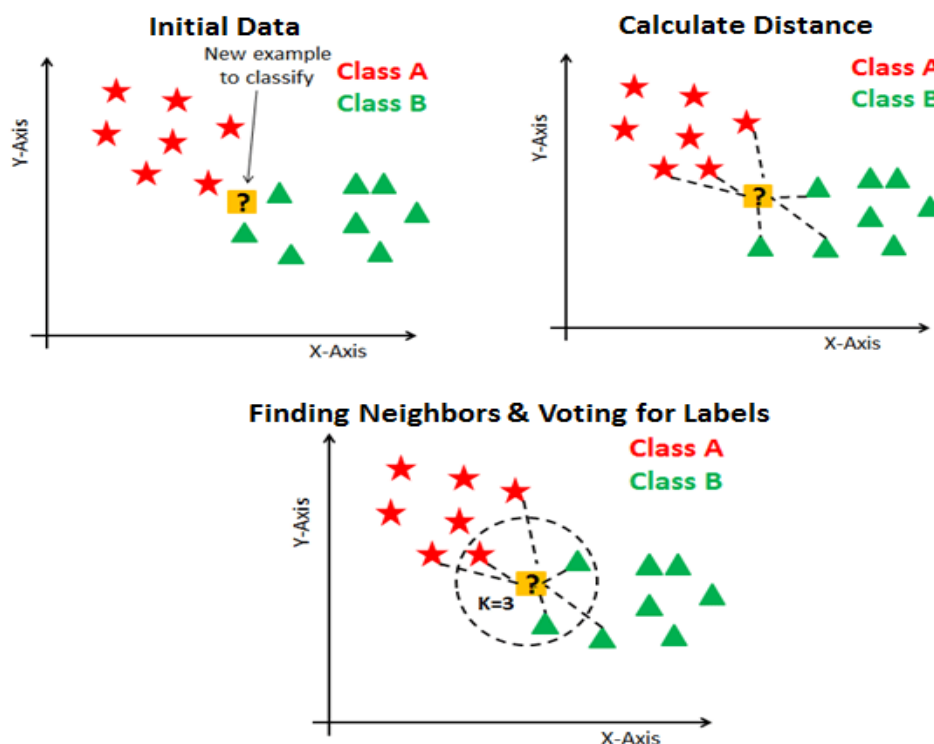
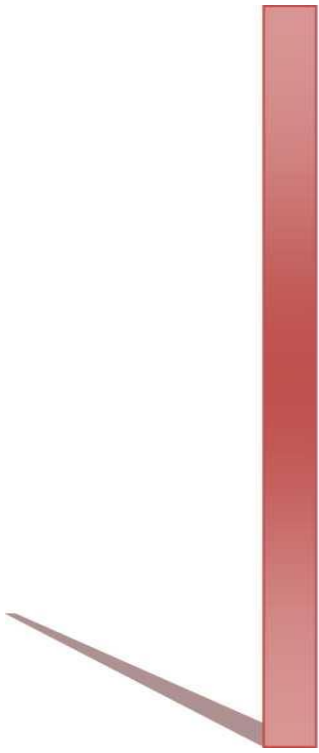


Figure II .13 : Méthode des K plus proches voisins (KNN)

### II .4 Conclusion :

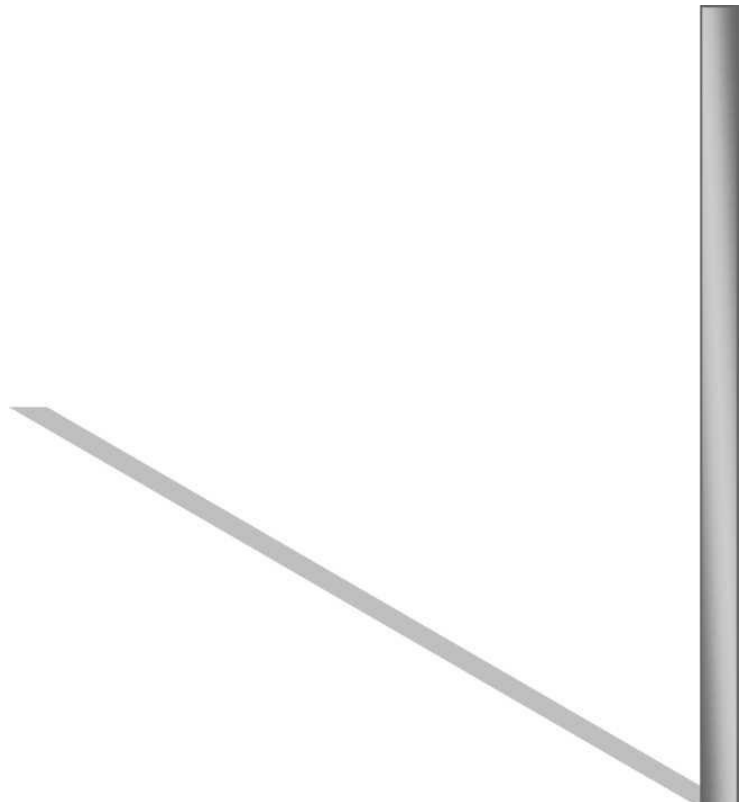
Dans ce chapitre nous avons donné les modalités biométriques liées à la main, et nous avons parlé aussi des quelques algorithmes utilisés dans le domaine de la biométrie pour le prétraitement ; l'extraction des caractéristiques et pour la classification.





