



République Algérienne Démocratique et Populaire



Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Akli Mohand Oulhadj de Bouira

Faculté des Sciences et des Sciences Appliquées

Département d'Informatique

# Mémoire de Master

## en Informatique

*Spécialité : Génie des systèmes informatiques*

## Thème

---

Reconnaissance biométrique multimodale par fusion  
des empreintes d'articulation des doigts.

---

Encadré par

- MR HACINE GHERBI AHCINE

Réalisé par

- IMINE BELAID LYES
- BACHOUCHE OUSSAMA

2022/2023



## التصريح الشرفي الخاص بالالتزام بقواعد النزاهة العلمية

لإنجاز بحث

انا الممضي اسفله،

السيد(ة) Imine Belaid Lya .....الصفة: طالب ( ماستر / دكتوراه )

الحامل(ة) لبطاقة التعريف الوطنية: ١٥٤١.١٢.١٩٥.....والصادرة بتاريخ 2022/06/16

المسجل(ة) بكلية / معهد sciences et des sciences appliquées  
Informatique.....قسم

تخصص: Génie système informatique.....

والمكلف(ة) بإنجاز اعمال بحث(مذكرة، التخرج، مذكرة ماستر، مذكرة ماجستير، اطروحة دكتوراه).

عنوانها: Reconnaissance biométrique multimodale par fusion des empreintes  
d'adhésion des doigts.....

أصرح بشرفي اني ألتزم بمراعاة المعايير العلمية والمنهجية الاخلاقيات المهنية والنزاهة الاكاديمية المطلوبة  
في انجاز البحث المذكور أعلاه.

توقيع المعني (ة)

التاريخ: 2023/06/23

I

البويرة في: 2023/07/01

هيئة مراقبة السرقة العلمية:

الامضاء

الامضاء  
الجامعة الجزائرية للدراسات والبحوث  
كلية العلوم والعلوم التطبيقية  
البويرة

%

98

النسبة:



## التصريح الشرفي الخاص بالالتزام بقواعد النزاهة العلمية

انا الممضي اسفله،

السيد(ة) ياسمين أسامة الصفة: طالب ( ماستر / دكتوراه )

الحامل(ة) لبطاقة التعريف الوطنية: 400874741 والصادرة بتاريخ 03-06-2022

المسجل(ة) بكلية / معهد العلوم والعلوم التطبيقية قسم الإعلام الإلكتروني  
تخصص: الهندسة في نظم المعلومات

والمكلف(ة) بإنجاز اعمال بحث (مذكرة، التخرج، مذكرة ماستر، مذكرة ماجستير، اطروحة دكتوراه).

عنوانها: Reconnaissance biométrique multimodale

par fusion des empreintes d'articulation de dents

أصح بشرفي اني ألتزم بمراعاة المعايير العلمية والمنهجية الاخلاقيات المهنية والنزاهة الاكاديمية المطلوبة  
في انجاز البحث المذكور أعلاه.

التاريخ: 2023-07-10

توقيع المعني(ة)

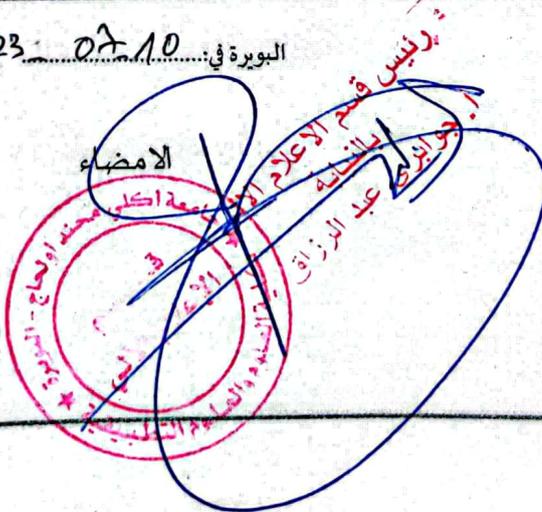
البويرة في: 2023-07-10

هيئة مراقبة السرقة العلمية:

%

28

النسبة:



# *Remerciements*

Nous remercions **Dieu** le tout puissant de nous avoir donné la santé et la volonté d'entamer et de terminer ce travail.

Nous tenons à remercier nos parents pour tous leurs sacrifices, ainsi que tous les membres de nos familles et nos amis.

Nos vifs remerciements à Mr HACINE GHERBI Ahcine pour avoir accepté de diriger ce travail.

Nous remercions aussi tout le personnel de la direction D'ALGERIE TELECOM où j'ai fait mon stage.

A toutes les personnes qui ont participé de près ou de loin à l'élaboration de ce rapport, mille mercis

Enfin, ma reconnaissance va également aux membres du jury pour l'intérêt qu'ils ont manifesté pour ce travail, en honorant par leur présence.

# *Dédicaces*

C'est avec un immense plaisir que je dédie mon mémoire à ma famille, qui a été mon roc et ma source de soutien inconditionnel tout au long de mon parcours académique. Je souhaite exprimer ma gratitude à mon frère aîné, qui a été mon garde-malade dévoué pendant mon hospitalisation, et au chirurgien qui a sauvé ma vie, ainsi qu'à tout le personnel médical, en particulier le Dr MEZOUED, pour son expertise et son soin exceptionnel.

Je tiens également à rendre hommage à mes amis et mes collègues, en particulier mon binôme Lyes et mon meilleur ami depuis l'enfance H. Fateh, ainsi que mes anciens collègues M. Youcef et D. Kouceila.

Je tiens à exprimer ma reconnaissance envers mes professeurs à l'université, qui ont partagé leur savoir et leur expertise, et m'ont guidé tout au long de mes études. Leur passion pour l'enseignement a été une source d'inspiration pour moi. Un mot spécial à mon encadrant, suite à son accompagnement, ses conseils précieux et son soutien constant, pour la réalisation de ce mémoire.

Enfin, je souhaite adresser mes remerciements au Directeur de mon premier poste et à mes collègues de travail, qui ont contribué au développement et à l'enrichissement de mon bagage professionnel.

*OUSSAMA.*

# *Dédicaces*

Je dédie ce modeste travail :

A mes chers parents qui m'ont soutenu tout au long de mes études et à qui je souhaite une longue vie.

A mes très chères sœurs (Amel, Massissilia, Lynda, Sabrina) et leurs maris.

A mes tendres neveux Yanis et Aris et ma chère nièce Lina.

A toute ma famille paternelle et maternelle.

A mon binôme Oussama, mes amis et amies, ainsi que toute ma promotion.

A toute personne qui m'a soutenu de près ou de loin durant ce travail.

*LYES.*

## ملخص

الغرض من هذا العمل هو تقديم نهج تعريف متعدد الوسائط للتعرف على الأشخاص باستخدام بصمات مفاصل الأصابع، حيث يتم استخدام الخوارزمية غابور بانك لاستخراج خصائص بصمات مفاصل الأصابع وتقنية التحليل التمييزي الخطي لتقليل الأبعاد. يشتمل نظامنا أيضًا على واجهة لاختبار وتقييم النظام باستخدام طرق بيومترية مختلفة. أظهرت النتائج التجريبية فاعلية نهجنا في قاعدة بيانات بوليو. يفتح هذا البحث آفاقًا واعدة لتطبيق التعريف متعدد الوسائط بناءً على بصمات أصابع مفاصل الأصابع في مجالات مثل الأمان والمصادقة البيومترية. تحديد الكلمات المفتاحية : الوسائط المتعددة، بصمات الأصابع ، نظام القياسات الحيوية ، غابور بانك

## Résumé

Le but de ce travail est de présenter une approche d'identification multimodale des personnes basé sur les empreintes d'articulations des doigts (FKP), en utilisant un descripteur Gabor Bank pour extraire les caractéristiques des empreintes d'articulations des doigts et une technique de réduction de dimensionnalité le LDA. Notre système intègre également une interface permettant de tester et d'évaluer le système en utilisant différentes modalités biométriques. Les résultats expérimentaux ont démontré l'efficacité de notre approche sur la base de données "PolyU". Cette recherche ouvre des perspectives prometteuses pour l'application de l'identification multimodale basée sur les empreintes d'articulations des doigts dans des domaines tels que la sécurité et l'authentification biométrique.

**Mots clés :** identification, multimodale, empreintes d'articulations des doigts (FKP), système biométrique, Gabor Bank.

## Abstract

The purpose of this work is to present a multimodal identification approach of people based on finger joint prints (FKP), using a Gabor Bank descriptor to extract the characteristics of finger joint prints and a technique of dimensionality reduction the LDA. Our system also incorporates an interface to test and evaluate the system using different biometric modalities. The experimental results demonstrated the effectiveness of our approach on the "PolyU" database. This research opens promising perspectives for the application of multimodal identification based on fingerprints of finger joints in areas such as security and biometric authentication.

**Key words :** identification, multimodal, finger joint prints (FKP), biometric system, Gabor Bank.

# Table des matières

|   |             |
|---|-------------|
| <b>Table des matières</b>   | <b>i</b>    |
| <b>Table des figures</b>  | <b>iv</b>   |
| <b>Liste des tableaux</b>   | <b>vii</b>  |
| <b>Liste des abréviations</b>   | <b>viii</b> |
| <b>Introduction générale</b>  | <b>1</b>    |
| <b>1 Biométrie pour l'identification</b>                                | <b>4</b>    |
| 1.1 Introduction . . . . .  | 4           |
| 1.2 La biométrie . . . . .  | 5           |
| 1.2.1 Un bref historique de la biométrie : . . . . .                    | 5           |
| 1.2.2 Définition de la biométrie : . . . . .                            | 5           |
| 1.2.3 Modalités biométriques : . . . . .                                | 7           |
| 1.3 Système Biométrique . . . . .                                       | 18          |
| 1.3.1 Le principe fonctionnement d'un système biométrique : . . . . .   | 18          |
| 1.3.2 Architecture d'un système biométrique : . . . . .                 | 20          |
| 1.3.3 Evaluation des performances des systèmes biométriques : . . . . . | 24          |
| 1.3.4 Les points vulnérable d'un système biométrique : . . . . .        | 29          |
| 1.4 État de l'art sur l'empreinte d'articulation (FKP) : . . . . .      | 31          |
| 1.5 Applications des systèmes biométriques : . . . . .                  | 34          |
| 1.6 Marché de la biométrie : . . . . .                                  | 36          |
| 1.7 Conclusion . . . . .  | 37          |

---

|          |  |           |
|----------|--|-----------|
| <b>2</b> | <b>Système de reconnaissance des formes</b>                        | <b>38</b> |
| 2.1      | Introduction . . . . .   | 38        |
| 2.2      | La reconnaissance des formes : . . . . .                           | 39        |
| 2.2.1    | Définition : . . . . .   | 39        |
| 2.2.2    | Domaine d'application : . . . . .                                  | 39        |
| 2.3      | Processus de la reconnaissance des formes : . . . . .              | 41        |
| 2.3.1    | L'acquisition : . . . . .  | 41        |
| 2.3.2    | Prétraitement : . . . . .  | 41        |
| 2.3.3    | Analyse et segmentation : . . . . .                                | 51        |
| 2.3.4    | Extraction des caractéristiques : . . . . .                        | 54        |
| 2.3.5    | Apprentissage : . . . . .  | 62        |
| 2.3.6    | Post traitement : . . . . .  | 64        |
| 2.3.7    | Décision : . . . . .   | 64        |
| 2.4      | Objectif et les enjeux de la reconnaissance des formes : . . . . . | 65        |
| 2.5      | Conclusion : . . . . .   | 66        |
| <b>3</b> | <b>Expérimentations, Résultats et discussions</b>                  | <b>67</b> |
| 3.1      | Introduction . . . . .   | 67        |
| 3.2      | Architecture globale du système : . . . . .                        | 67        |
| 3.2.1    | Acquisition d'image : . . . . .                                    | 69        |
| 3.2.2    | Prétraitement : . . . . .  | 69        |
| 3.2.3    | Extraction des caractéristiques : . . . . .                        | 70        |
| 3.2.4    | Réduction de la dimension : . . . . .                              | 71        |
| 3.2.5    | Classification : . . . . .   | 71        |
| 3.2.6    | Systèmes proposés : . . . . .                                      | 72        |
| 3.3      | Environnement du travail : . . . . .                               | 73        |
| 3.4      | Résultats et discussion : . . . . .                                | 75        |
| 3.5      | Interface : . . . . .  | 94        |
| 3.5.1    | Description de l'interface : . . . . .                             | 94        |
| 3.5.2    | Objectif de l'interface : . . . . .                                | 94        |
| 3.5.3    | Utilisation de l'interface : . . . . .                             | 95        |
| 3.5.4    | Les avantages et les limites de l'interface : . . . . .            | 104       |
| 3.6      | Conclusion . . . . .   | 104       |

|                            |            |
|----------------------------|------------|
| <b>Conclusion générale</b> | <b>105</b> |
| <b>Bibliographie</b>       | <b>107</b> |

# Table des figures

|      |  |    |
|------|--|----|
| 1.1  | ADN [1]. . . . .   | 7  |
| 1.2  | La veine de la main [2] . . . . .  | 8  |
| 1.3  | La reconnaissance faciale [3]. . . . .   | 8  |
| 1.4  | Empreinte digitale [4] . . . . .   | 9  |
| 1.5  | La reconnaissance de l'iris [5]. . . . .   | 9  |
| 1.6  | La reconnaissance de la rétine [6]. . . . .  | 10 |
| 1.7  | La reconnaissance de la géométrie de la main [7]. . . . .  | 10 |
| 1.8  | Empreintes des articulations des doigts (FKP) [8]. . . . .   | 11 |
| 1.9  | La reconnaissance de la signature [9]. . . . .   | 12 |
| 1.10 | La reconnaissance vocale [10]. . . . .   | 12 |
| 1.11 | La reconnaissance de la démarche [7] . . . . .   | 13 |
| 1.12 | La reconnaissance de la dynamique de frappe au clavier [11]. . . . .   | 14 |
| 1.13 | Mode enrôlement . . . . .  | 18 |
| 1.14 | Mode authentification [12]. . . . .  | 19 |
| 1.15 | Mode identification [12]. . . . .  | 20 |
| 1.16 | L'architecture générale d'un système biométrique [13] . . . . .  | 22 |
| 1.17 | Matrice de confusion [14]. . . . .   | 25 |
| 1.18 | Taux de vraisemblance des utilisateurs légitimes et des imposteurs dans un système biométrique [15]. . . . . | 28 |
| 1.19 | Courbe ROC [16] . . . . .  | 28 |
| 1.20 | Courbe CMC [17] . . . . .  | 29 |
| 1.21 | Points d'attaques possibles dans un système biométrique. . . . .   | 29 |
| 1.22 | Empreintes des articulations des doigts [18] . . . . .   | 34 |

|      |  |    |
|------|--|----|
| 1.23 | Progression du marché mondiale de la biométrie [19]. . . . .                                     | 36 |
| 1.24 | Parts de marché des divers technologie biométriques [19]. . . . .                                | 36 |
| 2.1  | Schéma de processus de reconnaissance des formes [20] . . . . .                                  | 41 |
| 2.2  | Représentation 3D d'une courbe gaussienne en deux dimensions [21]. . . . .                       | 43 |
| 2.3  | Filtrage gaussien à une images [22]. . . . .   | 44 |
| 2.4  | Appliquer filtre médian sur un pixel [23]. . . . .   | 45 |
| 2.5  | Appliqué filtrage médian à une image [23]. . . . .   | 46 |
| 2.6  | Appliquer filtre bilatéral sur un pixel [24]. . . . .  | 46 |
| 2.7  | La combinaison des poids spatiaux et l'intensité pour préserver les contours.<br>[24]. . . . .   | 47 |
| 2.8  | Appliqué filtrage bilatéral à une image [24]. . . . .  | 47 |
| 2.9  | La transformation T permet d'égaliser l'histogramme et d'améliorer le<br>contraste [25]. . . . . | 50 |
| 2.10 | Matrice des pixels d'une partie d'une image donnée [26]. . . . .                                 | 51 |
| 2.11 | Localisation de l'axe X [27]. . . . .  | 52 |
| 2.12 | Image coupée [27]. . . . .   | 52 |
| 2.13 | Applications de contour Canny [27]. . . . .  | 52 |
| 2.14 | Codage [27]. . . . .   | 53 |
| 2.15 | Image ROI [27]. . . . .  | 53 |
| 2.16 | Filtre de Gabor [28]. . . . .  | 56 |
| 2.17 | Sous-images de l'image originale et grandeurs des résultats de filtre Gabor<br>[29]. . . . .     | 57 |
| 2.18 | Création des cellules blocs [30]. . . . .  | 58 |
| 2.19 | Création des cellules blocs [30]. . . . .  | 58 |
| 2.20 | Création d'histogramme pour chaque cellule [30]. . . . .   | 59 |
| 2.21 | des étapes pour génération du vecteur des caractéristiques par la méthode<br>LPQ [31]. . . . .   | 61 |
| 2.22 | Apprentissage supervisé [32]. . . . .  | 63 |
| 2.23 | Apprentissage non supervisé [33]. . . . .  | 63 |
| 2.24 | Apprentissage par renforcement [34]. . . . .   | 64 |
| 3.1  | L'architecture générale de notre système . . . . .   | 68 |

|  |     |
|--|-----|
| 3.2 Quelques images de la base de données PolyU . . . . .                      | 70  |
| 3.3 Résultat de l'application du Filter Gabor Bank sur une image FKP . . . . . | 70  |
| 3.4 résultat d'application du HOG sur une image FKP . . . . .                  | 71  |
| 3.5 Courbe ROC de la méthode Gabor Bank du système unimodal. . . . .           | 76  |
| 3.6 Courbe CMC de la méthode Gabor Bank du système unimodal. . . . .           | 77  |
| 3.7 Courbe ROC de la méthode LPQ du système unimodal. . . . .                  | 78  |
| 3.8 Courbe CMC de la méthode LPQ du système unimodal. . . . .                  | 79  |
| 3.9 Courbe ROC de la méthode HOG du système unimodal. . . . .                  | 80  |
| 3.10 Courbe CMC de la méthode HOG du système unimodal. . . . .                 | 81  |
| 3.11 Courbe ROC de la méthode Gabor Bank du système multimodal. . . . .        | 83  |
| 3.12 Courbe CMC de la méthode Gabor Bank du système multimodal. . . . .        | 83  |
| 3.13 Courbe ROC de la méthode LPQ du système multimodal. . . . .               | 85  |
| 3.14 Courbe CMC de la méthode LPQ du système multimodal. . . . .               | 86  |
| 3.15 Courbe ROC de la méthode HOG du système multimodal. . . . .               | 88  |
| 3.16 Courbe CMC de la méthode HOG du système multimodal. . . . .               | 88  |
| 3.17 Comparaison ROC entre les 3 descripteurs dans un système multimodal. . .  | 91  |
| 3.18 Comparaison CMC entre les 3 descripteurs dans un système multimodal. . .  | 92  |
| 3.19 Interface d'utilisateur . . . . .   | 95  |
| 3.20 Bouton charger image . . . . .  | 96  |
| 3.21 Bouton identification . . . . .   | 96  |
| 3.22 Bouton effacer tout . . . . .   | 97  |
| 3.23 Boutons de sélection . . . . .  | 97  |
| 3.24 Bouton de niveau gris . . . . .   | 98  |
| 3.25 Bouton Redimensionnement . . . . .  | 98  |
| 3.26 Slider de luminosité (Brightness) . . . . .                               | 99  |
| 3.27 Slider de contraste . . . . .   | 99  |
| 3.28 Zone des messages . . . . .   | 100 |
| 3.29 Zone de résultat . . . . .  | 101 |
| 3.30 Schéma d'utilisation de l'interface . . . . .                             | 101 |
| 3.31 Les étapes d'utilisation de l'interface . . . . .                         | 102 |
| 3.32 Le fonctionnement du l'interface . . . . .                                | 103 |

# Liste des tableaux

|      |  |    |
|------|--|----|
| 1.1  | Les avantages et les inconvénients des différents modalités biométriques [35]. | 17 |
| 3.1  | Résultats de ROR et EER de Gabor Bank du Système unimodal. . . . .             | 75 |
| 3.2  | Résultats de ROR et EER de LPQ du Système unimodal. . . . .                    | 77 |
| 3.3  | Résultats de ROR et EER de HOG du Système unimodal. . . . .                    | 79 |
| 3.4  | Résultats de ROR et EER de Gabor Bank du Système multimodal. . . . .           | 82 |
| 3.5  | Résultats de ROR et EER de LPQ du Système multimodal. . . . .                  | 84 |
| 3.6  | Résultats de ROR et EER de HOG du Système multimodal. . . . .                  | 87 |
| 3.7  | Comparaison ROR de 3 descripteurs pour le système monomodale . . . . .         | 89 |
| 3.8  | Comparaison EER de 3 descripteurs pour le système monomodale . . . . .         | 89 |
| 3.9  | Comparaison ROR de 3 descripteurs pour le système multimodale . . . . .        | 90 |
| 3.10 | Comparaison l'EER de 3 descripteurs pour le système multimodale . . . . .      | 90 |
| 3.11 | Comparaison des ROR avec certains travaux dans la littérature. . . . .         | 93 |

# Liste des abréviations

- FKP : Finger Knuckle Print.
- ADN : Acide Désoxyribose Nucléique.
- FAR : False Accept Rate (Taux de fausse acceptation).
- FRR : False Reject Rate (Taux de faux rejet).
- EER : Error Equal Rate (Taux d'égal erreur).
- ROC : Receiver Operating Characteristic.
- CMC : Cumulative Match Score Curs.
- SQI : Self-Quotient Image.
- RDF : Reconnaissance Des Formes.
- ROI : Region of Interest (Région d'intérêt).
- LBP : Méthode Binaire Locale.
- LDA : Linear Discriminate Analysis.
- HOG : Histogram Of Oriented Gradients.
- LPQ : Local Phase Quantization.
- ROR : Rank One Recognition Rate.
- K-NN : K-Nearest Neighbors.
- LIF : Left Index Finger.
- LMF : Left Major Finger
- RIF : Right Index Finger
- RMF : Right Major Finger
- PhD : Pretty helpful Development.

# Introduction générale

L'utilisation de la biométrie est devenue de plus en plus répandue ces dernières années, offrant un moyen très précis et sécurisé d'identifier les individus. Les systèmes biométriques utilisent des caractéristiques physiques ou comportementales uniques, telles que les empreintes digitales, les modèles d'iris, les traits du visage ou les modèles de voix, pour authentifier l'identité. Cette technologie a trouvé des applications dans divers domaines, notamment l'application de la loi, le contrôle d'accès et le contrôle des frontières. La biométrie a le potentiel de transformer la façon dont nous identifions les individus, en la rendant plus rapide, plus précise et plus sûre que les méthodes traditionnelles.

Il existe traditionnellement deux manières d'identifier un individu. La première méthode est basée sur la connaissance d'un mot de passe utilisé par la personne par exemple ou le code du verrouillage de téléphone portable ou une carte bancaire. La seconde méthode est basée sur une possession qui peut être une pièce d'identité, une clef ou un badge, etc. L'utilisation de ces deux méthodes ensemble peut augmenter la sécurité. Cependant, ils sont faibles et vous risquez d'oublier votre mot de passe ou de perdre votre carte d'identité ou votre badge.

Malgré les avantages de la technologie biométrique, les implications éthiques et sociales de son utilisation suscitent des inquiétudes. Les systèmes biométriques peuvent perpétuer les préjugés et la discrimination, en particulier contre les groupes marginalisés. De plus, la collecte, le stockage et l'utilisation des données biométriques soulèvent des problèmes liés à la confidentialité, à la surveillance et à la sécurité des données. Alors que la technologie biométrique devient de plus en plus répandue, il est important d'examiner ses avantages et ses limites, ainsi que son impact sur les systèmes de la sécurité. Ici nous examinerons brièvement les principales technologies biométriques utilisées aujourd'hui. En

ce qui concerne les caractéristiques physiques, nous aborderons la reconnaissance faciale, les thermogrammes faciaux, les empreintes digitales, la géométrie de la main, la rétine et l'iris. Parmi les caractéristiques comportementales, nous explorerons les systèmes basés sur la voix et la signature. Il convient de mentionner qu'il existe d'autres méthodes biométriques basées sur des caractéristiques telles que les veines de la main, l'ADN, l'odeur corporelle, la forme de l'oreille, la forme des lèvres, le rythme de frappe sur un clavier, et même la démarche, qui ne seront pas abordées ici. Il est important de noter qu'aucune caractéristique biométrique n'est universellement idéale. Chaque application requiert des mesures biométriques adaptées en fonction de ses besoins spécifiques.

L'empreinte de l'articulation du doigt, également connue sous le nom de FKP (finger knuckle print), est l'un des nombreux traits utilisés en biométrie. Cette fonctionnalité a attiré l'attention des chercheurs car elle repose sur des images facile à capture, ce qui permet un traitement rapide et une stabilité à vie des individus.

Ce travail vise à réaliser un système de reconnaissance des personnes par leurs empreintes d'articulation des quatres doigts. Le manuscrit est séparé en quatre chapitres comme le suivant :

Le premier chapitre de ce mémoire est consacré à la biométrie. Nous commencerons par une introduction, ensuite, nous explorerons les fondements de la biométrie, son historique et les différentes modalités biométriques. Enfin, nous conclurons ce chapitre en résumant les principaux points abordés.

Dans le deuxième chapitre nous présenterons le système de reconnaissance des formes. Nous débuterons par une introduction, nous examinerons ensuite les différentes étapes du processus de reconnaissance des formes. Nous discuterons également des objectifs et des enjeux de la reconnaissance des formes

Le troisième chapitre sera dédié aux résultats et aux discussions. Nous présenterons l'architecture globale de notre système de reconnaissance biométrique multimodale par fusion des empreintes d'articulation des doigts, en mettant en évidence les différentes étapes. Nous discuterons des résultats obtenus lors des tests et des évaluations réalisés. Nous aborderons également l'environnement de travail dans lequel notre système a été développé. Enfin, nous conclurons ce chapitre en présentant les résultats obtenus, et nous présentons l'interface utilisé pour tester l'approche proposé de notre mémoire.