# *Chapitre III*

*Résultats expérimentaux et discussions*



# Chapitre III : Résultats expérimentaux et discussions

## III.1. Introduction :

Ce chapitre représente une nouvelle méthode pour la reconnaissance de l'empreinte de l'articulation de doigt FKP. Les résultats expérimentaux finals de la reconnaissance FKP en utilisant le descripteur LPQ et RI-LPQ pour extraire les caractéristiques et le SVM pour la classification de ces vecteurs ont été aussi présentés.

## III.2. Que signifie MATLAB (MATrix LA Boratory) :

- **MATLAB** est un logiciel de calcul matriciel à syntaxe simple. Avec ses fonctions spécialisées.
- Il peut être aussi considéré comme un langage de programmation adapté pour les problèmes scientifiques.
- Est un interpréteur : les instructions sont interprétées et exécutées ligne par ligne et il fonctionne dans plusieurs environnements tels que Xwindows, Windows, Macintosh.

Il existe deux (02) modes de fonctionnement :

- ✓ Mode interactif : MATLAB exécute les instructions au fur et à mesure qu'elles sont données par l'utilisateur.
- ✓ Mode exécutif : MATLAB exécute ligne par ligne un "fichier M" (programme en langage MATLAB).

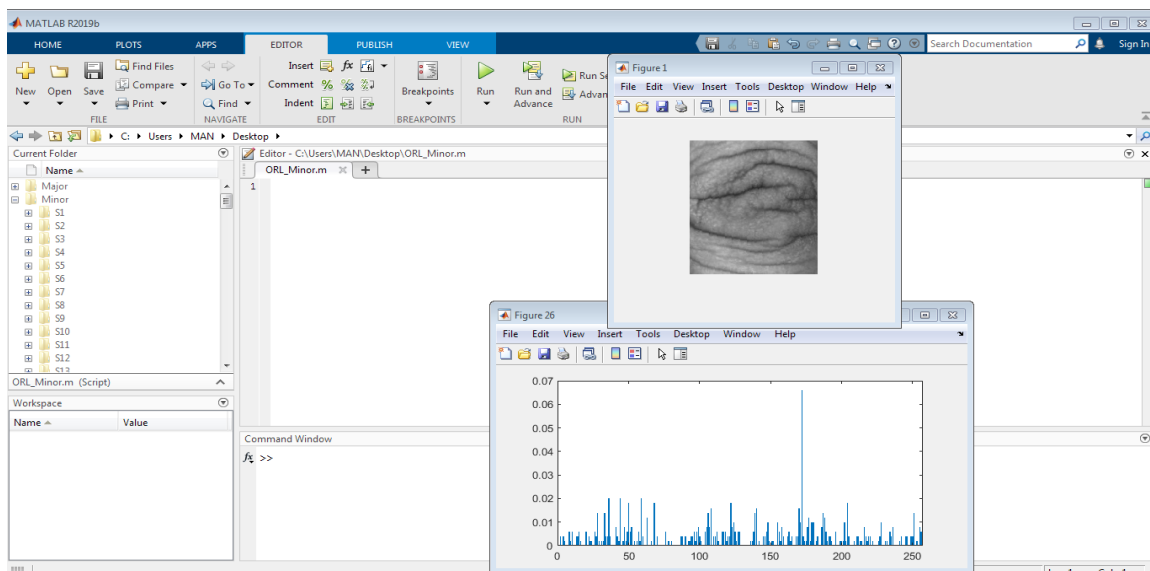


Figure III. 1 : Présentation de MATLAB

## III.3. Expérience sur les images FKP :

### III.3.1. Base de données :

La base de données d'images des doigts sans contact de l'Université polytechnique d'Hong Kong (version 1.0) est fournie par des volontaires masculins et féminins. Cette base de données a été en grande partie acquise sur le campus de l'Université polytechnique d'Hong Kong et sur le campus IIT de Delhi entre 2006 et 2013 en utilisant une configuration sans contact qui utilise simplement une caméra portative. Cette base de données contient 2515 images dorsales du doigt (majeur et mineur ensemble) de 503 sujets, toutes les images sont au format bitmap (\*.bmp). Dans cet ensemble de données, environ 88% des sujets ont moins de 30 ans. Cette base de données fournit également deux images des articulations des doigts acquises après un très long intervalle (4 à 7 ans) pour vérifier la stabilité du pli des articulations et des lignes courbes. [33]

La figure III.2 suivante représente image de notre base de données



**Figure III.2:** Quelques images de la base de données Poly U-FKP(a) Majeur et (b) Mineur.

### III.3.2. Protocole de test :

L'identification par l'empreinte FKP est une procédure de comparaison un contre plusieurs pour identifier une image FKP de test.

Les 5 images de l'empreinte FKP sont divisées en deux groupes :

- ✓ Images d'apprentissages : Les trois premières images de chaque personne servent pour la phase d'apprentissage.
- ✓ Images de Tests : Les deux restantes images de chaque individu servent pour la réalisation des différents tests (phase de test).

### III .3.3. Acquisition des données :

Le mécanisme d'acquisition des images de cette base de données :

Chacune des images acquises est d'abord soumise à une binarisation à l'aide du seuillage d'Otsu. Les images résultantes sont nettoyées (débruité) en supprimant automatiquement le régions / pixels (<100 pixels), afin que le plus long objet représentant le doigt soit uniquement conservé. La forme du doigt binarisée est utilisé pour estimer l'emplacement de doigt à partir de la coque convexe des images.

La détection des contours de l'image résultante est utilisée pour localiser le centre d'image de l'articulation du doigt (mineur et majeur ). Ceci est réalisé en estimant l'emplacement du centre de gravité de l'image détectée de bord résultante et segmenter une région de taille fixe (160 × 180 pixels) qui représente l'image de la région des articulations de doigts. La figure suivante représente le dispositif de le dispositif d'acquisition de FKP:



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

### III .3.4. Taux de reconnaissance :

Le taux de reconnaissance permet d'évaluer la qualité du classifieur par rapport au problème pour lequel il a été conçu. Ce taux est évalué grâce à une base de test qui contient des formes décrites dans le même espace de représentation que celles utilisées pour l'apprentissage. Elles sont aussi étiquetées par leur classe réelle d'appartenance afin de pouvoir vérifier les réponses du classifieur.

En général, quand les échantillons étiquetés à disposition sont suffisamment nombreux, ils sont séparés en deux parties disjointes et en respectant les proportions par classes de la base initiale. Une partie sert pour former la base d'apprentissage et l'autre pour former la base de test. Le découpage le plus courant est de 1/2 pour l'apprentissage et le 1/2 restant pour la base de test.

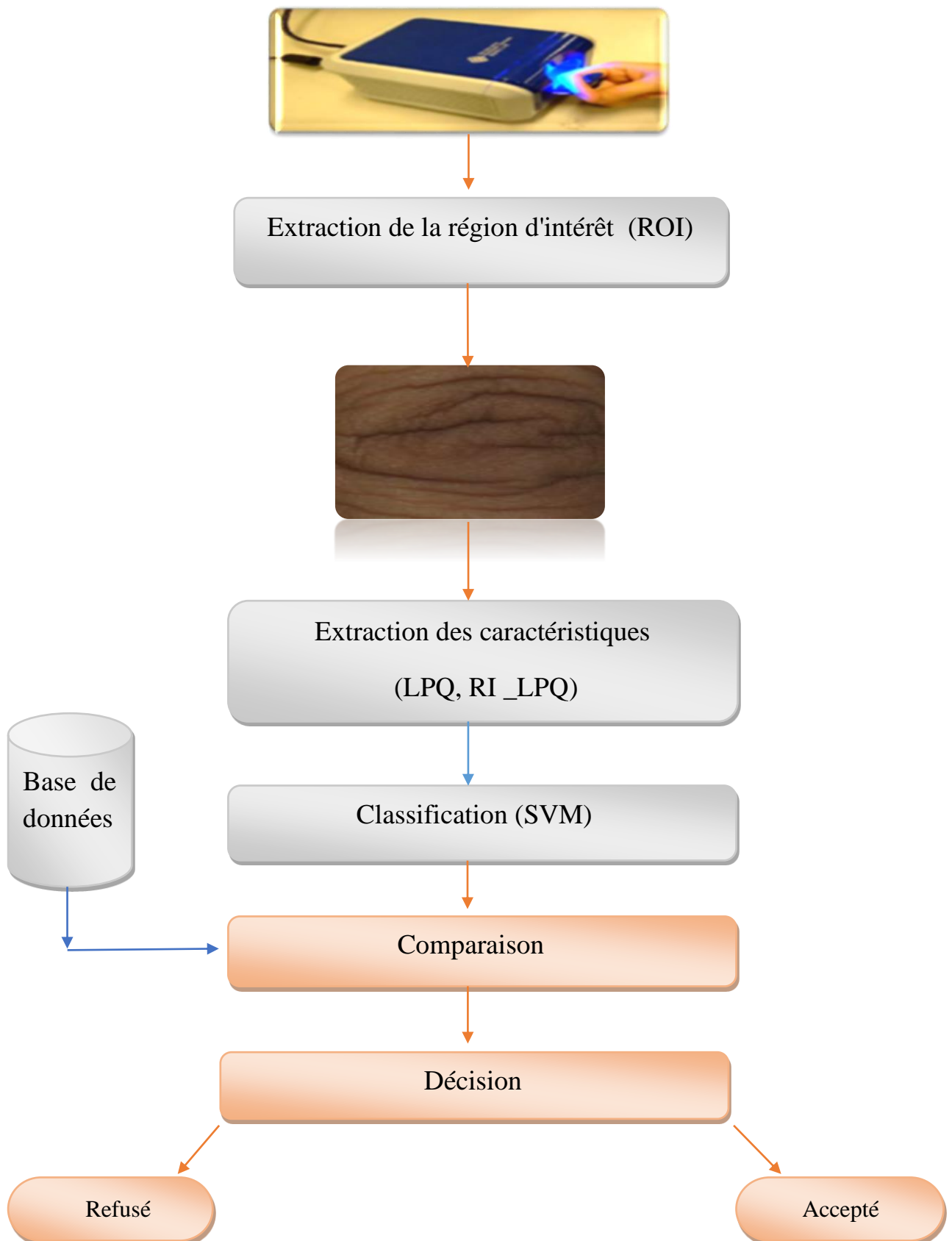
Les performances en termes de taux de reconnaissance sont alors déterminées en présentant au classifieur chacun des exemples de la base de test et en comparant la classe donnée en résultat à la vraie classe [34].