Finalement, dans la conclusion générale de ce mémoire de fin d'études, nous ferons une

synthèse des principaux résultats obtenus et des contributions apportées dans le domaine de la reconnaissance biométrique multimodale par fusion des empreintes d'articulation des doigts.

# Biométrie pour l'identification

## 1.1 Introduction

Les méthodes de sécurité classique ou l'utilisation de caractéristiques personnelles comme les marques traditionnelle (carte, badge, clé, mot de passe etc.) qui sont utilisés pour valider l'identité d'une personne n'est pas une solution fiable d'authentification. Il est donc recommandé de développer des nouvelles solutions technologiques et des méthodes d'authentification personnelle plus cohérentes et plus réalistes pour contrôler la criminalisation et la fraude quotidiennes dans diverses activités sociales et commerciales. Parmi ces technologies, **la biométrie** s'est rapidement distinguée comme la plus pertinente pour identifier et authentifier les personnes de manière fiable et rapide, en fonction de caractéristiques biologiques uniques.

Dans ce chapitre nous introduirons tout d'abord quelques notions et définitions de base liées à la biométrie et jeter un coup d'oeil à son l'historique et nous explorerons les différentes modalités biométriques existantes. Ensuite, nous allons présenter les conditions nécessaires pour être qualifier de la biométrie, les modalités et les technologies biométriques telle que leurs définition leurs avantages, les inconvénients, leurs capteurs utilisés et les applications de chacun nous avons discuté un peu à l'identification et l'authentification.

Dans notre démarche d'évaluation, nous discuterons des méthodes utilisées pour mesurer les performances des systèmes biométriques. Enfin, nous aborderons les points vulnérables et une petite comparaison entre les modalités les plus utilisées et nous terminerons ce chapitre avec une conclusion qui résume tout.

## 1.2 La biométrie

### 1.2.1 Un bref historique de la biométrie :

La biométrie est une préoccupation depuis des siècles. Prouver son identité de manière fiable a été fait à l'aide de plusieurs techniques. Depuis longtemps, les gens connaissent le caractère unique des empreintes digitales, ce qui signifie que les signatures d'empreintes digitales suffisent à confirmer l'identité d'une personne. En effet, deux siècles avant Jésus-Christ, l'Empereur Ts-In-She authentifiait certains scellés de l'empreinte digitale.

Il y a 1000 ans, Les Chinois ont été les premiers à utiliser les empreintes digitales à des fins de signature de documents [36].

Au début du XIX<sup>e</sup> siècle en France, Alphonse Bertillon fait ses premiers pas dans la police scientifique. Il propose la première méthode biométrique que l'on peut qualifier d'approche scientifique : le bertillonnage qui est basé sur un ensemble de mesures anthropométriques comme la longueur de la main ou la distance entre les yeux.

Depuis lors, de nombreuses autres caractéristiques physiques ont été étudiées pour reconnaître les humains. On peut citer les premiers travaux sur la reconnaissance faciale au Japon en 1973 par Takeo Kanade ou les travaux sur l'iris de John Daugman en 1994. Plusieurs chercheurs ont également proposé au début des années 2000 d'utiliser différentes biométries pour construire un système multimodal plus efficace que les systèmes existants sur une seule modalité. En 2010, le programme d'identité numérique le plus ambitieux au monde appelé Aadhaar (une identité pour tous) basée sur de multiples modalités a été introduite en Inde [37].

La biométrie est en constante évolution, notamment dans le domaine des documents d'identité sécurisés tels que les cartes d'identité, les passeports et les permis de conduire. Cette technologie fonctionne sur de nouvelles plates-formes, y compris les cartes à puce à microprocesseur.

### 1.2.2 Définition de la biométrie :

Le terme "biométrie" est dérivé de la combinaison de deux anciens termes grecs : "bios", qui signifie "vie", et "metron", qui se traduit par "mesure" [38].

La biométrie a émergé pour répondre aux lacunes des systèmes d'accès traditionnels. La littérature propose plusieurs définitions de la biométrie telles que :

« La biométrie se réfère à l'identification automatique d'une personne en se basant sur son comportement ou ses caractéristiques physiques distinctives. » [39].

«À l'origine, le terme "biométrie" était utilisé pour décrire l'application des méthodes de mesure mathématiques dans le domaine de la biologie. Aujourd'hui, il englobe un large éventail de techniques, d'appareils et de systèmes permettant aux machines de reconnaître les individus et de confirmer ou d'authentifier leur identité. » [40].

La biométrie englobe un ensemble de technologies qui utilisent des caractéristiques uniques, qu'elles soient physiques ou comportementales, telles que les empreintes digitales, les signatures, les iris, les voix, les visages et les démarches, pour vérifier l'identité d'une personne et la distinguer des autres. Elle offre ainsi une solution efficace pour prévenir la duplication, le vol et la fraude.

- **Les caractéristique de la biométrie :**

Les traits physiologiques, comportementales et biologiques de l'être humain doivent répondre à un certain nombre d'exigences biométriques pour être utilisés comme une modalité biométrique ou dans une application biométrique [41].

- **L'universalité** : Cela implique que chaque individu devrait avoir des caractéristiques.

- **Unicité (singularité)** : Cela suggère que deux individus ne devraient pas avoir les mêmes caractéristiques.

- **La permanence** : ce qui désigne que les caractéristiques doivent être invariantes avec le temps.

- **Recouvrement (collectability)** : Il est crucial que les informations puissent être collectées et mesurées de manière à être utilisées pour les comparaisons ultérieures.

- **Performance** : Cela se réfère à l'efficacité globale du système, incluant des aspects tels que la précision, la vitesse, la gestion des erreurs et la robustesse.

- **L'acceptabilité** : Cela fait référence au degré d'acceptation des individus au système biométrique.

- **Le contournement (circumvention)** : Cela fait référence à la vulnérabilité du système face à des techniques frauduleuses permettant de le tromper.

### 1.2.3 Modalités biométriques :

Il existe une gamme assez large de modalités biométriques, de nouvelles modalités étant ajoutées en permanence, En effet, aucune modalité ne peut garantir à la fois une précision suffisante et un confort d'utilisation dans toutes les conditions d'usage. Chaque modalité biométrique présente des avantages et des inconvénients spécifiques, et le choix dépend généralement de l'application considérée.

Il existe de nombreuses modalités biométriques et elles peuvent être classées en deux catégories :

■ **L'analyse des traces biologiques** : Implique l'utilisation de données biologiques spécifiques à l'être humain telle que l'ADN, l'odeur, l'urine et la salive. Toutefois, l'intégration de ce type de biométrie dans un système de reconnaissance courant est extrêmement complexe et n'est utilisée que dans des cas d'absolue nécessité, tels que les enquêtes criminelles ou les tests de paternité [42].

Les technologies les plus couramment utilisées comprennent les suivantes :

- **Acide DésoxyriboNucléique (ADN)** : Qui renferme le code génétique d'une personne, est considéré comme la marque biologique la plus fiable au monde . Utilisé couramment en criminologie pour l'identification d'un individu à travers un échantillon de peau, de cheveux ou de sang, son analyse nécessite toutefois des délais de plusieurs semaines, ce qui limite son utilisation dans les applications de reconnaissance en temps réel.[1].



FIGURE 1.1 – ADN [1].

- **La veine de la main** : Le réseau veineux palmaire est unique à chaque individu, même dans le cas de jumeaux identiques. Pour être identifié, il suffit de placer la paume de la main sur le lecteur, le motif veineux est ensuite détecté et comparé aux motifs

enregistrés afin d'authentifier l'individu.



FIGURE 1.2 – La veine de la main [2]

■ **L'analyse des caractéristiques physiques** : Elle est basée sur l'analyse de la morphologie ou le comportements d'un individu. Elle est généralement facile à mettre en œuvre et peut être regroupée en deux principales catégories :

- **La biométrie morphologique** :

- **La reconnaissance de visage** : Le visage humain est la plus répandue et la plus populaire. C'est aussi le plus accepté car il correspond à ce que les humains utilisent dans l'interaction visuelle. Les éléments considérés comme importants pour la reconnaissance faciale comprennent les yeux, la bouche et la structure générale du visage.



FIGURE 1.3 – La reconnaissance faciale [3].

- **Empreinte digitale** : L'empreinte digitale est le motif formé par les lignes de la peau des doigts et constitue une caractéristique unique pour chaque individu. Pour s'authentifier, l'utilisateur place son doigt sur un lecteur d'empreintes digitales. Le système de classification repose sur la reconnaissance de certains éléments

distinctifs appelés minuties, tels que les lacunes, les bifurcations, les deltas ou les impasses. Chaque doigt contient entre 50 et 200 de ces traits mineurs, fournissant ainsi un grand nombre de données pour l'extraction des caractéristiques.



FIGURE 1.4 – Empreinte digitale [4]

- **La reconnaissance de l'iris :** L'iris désigne la région colorée située entre le blanc de l'œil et la pupille (voir figure 1.5), L'image de l'iris est exceptionnellement structuré et offre de nombreuses caractéristiques de texture propres à chaque individu, cette image est photographié par un appareil qui contient une caméra infrarouges.



FIGURE 1.5 – La reconnaissance de l'iris [5].

- **La reconnaissance de la rétine** : est une méthode relativement ancienne par rapport à l'iris. Ce qui aide à différencier les individus dans cette méthode est le motif formé par les veines rétiniennes. La forme de ces veines est stable et propre à chaque individu. Les motifs générés héritent de cette stabilité de cette disposition, ce qui empêche les imposteurs de reproduire ces modèles. Cela garantit un très haut niveau de sécurité.[6].

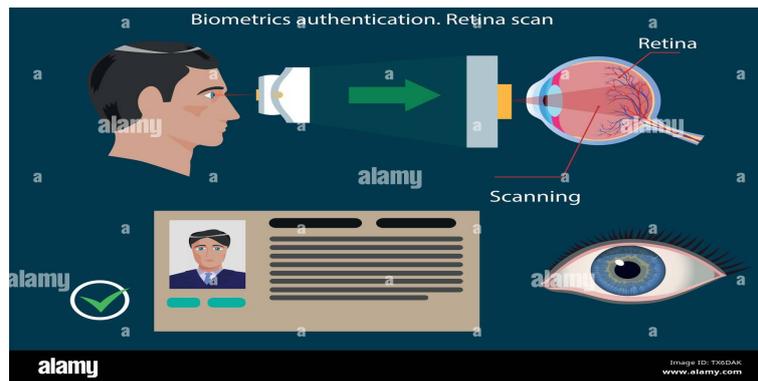


FIGURE 1.6 – La reconnaissance de la rétine [6].

- **La reconnaissance de la géométrie de la main** : Ce type de mesure consiste à prendre les dimensions des doigts, les caractéristiques des articulations, la paume et la forme de la main. Les systèmes biométriques utilisant la forme de la main sont simples à mettre en oeuvre et sont très bien acceptée par les utilisateurs. Cependant, ils sont facilement dupés par des jumeaux identiques ou des membres de la même famille. [43].

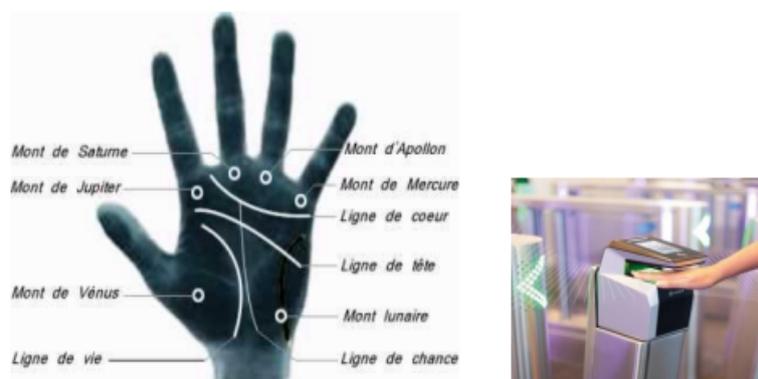


FIGURE 1.7 – La reconnaissance de la géométrie de la main [7].

- **Empreinte des articulations des doigts (FKP)** : Il s'agit d'une technologie biométrique qui se base sur la surface arrière du doigt, contenant des caractéristiques distinctives telles que les lignes primaires, les lignes secondaires et les crêtes. Ces caractéristiques peuvent être extraites à partir d'images à basse résolution. Récemment, une nouvelle approche biométrique basée sur la surface extérieure du doigt, appelée empreinte de l'articulation du doigt, a été développée. Étant donné que la main est composée de plusieurs doigts, le stockage d'informations uniques pour chaque doigt est important pour assurer une reconnaissance précise et robuste dans le domaine de l'identification. [8].

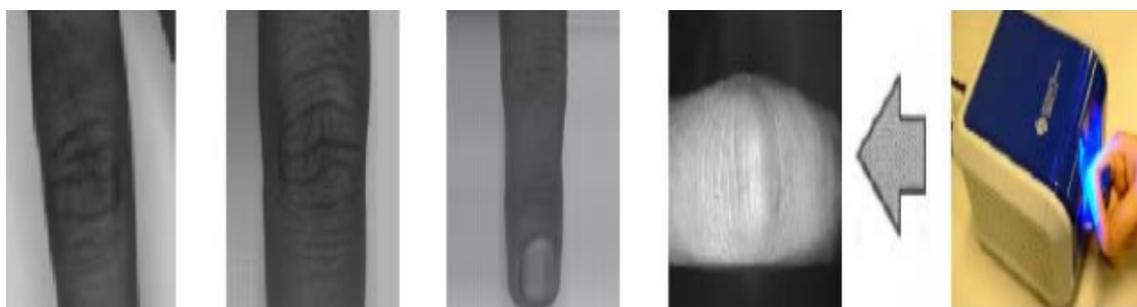


FIGURE 1.8 – Empreintes des articulations des doigts (FKP) [8].

- **La biométrie comportementale** : Cette méthode de reconnaissance se concentre sur les traits physiques en activité des individus, qui peuvent être communs et permettre de faire la distinction entre eux. Plus précisément, nous examinons le comportement des personnes.

À titre d'exemple nous citons :

- **La reconnaissance de la signature** : Chaque personne a une signature unique qui peut être utilisée pour les identifier. Par rapport à d'autres biométries, elle a l'avantage d'être largement utilisée pour les transactions. Pour cette raison, une signature est généralement bien acceptée comme moyen d'identification. Deux modes de reconnaissance sont disponibles : le mode statique et le mode dynamique.

**Mode statique** : Il utilise que l'information géométriques de la signature.

**Mode dynamique :** La capture des signatures s'effectue en utilisant une tablette graphique. Ce mode d'acquisition exploite à la fois des informations géométriques et dynamiques, ainsi que les variations de pression exercées sur la tablette graphique, parmi d'autres paramètres. Comparé au mode statique, le mode dynamique qui prend en compte ces aspects dynamiques offre une plus grande quantité d'informations, le rendant ainsi plus discriminant.



FIGURE 1.9 – La reconnaissance de la signature [9].

- **La reconnaissance vocale :** La reconnaissance vocale conçu à reconnaître les caractéristiques uniques de la voix de chaque individu. Ces caractéristiques sont influencées à la fois par l'anatomie (taille et forme de la gorge et de la bouche) et par des modèles de comportement acquis (hauteur de voix, manière de parler, tonalité). Ainsi, cette modalité biométrique est considérée à la fois comme physiologique et comportementale. La voix est directement affectée par des facteurs physiques tels que le nez, la bouche, les cordes vocales ainsi que des facteurs émotionnels, la langue maternelle, les conditions médicales et d'autres paramètres. Il est donc nécessaire d'appliquer des méthodes visant à éliminer certaines de ces variations.



FIGURE 1.10 – La reconnaissance vocale [10].

- **La reconnaissance de la démarche** : Il s'agit de reconnaître une personne par sa façon de marcher et de bouger. Lorsqu'une personne marche (voir figure 1.11), différentes parties du corps (jambes, genoux, bras, coudes, etc.), décrivent un mouvement spécifique qui se répète. Une caméra vidéo enregistre ces points mobiles et les envoie à un ordinateur qui les analyse. L'ordinateur enregistre la séquence de mouvement et effectue le calcul pour chaque point afin de créer la signature de la démarche telles que la vitesse et l'accélération dont il a besoin pour reconnaître chaque personne. Comparée aux autres méthodes telles que l'empreinte digitale ou l'iris, cette méthode de reconnaissance biométrique ne nécessite aucune intervention de l'utilisateur et permet une reconnaissance à distance, à condition que la démarche soit visible. De plus, il est difficile de la dissimuler. Toutefois, cette méthode présente l'inconvénient d'avoir un taux de reconnaissance relativement faible en raison de sa grande variabilité d'une personne à l'autre. En effet, plusieurs facteurs tels que l'âge, l'humeur, la maladie, la fatigue et la consommation d'alcool peuvent influencer la démarche, ce qui rend la reconnaissance moins fiable. [7].



FIGURE 1.11 – La reconnaissance de la démarche [7]

- **La dynamique de frappe au clavier** : Le typage dynamique, propre à chaque individu, fournit suffisamment d'informations pour confirmer l'identité d'un individu. Pour s'identifier, l'utilisateur doit entrer un mot ou une phrase fixe (comme un nom ou un mot de passe) et le logiciel extrait et analyse certains paramètres caractéristiques qui définissent cette personne, tels que :

- la vitesse de frappe.
- la suite de lettres.
- la mesure de temps de frappe.
- la pause entre chaque mot et la reconnaissance de mot(s) précis.

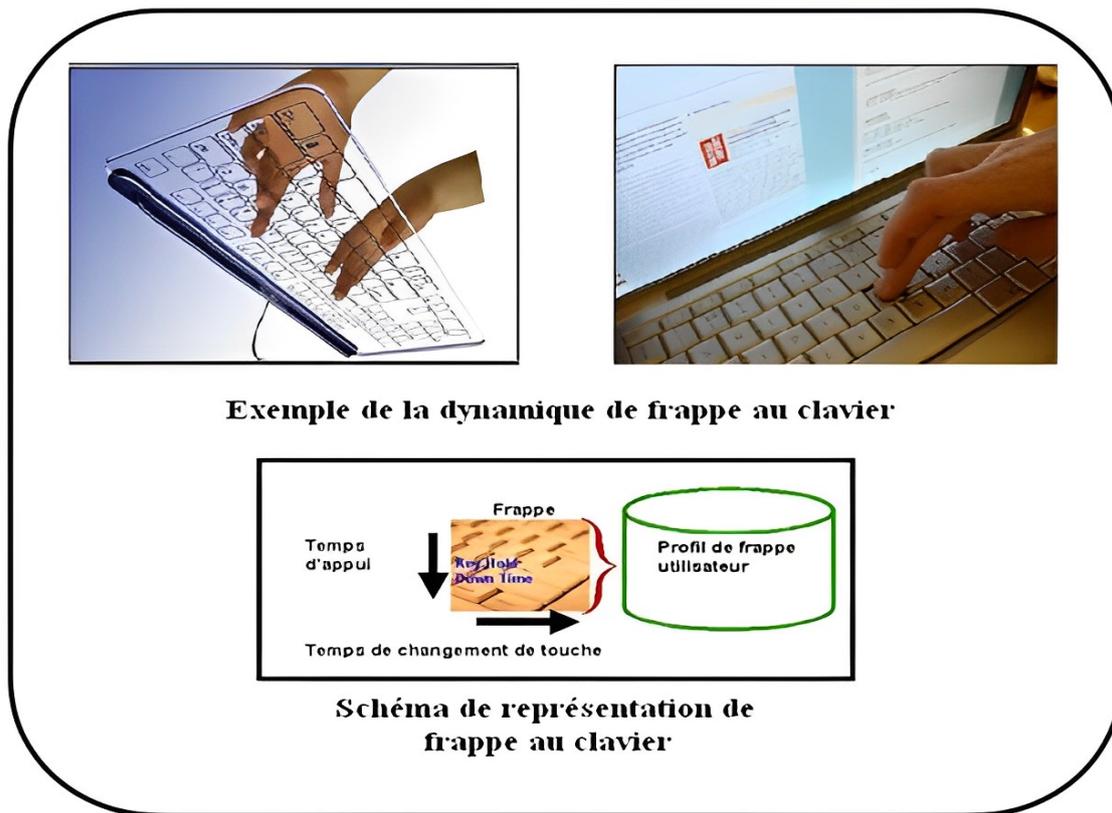


FIGURE 1.12 – La reconnaissance de la dynamique de frappe au clavier [11].

Chaque technologie a des avantages et des inconvénients selon l'application. Le tableau (1.1) résume une comparaison des traits biométriques.

| Modalité             | Avantage   | Inconvénient   |
|----------------------|--|--|
| Empreintes digitales | <ul style="list-style-type: none"> <li>-Prix faible.</li> <li>-La technologie la plus testée techniquement et la plus connue.</li> <li>-La petite taille du lecteur permet une intégration dans la plupart des applications.</li> <li>-Très discriminante et facile à mettre en oeuvre.</li> </ul>           | <ul style="list-style-type: none"> <li>-Exige un environnement propre.</li> <li>-Votre coopération est requise (placement correct des doigts sur le lecteur).</li> <li>-possibilité d'attaques (rémanence de l'empreinte,...).</li> <li>-L'enregistrement se fait par contact, ce qui peut entraîner des réticences d'ordre psychologique ou hygiénique.</li> </ul>                                |
| Visage               | <ul style="list-style-type: none"> <li>-Très bien acceptée par le public.</li> <li>-Simple et capable de fonctionner sans la collaboration de la personne (pas de contacte physique).</li> <li>-Une technologie peu coûteuse qui peut s'appuyer sur l'équipement d'acquisition des images actuel.</li> </ul> | <ul style="list-style-type: none"> <li>-Les vrais jumeaux identiques sont indiscernables</li> <li>-Techniques sensible au contexte (éclairage, emplacement, expression faciale...).</li> <li>-Sensible aux changements (barbe, moustache, lunette, chirurgie).</li> </ul>  |
| Iris                 | <ul style="list-style-type: none"> <li>-L'iris contient beaucoup d'informations.</li> <li>-Les vrais jumeaux ne sont pas confondus.</li> <li>-Les structures de l'iris restent toujours stables.</li> </ul>  | <ul style="list-style-type: none"> <li>-La fiabilité diminue avec la distance entre les yeux et la caméra.</li> <li>-Le matériel est plus coûteux avec exigences sur l'éclairage.</li> <li>-Les gens ont du mal à accepter ce genre de biométrie.</li> <li>-L'acquisition d'images peut causer un certain inconfort utilisateurs, cela peut empêcher certaines personnes de s'inscrire.</li> </ul> |

|                         |   |  |
|-------------------------|---|--|
| Rétine                  | <ul style="list-style-type: none"> <li>-Faible taux d'erreur (1 sur 10 millions).</li> <li>-Technique extrêmement précise (grande fiabilité).</li> <li>-Risques de fraude sont quasi nuls.</li> </ul>   | <ul style="list-style-type: none"> <li>-Pourrait être pareil pour les jumeaux ou des membres de la famille.</li> <li>-Système intrusif, l'oeil doit être placé à proximité du capteur.</li> <li>-Faible acceptation du public, taux d'alcoolémie élevé et le diabète altère le réseau veineux rétinien.</li> <li>-Les mesures doivent être prises à faible distance du capteur.</li> </ul> |
| La géométrie de la main | <ul style="list-style-type: none"> <li>-Bonne acceptation des usagers.</li> <li>-Facile à utiliser.</li> <li>-Une fiabilité élevée et un temps de traitement rapide.</li> <li>-Les résultats sont indépendants de l'humidité et de la propreté des doigts.</li> </ul> | <ul style="list-style-type: none"> <li>-Danger de faux consentement pour des jumeaux ou des membres et par des blessures.</li> <li>-Technique peu discriminante et sensible aux modifications ou altérations naturelles de la main (accident, vieillissement, arthrose).</li> <li>-difficile à utiliser pour les personnes souffrant d'arthrite.</li> </ul>                                |
| FKP                     | <ul style="list-style-type: none"> <li>-Modalité acceptable.</li> <li>-Facilité d'acquisition touchable et non touchable.</li> <li>-En fusionnant plusieurs FKP, peuvent construire un système biométrie solide et précise.</li> </ul>                                | <ul style="list-style-type: none"> <li>-Très similaire entre les jumeaux.</li> <li>-Un placement incorrect des doigts sur le lecteur peut entraîner une erreur.</li> </ul>   |
| ADN                     | <ul style="list-style-type: none"> <li>-Discrimination très précise entre les individus.</li> <li>-Elle simplifie largement la désignation du coupable.</li> </ul>  | <ul style="list-style-type: none"> <li>-Très cher.</li> <li>-Analyse trop lente pour obtenir les résultats et en particulier en temps réel.</li> </ul>   |

|                  |   |   |
|------------------|---|---|
| Veine de la main | <ul style="list-style-type: none"> <li>-Un réseau interne dur à dupliquer par un imposteur.</li> <li>-Technologie très fiable et ne nécessite pas de contact.</li> <li>-biométrie dite "sans trace".</li> </ul>   | <ul style="list-style-type: none"> <li>-Le capteur est fragile à l'éclairage, mais les fabricants ont prévus une protection pour limiter ce problème.</li> <li>-Pour une bonne reconnaissance, il faut poser correctement la main sur le capteur.</li> <li>-Très couteuse à mettre en œuvre.</li> </ul> |
| Signature        | <ul style="list-style-type: none"> <li>-Acceptation forte par l'utilisateur comme moyen d'identification.</li> <li>-Peut protéger l'ensemble de nos fichiers personnels.</li> </ul>   | <ul style="list-style-type: none"> <li>-Pas utilisable pour du contrôle d'accès.</li> <li>-Varie beaucoup durant le temps (impossible conserver la même forme de signature pour toute la vie).</li> <li>-Les utilisateurs ne sont pas habitués de signer sur une tablette graphique.</li> </ul>         |
| Voix             | <ul style="list-style-type: none"> <li>-Facile à mettre en œuvre et sécurisé.</li> <li>-Largement accepté car le son est un signal naturel.</li> <li>-Dynamique des ondes produites sont uniques.</li> <li>-Une des rares techniques pour reconnaître quelqu'un de loin.</li> </ul> | <ul style="list-style-type: none"> <li>-La sensibilité au bruit et l'état physique et émotionnel de l'individu.</li> <li>-Possibilité de falsification à l'enregistrement.</li> <li>-Nécessite une excellente qualité audio.</li> </ul>   |
| Démarche         | <ul style="list-style-type: none"> <li>-Il peut être vu de loin avec une caméra basse résolution et observée ainsi de n'importe quel angle.</li> <li>-Très acceptable par les individus.</li> </ul>   | <ul style="list-style-type: none"> <li>-Il est sensible aux changements d'habits, chaussures et surface.</li> <li>-Ne pas rester invariant en particulier sur une grande période de temps, en raison de grandes fluctuations de poids ou à cause d'ébriété.</li> </ul>                                  |

TABLE 1.1 – Les avantages et les inconvénients des différentes modalités biométriques [35].

## 1.3 Système Biométrique

Est un système de reconnaissance de formes utilise des données biométriques individuelles, construit des modèles et les compare à un ensemble de données préexistant pour exécuter des actions ou prendre des décisions basées sur la comparaison. [44].

### 1.3.1 Le principe fonctionnement d'un système biométrique :

Le système de reconnaissance biométrique peut être divisé en trois principaux modes : enrôlement, authentification et identification.

- **Mode enrôlement** : Pour l'enregistrement d'un utilisateur dans un système biométrique pour la première fois il faut d'abord passer par cette étape, implique l'enregistrement d'une ou plusieurs modalités biométriques dans une base de données pour une future comparaison. Cela peut inclure des informations biographiques voire le nom et le sexe.

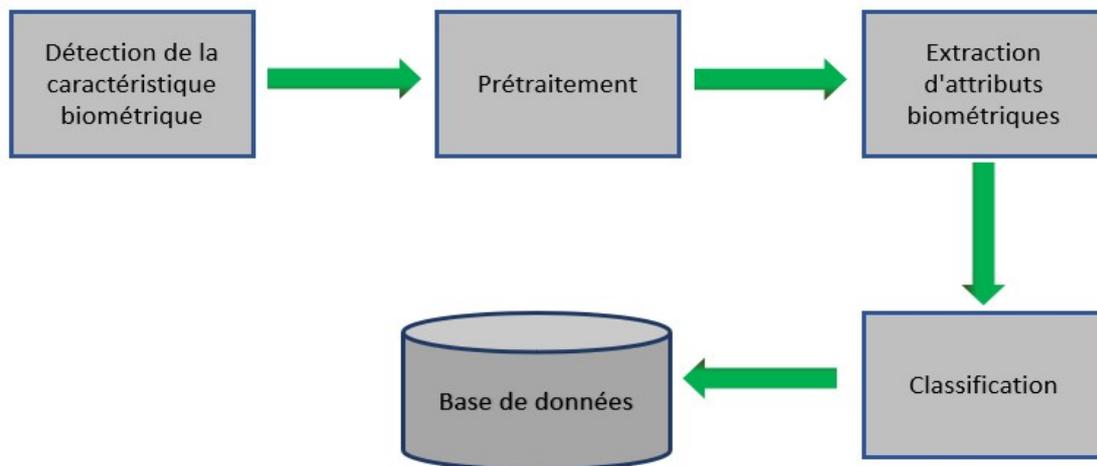


FIGURE 1.13 – Mode enrôlement

- **Mode authentification** : L'authentification biométrique est une méthode utilisée pour vérifier l'identité d'une personne et garantir un accès sécurisé à un système électronique en se basant sur des caractéristiques biologiques uniques. Dans ce processus, une comparaison "un à un" est effectuée, où le système valide l'identité d'une personne en comparant les données biométriques fournies avec le modèle biométrique de cette personne stocké dans la base de données du système.

L'individu qui souhaite être identifié fournit généralement une preuve d'identité, telle qu'un PIN, un nom d'utilisateur ou une carte d'identité. Le système doit répondre à la question suivante : Est-ce que je suis réellement la personne que je prétends être ? [12]

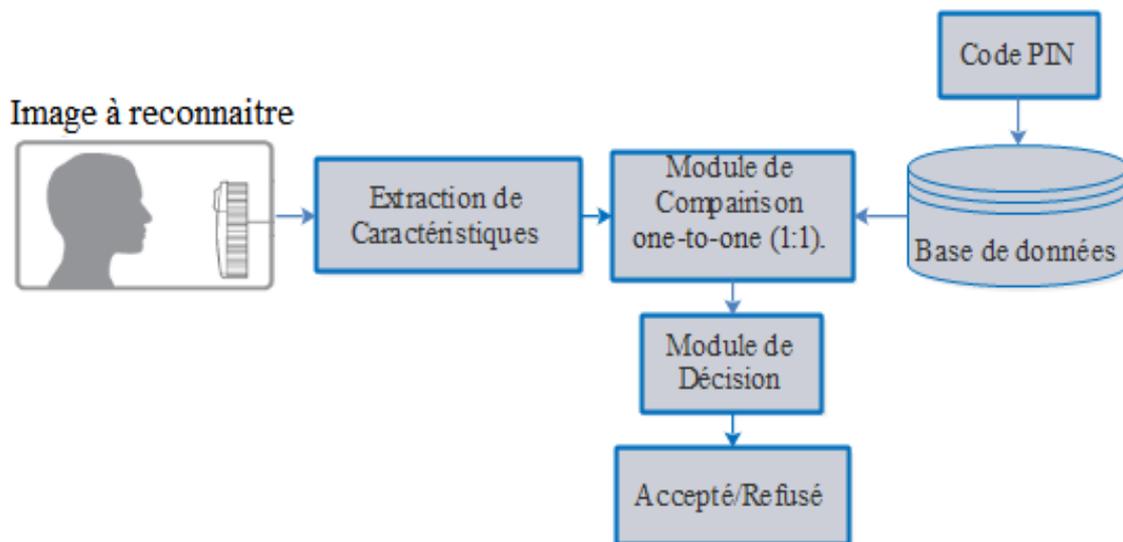


FIGURE 1.14 – Mode authentification [12].

- **Mode identification** : Le système doit déterminer qui est la personne. Il répond à la question de type : qui êtes-vous ? Dans ce mode, le système compare l'échantillon biométrique de l'individu et les différents modèles contenus dans la base de données lors de la phase d'enrôlement (type 1 : N), un échoue si l'individu n'est pas inscrit dans la base de données du système dans le cas contraire il va être accepté. L'identification peut décomposer en deux modes opératoires :

**Identification en mode ensemble fermé** : c'est-à-dire que tous ceux qui utilisent le système ont un modèle dans la base de données. Lorsque l'échantillon a un degré quelconque de similitude avec les échantillons du système, la personne sera acceptée.

**Identification en mode ensemble ouvert** : Dans le cas où l'utilisateur n'est pas accepté (rejeté) cela implique qu'il n'est pas enrôlé dans le système biométrique, et que la plus grande similarité entre l'échantillon et tous les modèles inférieure ou supérieure au seuil de sécurité fixé [12].

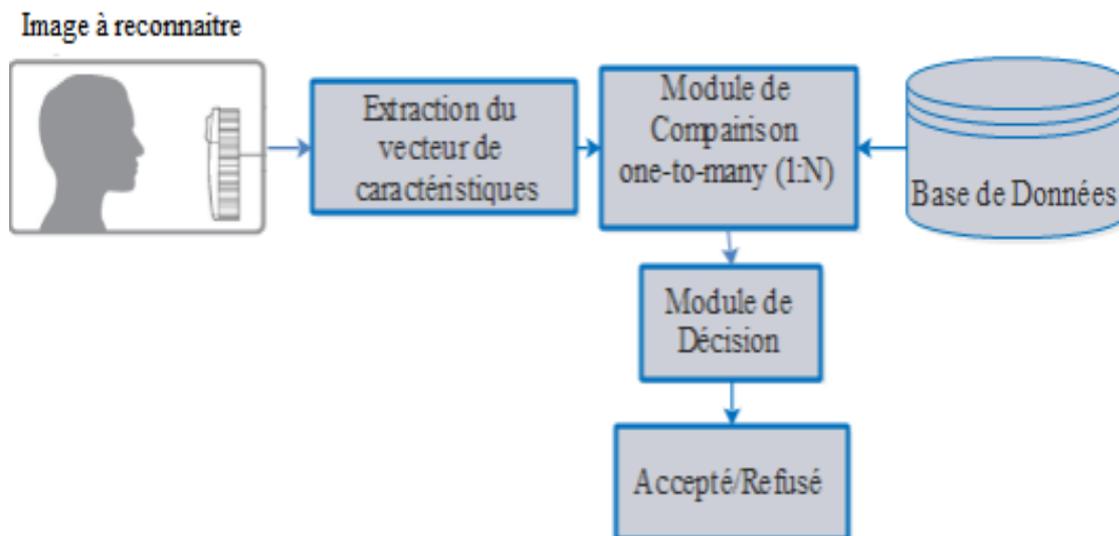


FIGURE 1.15 – Mode identification [12].

### 1.3.2 Architecture d'un système biométrique :

■ **Systèmes biométriques monomodale :** Il s'agit d'un système biométrique à statut unique qui peut reconnaître les individus à partir d'une seule source d'informations pertinentes, mais il souffre de quelques problèmes, notamment des données de capteur alarmantes, l'incapacité de faire la distinction entre la biométrie, le manque d'universalité et les attaques par usurpation d'identité. Ce système est composé de quatre modules : l'acquisition, traitement des données, l'extraction des caractéristiques, la comparaison (module de correspondance) et la prise de décision.

- **Acquisition des données :** Lors de cette étape, les données biométriques d'un individu sont recueillies. Pour capturer les données biométriques physiques, divers dispositifs peuvent être utilisés, tels qu'une caméra, un lecteur d'empreintes digitales, etc. Les informations recueillies sont ensuite sauvegardées sous forme d'image numérique afin d'être traitées ultérieurement.
- **Traitement des données :** Cette étape est utilisée pour réduire le bruit et mettre en évidence les paramètres pertinents et utiles. Cela est réalisé en appliquant une série d'opérations consécutives, telles que le filtrage, la normalisation, etc. L'objectif est de préparer les données biométriques pour une analyse plus précise et efficace.

- **Extraction des caractéristiques** : L'extraction de caractéristiques est le processus par lequel des données uniques sont extraites de l'échantillon et un modèle est créé. Le modèle pour deux personnes doit être différent et pour différents échantillons de la même personne doit être suffisamment similaire.  
Deux types d'approches sont utilisés pour extraire des modèles, la première est que certaines caractéristiques uniques significatives sont prédéfinies et prouvées, par exemple les minuties et les pores sur les empreintes digitales et les yeux, à ce stade, ces caractéristiques sont extraites et transformées en code mathématique. La seconde est qu'aucune caractéristique significative n'est trouvée et que l'échantillon est transformé ou projeté dans d'autres dimensions afin que le bruit soit exploité et que la quantité globale de données soit réduite. Appelons cet échantillon transformé "données raffinées". Ensuite, de nombreux tests sont effectués et il doit être prouvé que la donnée raffinée varie très légèrement pour les échantillons de la même personne, mais diffère fortement des échantillons de deux personnes. Après cette preuve, les données raffinées deviennent des modèles. La voix, l'iris, la rétine et une partie de l'identification du visage utilisent cette approche. La transformation de Fourier (fourier transformation) et la transformation en ondelettes (wavelet transformation) sont les algorithmes les plus couramment utilisés dans cette approche. Cette approche ressemble à la méthode statistique de la reconnaissance de formes traditionnelle dans une certaine mesure [45].
- **Comparaison (module de correspondance)** : c'est un processus par lequel l'ensemble des caractéristiques biométriques extraites est comparé à un standard stocké dans le système (base de données). Étant donné que même les échantillons d'un même individu peuvent différer de temps à autre, l'algorithme de comparaison doit tolérer un léger changement chez le même individu en distinguant les différents individus. Par exemple : le doigt peut entrer en contact avec le scanner en direct à différents endroits, directions et pressions, donc en pratique, il n'y a pas deux échantillons exactement identiques.
- **Décision** : cette étape vérifie l'identité revendiquée d'un utilisateur ou détermine l'identité d'un individu sur la base des similitudes entre les caractéristiques extraites et les modèles stockés.

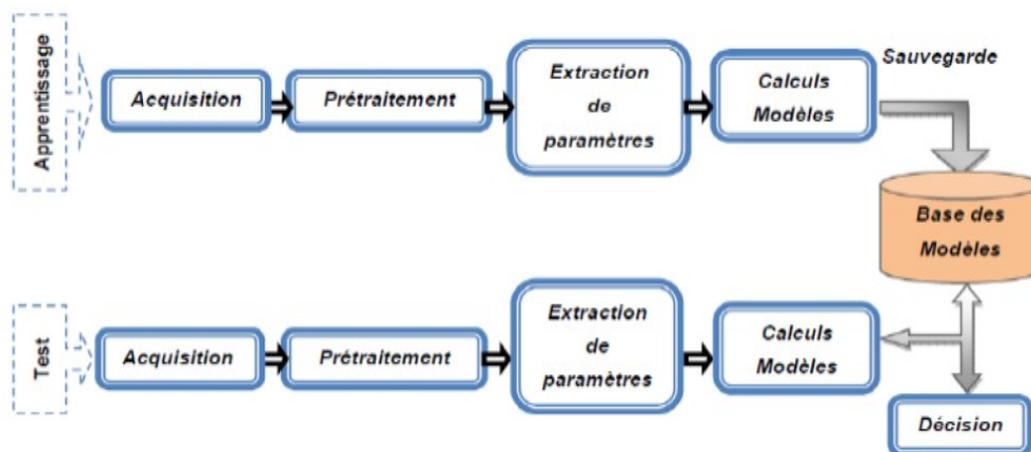


FIGURE 1.16 – L'architecture générale d'un système biométrique [13]

■ **Systèmes biométriques multimodaux** : Les systèmes biométriques uni-modaux ont des limitations dans la performance car ils sont basés sur le degré de correspondance entre les données biométriques comparées, qui ne garantit pas avec certitude une bonne identification. De plus, les systèmes biométriques sont souvent affectés par les problèmes suivants :

- Bruit introduit par le capteur : Les données biométriques collectées peuvent contenir du bruit. Le bruit est généralement causé par une défaillance du capteur ou un mauvais entretien, comme de la poussière sur le capteur d'empreintes digitales ou images floues des visages et de l'iris en raison de réglages incorrects de l'appareil photo. La qualité des échantillons biométriques est essentielle au taux de reconnaissance du système, et les données bruyantes peuvent sérieusement affecter la précision.

- Non universalité : Toutes les modalités biométriques ne sont pas universelles. Cela signifie que certaines personnes peuvent ne pas être en mesure de fournir des modalités biométriques adaptées à leur système particulier. Le National Institute of Standards and Technologies (NIST) a rapporté que environ 2% de la population n'est pas en mesure d'obtenir des empreintes digitales de haute qualité en raison de handicaps liés aux mains ou de travaux manuels répétitifs. De même, les personnes ayant de très longs cils ou des anomalies oculaires peuvent ne pas fournir des images de l'iris et de la rétine de qualité suffisante pour une détection automatique. Cette non-universalité entraîne des erreurs d'enrôlement ("Failure to Enroll" ou FTE) et/ou des erreurs de

capture ("Failure to Capture" ou FTC) dans un système biométrique.

- Manque d'individualité : Il est possible d'avoir des similitudes relativement importantes entre les caractéristiques extraites des données biométriques de différentes personnes. Par exemple, certaines parties de la population peuvent avoir des apparences faciales presque identiques en raison de facteurs génétiques. Ce manque d'unicité augmente le taux de fausse acceptation ("False Accept Rate" ou FAR) d'un système biométrique [46].

- Manque de représentation invariante : Un défi majeur réside dans la représentation invariante des données biométriques. En effet, lors de la phase de reconnaissance, les données biométriques collectées chez un individu peuvent différer de celles utilisées pour créer son modèle lors de la phase d'enrôlement. Ce phénomène est connu sous le nom de "variations intra-classe". Ces variations peuvent être causées par une interaction inadéquate entre l'utilisateur et le capteur, l'utilisation de capteurs différents lors de l'enrôlement et de la vérification, des changements dans les conditions environnementales ou des modifications inhérentes à la modalité biométrique, comme les rides liées au vieillissement ou la présence de cheveux dans une image faciale [47]. Idéalement, les caractéristiques extraites des données biométriques devraient être relativement stables face à ces variations. Cependant, la plupart des systèmes biométriques ne parviennent pas à obtenir cette invariance, ce qui nécessite l'utilisation d'algorithmes complexes pour prendre en compte ces différences. Les variations intra-classe importantes ont tendance à augmenter le taux de faux rejets ("False Reject Rate" ou FRR) d'un système biométrique.[46].

Ainsi à causes de ces limitations, les taux d'erreurs associés aux systèmes biométriques uni-modaux sont élevés, ce qui les rend inacceptable dans un déploiement d'applications critiques de sécurité. Pour pallier ces inconvénients et les limitations rencontrées, une solution consiste à utiliser plusieurs modalités biométriques au sein d'un même système, on parle alors de système biométrique multimodale. La biométrie multimodale fait référence à l'utilisation de plus d'une source d'information pour identifier un individu, par exemple un système biométrique multimodal peut utiliser la reconnaissance d'empreinte d'articulation et la reconnaissance de l'empreinte digitale pour confirmer l'identité d'un utilisateur. De plus, l'utilisation de différentes méthodes biométriques réduit le risque de ne pas pouvoir s'enregistrer ainsi que la robustesse aux fraudes.

### 1.3.3 Evaluation des performances des systèmes biométriques :

Chaque modalité biométrique a ses forces et ses faiblesses, et le choix dépend de l'application visée. On ne s'attend à ce qu'aucune modalité biométrique ne réponde efficacement aux exigences de toutes les applications. Il est impossible d'obtenir une similarité 100% entre le fichier "signature" créé lors de l'enrôlement et le fichier "signature" créé lors de la vérification. Plusieurs études ont été menées afin d'évaluer les performances des systèmes biométriques. Ces études sont basées sur divers critères d'évaluation, que sont la précision, la fiabilité, l'intrus vite, coût et l'effort.

■ **Matrice de confusion** : Une matrice de confusion est un outil qui résume les prédictions d'un modèle de classification pour un problème donné. Il compare les données réelles pour la variable cible avec les prédictions faites par le modèle. Les prédictions correctes et incorrectes sont affichées et ventilées par catégorie, ce qui permet de les comparer à des valeurs définies.

Aussi appelées matrice de contingence, cette matrice permet d'évaluer les performances des modèles de classification et des algorithmes utilisés. Elle visualise la confusion que le modèle peut causer lors de la réalisation de prédictions. Dans sa forme la plus simple, il consiste en une matrice de taille 2x2 pour les problèmes de classification binaire (vrai/faux). [48].

- **Calcul d'une matrice de confusion** :

La création d'une matrice de confusion nécessite un ensemble de données de test ou de validation, accompagné des valeurs de résultats attendues. Pour chaque ligne de l'ensemble de données de test, des prédictions sont effectuées. La matrice de confusion organise les prédictions justes et fausses pour chaque classe en fonction de la classe prédite. Chaque ligne de la matrice représente une classe prédite, tandis que chaque colonne représente une classe réelle.

Les prédictions où les résultats sont enregistrés dans les cellules correspondantes aux classes réelles. Ces résultats peuvent être des prédictions positives correctes, appelées "vraies positives" (true positives), des prédictions négatives correctes, appelées "vraies négatives" (true negatives), des prédictions positives incorrectes, appelées "fausses positives" (false positives), ou des prédictions négatives incorrectes, appelées "fausses négatives" (false negatives) [48].

Les matrices de confusion offrent l'avantage d'être faciles à lire et à interpréter. Elles permettent une visualisation rapide des données et des statistiques pour analyser les performances d'un modèle et détecter des tendances utiles pour ajuster les paramètres. Lorsqu'il s'agit de problèmes de classification impliquant trois classes ou plus, la matrice de confusion peut être étendue en ajoutant des lignes et des colonnes pour tenir compte de toutes les classes.

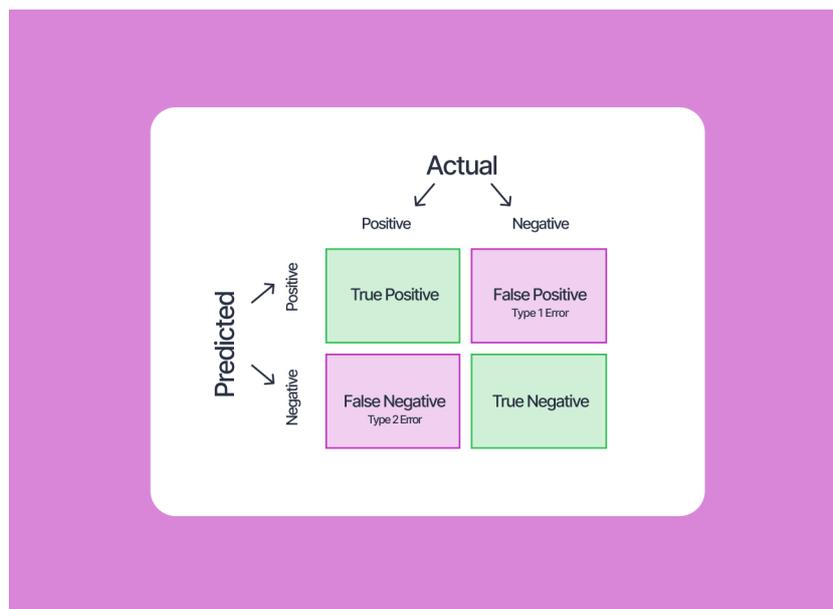


FIGURE 1.17 – Matrice de confusion [14].

- **Les terminologies de la matrice de confusion :**

La matrice de confusion comprend quatre termes essentiels : vrais positifs (TP), vrais négatifs (TN), faux positifs (FP) et faux négatifs (FN). Chacun de ces termes a une signification spécifique dans l'évaluation des performances d'un modèle de classification :

1. TP (vrais positifs) : Le modèle a prédit positive et la valeur réelle était également positive.
2. TN (vrais négatifs) : Le modèle a donné la prédiction négative, et la valeur réelle était également négative.
3. FP (faux positifs) : Le modèle a prédit positive, mais la valeur réelle est négative.
4. FN (faux négatifs) : Le modèle a prédit négative, mais la valeur réelle est positive.

- **Les métriques :** Diverses métriques peuvent être calculées à partir de la matrice de confusion pour faciliter son interprétation. Parmi celles-ci, on retrouve l'accuracy (exactitude), le taux d'erreur, la précision et le rappel. Ces indicateurs permettent d'évaluer plus précisément la qualité et la précision du modèle [14].

**-Accuracy :** C'est l'un des paramètres importants pour déterminer la précision des problèmes de classification. il définit la fréquence à laquelle le modèle prédit la sortie correcte. il peut être calculé comme le rapport du nombre de prédictions correctes faites par le classificateur à tout le nombre de prédictions faites par les classificateurs.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (1.1)$$

**-Taux d'erreur :** Définit la fréquence à laquelle le modèle donne la mauvaise prédiction. La valeur du taux d'erreur peut être calculée comme le nombre de prédictions incorrectes sur tout le nombre de prédictions faites par le classificateur.

$$Taux\ d'erreur = \frac{FP + FN}{TP + TN + FP + FN} \quad (1.2)$$

**-Precision :** Il peut être défini comme le nombre de sorties correctes fournies par le modèle ou parmi toutes les classes positives qui ont prédit correctement par le modèle, combien d'entre elles étaient réellement vraies.

$$Precision = \frac{TP}{TP + FP} \quad (1.3)$$

**-Rappel (Recall) :** Il est défini comme le nombre total de classes positives, comment notre modèle a prédit correctement. le rappel doit être le plus élevé possible.

$$Recall = \frac{TP}{TP + FN} \quad (1.4)$$

Il existe plusieurs façons d'en mesurer la performance :

- **En mode authentification :** L'exactitude d'un système biométrique est déterminée en mesurant deux taux d'erreur le FRR (Taux de Faux Rejet) et le FAR (Taux de Fausse Acceptation).

- FRR (le taux de faux rejet) : Se réfère à la fréquence à laquelle nous rejetons une personne qui devrait être accepté par le système biométrique.

$$\text{FRR} = \frac{\text{FR}(\theta)}{M}$$

**FR** : Le nombre des faux rejets.      **M** : Le nombre totale d'accée client.

- FAR (le taux de fausse acceptation) : Se réfère à la fréquence à laquelle nous acceptons une personne qui devrait être rejetée par le système biométrique.

$$\text{FAR} = \frac{\text{FA}(\theta)}{N}$$

**FA** : nombres des imposteurs acceptés.      **N** : Le nombre total de test imposteurs.

- EER (le taux d'égale erreur) : Est la valeur où le FRR est égal au FAR. Plus la valeur de l'EER est faible, plus le système est meilleur.

- Les deux taux FAR et FRR sont dépendants du seuil de décision ( $\theta$ ) fixé dans le module de décision. IL faut bien choisir une valeur optimale du seuil de décision parce qu'elle influe sur la performance et la fiabilité du système biométrique. En effet, Une valeur de seuil élevé implique un grand nombre de faux rejet, par contre une valeur de seuil faible implique un nombre important de fausses acceptations.