Le Taux de Reconnaissance Totale (TR) est simplement défini par :

$$\mathbf{TR(\%)} = \frac{\text{Nombre d'empreinte bien classé}}{\text{Nombre total d'empreinte de test}} \quad (\text{III.1})$$

### III .3.5. Présentation du système :

Cette section présente notre système de reconnaissance basé sur l'FKP qui est conçu en base sur la fonction LPQ au niveau de la phase d'extraction des paramètres :



**Figure III.4 :** Schéma proposé du système de reconnaissance de FKP

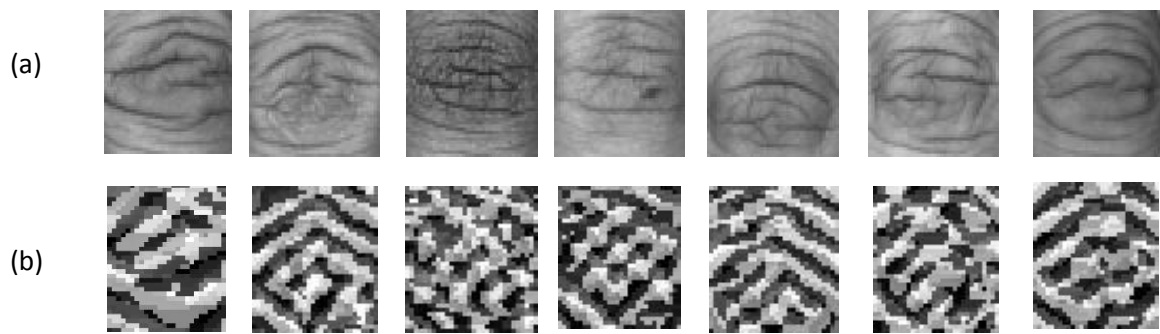


Figure III.5 : (a) Images FKPs, (b) Leur images LPQs

### III.4. Résultats et discussion :

Pour obtenir les résultats des tests, chaque vecteur de l'image de test a été comparé avec tous les vecteurs dans la base des références. Si les deux vecteurs sont de la même classe (même personne), la mise en correspondance entre eux serait comptée comme un client, sinon il aurait été considéré comme un imposteur, l'objectif est d'évaluer le taux de reconnaissance de l'algorithme utilisé, en suivant un protocole de test se base sur la mesure du taux de reconnaissance. [10]

#### III.4.1. Les résultats obtenus par la méthode LPQ :

Le descripteur de quantification de phase locale (LPQ) caractérisé par :

$LPQ_{desc} = lpq(img, winSize, decorr, freqestim, mode)$

- ✓ Format de l'image en échelle de gris à analyser (**img**).
- ✓ Taille de la fenêtre locale (**winsize**).
- ✓ La décorrélation (**decorr**) : Les valeurs possibles sont:
  - 0 : pas de décorrélation.
  - 1 : décorrélation.
- ✓ Estimation de fréquence locale (**freqestim**) : Les valeurs possibles sont:
  - 1 : STFT avec fenêtre uniforme .
  - 2 : STFT avec fenêtre gaussienne .
  - 3 : Paire de filtres en quadrature dérivée gaussienne.
- ✓ mode: définit le type de sortie souhaité. Les choix possibles sont:
  - nh : histogramme normalisé de LPQ.
  - h : histogramme non normalisé des mots de code LPQ.
  - im : image du mot de passe LPQ.



## Chapitre III : Résultats expérimentaux et discussions

On a appliqué notre algorithme LPQ sur 200 individus de la base de données de test Les tableaux suivants donnent un résumé des résultats de taux de reconnaissance obtenu. ( Le mode est toujours « nh »).

### III.4.1.1. La taille de fenêtre (winsize) :

Tableau III.1 : TR en utilisant les différentes tailles de fenêtre.

Winsize \ TR	3	5	7	9	11	13	15
Majeur	77.5%	94.25%	94.25%	96.5%	96.75%	96.25%	96.5%
Mineur	64%	81.5%	84%	85.5%	87.5%	89%	90.25%

A partir de Tableau III.1 ; nous avons fixé : Winsize « 11 » donne le meilleur TR pour Majeur.

Et Winsize « 15 » donne le meilleur TR pour Mineur.

### III.4.1.2. Décorrélation (decorr):

Tableau III.2 :TR en utilisant les différentes décorrélation.