La figure 1.18 représente la distribution théorique des taux de correspondance des vrais utilisateurs et les imposteurs. Les deux taux d'erreurs, FAR et FRR sont liés et dépendent d'un seuil ( $\theta$ ) de décision qui doit être ajusté en fonction de la caractéristique ciblée du système biométrique.

- Seuil bas veut dire que le système accepte les utilisateurs légitimes mais inclu aussi l'imposteurs

- Seuil haut veut dire que le système rejet tous les imposteurs mais il peut aussi refuser les vrais utilisateurs, par exemple si on fait un seuil à 90% la majorité des utilisateurs légitimes vont être refusés, (Le système sera robustes aux imposteurs mais rejetteras aussi les vrais utilisateurs).

- On appelle un système idéal lorsque l'intersection entre l'imposteur et l'utilisateur converge vers le 0, c'est-à-dire le système est entrain d'accepter et de refuser.

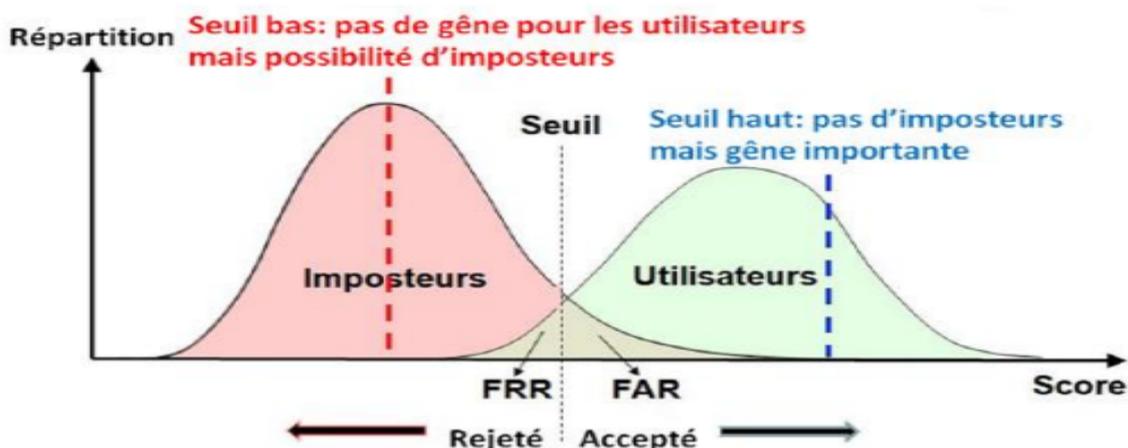


FIGURE 1.18 – Taux de vraisemblance des utilisateurs légitimes et des imposteurs dans un système biométrique [15].

- Courbe des caractéristiques :** L'utilisation de la courbe ROC (Receiver Operating Characteristics) est très fréquente pour représenter graphiquement les performances d'un système de vérification pour les différentes valeurs de seuil ( $\theta$ ), elle représente la variation de taux FRR en fonction du taux de FAR. Le taux d'erreur égal (Equal Error Rate ou EER) correspond au point  $FAR=FRR$ , c'est-à-dire graphiquement à l'intersection de la courbe ROC avec la première bissectrice. pour l'évaluation de tels systèmes d'authentification. Il est fréquemment utilisé pour donner un aperçu de la performance d'un système biométrique. Cependant, il est important de souligner que l'EER ne résume en aucun cas toutes les caractéristiques d'un système biométrique. Le seuil doit donc être ajusté en fonction de l'application ciblée : haute sécurité, basse sécurité ou compromis entre les deux.

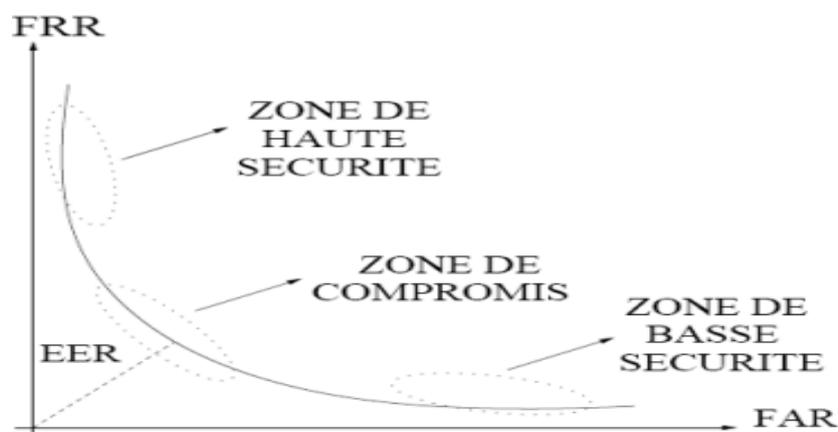


FIGURE 1.19 – Courbe ROC [16]

■ **En mode identification** : Les tests d'identification sont généralement effectués à l'aide d'une courbe CMC (Cumulative Match Characteristics). Cette courbe illustre le pourcentage de personnes identifiées en fonction du rang. Un système est considéré de rang 1 s'il sélectionne la personne la mieux semblable correspondant à l'identité revendiquée. On dit qu'un système reconnaît à un rang donné, lorsque parmi les  $n$  meilleurs images, il choisit celui qui correspond le mieux à l'image d'entrée. Il est évident que plus le rang est bas, plus le système est performant [17].

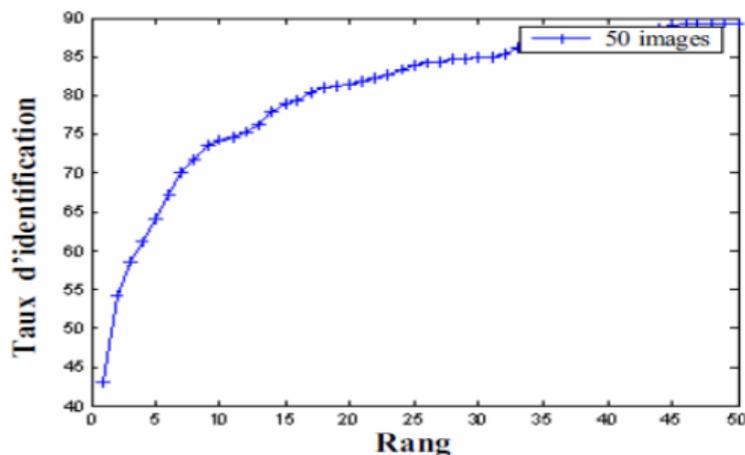


FIGURE 1.20 – Courbe CMC [17]

### 1.3.4 Les points vulnérable d'un système biométrique :

Un système biométrique peut être modélisé dans le cadre d'un système de reconnaissance de formes. Les étapes d'un tel système sont illustrées avec les possibilités d'attaque dans la figure (1.21).

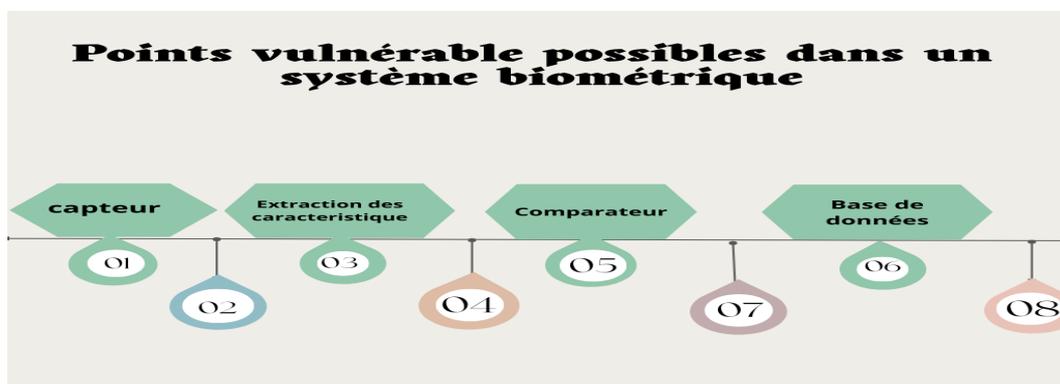


FIGURE 1.21 – Points d'attaques possibles dans un système biométrique.

Expliquons maintenant brièvement les huit scénarios d'attaque possibles :

1. Cette méthode d'attaque consiste à présenter de fausses données biométriques au capteur, lors de l'entrée dans le système, la reproduction possible d'une caractéristique biométrique est présentée. Il s'agit, par exemple, un faux doigt, un masque facial ou une copie de la signature.

2. Ce mode d'attaque resoumet des signaux biométriques numérisés enregistrés précédemment : un signal enregistré est rejoué au système en évitant le capteur. Par exemple, présenter une ancienne copie d'une image d'empreinte digitale ou d'un signal audio précédemment enregistré.

3. Remplacer le processus d'extraction des caractéristiques : l'extracteur des caractéristiques est attaqué à l'aide d'un Cheval de Troie (logiciel en apparence légitime, mais qui contient une fonctionnalité malveillante), de façon à ce qu'il produise des caractéristiques présélectionnés par l'attaquant.

4. Falsification de la représentation des caractéristiques biométriques : Les caractéristiques extraites du signal d'entrée sont remplacées par d'autres caractéristiques différentes et frauduleuses.

5. Corrompre le Matcher : le Matcher est attaqué et corrompu de manière qu'il produise des score de correspondance avec l'intrus.

6. Déformer les modèles enregistrés (Template) : sachant que la base de données peut être locale ou distante. Les données peuvent être distribuées sur plusieurs serveurs. Dans ce cas, un attaquant pourrait tenter de modifier un ou plusieurs modèles contenus dans la base de données, ce qui entraînerait une autorisation de la personne malhonnête (Fausse acceptation) ou bien le refus de service à la personne associée au modèle (Template) déformé. Un système basé sur carte à puce est particulièrement vulnérable face à ce type d'attaque.

7. Attaque de canal entre les modèles enregistrés et le matcher : les modèles stockés sont envoyés au matcher via un canal de communication. Les données transitant par ce canal peuvent être interceptées et modifiées.

8. Ignorer la décision finale : si la décision finale du comparaison peut être annulée par un hacker, c'est tout le système d'authentification qui est remis en cause. Même si le cadre de reconnaissance de Pattern présente d'excellentes performances, le simple fait de remplacer

le résultat de la correspondance le rendait inutile.

## 1.4 État de l'art sur l'empreinte d'articulation (FKP) :

Récemment, la surface externe autour du doigt en particulier l'empreinte d'articulation du doigt, qui fait référence à la forme unique de la partie supérieure du doigt, s'est avérée tout à fait unique et sert de modalité biométrique distincte. L'objectif des systèmes biométriques basés sur FKP est de déterminer les caractéristiques des articulations des doigts d'une personne (telles que les lignes au niveau des articulations) afin de distinguer les personnes dans les tâches cognitives. L'avantage principale de la modalité FKP est que la main contient plusieurs doigts (figure 1.22), ce qui permet une excellente marge d'erreur lors de l'utilisation de la fusion de tous ces doigts, et de plus, les articulations, occupe une grande surface et donc riche en informations biométrique ce qui permet d'augmenter le taux d'identification du système biométrique, ce qui la rendue un centre d'attention exploré par de nombreux chercheurs.

**Woodard and Flynn** (2005) [49], ont été parmi les premiers à envisager l'utilisation de cette modalité spécifique dans le domaine de l'authentification biométrique. Leur contribution se traduit par un algorithme novateur qui se base sur l'extraction en 3D de la surface du doigt à partir de données capturées par un capteur 3D, tel que le modèle Minolta 900/910. Leurs efforts valident le caractère unique de la surface arrière du doigt en tant que caractéristique biométrique potentielle. Cependant, leur travail ne s'est pas concentré uniquement sur les points d'articulation, mais ils ont utilisé toute la surface du dos du doigt pour l'authentification. Mais ce capteur n'est pas acceptable pour une utilisation pratique en raison du coût et le prétraitement de la surface du doigt à 3D augmente le temps et la complexité du système qui limite son utilisation pour les applications biométriques en ligne.

En 2007 **Kumar et Ravikanth** [50] ont réalisé une étude approfondie sur l'acquisition et l'extraction des points d'articulation du dos de la main. Ils ont utilisé un appareil photo numérique abordable (Canon Powershot A620) pour capturer l'image du dos de la main, qui a ensuite été utilisée pour extraire les points d'articulation en tant que région d'intérêt (ROI). Différentes techniques telles que l'Analyse en Composantes Principales (PCA), l'Analyse Discriminante Linéaire (LDA) et l'Analyse en Composantes Indépen-

dantes (ICA) ont été utilisées pour extraire des caractéristiques à partir de ces points d'articulation. Ces travaux ont accordé une attention particulière à la validation de l'unicité de la surface externe supérieure du doigt, mais n'ont pas proposé de solution pratique. D'autre part, la méthode mentionnée dans [49] se concentre principalement sur les informations de la forme 3D du dos du doigt, mais n'exploite pas pleinement les informations de texture. Les méthodes d'analyse de sous-espace utilisées dans [50] ne parviennent pas efficacement à extraire les lignes distinctives et les attributs de la surface du dos du doigt. En revanche, dans l'article [51], les auteurs ont développé un système de reconnaissance des empreintes d'articulation, en mettant spécifiquement l'accent sur l'appareil d'acquisition. Ils ont mis en place une détection de la région d'intérêt, puis ont utilisé un filtre de Gabor 2D pour extraire les informations sur l'orientation locale. Pour la comparaison entre deux empreintes, ils ont utilisé la distance angulaire pour mesurer la similarité entre les codes correspondant aux images. Bien que le développement d'un nouvel appareil d'acquisition ait été réalisé, le temps d'exécution reste un problème majeur, principalement en raison des opérations de correspondance (16,585,920 au total) et de mesure de similarité. Le temps total d'exécution pour une seule vérification prend environ 1 seconde. Malgré cela, les résultats obtenus ont démontré un taux de reconnaissance de 97%, un taux de fausses alarmes (FAR) de 0,02% et un taux d'erreur d'égale probabilité (EER) de 1,09%.

Par la suite, le **Centre de Recherche Biométrique de l'Université Polytechnique de Hong Kong** a développé un dispositif en temps réel capable de capturer des empreintes d'articulation et de les utiliser pour créer une vaste base de données. En 2011 **A. Morales et al** [52] ils ont constaté que les images d'empreintes d'articulation présentaient davantage de bruit par rapport aux empreintes palmaires. Pour remédier à cela, les chercheurs ont proposé une approche en deux étapes. Tout d'abord, ils ont appliqué un filtre de Gabor en 2D pour améliorer la visibilité des lignes de l'empreinte d'articulation. Ensuite, ils ont utilisé les descripteurs Scale-Invariant Feature Transform (SIFT). Pour renforcer encore davantage les lignes d'articulation, l'algorithme Contrast Limited Adaptive Histogram Equalization (CLAHE) a été appliqué après le filtre de Gabor pour améliorer le contraste.

**Lin Zhang et al** (2011) [53] choisissent d'extraire les caractéristiques biométrique à l'aide d'une ondelette de Gabor. Leur contribution consiste en la conception d'un système biométrique basé sur la combinaison de l'information locale et globale pertinente

à la modalité FKP. Particulièrement, les caractéristiques biométrique qui représentent la mesure de l'orientation locale sont obtenues à l'aide des filtres de Gabor. Cependant, plus l'échelle des filtres de Gabor augmente plus la transformation avec ces filtres converge vers la transformée de Fourier discrète de l'image entière. Par conséquent, la DFT de l'image entière offre un ensemble de coefficient permettant de représenter l'information globale de la modalité FKP. Leurs résultats expérimentaux sur une base de données contenant 165 personnes indiquent que le système peut fonctionner avec une erreur égale à 0.402%. Les mêmes auteurs [54] ont combinés l'orientation et l'amplitude de l'information extraite par le filtrage de Gabor. Ils ont montré que la fusion de tous les doigts permet d'atteindre des taux d'erreur nul.

**Zahra S et al** [55] (2011) Dans cette étude, les chercheurs ont utilisé une banque de filtres de Gabor pour extraire les caractéristiques des empreintes d'articulation. Ils ont combiné les techniques PCA et LDA pour réduire la dimension de l'espace des caractéristiques. La classification a été réalisée en utilisant la distance euclidienne. Ce travail a également exploré la combinaison de quatre empreintes d'articulation appartenant au même individu au niveau des caractéristiques. La base de données PolyU a été utilisée pour évaluer les performances de la méthode proposée. Les résultats obtenus ont montré un taux d'identification de 98,79% et un taux de vérification de 91,8%.

En 2013 **Chetana Hegde et al** [56] ont proposé trois algorithmes distincts pour la reconnaissance des empreintes d'articulation. La première approche utilise une transformée de Radon pour l'extraction des caractéristiques, avec une étape de prétraitement comprenant la détection des contours et l'application d'un filtre médian. Ensuite, en utilisant la morphologie mathématique et l'étirement, les résultats obtenus montrent un taux de fausses acceptations (FAR) de 1,55% et un taux de fausses rejets (FRR) de 1,02%. La deuxième méthode repose sur l'utilisation des ondelettes de Gabor pour l'extraction des caractéristiques. Les chercheurs ont d'abord éliminé le bruit et augmenté l'intensité en utilisant des coefficients de corrélation. Les résultats obtenus ont montré un FAR de 1,24% et un FRR de 1,11%. Quant au dernier algorithme, il vise à reconnaître les parties endommagées de l'empreinte d'articulation. Les chercheurs ont créé 450 empreintes d'articulation corrompues en introduisant du bruit et en supprimant de manière aléatoire certaines valeurs de pixels de l'image d'empreinte d'articulation. Le taux de détection obtenu pour cette méthode est de 95,33%.

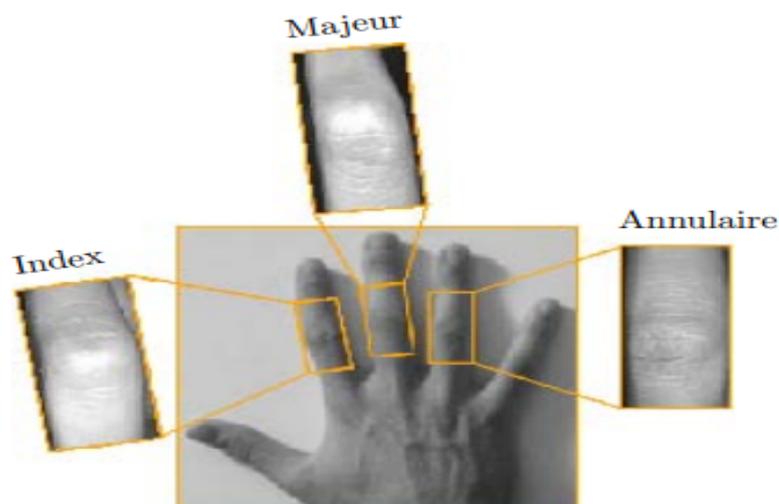


FIGURE 1.22 – Empreintes des articulations des doigts [18]

## 1.5 Applications des systèmes biométriques :

Les systèmes biométriques trouvent une utilisation dans de nombreuses applications variées. Ils offrent des avantages en termes de sécurité et de commodité dans la vie quotidienne. On identifie trois domaines spécifiques qui intègrent des solutions biométriques pour répondre à leurs besoins spécifiques :

- **Application légale :**

1. Justice et application de la loi : Ce domaine a une longue relation avec la technologie biométrique, et cette collaboration a conduit à d'importantes avancées dans la gestion de l'identité. Aujourd'hui, la police utilise une approche multimodale de la biométrie, combinant la reconnaissance des empreintes digitales, du visage et de la voix pour renforcer la sécurité publique. Ces technologies jouent un rôle crucial dans la localisation de personnes recherchées, l'identification de corps, la recherche d'enfants disparus, et bien d'autres applications.

- **Application gouvernementales :** Ces applications comprennent les projets telles que :

1. Le contrôle aux frontières et aéroport : La technologie biométrique trouve une application essentielle dans le contrôle aux frontières et les aéroports. Elle permet d'automatiser le processus de passage des frontières, offrant un contrôle efficace et robuste des passagers. Les initiatives de contrôle automatisé et les

systèmes de pré-vérification accélèrent les formalités pour les voyageurs internationaux, améliorant ainsi l'efficacité des agences gouvernementales et renforçant la sécurité des frontières.

2. Gestion des identités : La biométrie est utilisée dans la gestion des identités pour établir et vérifier l'identité des individus dans des domaines tels que les cartes d'identité et les permis de conduire. Elle aide à prévenir la fraude d'identité et à garantir l'authenticité des documents d'identité.
3. Santé : La biométrie facilite l'accès rapide et précis aux dossiers médicaux, qui sont parmi les documents personnels les plus importants. Les médecins de la santé peuvent bénéficier de cette technologie pour une gestion efficace des dossiers et une meilleure prise en charge des patients.

- **Application Commerciales :**

1. Le contrôle d'accès physique : La biométrie est largement utilisée pour le contrôle d'accès aux bâtiments, aux zones sécurisées, aux systèmes informatiques et aux dispositifs électroniques. Elle permet de garantir que seules les personnes autorisées peuvent accéder à ces zones sensibles.
2. Applications financières : La biométrie est utilisée dans les systèmes de paiement et d'authentification financière, tels que les systèmes de reconnaissance vocale pour les services bancaires par téléphone, les empreintes digitales pour les transactions en ligne, et les technologies de reconnaissance faciale pour les paiements mobiles.
3. Applications grand public : La biométrie est largement intégrée dans les appareils électroniques grand public tels que les smartphones, les tablettes et les ordinateurs portables. Elle offre des méthodes d'authentification telles que la reconnaissance d'empreintes digitales, faciales, vocales, et d'autres, permettant ainsi de sécuriser l'accès aux appareils et aux données personnelles.
4. La sécurité de données électroniques : Les données biométriques peuvent être utilisées pour crypter les données électroniques. Les systèmes de contrôle d'accès biométriques sont également utilisés pour restreindre l'accès aux données électroniques.

## 1.6 Marché de la biométrie :

Le marché biométrique connaît une croissance rapide, avec une augmentation des revenus dans divers secteurs, notamment les applications juridiques, le secteur public, le contrôle des systèmes d'information et le commerce électronique. Les marchés émergents comme les systèmes d'information, le commerce électronique, accès physique et la surveillance devraient générer des revenus plus importants que les secteurs matures comme l'identification criminelle et l'identification des personnes.

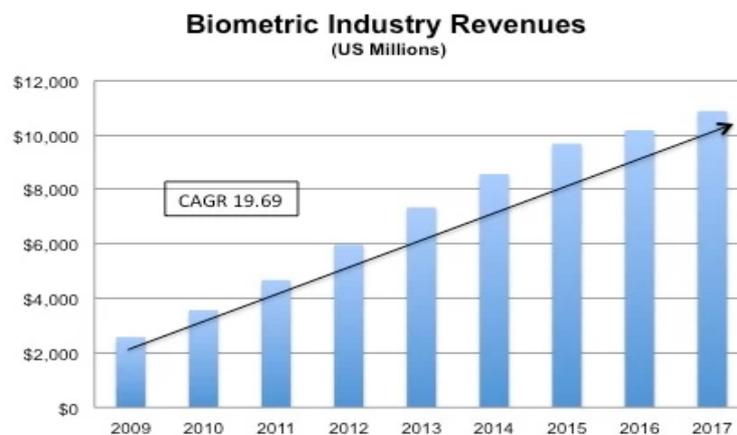


FIGURE 1.23 – Progression du marché mondiale de la biométrie [19].

Les empreintes digitales restent la technologie biométrique dominante sur le marché, représentant près de 50% du chiffre d'affaires total, à l'exclusion des applications judiciaires.

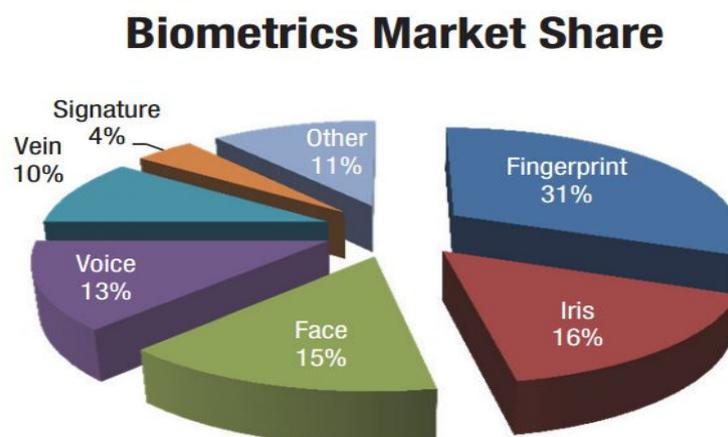


FIGURE 1.24 – Parts de marché des divers technologie biométriques [19].

## 1.7 Conclusion

Dans ce chapitre, nous avons exploré le domaine de la biométrie et ses multiples facettes. Nous avons commencé par retracer l'histoire de la biométrie. De là, nous avons donné une définition claire de la biométrie, en insistant sur son principe fondamental qui repose sur l'utilisation des caractéristiques uniques pour l'identification des individus. Nous avons ensuite examiné les différentes modalités biométriques disponibles. Chaque modalité présente ses avantages et ses limitations. En poursuivant, nous avons exploré le fonctionnement d'un système biométrique, en détaillant les différentes étapes impliquées dans le processus d'identification.

L'évaluation des performances des systèmes biométriques a également été abordée, en soulignant les mesures d'évaluation couramment utilisées. Cependant, malgré les avantages et les progrès réalisés dans le domaine de la biométrie, nous avons également identifié des points vulnérables auxquels les systèmes biométriques peuvent être exposés.

Enfin, nous avons exploré les différentes applications des systèmes biométriques, soulignant leur utilisation dans des domaines, chaque application présente des exigences spécifiques et des défis particuliers. Dans le chapitre suivant nous allons présenter le système de reconnaissance des formes.

# Système de reconnaissance des formes

## 2.1 Introduction

L'idée de construire des machines capables de simuler des humains pour aider à certaines tâches ou même remplacer les humains est antérieure aux ordinateurs. Avec leur apparition, il est devenu possible d'élargir la gamme de tâches pouvant être simulées à des tâches qui reposent sur des capacités mentales telles que la perception et la pensée logique. Le problème que la reconnaissance de formes (RDF) cherche à résoudre consiste à associer des étiquettes à des données sous forme d'images ou de signaux. Le problème que la reconnaissance de formes (RDF) consiste à associer des étiquettes à des données (sous forme d'images ou de signaux). En reconnaissance de formes, une méthode générale a été développée pour extraire automatiquement des informations de données sensibles afin de caractériser des classes de formes (apprentissage) et d'affecter automatiquement des données à ces classes (reconnaissance).

En plus des recherches sur les méthodes de détection, le traitement d'images et la vision par ordinateur, ces domaines ont focalisé le problème de la reconnaissance sur des données spécifiques, mais par ailleurs ils ont permis de situer la reconnaissance dans un processus plus vaste d'interprétation d'image impliquant des niveaux de perception et des connaissances propres au domaine [57].

Les systèmes biométriques ont des limites quant à l'enregistrement et à l'utilisation des informations obtenues. Parce que leur taille est très grande et que la différence réside dans leur source. Pour résoudre ces problèmes et améliorer les performances de ces systèmes, les chercheurs ont ajouté une étape avant l'extraction des caractéristiques en prétraitant

les images SCP (marques d'articulation et classification). Ce chapitre commence par un aperçu de la reconnaissance de formes (définition, domaines d'application, objectifs et défis), puis le processus RDF, puis les techniques RDF, et une évaluation des performances de RDF avant cela. Décrit les limites et les défis de la reconnaissance des formes de parole. Enfin, concluez par une conclusion.

## 2.2 La reconnaissance des formes :

### 2.2.1 Définition :

La reconnaissance des formes (ou des images) est une branche de l'intelligence artificielle qui concerne la classification de données en fonction de leur apparence visuelle. Elle consiste à trouver des motifs, des structures ou des caractéristiques dans des images ou des données, et à utiliser ces informations pour identifier ou classer des objets, des personnes, des événements, etc.

La reconnaissance des formes (ou reconnaissance d'image) peut être définie comme « l'ensemble des méthodes mathématiques et informatiques permettant d'extraire automatiquement des informations à partir d'images, dans le but de les interpréter et de les utiliser pour la prise de décision ou la réalisation de tâches spécifiques. »

Une autre définition de la reconnaissance des formes est proposée « l'analyse de données visuelles ou autres données complexes pour extraire des informations pertinentes ». » [58]

La reconnaissance des formes peut être appliquée dans différents domaines tels que la vision par ordinateur, la reconnaissance de la parole, la biométrie, la surveillance, l'analyse des données, etc.

### 2.2.2 Domaine d'application :

La reconnaissance des formes a connu toujours une croissance rapide, en raison de l'explosion des données visuelles. La reconnaissance des formes dans les images est utilisée pour extraire des informations importantes à partir des images dans nombreux domaines, notamment la médecine, la sécurité, la surveillance, la reconnaissance de caractères, l'industrie, et bien plus encore. La RDF est donc une clé pour la compréhension et l'analyse des données visuelles, elle offre des avantages considérables dans divers domaines d'ap-

plication. Les techniques de reconnaissance des formes dans les images ont évolué au fil du temps, et de nouvelles approches sont constamment développées pour répondre aux besoins spécifiques des différents domaines d'application.

- **Domaine médicale :** La reconnaissance de formes a de nombreuses applications en médecine, telles que la classification des tumeurs à l'aide d'images IRM, la détection de la rétinopathie diabétique à l'aide d'images du fond d'œil et la segmentation du tissu cérébral dans des images de tomographie par ordinateur. La reconnaissance de formes est également utilisée pour diagnostiquer des maladies telles que le cancer du sein et le glaucome. [59].
- **Domaine de la sécurité et de la surveillance :** La RDF est très vaste dans le domaine de la surveillance vidéo, elle est largement utilisée pour la détection de comportements suspects et l'identification de personnes. Des approches telles que l'analyse de mouvement et la détection de formes sont couramment utilisées pour la détection d'activités anormales dans les vidéos de surveillance. En outre, la reconnaissance des formes est également utilisée dans l'analyse des empreintes digitales pour l'identification des personnes, qui est l'une des méthodes les plus courantes utilisées pour la vérification d'identité dans les systèmes de sécurité [60].
- **Domaine de l'industrie :** L'utilisation de la reconnaissance des formes dans l'industrie permet d'améliorer l'efficacité et la qualité des processus de production. Par exemple, la reconnaissance de pièces défectueuses peut aider à identifier les erreurs de fabrication plus rapidement, ce qui permet de réduire les coûts et d'améliorer la qualité des produits finis. Les systèmes de reconnaissance de formes sont également utilisés pour l'inspection de produits, en particulier dans les industries alimentaires et pharmaceutiques, afin de garantir la conformité aux normes de sécurité et de qualité [61].

## 2.3 Processus de la reconnaissance des formes :

Le processus de reconnaissance des formes est une étape cruciale pour la classification et la prise de décision à partir de données non structurées. Il consiste à extraire des caractéristiques significatives des données d'entrée, à les réduire si nécessaire, puis à utiliser un algorithme de classification pour affecter une étiquette ou une catégorie aux données. Le processus peut être supervisé ou non supervisé, selon la disponibilité des étiquettes pour les données d'entraînement. Le choix de la méthode de classification dépend du type de données et du problème à résoudre.

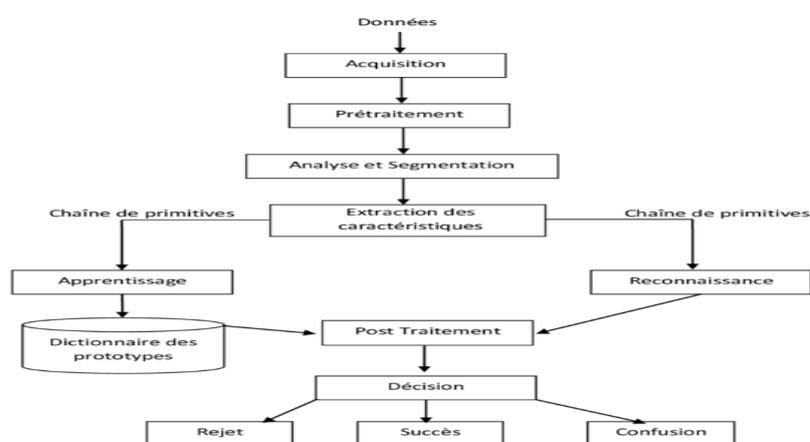


FIGURE 2.1 – Schéma de processus de reconnaissance des formes [20]

### 2.3.1 L'acquisition :

Cette étape consiste à acquérir les images des empreintes d'articulation des doigts à partir d'un dispositif de capture tel qu'une caméra numérique ou un scanner, les convertir en des grandeurs numériques. Les images peuvent être acquises dans différentes conditions d'éclairage et de positionnement des doigts, et en différentes tailles.

### 2.3.2 Prétraitement :

Est une étape très importante dans le système de reconnaissance des formes, elle vise à améliorer la qualité de l'image et à réduire le bruit pour faciliter les étapes suivantes de l'analyse. Les opérations de prétraitement des images peuvent inclure le filtrage de l'image pour éliminer le bruit, la normalisation pour mettre les images à l'échelle, et la correction de la luminosité et du contraste pour augmenter la clarté.

■ **Filtrage** : Le filtrage est une technique de traitement d'images qui vise à modifier ou améliorer les propriétés d'une image en appliquant des filtres à des parties spécifiques ou à l'ensemble de l'image. Les filtres sont des matrices de coefficients numériques qui peuvent être conçus pour effectuer diverses opérations sur l'image, telles que la suppression du bruit, la détection de contours ou l'amélioration de la netteté. Cependant, le filtrage doit être utilisé avec précaution car il peut altérer l'information contenue dans l'image et entraîner une perte de détails [62].

Différents types de filtres numériques peuvent être utilisés : des filtres de convolution linéaire ou non-linéaire [63].

- **Filtrage linéaire** :

Les filtres linéaires sont ceux qui appliquent une transformation linéaire à l'image en utilisant une matrice de convolution. Par exemple, le filtre gaussien et le filtre moyenneur sont des filtres linéaires, car ils appliquent une matrice de convolution pour calculer une nouvelle valeur de pixel.

- **Filtre gaussien** : Est une technique de filtrage d'images qui applique une fonction gaussienne en utilisant une matrice de convolution pour réduire le bruit et lisser l'image. La fonction gaussienne est une distribution de probabilité qui a une forme de cloche symétrique et continue. En appliquant le filtre gaussien à une image, les valeurs de chaque pixel sont remplacées par une moyenne pondérée des pixels voisins, où les poids sont calculés en fonction de la distance des pixels voisins par rapport au pixel central. Le filtre gaussien est souvent utilisé en prétraitement d'images pour éliminer le bruit et améliorer la qualité de l'image [64].

Il est défini dans deux dimensions comme suite :

$$G(x, y) = \frac{1}{2\pi\sigma^2} e^{-\frac{(x^2+y^2)}{2\sigma^2}}$$

Tel que,  $\sigma$  est l'écart type.

Cela signifie que la qualité de lissage dépend de l'écart type  $\sigma$  choisi, s'il est élevé l'image résultante est plus lissante.

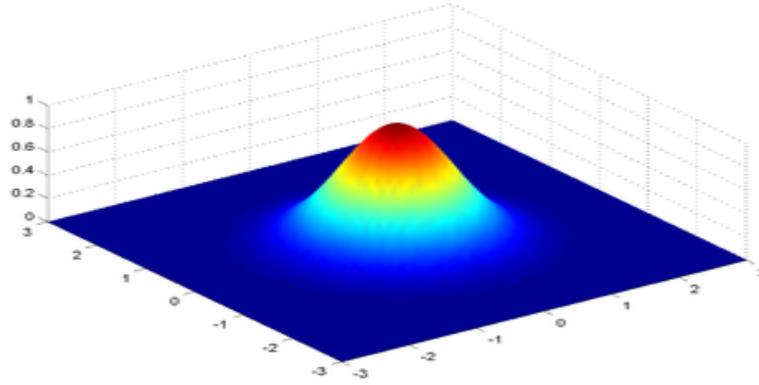


FIGURE 2.2 – Représentation 3D d'une courbe gaussienne en deux dimensions [21].

Si par exemple  $\sigma=0.8$  on obtient un filtre de 3x3 comme suivant :

$$\begin{array}{|c|c|c|} \hline G(-1,-1) & G(0,-1) & G(1,-1) \\ \hline G(-1,0) & G(0,0) & G(1,0) \\ \hline G(-1,1) & G(0,1) & G(1,1) \\ \hline \end{array} \simeq \frac{1}{16} \cdot \begin{array}{|c|c|c|} \hline 1 & 2 & 1 \\ \hline 2 & 4 & 2 \\ \hline 1 & 2 & 1 \\ \hline \end{array}$$

Et  $\sigma=1$  pour un filtre 5x5 donne :

$$\frac{1}{300} \cdot \begin{array}{|c|c|c|c|c|} \hline 1 & 4 & 6 & 4 & 1 \\ \hline 4 & 18 & 30 & 18 & 4 \\ \hline 6 & 30 & 48 & 30 & 6 \\ \hline 4 & 18 & 30 & 18 & 4 \\ \hline 1 & 4 & 6 & 4 & 1 \\ \hline \end{array}$$

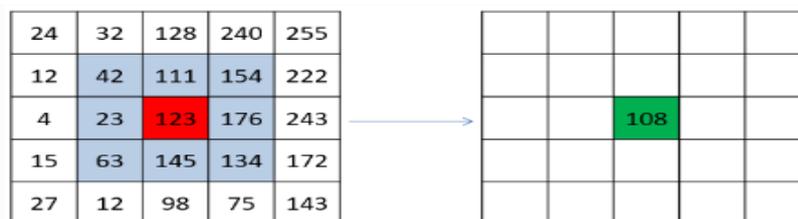


FIGURE 2.3 – Filtrage gaussien à une images [22].

La taille du filtre gaussien dépend de  $\sigma$  qui doit être proportionnel à l'écart-type du bruit, en général en utilise une valeur  $\sigma < 1$  pour réduire le bruit et des valeurs  $\sigma > 1$  pour crée des masques flous personnalisés.

- **Filtre moyennneur** : Est une opération de traitement d'images utilisée pour réduire le bruit dans une image et/ou flouter une image, il utilise un noyau de convolution qui prend la moyenne des valeurs des pixels voisins et assigne cette valeur à un pixel central de l'image. Cette opération est effectuée pour chaque pixel de l'image, ce qui permet de réduire le bruit dans l'image et de flouter l'image.

Le filtre moyennneur fait partie des filtres linéaires car il applique une matrice de convolution pour calculer une nouvelle valeur de pixel en fonction des valeurs des pixels voisins. Concrètement, la valeur filtrée d'un pixel  $p$  est égale à la moyenne des valeurs des pixels proches de  $p$ . En général, on définit les « pixels proches de  $p$  » comme l'ensemble de pixels contenus dans un carré de largeur  $k$  centré sur  $p$ .



$$\frac{42+111+154+23+63+145+134+176}{9} = 108$$

La valeur du pixel  $p$  sera = 108.

Cette opération est répétée pour tous les pixels de l'image.

- **Complexité des filtres linéaires** : La complexité des filtres linéaires est généralement en  $O(v^2 \cdot N)$ , si  $N$  est un nombre de pixels dans l'image et  $v$

le côté de fenêtre carrée sur laquelle le filtrage est fait, donc le coût de la complexité grandit vite avec l'étendue du filtre.

- **Filtrage non linéaire :**

Les filtres non-linéaires sont définis comme des opérations de traitement d'images qui peuvent utiliser des noyaux variables et peuvent être adaptatifs en fonction de l'image traitée. En utilisant des fonctions non-linéaires telles que la valeur absolue ou la valeur maximale, les filtres non-linéaires peuvent capturer des caractéristiques d'image plus complexes que les filtres linéaires, ce qui les rend plus adaptés pour certaines tâches de traitement d'images.

- **Filtre médian :** Est couramment utilisé pour la suppression du bruit impulsionnel dans les images, il fonctionne en remplaçant les valeurs de pixels avec la valeur médiane de cette zone. Cela se fait par itération à travers chaque pixel d'une image et en regardant ses voisins dans une distance spécifiée. Ces valeurs de pixels sont ensuite réunies et triées. La valeur dans le milieu de l'ensemble résultant est choisie pour être la nouvelle valeur de pixel central. A titre d'exemple considérons la fenêtre de pixels 3x3 présentée par le tableau suivant :

Pour un pixel  $p = 250$  qui est au milieu de la table.

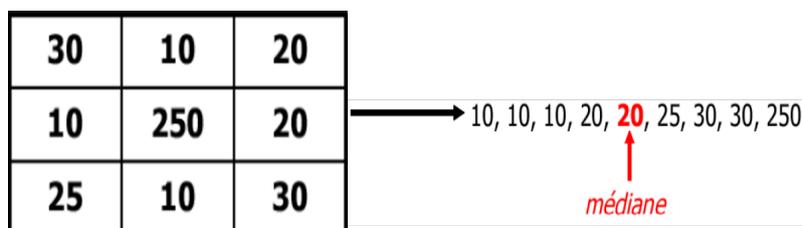


FIGURE 2.4 – Appliquer filtre médian sur un pixel [23].

Donc la nouvelle valeur de pixels  $p$  est : 20

Voici une illustration de filtre médian de 5x5 appliqué sur une image :

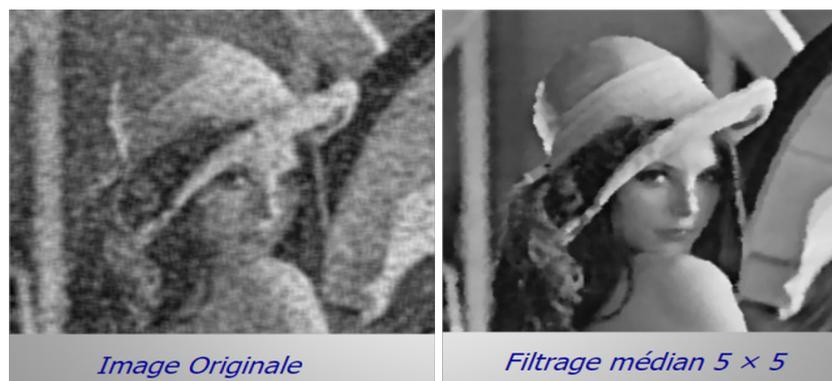


FIGURE 2.5 – Appliqué filtrage médian à une image [23].

- **Filtre bilatéral** : Est aussi une technique d'élimination du bruit dans le traitement des images, l'idée de base de ce filtre est d'ajouter des poids à la convolution qui tiennent compte la distance entre les pixels. Dans les filtres linéaires la luminance varie lentement car les pixels voisins ont des illuminances voisines, si cette hypothèse n'est pas respectée il est nécessaire de penser à une notion de proximité entre les pixels sans avoir recours à un processus itératif, et c'est ce que le filtre bilatéral fait [24].

On utilise en général une distribution gaussienne pour choisir les poids des pixels.

Par exemple : deux pixels C et S :

$$W_c = e^{-\frac{x^2}{2\sigma^2}} \quad W_s = e^{-\frac{x^2}{2\sigma^2}}$$

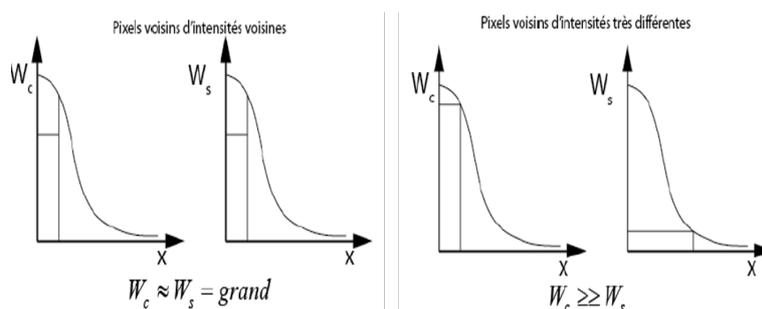


FIGURE 2.6 – Appliquer filtre bilatéral sur un pixel [24].

Résultat de l'application du filtre bilatéral :

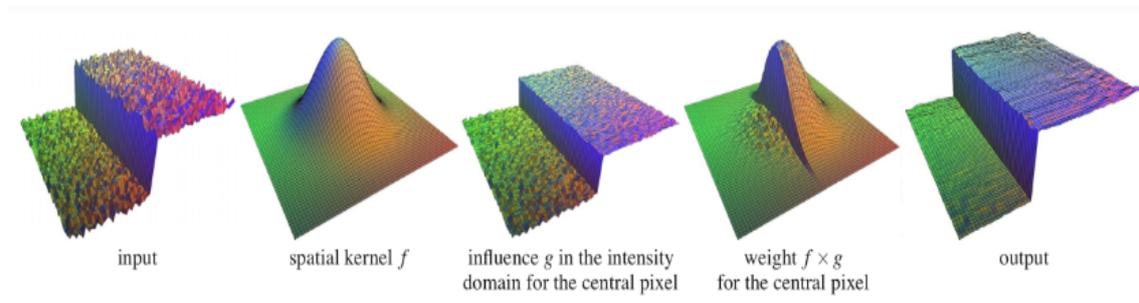


FIGURE 2.7 – La combinaison des poids spatiaux et l'intensité pour préserver les contours. [24].

- Signal bruité avec une discontinuité d'illuminance.
- Noyau 'spacial'  $W_c$ .
- Influence de l'illuminance sur le noyau spatial  $W_c * W_s$ .
- La discontinuité est préservée.
- Résultat.

Voici une illustration de filtre bilatéral appliqué sur une image :



FIGURE 2.8 – Appliqué filtrage bilatéral à une image [24].

- **Complexité des filtres non linéaires** : Selon la nature des filtres non-linéaires qui impliquent des opérations mathématiques plus complexe à chaque pixel de l'image, leur complexité est plus par rapport aux filtres linéaires, et le temps de peut-être plus long, ce qui peut affecter les performances en temps réel de certains systèmes de traitement d'images.[65]

■ **Binarisation** : Est une technique couramment utilisée en traitement d'images pour convertir une image en niveaux de gris en une image binaire en noir et blanc, où les pixels sont soit noirs (0) soit blancs (1) [66]. Cette technique est souvent utilisée comme

étape préliminaire dans la reconnaissance de caractères et la segmentation d'images. La binarisation peut être effectuée en utilisant des seuils statiques ou adaptatifs, où le seuil est déterminé en fonction des caractéristiques de l'image [67]. Il existe plusieurs techniques de binarisation mais la technique de seuillage est la plus populaire.

- **Seuillage :**

Consiste à diviser l'image en deux parties distinctes en fonction d'une valeur seuil choisie. Les pixels qui ont une intensité supérieure à un seuil prédéfini et les pixels qui ont une intensité inférieure ou égale à ce seuil  $T_p$ . Le choix du seuil est important car il peut influencer grandement la qualité de la binarisation. L'opération de seuillage est donnée par la formule [68] :

$$I_b(i, j) = \begin{cases} 1 & I_0(i, j) \geq T_P \\ 0 & \text{Autrement} \end{cases}$$

Avec  $I_b$  l'image binaire obtenue et  $I_0$  l'image après le filtrage.

Parmi les types de seuillage, on cite :

- **Seuillage global :** Est la technique la plus simple de binarisation qui consiste à appliquer le même seuil c'est-à-dire un seuil global, à tous les pixels de l'image. Le seuil est déterminé en utilisant des méthodes de calcul basées sur des caractéristiques globales de l'image, telles que la moyenne ou la médiane de l'intensité des pixels. Cette technique est souvent utilisée pour des images à contraste élevé et uniforme, mais ce n'est pas le cas pour les images qui ont une distribution d'intensité non uniforme [69].
- **Seuillage local :** Il est utilisé pour les images à contraste variable. Il consiste à diviser l'image en plusieurs régions et à appliquer un seuillage différent pour chaque région où la valeur du seuil ne peut pas être définie de manière globale pour l'ensemble de l'image [70].
- **Seuillage adaptatif :** Cette méthode est similaire au seuillage local, mais le seuil est adapté dynamiquement pour chaque pixel en fonction de son voisinage.
- **Seuillage multiple :** Cette méthode consiste à utiliser plusieurs seuils pour

diviser l'image en plusieurs classes.

- **Normalisation** : Est définie comme une technique de traitement d'image qui transforme l'intensité des pixels de l'image de manière à réduire les effets de l'éclairage et de la géométrie. Cela permet de rendre les images plus cohérentes et donc plus facilement comparables pour des tâches telles que la reconnaissance. La normalisation peut être appliquée à différents aspects de l'image, tels que la luminosité, le contraste et l'échelle, en fonction de l'objectif de l'application.

Dans le processus des systèmes de reconnaissance des images FKP, la normalisation vise à mettre les images sur une échelle commune, ou aligner tous les empreintes FKP de la même manière dans leurs images associées, elle est nécessaire pour extraire efficacement les similarités et les dissimilarités des FKP, soit par l'ajustement de la luminosité, le contraste ou la couleur afin de réduire la variation entre les images et faciliter leur comparaison et leur traitement.

La normalisation peut être effectuée en utilisant des méthodes et des algorithmes telles que :

- LBP-based histogram equalization (LBHE).
- Contrast limited adaptive histogram equalization (CLAHE).
- Non-parametric weighted feature extraction (NpWFE).
- Spatially Adaptive Normalization (SPAN).
- Unsupervised Texture Segmentation and Texture Normalization (UTSTN).
- Adaptive histogram Equalization (AHE).
- Min-max mapping.
- Z-score normalization.

- **Adaptive histogram equalization (AHE)** : L'égalisation d'histogramme adaptative (AHE) est une méthode d'amélioration de la qualité visuelle de l'image en augmentant le contraste local, elle est conçue pour être largement applicable et ayant une efficacité démontrée. L'AHE utilise des histogrammes locaux, contrairement à l'égalisation d'histogramme classique qui utilise un histogramme global pour ajuster la luminosité de toute l'image, ces histogrammes locaux permettent d'ajuster la luminosité de petites régions de l'image. Cette approche permet d'éviter une surexposition ou une sous-exposition locale de l'image tout en préservant les détails locaux et en améliorant le contraste global [25]. Il fonctionne de la

manière suivante :

1. Deviser l'image en petites régions rectangulaires appelées 'Tuiles'.

$$\text{Tuiles} = [I(i : i+M, j : j+N)]$$

2. pour chaque région on calcule l'histogramme normalisé.

$$P(k) = P_x(x_k) = P(x = x_k) = \frac{n_k}{n}$$

$P(k)$  : L'histogramme normalisé sur  $[0,1]$ , et  $n$  le nombre total de pixel dans la tuile,  $n_k$  le nombre de pixel ayant la valeur  $k$  dans la tuile.

3. on calcule la fonction de la distribution cumulative l'histogramme  $P(k)$ .

$$f(x_k) = \sum_{j=0}^k P_x(x_j)$$

$f(x_k)$  Est l'histogramme cumulé.

4. appliquer la transformation normalisée à l'histogramme calculé.

$$T(x_k) = (l - 1) \cdot f(x_k) = (l - 1) \sum_{j=0}^k P_x(x_j)$$

$l$  Est le nombre de niveaux de gris dans la tuile, (par exemple  $l=256$  pour 8 bits).