Decorr \ TR	0	1
Majeur	95.75%	96.75%
Mineur	87%	90.25%

La meilleure valeur pour la décorrélation est « 1 » dont les TRs :96.75% pour Majeur et 90.25% pour Mineur.

## III.4.1.3. L'estimation de fréquence locale (freqestim):

Tableau III.3 :TR en utilisant les différentes estimations de fréquence locale.

Freqestim \ TR	1	2	3
Majeur	96.75%	95.75%	96.75%
Mineur	90.25%	90.75%	89.75%

Le meilleur taux de reconnaissance est obtenu par la valeur : « 1 » pour Mineur et Majeur. Nous avons donc fixé cette valeur pour notre travail .Pour meilleur taux de reconnaissance de l'algorithme LPQ et d'après le tableau précédent on peut en conclure :

Les meilleurs paramètres pour : Majeur : LPQdesc = lpq (160×180,11 , 1, 1, nh)

Mineur :LPQdesc = lpq (160×180 ,15, 1, 1, nh)

## III.4.2. Les résultats obtenus par la méthode RI-LPQ :

La méthode RI-LPQ est basée sur quatre paramètres essentiels :

- ✓ La taille de fenêtre (winsize).
- ✓ Le nombre d'angle (numAngl).
- ✓ Le nombre des blocs (nombre de pixels).
- ✓ Le mode (h, nh,im).

On a appliqué notre algorithme RI- LPQ sur 200 individus de la base de données. Nous avons varié chaque fois les valeurs des quatre paramètres afin de fournir les meilleurs taux de reconnaissance (TR) de notre système. Les résultats sont représentés dans les tableaux suivants :

# Chapitre III : Résultats expérimentaux et discussions

## III.4.2.1. La taille de fenêtre (winsize) :

Tableau III.4 : TR en utilisant les différentes tailles de fenêtre.

Win size \ TR	3	5	7	9	11	13	15
Majeur	63.25%	87.5%	86.5%	91.25%	93%	94.25%	95.25%
Mineur	52.75%	60.25%	69.75%	74%	78.75%	81.25%	87.25%

Nous avons remarqué à partir de ce tableau que la taille de fenêtres « 15 » donne meilleurs taux de reconnaissance « 95.25 % » pour Majeur et « 87.25 % » pour Mineur par rapport aux les autres tailles. Alors la taille de fenêtre «15» a été fixée.

## III.4.2.2. Le nombre d'angle (numAngl) :

Tableau III.5 : TR en utilisant les différents nombres d'angle.

numAngl \ TR	2	4	6	8	10	12	14
Majeur	95.25%	96.25%	96.5%	97%	95%	95.5%	96.5%
Mineur	87.25%	90%	94%	93%	91.5%	92%	92%

A partir des résultats obtenus nous avons fixé le nombre d'angle à « 8 » qui nous a donné le plus grand TR « 97% » pour Majeur. Et nous avons fixé le nombre d'angle à « 6 » qui nous a donné le plus grand TR 94% pour Mineur.

## Chapitre III : Résultats expérimentaux et discussions

### III.4.3.3. La taille de bloc (nombre de pixels) :

Tableau III.6 : TR en utilisant les différentes tailles de bloc N×N

N×N TR	45×40	90×80	135×120	180×160	225×200	270×240	315×280
Majeur	98.25%	96.75%	96.5%	97%	95.75%	94.75%	92.75%
Mineur	95.5%	96.5%	94%	94%	91%	87.25%	82.5%

À travers les résultats obtenus par les différentes tailles de bloc, On remarque que :

La taille de bloc 45× 40pixels donne meilleur taux de reconnaissance qui égale à 98.25 % pour Majeur. Mais pour le Mineur la meilleure taille de bloc qui nous a donné le plus grand TR est 90×80pixels. Nous avons fixé la taille de bloc 45×40 pixels pour Majeur et 90×80pixels pour Mineur.

Donc à partir des expériences précédant, pour améliorer le TR nous avons fixé les paramètres de RI-LPQ comme suit :

- Pour le Majeur :
  - ✓ La taille de fenêtre : 15
  - ✓ Le nombre d'angle : 8
  - ✓ Le nombre de blocs : 45×40
  - ✓ Le mode : nh
- Pour le Mineur :
  - ✓ La taille de fenêtre : 15
  - ✓ Le nombre d'angle : 6
  - ✓ Le nombre de blocs : 90×8
  - ✓ Le mode : nh