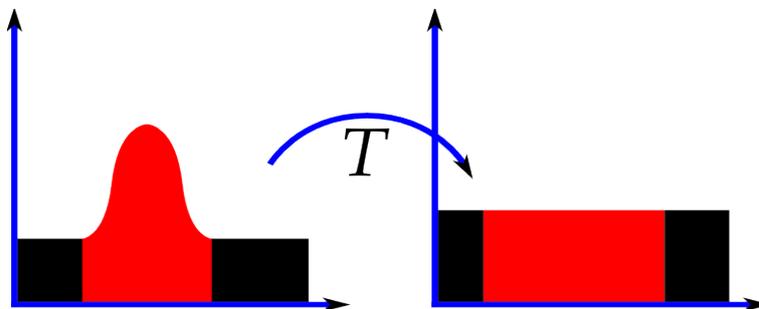


FIGURE 2.9 – La transformation  $T$  permet d'égaliser l'histogramme et d'améliorer le contraste [25].

5. combiner les tuiles voisines pour former l'image finale.

- **Min-Max Mapping** : L'algorithme Min-Max Mapping est une technique de normalisation d'images qui utilise une transformation linéaire pour étirer les niveaux de gris de l'image d'entrée entre un minimum et un maximum défini. Cette technique est souvent utilisée pour améliorer le contraste de l'image et rendre les détails plus visibles [26].

Exemple, considérons une matrice comme suivante :

|     |     |     |     |     |     |     |
|-----|-----|-----|-----|-----|-----|-----|
| 123 | 143 | 122 | 167 | 90  | 171 | 200 |
| 70  | 72  | 75  | 78  | 254 | 212 | 199 |
| 122 | 134 | 90  | 93  | 123 | 128 | 112 |
| 156 | 157 | 167 | 208 | 198 | 190 | 80  |
| 123 | 110 | 129 | 135 | 145 | 126 | 85  |
| 130 | 123 | 125 | 124 | 156 | 176 | 90  |
| 105 | 101 | 90  | 80  | 78  | 67  | 57  |

FIGURE 2.10 – Matrice des pixels d'une partie d'une image donnée [26].

Min = 90, Max = 198 on a donc  $208 > \max$  d'où la valeur 208 ça sera remplacé par 198 dans le cas du Max.

### 2.3.3 Analyse et segmentation :

Cette étape est également importante pour identifier la région d'intérêt (ROI), ou l'empreinte d'articulation des doigts, dans notre cas, dans l'image et la segmenter à partir de l'image de fond. Cela permet de réduire la taille de l'image à traiter et éliminer les informations inutiles qui pourraient perturber le processus de reconnaissance et pour avoir des décisions plus fiables.

- La segmentation peut être effectuée en déterminant d'abord l'axe du système de coordonnées X, qui est considéré comme la limite inférieure des doigts. Il est facile de le faire par le détecteur de Canny [27] comme la figure (2.11) montre.

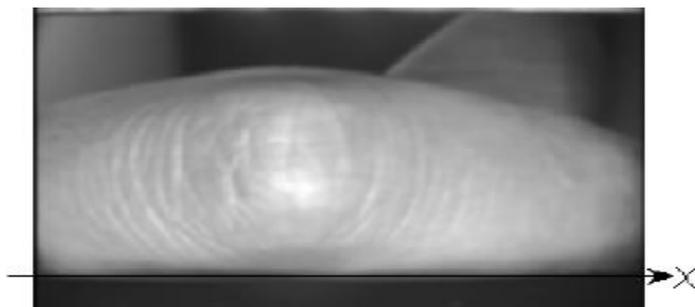


FIGURE 2.11 – Localisation de l'axe X [27].

- Ensuite on diminue la taille de l'image, les limites gauches et droites sont des valeurs fixes et les limites inférieures et supérieures sont calculés selon la largeur des doigts, comme la montre la figure (2.12)

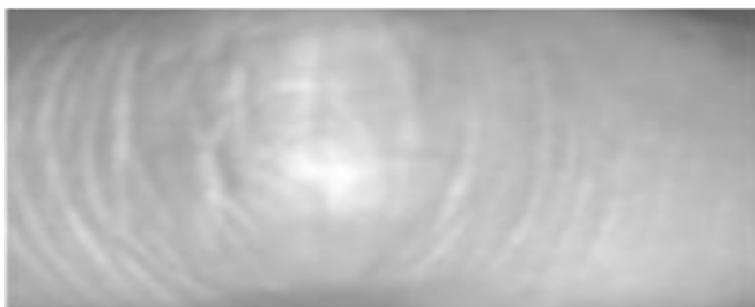


FIGURE 2.12 – Image coupée [27].

- On applique le contour de Canny pour la deuxième fois sur l'image coupée et on obtient (figure 2.13).



FIGURE 2.13 – Applications de contour Canny [27].

- Avec une analyse visuelle des images FKP on peut remarquer que les lignes caractéristiques sont de deux types : gauche et droite par rapport aux ROI de l'articulation, ce qui permet de faire un codage de la direction aux pixels par affecter les valeurs -1, 0 et 1 pour les pixels situés à droite et au milieu et à gauche de l'articulation phalangienne.

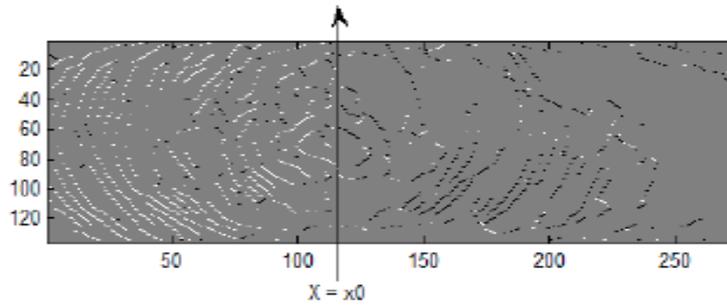


FIGURE 2.14 – Codage [27].

Grâce à les axes X et Y, il possible maintenant de localisé le ROI (région d'intérêt), comme la montre la figure (2.15).

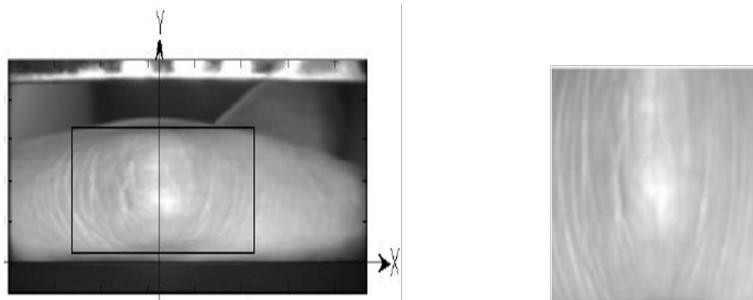


FIGURE 2.15 – Image ROI [27].

### 2.3.4 Extraction des caractéristiques :

L'extraction de caractéristiques est le processus de sélection et de représentation des informations pertinentes d'une image, afin de faciliter l'analyse ou la reconnaissance d'objets ou de motifs dans cette image. Elle consiste à extraire des informations utiles et discriminantes à partir de l'image brute, telles que des motifs locaux, des textures, des formes ou des couleurs, et à les représenter sous forme de vecteurs de caractéristiques. Ces vecteurs peuvent ensuite être utilisés pour l'apprentissage de modèles de reconnaissance d'objets ou pour la comparaison de motifs dans des tâches de recherche ou de correspondance d'images [71].

■ **Méthode d'extraction des caractéristique** : Il existe de nombreuses méthodes pour extraire des caractéristiques des images, et d'après [72] ils sont divisés en des méthodes globales, locales et hybrides.

- **Méthodes globale** : Les méthodes globales d'extraction de caractéristiques sont des approches qui considèrent l'ensemble de l'image comme une entité, sans tenir compte des variations locales de texture ou de forme, et extraient des informations à partir de la totalité de l'image. Ces méthodes s'appuient souvent sur des caractéristiques géométriques pour représenter l'image sous forme de vecteurs de caractéristiques [73]. Les méthodes globales ont l'avantage de prendre en compte l'ensemble de l'image et donc de mieux capturer les informations globales de l'image, et aussi simples et efficaces, mais elles peuvent manquer de robustesse aux variations locales et aux déformations, ce qui peut réduire leur précision dans des tâches de reconnaissance d'objets ou de motifs complexes [74]. Parmi les méthodes qui base sur ce principe :

- Linear Discriminant Analysis (LDA).
- Support Vector Machine (SVM).
- Principal Component Analysis (PCA).

- **Analyse de discrimination linéaire (LDA)** : L'algorithme LDA a été développé par Belhumeur de l'université de Yale (USA) en 1997. LDA est une méthode d'analyse des données couramment utilisée pour la réduction de dimensionnalité d'un vecteur de caractéristiques et la classification supervisée. Son rôle est de trouver une projection linéaire des données qui maximise les variations entre les images d'individus différents (interclasse) et minimise la variance à l'intérieur de

chaque classe, c'est-à-dire les images d'un même individu.

LDA se concentre principalement sur la projection des caractéristiques dans un espace de dimension supérieure vers des dimensions inférieures. Vous pouvez y parvenir en trois étapes :

- Comme la projection spatiale de dimension inférieure, également appelée critère de Fisher. Tout d'abord, vous devez calculer la séparabilité entre les classes qui est la distance entre la moyenne des différentes classes. C'est ce qu'on appelle la variance interclasses après on a l'équation Sb.

$$S_b = \sum_{j=1}^c (\mu_j - \mu)(\mu_j - \mu)^T \quad (2.1)$$

- Deuxièmement, calculez la distance entre la moyenne et l'échantillon de chaque classe. On l'appelle aussi la variance intra-classe.

$$S = \sum_{j=1}^c \sum_{i=1}^{N_j} (x_{ji} - \mu_j)(x_{ji} - \mu_j)^T \quad (2.2)$$

- Enfin, construisez l'espace de dimension inférieure qui maximise la variance interclasses et minimise la variance intra-classe. P est considéré.

$$w_{\text{opt}} = \arg \max_w \left( \frac{w^T S_b w}{w^T S_w w} \right) = (w_1, w_2, w_3, \dots, w_m) \quad (2.3)$$

- **Méthodes locales :** Les méthodes locales d'extraction des caractéristiques se concentrent sur des zones locales de l'image, ou sur la description de petits patches ou de zones de l'image, appelés descripteurs locaux, pour extraire des informations pertinentes. Ces descripteurs sont extraits à partir de la région d'intérêt dans l'image, ce qui permet d'obtenir des informations plus détaillées sur les caractéristiques locales de l'objet à reconnaître [75].

Les méthodes locales peuvent être sensibles aux variations d'échelle, de rotation et d'illumination, et peuvent nécessiter une grande quantité de temps de calcul pour extraire les caractéristiques de l'ensemble de l'image. Parmi les méthodes les plus courantes d'extraction de caractéristiques locales, on peut citer :

- les descripteurs de texture basés sur des filtres de Gabor.
- SIFT (Scale-Invariant Feature Transform).
- SURF (Speeded-Up Robust Features).
- BSIF (Binarized Statistical Image Features).

- **Filtre de Gabor** : Est un filtre utilisé dans le traitement d'images pour la détection de structures d'une certaine orientation et fréquence. Il a été initialement développé par Dennis Gabor dans le cadre de la théorie des ondelettes en 1946. Le filtre Gabor est largement utilisé dans la vision par ordinateur et le traitement d'images [28].

Le filtre Gabor est basé sur une fonction mathématique appelée ondelette de Gabor, qui est définie comme une fonction sinusoidale modulée par une gaussienne. Cette fonction peut être définie en deux dimensions pour le traitement d'images. En pratique, le filtre Gabor est implémenté en convoluant l'image d'entrée avec une banque de filtres Gabor à différentes orientations et fréquences [28]. La fonction est comme suivant :

$$h(x, y) = g(x, y) \exp(2i\pi f(x \cos \Phi + y \sin \Phi)) \quad (2.4)$$

Ou bien

$$g(x, y) = \exp\left(-\frac{x^2 + y^2}{2a^2}\right) \exp(2\pi\theta i(x \cos \Phi + y \sin \Phi)) \quad (2.5)$$

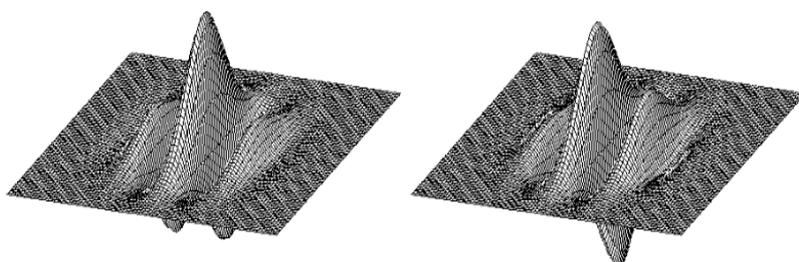


FIGURE 2.16 – Filtre de Gabor [28].

Les réponses des filtres situés dans le demi-plan de fréquence inférieure n'ont pas besoin d'être calculées explicitement, car elles peuvent être générées par la conjugaison complexe de la réponse du filtre située de l'autre côté de l'origine. Les images suivantes montrent l'image originale et les résultats du filtre de Gabor pour différents facteurs d'échantillonnage. La taille de l'image d'entrée est choisie de manière à ce que les résultats du filtre aient toujours la même taille après le sous-échantillonnage [29]. Sur le côté gauche des images suivantes, les (sous-)images d'entrée d'origine et les résultats de filtre superposés pour toutes les orientations

sont affichés. Sur le côté droit, le résultat du filtre sous-échantillonné est affiché pour chaque orientation.

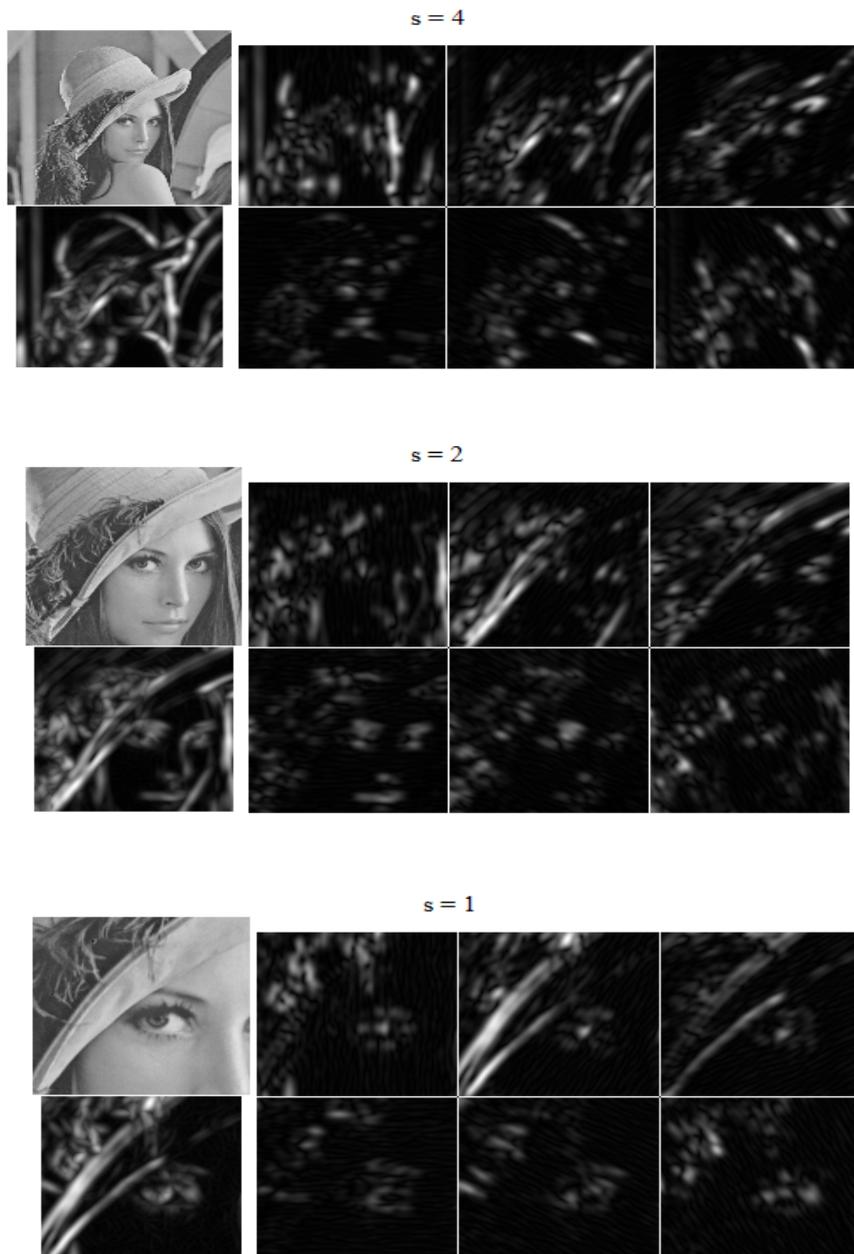


FIGURE 2.17 – Sous-images de l'image originale et grandeurs des résultats de filtre Gabor [29].

- **Histogramme des gradients orientés (HOG)** : Histogram of Oriented Gradients, est un descripteur de caractéristiques souvent utilisé pour extraire des caractéristiques à partir de données d'image. Il est largement utilisé dans les tâches de vision par ordinateur et traitement d'image pour la détection d'objets. Il analyse la distribution des orientations des bords dans un objet pour décrire sa forme

et son apparence. La méthode HOG consiste à diviser l'image en petites cellules puis à calculer l'amplitude et l'orientation du gradient pour chaque pixel d'une image et enfin, le HOG générerait un histogramme pour chacune de ces cellules séparément. Les histogrammes sont créés en utilisant les gradients (Magnitude) et les orientations des valeurs de pixel, d'où le nom "Histogramme de gradients orientés".

Voici le processus de calcul de l'histogramme des gradients orientés [30] :

### 1. La création des cellules et blocs :

Cette étape permet de diviser l'image entrée en 8\*8 cellules et créer des bloc, en combinant chaque 2\*2 cellules en un seul bloc avec un chevauchement de 50%.

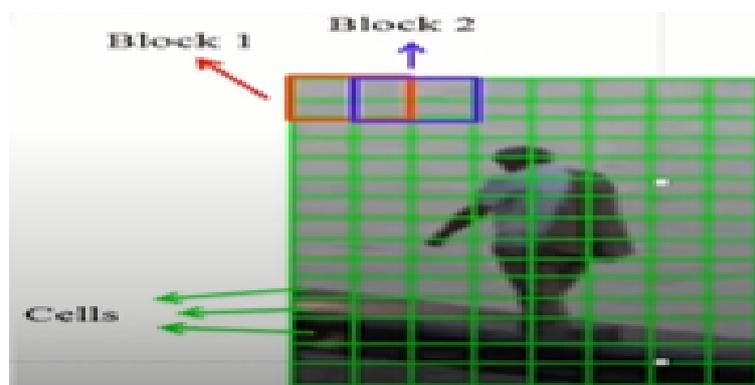


FIGURE 2.18 – Création des cellules blocs [30].

### 2. Calcul des gradients (direction x et y) :

|     |     |    |     |     |
|-----|-----|----|-----|-----|
| 121 | 10  | 78 | 96  | 125 |
| 48  | 152 | 68 | 125 | 111 |
| 145 | 78  | 85 | 89  | 65  |
| 154 | 214 | 56 | 200 | 66  |
| 214 | 87  | 45 | 102 | 45  |

FIGURE 2.19 – Création des cellules blocs [30].

On a mis en surbrillance la valeur de pixel 85. Maintenant, pour déterminer le gradient (ou le changement) dans la direction x, nous devons soustraire la valeur de gauche de la valeur de pixel de droite. De même, pour calculer le gradient dans

la direction y, nous soustrairons la valeur du pixel en dessous de la valeur du pixel au-dessus du pixel sélectionné. Par conséquent, les gradients résultants dans la direction x et y pour ce pixel sont :

$$\text{Changement dans la direction X}(G_x) = 89 - 78 = 11.$$

$$\text{Changement dans la direction Y}(G_y) = 68 - 56 = 8.$$

Ce processus nous donnera deux nouvelles matrices, l'une stockant les gradients dans la direction x et l'autre stockant les gradients dans la direction y.

### 3. Calculer la magnitude et l'orientation :

En utilisant les gradients que nous avons calculés à la dernière étape, nous allons maintenant déterminer la magnitude et l'orientation de chaque valeur de pixel en utilisant les équations (3.1) et (3.2) et nous allons avoir deux matrices l'une stockant les valeurs de magnitude et l'autre stockant les valeurs d'orientation :

$$|G(x, y)| = \sqrt{G_x(x, y)^2 + G_y(x, y)^2} \tag{2.6}$$

$$a(x, y) = \arctan\left(\frac{G_y(x, y)}{G_x(x, y)}\right) \tag{2.7}$$

### 4. Créer l'histogramme de 9 bins :

La création d'un histogramme pour chaque cellule tel que l'orientation sur l'axe des X et la fréquence sur l'axe des Y.

- pour l'orientation de chaque pixel, nous ajoutons sa magnitude correspondante dans le tableau des fréquences.
- Les valeurs de magnitude sont ajoutées dans la case 0, si l'orientation correspondante est dans la plage 0-19.

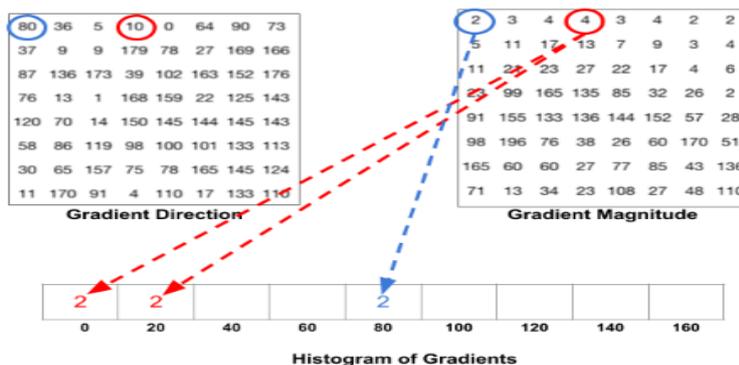


FIGURE 2.20 – Création d'histogramme pour chaque cellule [30].

### 5. vecteur de caractéristique finale de HOG :

Chaque histogramme, on le met à la valeur qui lui correspond dans la matrice (concaténation les histogrammes dans une matrice 1D).

### 6. Normalisation :

Les gradients de l'image sont sensibles à l'éclairage global, on peut réduire cette variation d'éclairage en normalisant les gradients en faisant une normalisation.

- **Quantification de la phase locale (LPQ) :** (en anglais Local Phase Quantization (LPQ)) est un algorithme d'extraction de caractéristiques largement utilisé dans diverses technologies biométriques. Cette approche a été introduite pour la première fois par Ojansivu et al. La méthode sert à diviser l'image en  $N \times N$  petites régions égales, et extrait les informations locales et utiles de l'image dans chaque région. LPQ extrait les informations en utilisant la transformée de Fourier discrète de chaque pixel  $x$ , comme indiqué dans l'équation (2.8).

$$X[k] = \sum_{n=0}^{N-1} x[n] \cdot e^{-i2\pi kn/N} \quad (2.8)$$

IL est possible de généralisée la méthode LPQ dans quatres étapes. Tout d'abord, appliquer l'opérateur (LPQ) sur l'image d'entrée pour avoirr une image étiquetée. Ensuite, diviser l'image résultante en petites régions. Pour chacun d'eux, construit un histogramme des étiquettes pour obtenir les vecteurs des caractéristiques d'articulation du doigts locaux (FKP). Une représentation globale des articulations des doigts (FKP) (un vecteur des caractéristiques globales qui représente l'image entière) est obtenu en combinant tous les vecteurs. La dernière partie de la figure (2.21) résume toutes les étapes montionnées [31].

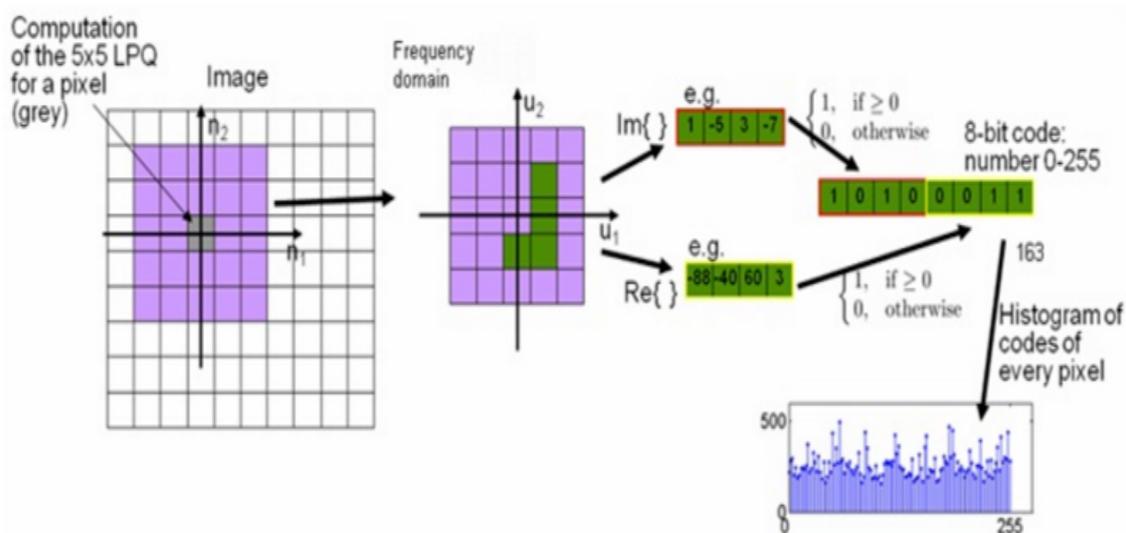


FIGURE 2.21 – des étapes pour génération du vecteur des caractéristiques par la méthode LPQ [31].