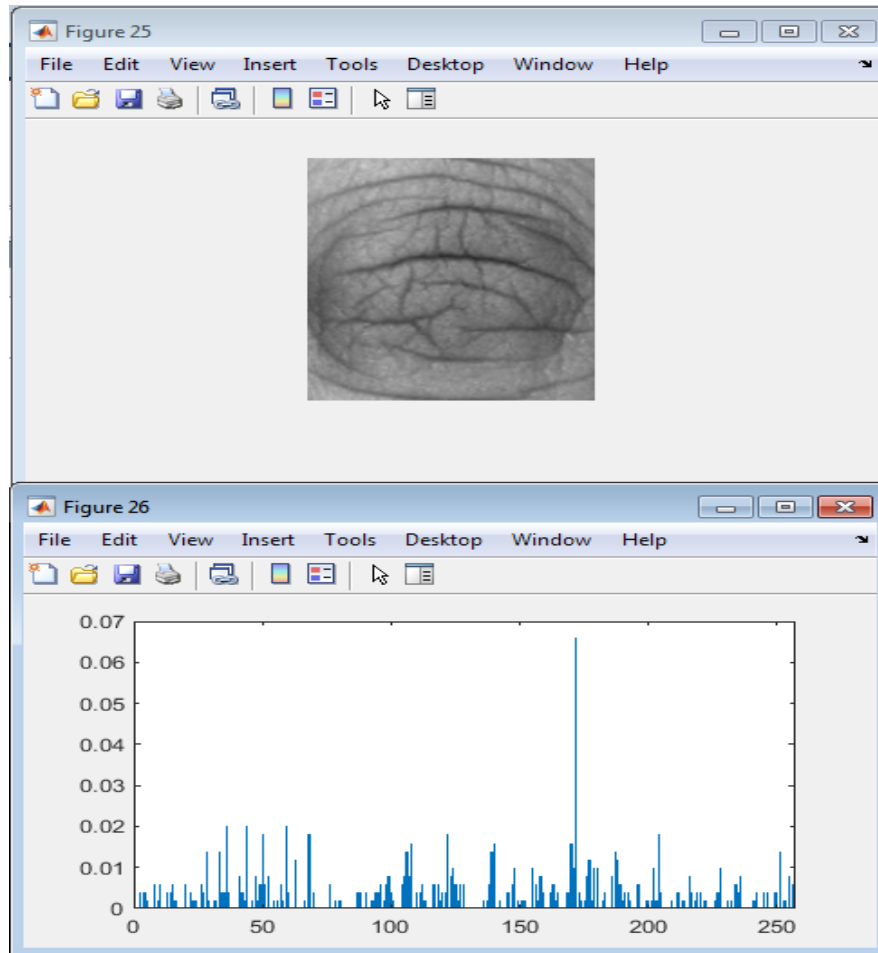


Figure III.6 : Exemple de l'histogramme d'une image FKP.

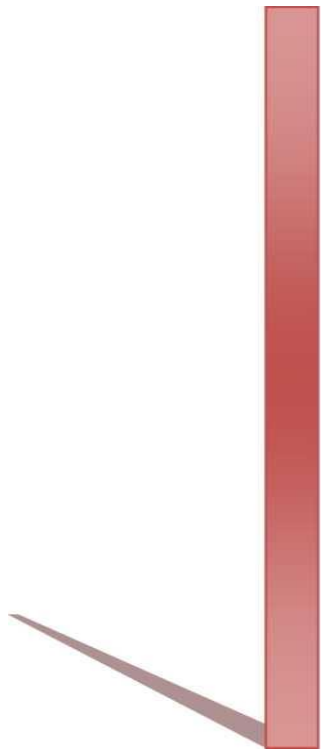
### III.5. Comparaison entre les méthodes LPQ et RI-LPQ dans le système de La reconnaissance des individus par leur FKPs :

Les meilleurs résultats ont été obtenus par la méthode RI-LPQ qui donne un TR= **98.25%** pour le majeur et un TR = **96.5%** pour le mineur.

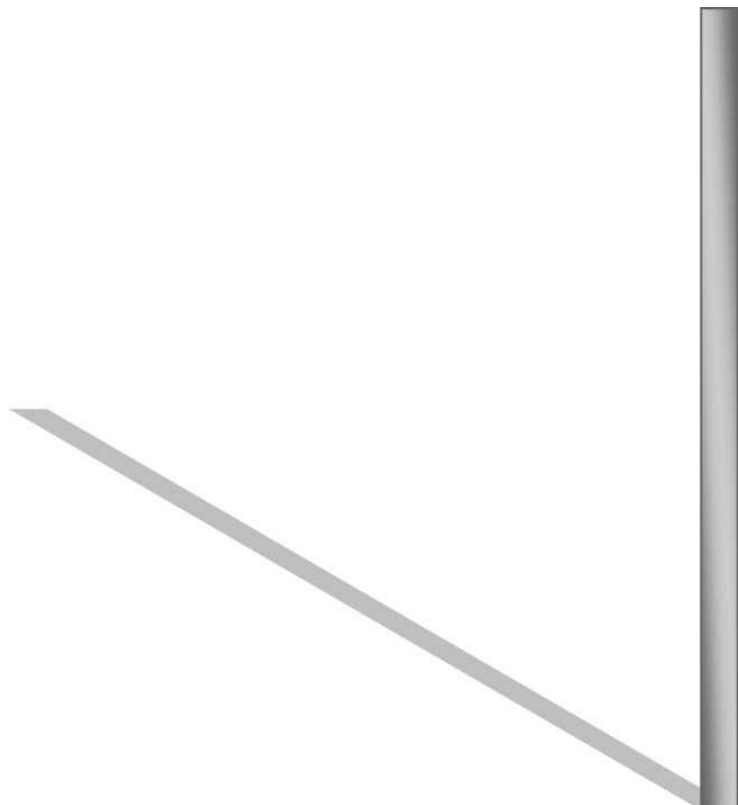
On conclut que la méthode RI-LPQ est meilleure que la méthode LPQ.