- **Méthode hybride** : Les méthodes hybrides combinent à la fois des informations globales et locales pour extraire des caractéristiques de l'image. Ces méthodes cherchent à tirer parti des avantages des méthodes globales et locales pour améliorer les performances de la reconnaissance [76].
- **Comparaison entre les trois méthodes** : Il est difficile de faire une comparaison générale des performances des méthodes locales, globales et hybrides car cela dépend des différentes techniques d'extraction de caractéristiques et des modèles utilisés. Cependant en générale il est possible de conclure que :
  - **Temps de réponse** : les méthodes locales ont généralement des temps de réponse plus rapides que les méthodes globales, car elles travaillent sur des zones spécifiques de l'image plutôt que sur l'ensemble de l'image. Les méthodes hybrides ont un temps de réponse intermédiaire, car elles combinent à la fois des caractéristiques locales et globales.
  - **Complexité** : Les méthodes globales ont tendance à être plus simples en termes de complexité car elles travaillent sur l'ensemble de l'image, tandis que les méthodes locales nécessitent une analyse plus fine et détaillée de l'image. Les méthodes hybrides ont une complexité intermédiaire, car elles combinent à la fois des caractéristiques locales et globales.

- **Occurrence** : Les méthodes locales ont tendance à être plus robustes à des changements mineurs dans les images, car elles se concentrent sur des régions spécifiques. Les méthodes globales peuvent être plus vulnérables aux changements dans les conditions d'éclairage ou d'orientation de l'image. Les méthodes hybrides ont une occurrence intermédiaire, car elles combinent les avantages des deux méthodes.
- **Fiabilité** : Les méthodes globales peuvent être plus fiables que les méthodes locales en raison de leur capacité à prendre en compte des informations globales dans l'image. Cependant, les méthodes locales peuvent être plus fiables dans certaines situations, car elles peuvent détecter des caractéristiques spécifiques de l'image qui sont importantes pour la tâche. Les méthodes hybrides ont une fiabilité intermédiaire, car elles combinent à la fois des caractéristiques locales et globales.

### 2.3.5 Apprentissage :

Cette phase implique l'utilisation de données préalablement annotées pour caractériser les classes de formes et pour entraîner un modèle d'apprentissage automatique afin qu'il puisse apprendre à reconnaître les motifs et les relations dans les données. Il existe trois types d'apprentissage : apprentissage supervisé et non supervisé et l'apprentissage par renforcement.

- **Apprentissage supervisé** : Dans l'apprentissage supervisé, on utilise un ensemble de données d'entraînement étiquetées (labeled data) où chaque exemple est associé à une sortie désirée connue. L'objectif est de trouver une fonction qui peut prédire la sortie pour un nouvel exemple en fonction des entrées. Le processus d'apprentissage implique la mise à jour de paramètres de modèle en fonction des prédictions de sortie par rapport à la sortie désirée pour chaque exemple dans l'ensemble de données d'entraînement [77].

Les modèles d'apprentissage supervisé les plus couramment utilisés sont les régressions linéaires, les réseaux de neurones artificiels, les arbres de décision, les machines à vecteurs de support.

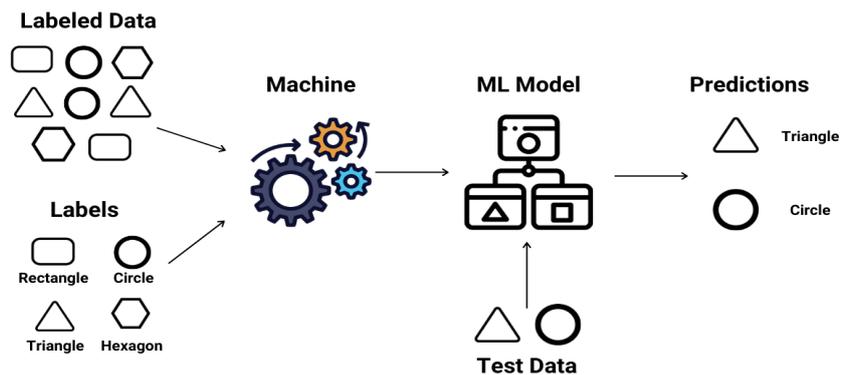


FIGURE 2.22 – Apprentissage supervisé [32].

- **Apprentissage non supervisé** : L'apprentissage non supervisé est une méthode d'apprentissage automatique où les données ne sont pas étiquetées (unlabeled data) et/ou le modèle doit découvrir des structures ou des patterns dans les données sans supervision. Cette méthode est souvent utilisée pour explorer les données, détecter les anomalies, segmenter les données et réduire la dimensionnalité [78].

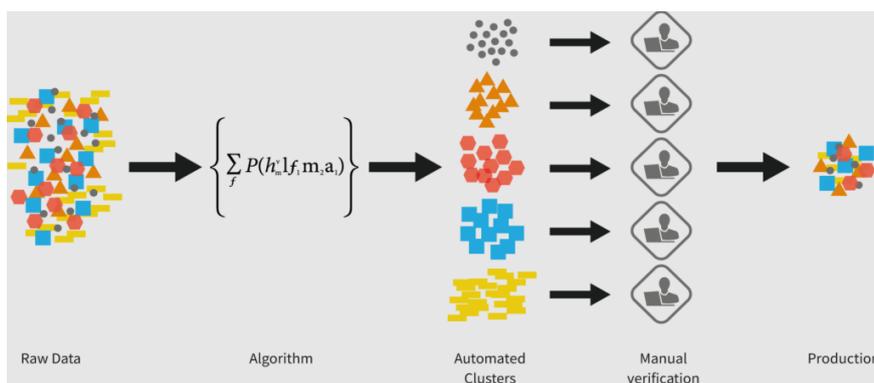


FIGURE 2.23 – Apprentissage non supervisé [33].

- **Apprentissage par renforcement** : L'apprentissage par renforcement est une méthode qui consiste à optimiser de manière itérative un algorithme uniquement à partir des actions qu'il entreprend et de la réponse associée de l'environnement dans lequel il évolue.

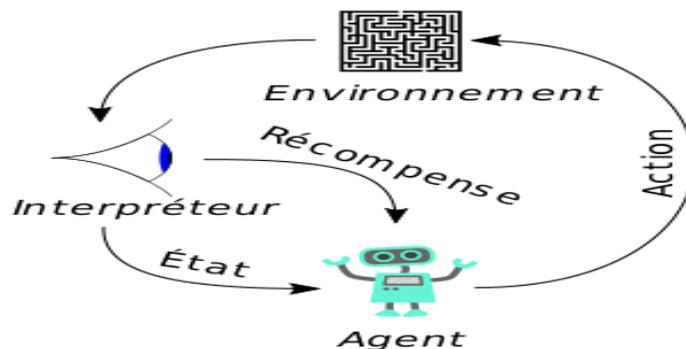


FIGURE 2.24 – Apprentissage par renforcement [34].

Cette méthode permet aux machines et aux agents de déterminer automatiquement le comportement idéal dans un contexte spécifique pour maximiser ses performances. Une simple rétroaction de récompense, connue sous le nom de signal de renforcement, est nécessaire pour que l'agent apprenne quelle action est la meilleure.

### 2.3.6 Post traitement :

Cette étape consiste à traiter les sorties du modèle pour améliorer la qualité des résultats de reconnaissance. Les opérations de post-traitement peuvent inclure la suppression du bruit, la correction d'erreurs pour améliorer la précision de la reconnaissance.

### 2.3.7 Décision :

Cette phase consiste à prendre une décision sur l'identité de l'utilisateur en fonction des empreintes d'articulation des doigts reconnues. La décision peut être prise en utilisant un modèle de classification entraîné pour classer les empreintes d'articulation des doigts en différentes catégories, ou en utilisant des méthodes de comparaison de caractéristiques entre des images entrées et les images stockées dans une base de données [79].

## 2.4 Objectif et les enjeux de la reconnaissance des formes :

Les objectifs de la reconnaissance des formes sont multiples et varient selon les applications. Tout d'abord, la RDF permet de détecter et d'identifier des objets dans des images, ce qui est particulièrement utile dans des domaines tels que la surveillance, la sécurité et la reconnaissance de visages. De plus, la RDF peut être utilisée pour classer des données en différentes catégories, ce qui est utile dans des domaines tels que la médecine et la bio-informatique [80].

En outre, elle peut être utilisée pour prédire des tendances et des événements futurs en analysant des données historiques, ce qui est particulièrement utile dans des domaines tels que la finance, la météorologie et la gestion des stocks [81].

Cependant, malgré les nombreux avantages offerts par la reconnaissance des formes, il y a aussi des enjeux liés à cette technologie. Les principales préoccupations sont liées à la sécurité et à la vie privée, car les systèmes de reconnaissance des formes peuvent être utilisés pour surveiller les individus sans leur consentement. De plus, la variabilité des données, le bruit et les imprécisions des données ainsi que la complexité des données peuvent rendre difficile la reconnaissance des formes. Enfin, il est important de noter que la reconnaissance des formes n'est pas infaillible et peut encore présenter des taux d'erreur significatifs [82].

## 2.5 Conclusion :

A travers ce chapitre nous avons présenté le processus du système de reconnaissance des formes, en disant qu'elle est un domaine de l'intelligence artificielle qui a pour objectif de permettre aux machines de reconnaître et de comprendre les caractéristiques uniques observées de chaque individu. Les systèmes de reconnaissance des formes sont constitués d'une succession d'étapes allant de l'acquisition des données jusqu'à la prise de décision en passant par la segmentation pour isoler les régions d'intérêt, l'extraction des caractéristiques permettant d'extraire les informations pertinentes des empreintes d'articulation.

Les méthodes utilisées dans chaque étape dépendent des caractéristiques de la tâche à accomplir et des types de données à traiter. Les méthodes d'apprentissage permettent aux machines d'apprendre à partir d'exemples et de s'améliorer au fil du temps. Enfin, l'étape de décision permet de prendre une décision en se basant sur les caractéristiques extraites et les modèles appris.

Ce domaine de recherche continue d'évoluer et de susciter l'intérêt de la communauté scientifique, ouvrant de nouvelles perspectives pour la sécurisation et l'identification fiables des individus.

Dans le chapitre suivant, nous mettrons en pratique les concepts et les techniques de reconnaissance multimodale des personnes basées sur les empreintes d'articulation des doigts. Nous présenterons une interface qui exploite ces principes pour l'identification des individus. Tout au long de ce chapitre, nous examinerons en détail des étapes de l'architecture global du système, ainsi que le système proposé. Nous discuterons de l'environnement dans lequel nous avons travaillé, ensuite, nous présenterons les résultats obtenus et entamerons une discussion approfondie à leur sujet. De plus, nous décrirons l'interface que nous avons créée pour les tests, accompagnée d'un guide d'utilisation illustré par des captures d'écrans et nous discuterons de ses avantages et ses limites. Enfin nous terminerons par une conclusion.

## Expérimentations, Résultats et discussions

### 3.1 Introduction

Dans ce chapitre, nous présentons les expériences que nous avons menées pour évaluer les performances d'un système biométrique basé sur l'identification des individus par leurs empreintes d'articulation des doigts (FKP). Nous commencerons par présenter l'architecture globale du système que nous avons développé. Ensuite, nous décrirons l'environnement de travail que nous avons utilisé.

Notre étude présente une évaluation des méthodes que nous avons utilisées. Parmi ces méthodes figurent le Filtre Gabor Bank, LPQ et HOG. Nous avons évalué ces méthodes dans deux contextes distincts : le contexte monomodal et le contexte multimodal.

L'objectif de notre évaluation était de comparer les performances des différentes méthodes d'extraction des caractéristiques dans des scénarios monomodaux et multimodaux.

Finalement, nous avons développé une interface dédiée qui permet d'illustrer visuellement la performance de notre modèle.

### 3.2 Architecture globale du système :

Dans le cadre de notre étude, nous avons réalisé des expériences unimodales et des propositions multimodales pour analyser une base de données polyU FKP comprenant quatre modalités distinctes : LIF, RIF, LMF et RMF.

Tout d'abord, nous avons appliqué filtre Gabor Bank pour extraire les caractéristiques des images. Cette méthode nous a permis de capturer les informations texturales impor-

tantes dans les différentes modalités. Ensuite, nous avons utilisé deux autres descripteurs : LPQ (Local Phase Quantization) et HOG (Histogram of Oriented Gradients). Ces descripteurs nous ont permis d'extraire des informations spécifiques liées à la phase locale et aux gradients d'orientation, respectivement. Dans le but de réduire la dimensionnalité des vecteurs de caractéristiques obtenus, nous avons appliqué une technique appelée LDA (Linear Discriminant Analysis). Enfin, pour l'étape de classification, nous avons opté pour l'algorithme du (K-NN).

Finalement, nos expériences ont exploré différentes modalités de la base de données polyU FKP en utilisant des descripteurs tels que filtre Gabor Bank, LPQ et HOG. Nous avons également évalué l'efficacité de la réduction de dimensionnalité LDA et utilisé l'algorithme KNN pour la classification. Ces résultats nous ont permis de mieux comprendre les performances des différentes approches dans le contexte de la reconnaissance FKP.

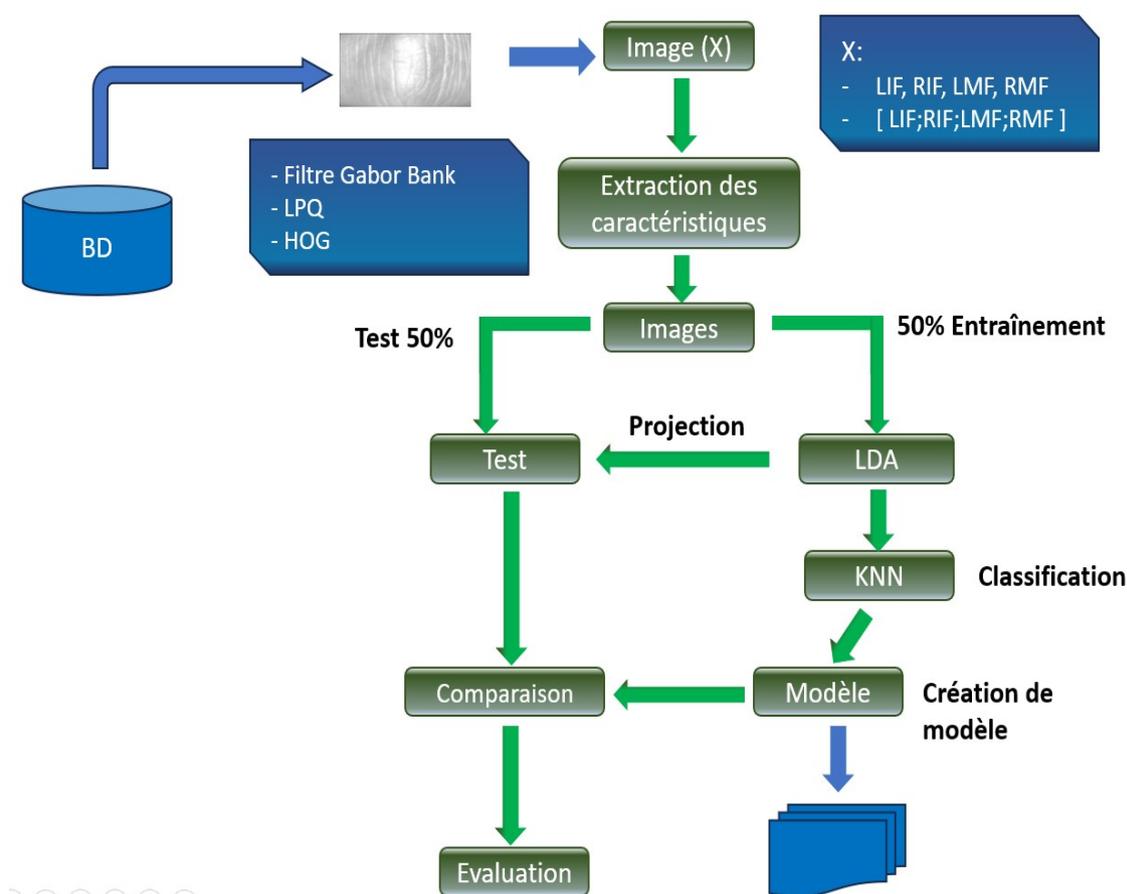


FIGURE 3.1 – L'architecture générale de notre système

### 3.2.1 Acquisition d'image :

Dans cette étape on a utilisé la base de données (PolyU) de l'université polytechnique de Hong Kong pour évaluer la méthode proposée. Cette base de données FKP contient 7920 photos de 660 doigts différents récoltées auprès de 165 personnes dont 125 hommes et 40 femmes. Parmi eux, 143 répondants ont entre 20 et 30 ans et les autres entre 30 et 50 ans. Chaque personne fournit 48 images FKP différentes. Cependant, tous les individus de cette base de données partagent 12 images de l'index gauche (LIF), 12 images du majeur gauche (LMF), 12 images de l'index droit (RIF) et 12 images du majeur droit (RMF). Le nombre total d'images RMF ou RIF ou LIF ou LMF est 1980 images fournies par 165 personnes.

### Séparation de la base de données :

La séparation de la base de données est une étape très importante dans le processus de reconnaissance, elle consiste à définir les données de l'apprentissage et de test afin d'évaluer les performances du système de reconnaissance FKP sur des données différents de celles de test. Dans notre cas, la technique choisie pour séparer la base des données est la validation croisée 50/50 (répartition égale) tel que :

- Les 6 premières images d'empreintes d'articulation de chaque modalité sont utilisées pour l'apprentissage.
- Les 6 images restantes d'empreintes d'articulation de chaque modalité sont utilisées pour les tests.

### 3.2.2 Prétraitement :

Cette étape nous permet de faire quelques modifications tels que, la transformation de l'image original au niveau de gris .., Extraire la région d'intérêt est très importante pour obtenir un résultat plus précis. Dans les images de FKP, on trouve des parties non souhaitées (comme l'arrière-plan d'une image), ainsi que la région d'intérêt (ROI). La base de données (PolyU) utilisées dans notre travail, est une base qui a déjà subi des prétraitements, donc elle n'a pas besoin des prétraitements supplémentaires.

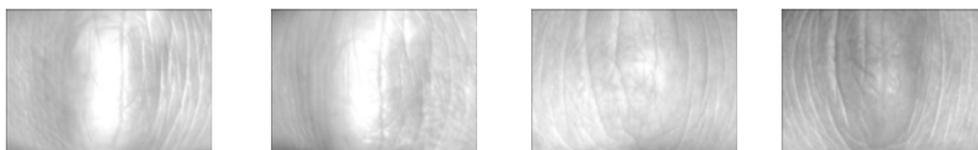


FIGURE 3.2 – Quelques images de la base de données PolyU

### 3.2.3 Extraction des caractéristiques :

On extrait de l'image du FKP les informations les plus pertinentes qui permettent de modéliser la modalité FKP d'une personne par un vecteur de fonctionnalités qui le caractérise. Dans cette étude, nous avons exploré différentes méthodes d'extraction de caractéristiques, notamment le filtre Gabor Bank, LPQ (Local Phase Quantization) et HOG (Histogram of Oriented Gradients).

- **Filter Gabor Bank** : Est une collection de filtre de Gabor qui permet de couvrir plus largement l'espace fréquentiel et de détecter un plus grand nombre d'orientation, ce qui le rend plus performant que filtre de Gabor, ce dernier est sensible aux rotations (orientations). Dans notre travail, nous avons appliqué le filtre Gabor Bank sur des photos provenant de la base de données PolyU FKP. Ces photos ont une dimension de 110x220. Nous avons utilisé une configuration de paramètres comprenant 5 échelles et 8 orientations (40 filtres). La figure( 3.3) montre le résultat d'application du filtre de Gabor Bank.

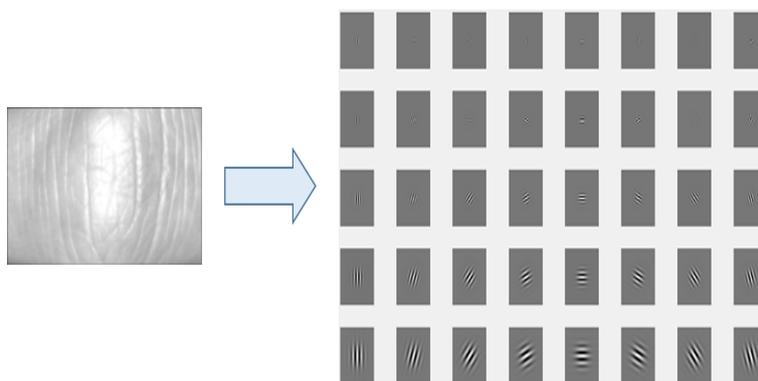


FIGURE 3.3 – Résultat de l'application du Filter Gabor Bank sur une image FKP

- **Histogramme des gradients orientés (HOG)** : Dans notre étude, nous avons appliqué le HOG sur une image provenant de la base de données PolyU FKP. La taille de la cellule que nous avons utilisée était de 15x15, ce qui correspond à la

taille de la région sur laquelle les gradients locaux sont calculés. En utilisant une taille de cellule de 15x15, nous avons pu capturer des informations sur les contours et les textures présents dans l'image et détecter l'objet. Cela nous permet d'obtenir des caractéristiques plus détaillées et spécifiques. La figure( 3.4) montre le résultat d'application du HOG sur une image FKP.

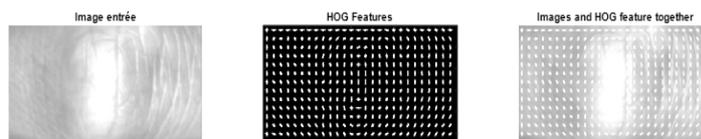


FIGURE 3.4 – résultat d'application du HOG sur une image FKP

- **Quantification de phase locale (LPQ) :** Dans notre travail, nous avons appliqué la méthode LPQ à une matrice d'images 'X' avec une taille de fenêtre de 15x15 pixels. Le résultat est un vecteur de caractéristiques.

### 3.2.4 Réduction de la dimension :

Nous avons utilisé LDA (Linear Discriminant Analysis) pour la réduction de la dimensionnalité des vecteurs de caractéristiques obtenus.

### 3.2.5 Classification :

Les résultats de l'étape d'extraction des paramètres est un vecteur de caractéristiques qui représente chaque images et pour les classifier nous avons proposé l'utilisation de la méthode de plus proche voisin (K-NN) avec une distance de Mahalanobis.

### 3.2.6 Systèmes proposés :

Les tests sur la base de données FKP ont été réalisés en six expérimentations divisés en deux catégories, système monomodale (expérimentations 1,2 et 3) et multimodale (expérimentations 4,5 et 6) :

**1-Première expérimentation :** Dans cette expérimentation, nous avons appliqué le filtre de Gabor Bank avec 5 échelles et 8 orientations (40 filtres) sur une modalité parmi les 4 (LIF, LMF, RIF et RMF) pour l'extraction de caractéristique, avec la méthode LDA pour la réduction de la dimension des vecteurs de caractéristiques et la classification KNN.

**2-Deuxième expérimentation :** Dans cette expérimentation, nous avons appliqué le descripteur phase locale quantification (LPQ) avec une taille de fenêtre carrée 15x15 pixels sur une modalité parmi les 4 (LIF, LMF, RIF et RMF) pour l'extraction de caractéristique, avec la méthode LDA pour la réduction de la dimension des vecteurs de caractéristiques et la classification K-NN.

**3-Troisième expérimentation :** Dans cette expérimentation, nous avons appliqué le descripteur Histogramme des gradients orientés (HOG) avec une taille de cellule 15x15 sur une modalité parmi les 4 (LIF, LMF, RIF et RMF) pour l'extraction de caractéristique ainsi que la méthode LDA pour la réduction de la dimension des vecteurs de caractéristiques et la classification KNN.

**4-Quatrième expérimentation :** Nous avons combinés des modalités différentes (LIF, LMF, RIF et RMF). Dans cette expérimentation, nous avons utilisé le filtre de Gabor Bank avec 5 échelles et 8 orientations (40 filtres) pour l'extraction de caractéristique avec la méthode LDA pour la réduction de la dimension des vecteurs de caractéristiques et la classification KNN.

**5-Cinquième expérimentation :** Nous avons combinés des modalités différentes (LIF, LMF, RIF et RMF). Dans cette expérimentation, nous avons utilisé le descripteur phase locale quantification (LPQ) avec une taille de fenêtre carrée 15x15 pixels ainsi que la méthode LDA pour la réduction de la dimension des vecteurs de caractéristiques et la classification K-NN.

**6-sixième expérimentation :** Nous avons combinés des modalités différentes (LIF, LMF, RIF et RMF). Dans cette expérimentation, nous avons utilisé le descripteur Histogramme des gradients orientés (HOG) avec une taille de cellule 15x15, ainsi que la méthode LDA pour la réduction de la dimension des vecteurs de caractéristiques et la classification KNN.

### 3.3 Environnement du travail :

#### ■ Environnement Logiciel :

Notre environnement logiciel est principalement basé sur MATLAB, que nous avons utilisé pour la majorité des opérations de traitement d'images, d'extraction de caractéristiques et d'apprentissage automatique. De plus, nous avons exploité des outils spécifiques tels que PhD Tools pour des tâches spécifiques liées à la reconnaissance des empreintes d'articulation des doigts.