### III.6. Conclusion :

Dans ce chapitre nous avons présenté notre système global de reconnaissance par l'empreinte des articulations de doigts FKP basée sur les algorithmes LPQ et RI-LPQ et SVM. La méthode RI-LPQ s'est plus efficace et plus fiable pour identifier l'empreinte de l'articulation du doigt (FKP) par rapport la méthode LPQ.



*Conclusion  
générale*





# Conclusion générale

## Conclusion générale :

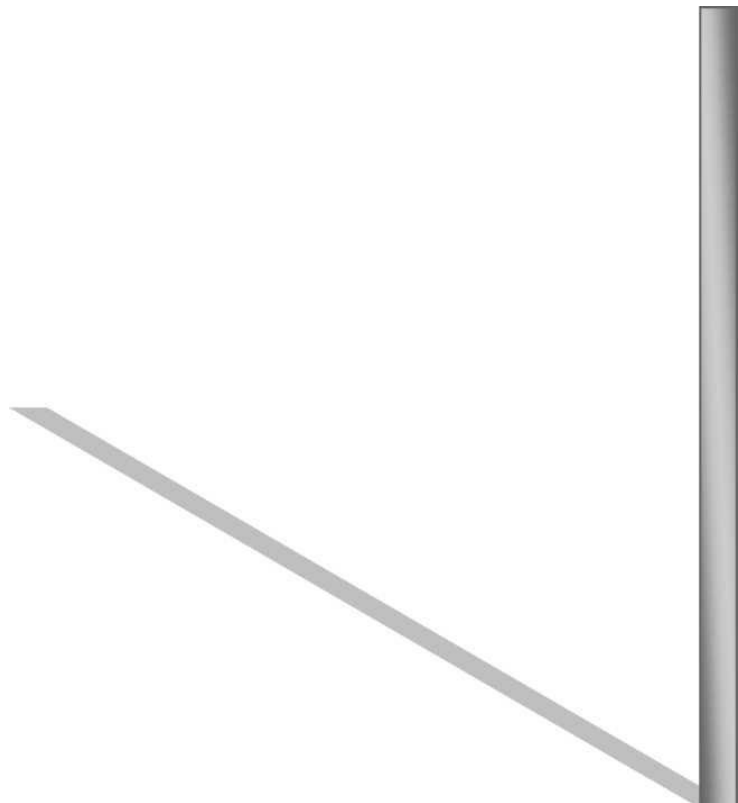
En raison de besoin des systèmes biométriques dans les applications tels que les systèmes d'entrée ou de sortie vers des institutions, de la surveillance dans les aéroports et applications dans les téléphone portables...etc. On a utilisé dans ce travail nouvelle méthode dans la reconnaissance biométrique, est l'empreinte d'articulation de doigts (majeur et mineur) par ce qu'elle est permanente et unique. Les résultats obtenus de système biométrique proposées sont très encourageants et ils indiquent que FKPs peuvent répondre aux exigences de sécurité, peuvent construire un système biométrique robuste et efficace. Nous avons suggéré deux méthode LPQ et RI\_LPQ en utilisant le SVM pour la classification.

Le système proposé est appliqué sur une base de données de 200 personnes dans le domaine des empreintes FKP et les résultats obtenus sont très intéressantes. En effet on est arrivé à un taux de reconnaissance peut idéal de 98.25% pour majeur et de 96.5% pour mineur, ce taux est très intéressant ce qui rend notre système fiable où il répond bien à l'objectif que nous sommes fixés au départ, ce qui signifie que la mise en œuvre du système permet de la reconnaissance d'individus. Nous proposons comme perspective la concentration sur l'évaluation de la performance de la reconnaissance 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.

Dans les futures expériences on peut utiliser d'autres algorithmes pour la classification tels que la KNN ou proposer un autre système multimodal basé sur les images de FKPs.



# *Bibliographie*



# Bibliographie

- [01] **BOUDJELLAL Soufiane**, détection et identification de personne par méthode biométrique UNIVERSITE TIZI- OUZOU.
- [02] **BERREDJEM Achref**, La reconnaissance des individus par leur empreinte des articulations des doigts, UNIVERSITÉ GUELMA, 2019
- [03] **Rania Bba** , chapitre 1 système de reconnaissance de visage, Academia .
- [04] **DIB Soumeya** , identification des individus par les technique multimodales , UNIVERSITE ORAN ,(2014-2015)
- [05] **MERAMRIA Nabila**, Reconnaissance de visages par Analyse Discriminante Linéaire (LDA), UNIVERSITE ANNABA ,(2016) .
- [06] **Halaimia Nabil** , reconnaissance biométrique via l'apprentissage approfond , UNIVERSITE TEBESSA, (2017-2018).
- [07] <https://www.memoireonline.com/02/13/6979/Reconnaissance-de-visages-par-Analyse-Discriminante-LineaireLDA-.html> par Amira Chiheb Université du 8 mai 45 de Guelma Algérie - Licence en informatique 2003 .Academia
- [08] **SADALAH Khedidja** , Identification biométrique des personnes par les empreintes palmaires, UNIVERSITE ANNABA, 2019.
- [09] **BENCHNANE Ibtissame** , Etude et mise au point d'un procédé biométrique multimodale pour la reconnaissance des individus , UNIVERSITE ORAN, 2015.
- [10] **CHAKOUR Alla Eddine**, Identification biométriques des personnes par les empreintes d'articulation du doigt, UNIVERSITE ANNABA , 2019.
- [11] **BOURENEB Aziza** , Identification des personnes par leurs empreintes palmaire, UNIVERSITÉ GUELMA , 2019
- [12] <http://www.journaldunet.com/solutions/0611/061127-biometrie/8.shtml>.
- [13] **TELIB Lina, BENAGGA, Abderahmane** , Reconnaissance des personnes basée sur l'empreinte de l'articulation de doigt, UNIVERSITÉ KASDI MARBEH OUARGLA, 2015-2016.
- [14] **CHAA Mourad**, thèse , système de reconnaissance de personne par des technique biométrique, UNIVERSITE Ferhat Abbas – SETIF , 2017
- [15] **MOHEMED ELAbed**, Évaluation de système biométrique. Cryptographie et sécurité [cs.CR]. Université de Caen, 2011.
- [16] **HAFS Toufik** , thèse, Reconnaissance Biométrique Multimodale basée sur la fusion en score de deux modalités biométriques : l'empreinte digitale et la signature manuscrite cursive en ligne UNIVERSITE ANNABA , 2016

# Bibliographie

- [17] Wang, H., Li, S. Z., Wang, Y., & Zhang, J. (2004, October). Self-quotient image for face recognition. In Image Processing, 2004. ICIP'04. 2004 International Conference on (Vol. 2, pp. 1397-1400). IEEE
- [18] Vitomir struc, the IN face toolbox v2.1 the Matlab toolbox for illumination invariant face recognition, faculty of Electrothechnical Engineering- university of Ljubljana, 2012
- [19] [https://en.wikipedia.org/wiki/Difference\\_of\\_Gaussians](https://en.wikipedia.org/wiki/Difference_of_Gaussians)
- [20] **Douidi Dahbia , Grini Soumia** . Identification et Reconnaissance Biométrique par l'Utilisation des Empreintes Palmaires ,Master Académique , université Akli Mohnad Oulhadj , Bouira 24.09.2017
- [21] <https://builtin.com/data-science/step-step-explanation-principal-component-analysis>
- [22] **Chiheb Amira , Bouhalit Nasereddine** .Reconnaissance de Visages par Analyse Discriminante Linéaire (LDA).Licence Informatique , Université du 8 Mai 45 , Guelma , 2003
- [23] [https://en.wikipedia.org/wiki/Log\\_Gabor\\_filter](https://en.wikipedia.org/wiki/Log_Gabor_filter)
- [24] <https://www.peterkovesi.com/matlabfns/PhaseCongruency/Docs/convexpl.html>
- [25] **Bilal Attallah, Amina Serir, Youssef Chahir, Abdelwahhab Boudjelal**. Histogram of gradient and binarized statistical image features of wavelet subband-based palmprint features extraction. Journal of Electronic Imaging, SPIE and IS&T, 2017, 26 (06), ff10.1117/1.JEI.26.6.063006ff. fihal-01823153f
- [26] **OUAMANE, Abdelmalik** ,*Reconnaissance Biométrique par Fusion Multimodale du Visage 2D et 3D*. Université Mohamed Khider - Biskra.2015
- [27] **CHOUCHANE Ammar** ,Analyse d'images d'expressions faciales et orientation de la tête basée sur la profondeur , Doctorat LMD en Génie Electrique ,Université Mohamed Khider Biskra 2016.
- [28] **SRZhou, JP Yin, JM Zhang** , Motif binaire local (LBP) et quantification de phase locale (LBQ) basée sur le filtre de Gabor pour la représentation de visage , 2013
- [29] **David RECHAL** , 'Analyse du potentiel des classifications de type SVM pour l'identification des parcelles arborées dans les images de télédétection à très haute résolution spatiale ' . Université Pierre et Marie Curie – Paris VI , 17 Mars 2008 – 12 Septembre 2008

# Bibliographie

[30] eduscol.education.fr/ Ministère de l'Éducation nationale et de la jeunesse - septembre 2019

[31] **Oumiloud Horiya. Mokeddem Asma**, Classification Non Supervisée : Application de k-means ,Université Abou Bakr Belkaid– Tlemcen ,2013-2014

[32]**BERRANI, Sid-Ahmed**, AMSALEG, Laurent, et GROS, Patrick. Recherche par similarités dans les bases de données multidimensionnelles : panorama des techniques d'indexation. Ingénierie des systèmes d'information, 2002

[33] <https://www4.com p.polyu.edu.hk/~csajaykr/database.php>

[34] **BENABDI Mouad** identification des personnes par les empreintes d'articulation des doigts etle deep Learning, Université M'SILA ,2019