- **Logiciel MATLAB :** MATLAB (MATrix LABoratory) est une plate-forme de programmation conçue spécifiquement pour les ingénieurs et les scientifiques afin d'analyser et de concevoir des systèmes et des produits qui transforment notre monde. Le cœur de MATLAB est le langage MATLAB, un langage matriciel permettant l'expression la plus naturelle des mathématiques computationnelles. Il offre des fonctionnalités avancées pour le traitement du signal, le traitement d'image, l'analyse des données et l'apprentissage automatique. Nous avons exploité les capacités de MATLAB pour effectuer diverses opérations sur les images d'empreintes d'articulation, telles que la lecture des images, le prétraitement, l'extraction des caractéristiques à l'aide de filtres de Gabor, LDA et bien plus encore.
- **PhD Tools :** La boîte à outils de reconnaissance faciale PhD (Pretty helpful Development functions) fournit une collection d'algorithmes, de fonctions et de scripts Matlab préprogrammés pour aider les chercheurs dans leurs activités de recherche et d'analyse de données. Elle a été créée comme un sous-produit de recherches et peut être téléchargée gratuitement. Le PhD Facial Recognition Toolkit comprend des implémentations de certaines technologies de reconnaissance faciale les plus connus, telles que l'analyse en composantes principales (PCA), l'analyse discriminante linéaire (LDA), l'analyse en composantes principales des noyaux

(KPCA) et l'analyse de Fisher des noyaux (KFA). Il propose des fonctions pour la construction et l'utilisation des filtres Gabor et tous les autres outils nécessaires pour créer une technologie de reconnaissance faciale basée sur Gabor. En plus des techniques répertoriées, il existe également de nombreux outils d'évaluation dans la boîte à outils pour vous aider à créer des courbes de performance et des mesures pour la reconnaissance faciale que vous évaluez. Ces outils sont utilisés pour calculer les caractéristiques de fonctionnement du récepteur (ROC), les courbes de performances attendues (EPC) et les courbes de score d'appariement cumulé (CMC). Plus important encore (surtout pour les débutants dans ce domaine), La boîte à outils comprend également plusieurs scripts de démonstration qui montrent comment créer et évaluer un système de reconnaissance faciale complet. Le script de démonstration montre comment aligner des images de visage, comment extraire des caractéristiques à partir d'images alignées, recadrées et normalisées, la manière de classer ces caractéristiques et enfin comment évaluer les performances de l'ensemble du système et de présenter les résultats sous la forme d'une courbe de performances et les indicateurs de performance correspondants.

- **Environnement matériel :** Nous avons utilisé un environnement matériel spécifique pour mener nos expériences et réaliser nos analyses. Nous avons travaillé avec un ordinateur HP EliteBook, qui offre des caractéristiques adaptées aux besoins de notre projet. Le HP EliteBook est équipé d'un système d'exploitation Windows 10 Professionnel, en version 64 bits, et un processeur Intel Core i5-5300U cadencé à 2.30 GHz. Ce processeur offre une puissance de calcul suffisante pour exécuter les tâches de traitement des données et d'apprentissage automatique nécessaires à notre système de reconnaissance, et une mémoire RAM de 8Go.

### 3.4 Résultats et discussion :

■ **Métrique de performance** : Pour savoir la performance de notre système en mode d'identification, nous avons utilisé le taux de reconnaissance de rang-1 (ROR) et la courbe CMC. En mode vérification, nous avons utilisé le EER, FAR et la courbe ROC.

■ **Système monomodal** : Les expériences du système monomodal consistent à l'utilisation d'une seule modalité. Les sous sections qui suivent fournissent l'évaluation des performances du système en mode identification/vérification.

Plusieurs tests ont été effectués en utilisant trois descripteurs différents, filtre Gabor Bank, quantification de phase locale (LPQ) et histogramme des gradients orientés (HOG).

Nous présentons ci-dessous les expérimentations :

- **Expérimentation 01** :

| Extraction de caractéristique | Reduction de dimension | Classification |
|-------------------------------|------------------------|----------------|
| Filtre Gabor Bank             | LDA                    | K-NN           |

Le tableau ci-dessous représente Les mesures (évaluation) de performances de cette expérimentation pour les deux modes (identification/vérification).

Les mesures de performance pour différents type de doigts (LIF, RIF, LMF, RMF) sont répertoriées dans le tableau (3.1) et les courbe ROC et CMC qui ont représentés dans les figures (3.5) et (3.6) respectivement.

| Mode identification | Mode verification |        |          |            |
|---------------------|-------------------|--------|----------|------------|
|                     | ROR               | EER(%) | (1%) FAR | (0.1%) FAR |
| LMF                 | 93.33             | 2.92   | 96.16    | 93.73      |
| RMF                 | 91.31             | 2.94   | 95.55    | 92.32      |
| LIF                 | 93.03             | 3.53   | 95.45    | 93.23      |
| RIF                 | 93.23             | 2.92   | 95.45    | 93.03      |

TABLE 3.1 – Résultats de ROR et EER de Gabor Bank du Système unimodal.

Nous concluons que la performance la plus haute est obtenue dans le cas de la modalité LMF, où le taux de reconnaissance du rang 1 (ROR) est 93.33%. Les

valeurs de performance relatives à chaque modalité mentionnée dans le tableau mettent en évidence la supériorité de la modalité LMF en termes de précision. La figure (3.6) présente la courbe CMC pour les différents modalités notamment LIF, LMF, RIF et RMF, ces courbes démontrent visuellement l'efficacité et la performance de notre système pour chaque modalité.

De plus, nous avons également évalué les performances de notre système en mode de vérification, où le système donne une haute précision à la modalité LMF par rapport aux modalités LIF, RIF et RMF. Une minimale erreur EER égal à 2.92% et 1% FAR de 96.16% et 0.1% FAR de 93,73% est ainsi obtenue pour la modalité LMF. En outre, le reste des modalités RMF et LIF, RIF donnent respectivement un EER égal à 2.94%, 3.53% et 3.94%.

La figure (3.5) présente les résultats de comparaison entre les quatre modalités sous forme de la courbe ROC. Ces derniers graphique montre bien la haute performance de la modalité LMF de couleur jaune.

Ces observations mettent en évidence l'excellence de la modalité LMF dans la reconnaissance et la vérification des FKPs, tandis que les modalités RMF, RIF et LIF présentent des performances comparables mais légèrement inférieures.

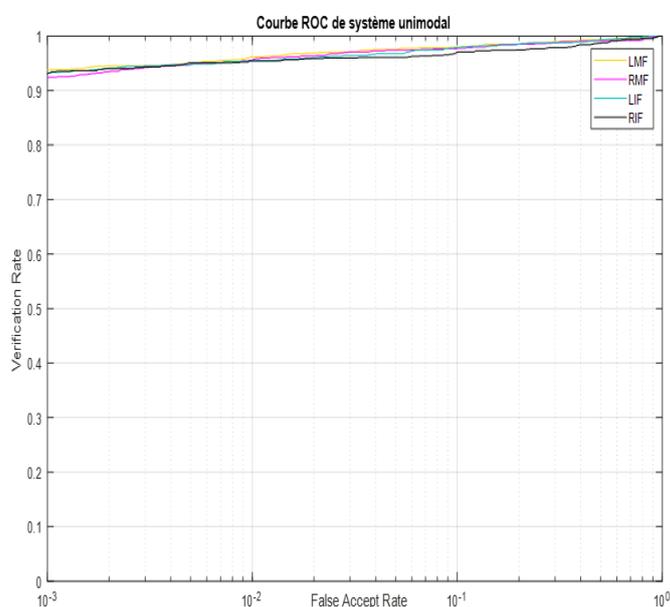


FIGURE 3.5 – Courbe ROC de la méthode Gabor Bank du système unimodal.

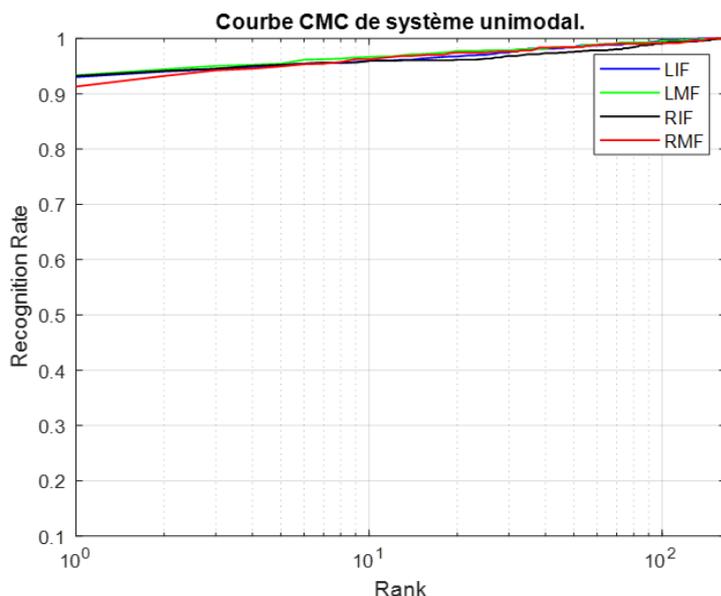


FIGURE 3.6 – Courbe CMC de la méthode Gabor Bank du système unimodal.

- **Expérimentation 02 :**

| Extraction de caractéristique | Reduction de dimension | Classification |
|-------------------------------|------------------------|----------------|
| LPQ                           | LDA                    | K-NN           |

Le tableau ci-dessous représente Les mesures (évaluation) de performances de cette expérimentation pour les deux modes (identification/vérification).

Les mesures de performance pour différents type de doigts (LIF, RIF, LMF, RMF) sont répertoriées dans le tableau (3.2) et les courbe ROC et CMC qui ont représentés dans la figure (3.7) et (3.8) respectivement.

| Mode identification | Mode verification |        |          |            |
|---------------------|-------------------|--------|----------|------------|
|                     | ROR               | EER(%) | (1%) FAR | (0.1%) FAR |
| <b>LMF</b>          | 85.86             | 3.80   | 92.63    | 85.56      |
| <b>RMF</b>          | 85.56             | 4.04   | 91.82    | 83.13      |
| <b>LIF</b>          | 84.95             | 3.96   | 92.53    | 84.65      |
| <b>RIF</b>          | 83.94             | 5.20   | 90.30    | 82.73      |

TABLE 3.2 – Résultats de ROR et EER de LPQ du Système unimodal.

- Selon les résultats présentés dans le tableau, il est évident que la modalité LMF

obtient une précision élevée par rapport aux modalités LIF, RIF et RMF, où le taux de reconnaissance du rang 1 (ROR) est 85,86%. Les valeurs de performance relatives à chaque modalité mentionnée dans le tableau mettent en évidence la supériorité de la modalité LMF en termes de précision. La figure (3.8) présente la courbe CMC pour les différents modalités notamment LIF, LMF, RIF et RMF, ces courbes démontrent visuellement l'efficacité et la performance de notre système pour chaque modalité.

De plus, nous avons également évalué les performances de notre système en mode de vérification, où le système donne une haute précision à la modalité LMF par rapport aux modalités LIF, RIF et RMF. Une minimale erreur EER égal à 3.80% et 1% FAR de 92.63% et FAR de 85,56% est ainsi obtenue pour la modalité LMF. La figure (3.7) présente les résultats de comparaison entre les quatre modalités sous forme de la courbe ROC. Ces derniers graphique montre bien la haute performance de la modalité LMF de couleur bleu-vert (Cyan).

Ces observations mettent en évidence l'importance de la modalité LMF dans la reconnaissance et la vérification des FKPs, tandis que les modalités RMF, RIF et LIF présentent des performances comparables mais légèrement inférieures.

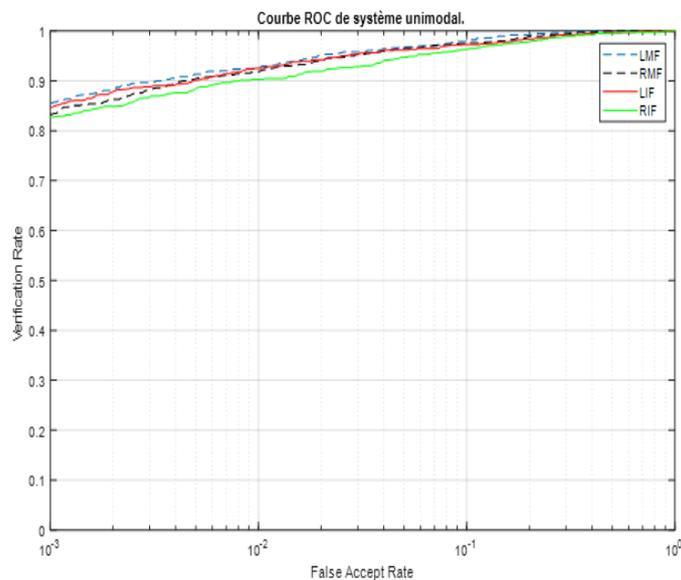


FIGURE 3.7 – Courbe ROC de la méthode LPQ du système unimodal.

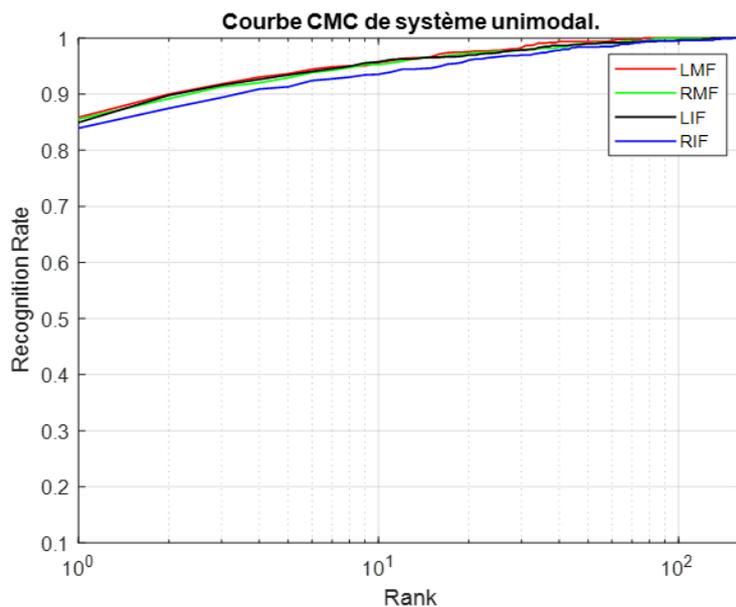


FIGURE 3.8 – Courbe CMC de la méthode LPQ du système unimodal.

- **Expérimentation 03 :**

| Extraction de caractéristique | Reduction de dimension | Classification |
|-------------------------------|------------------------|----------------|
| HOG                           | LDA                    | K-NN           |

Le tableau ci-dessous représente Les mesures (évaluation) de performances de cette expérimentation pour les deux modes (identification/vérification).

Les mesures de performance pour différents type de doigts (LIF, RIF, LMF, RMF) sont répertoriées dans le tableau (3.3) et les courbe ROC et CMC qui ont représentés dans la figure (3.9) et (3.10) respectivement.

| Mode identification | Mode verification |        |          |            |
|---------------------|-------------------|--------|----------|------------|
|                     | ROR               | EER(%) | (1%) FAR | (0.1%) FAR |
| <b>LMF</b>          | 79.70             | 7.68   | 84.75    | 78.18      |
| <b>RMF</b>          | 80.10             | 9.10   | 84.85    | 78.89      |
| <b>LIF</b>          | 76.50             | 9.09   | 82.73    | 74.34      |
| <b>RIF</b>          | 76.77             | 9.89   | 81.72    | 75.25      |

TABLE 3.3 – Résultats de ROR et EER de HOG du Système unimodal.

Nous concluons que la performance la plus haute est obtenue dans le cas de la modalité RMF, où le taux de reconnaissance du rang 1 (ROR) est 80,10%. Les valeurs de performance relatives à chaque modalité mentionnée dans le tableau, mettent en évidence la supériorité de la modalité RMF en termes de précision. La figure (3.10) présente la courbe CMC pour les différents modalités notamment LIF, LMF, RIF et RMF, ces courbes démontrent visuellement l'efficacité et la performance de notre système pour chaque modalité.

De plus, nous avons également évalué les performances de notre système en mode de vérification. Le système donne une haute précision à la modalité LMF par rapport aux modalités RMF et LIF, RIF. Une minimale erreur EER égal à 7.68% et 1% FAR de 84.75% et 0.1% FAR de 78,18% est ainsi obtenue pour la modalité LMF. En outre, les restes des modalités RMF et LIF, RIF donnent respectivement un EER égal à 9.10%, 9.09% et 9.89%.

La figure (3.9) présente les résultats de comparaison entre les quatre modalités sous forme de la courbe ROC. Ces derniers graphique montre bien la haute performance de la modalité LMF de couleur jaune.

Ces observations mettent en évidence l'importance de la modalité RMF dans la reconnaissance et la vérification des FKPs, tandis que les modalités RMF, RIF et LIF présentent des performances comparables mais légèrement inférieures.

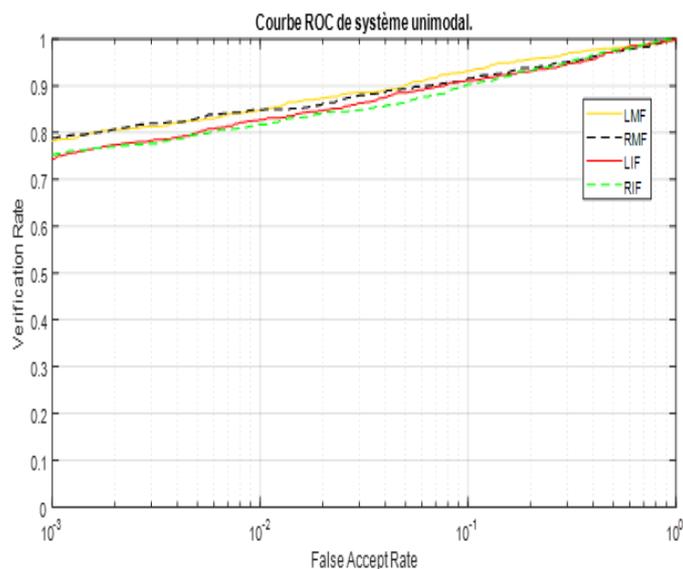


FIGURE 3.9 – Courbe ROC de la méthode HOG du système unimodal.

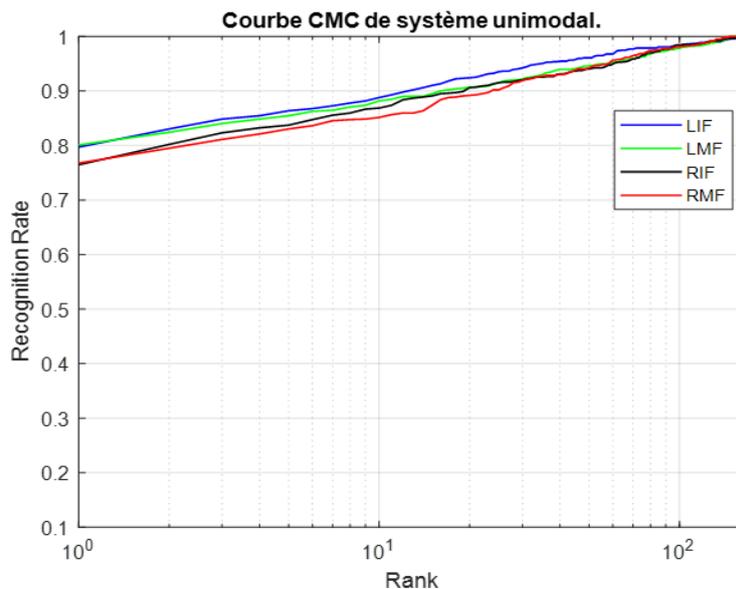


FIGURE 3.10 – Courbe CMC de la méthode HOG du système unimodal.

■ **Système multimodal** : Les expériences du système multimodal consistent à fusionner deux modalités ou quatre modalités différentes. Les sous-sections qui suivent fournissent l'évaluation des performances du système en mode identification/vérification. Plusieurs tests ont été effectués en utilisant trois descripteurs différents : filtre Gabor Bank, quantification de phase locale (LPQ) et histogramme des gradients orientés (HOG).

Nous présentons ci-dessous les expérimentations :

- **Expérimentation 04** :

| Extraction de caractéristique | Reduction de dimension | Classification |
|-------------------------------|------------------------|----------------|
| Filtre Gabor Bank             | LDA                    | K-NN           |

Le tableau ci-dessous représente les mesures (évaluation) de performances pour différents types de doigts (LIF, RIF, LMF, RMF) de cette expérimentation pour les deux modes (identification/vérification) et les courbes ROC et CMC sont représentées dans la figure (3.11) et (3.12) respectivement.

| Mode identification    | Mode verification |        |          |            |
|------------------------|-------------------|--------|----------|------------|
|                        | ROR               | EER(%) | (1%) FAR | (0.1%) FAR |
| <b>LIF-RIF</b>         | 98.18             | 0.81   | 99.29    | 98.48      |
| <b>RMF-LMF</b>         | 98.18             | 0.60   | 99.39    | 99.29      |
| <b>RIF-RMF</b>         | 98.78             | 0.45   | 99.59    | 99.09      |
| <b>LIF-LMF</b>         | 98.28             | 0.90   | 99.09    | 98.48      |
| <b>LIF-RMF</b>         | 98.08             | 0.71   | 99.29    | 98.48      |
| <b>LMF-RIF</b>         | 98.59             | 0.32   | 99.90    | 99.09      |
| <b>LIF-RIF-LMF-RMF</b> | 99.89             | 0.01   | 100.0    | 100.0      |

TABLE 3.4 – Résultats de ROR et EER de Gabor Bank du Système multimodal.

Nous concluons que la performance la plus haute est obtenue dans le cas de la fusion de quatre modalités (LIF, RIF, RMF et LMF), où le taux de reconnaissance du rang 1 (ROR) est 99.89%. Les valeurs de performance relatives à chaque combinaison de modalité mentionnée dans le tableau, mettent en évidence la supériorité de la combinaison entre les quatre modalités (LIF, RIF, RMF et LMF) en termes de précision. La figure (3.12) présente la courbe CMC pour les différentes modalités notamment (LIF, LMF, RIF et RMF), ces courbes démontrent visuellement l'efficacité et la performance de notre système pour chaque combinaisons.

De plus, nous avons également évalué les performances de notre système en mode de vérification, où le système donne une haute précision dans le cas de la fusion de quatre modalités (LIF, RIF, RMF et LMF) par rapport aux autres combinaisons. Une minimale erreur EER égal à 0.01% est ainsi obtenue pour la combinaison (LIF, RIF, RMF et LMF). En outre, les restes des combinaisons (LIF-RIF), (LMF-RMF), (RIF-RMF), (LIF-LMF), (LIF-RMF) et (LMF-RIF) donnent respectivement un EER égal à 0.81%, 0.60%, 0.45%, 0.90%, 0.71% et 0.32%.

La figure (3.11) présente les résultats de comparaison entre les sept combinaisons sous forme de la courbe ROC. Ces derniers graphique montre bien la haute performance de la combinaison de quatre modalités (LIF, RIF, RMF et LMF) de couleur jaune.

Ces observations mettent en évidence l'importance de la combinaison (fusion) de

quatre modalités (LIF, RIF, RMF et LMF) dans la reconnaissance et la vérification des FKPs, tandis que les autres combinaisons présentent des performances comparables mais légèrement inférieures.

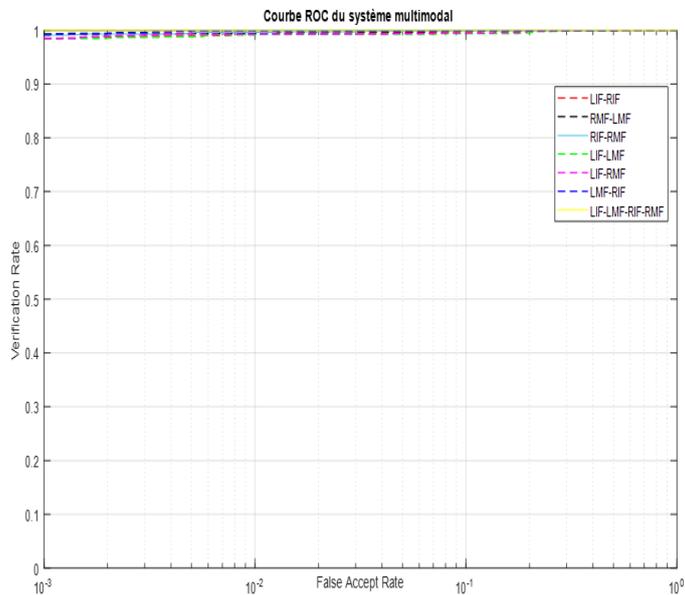


FIGURE 3.11 – Courbe ROC de la méthode Gabor Bank du système multimodal.

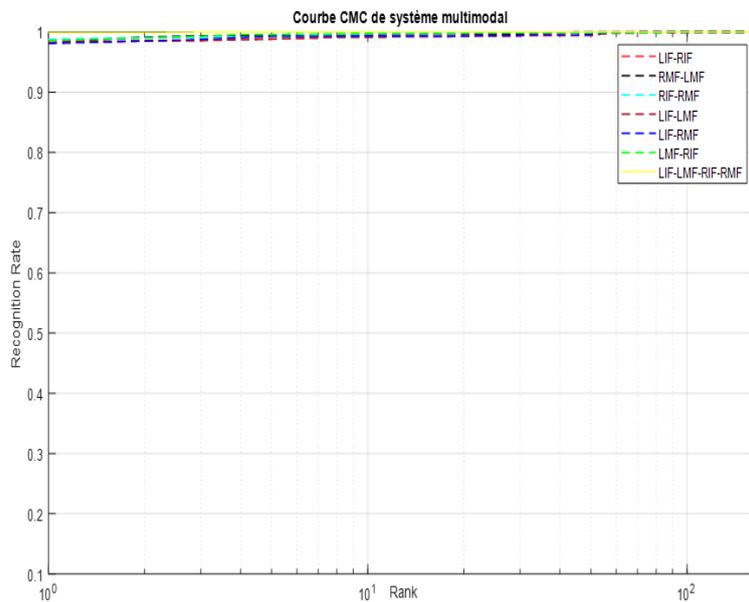


FIGURE 3.12 – Courbe CMC de la méthode Gabor Bank du système multimodal.

- **Expérimentation 05 :**

| Extraction de caractéristique | Reduction de dimension | Classification |
|-------------------------------|------------------------|----------------|
| LPQ                           | LDA                    | K-NN           |

Le tableau ci-dessous (3.5) représente Les mesures (évaluation) de performances pour différents type de doigts (LIF, RIF, LMF, RMF) de cette expérimentation pour les deux modes (identification/vérification) et les courbes ROC et CMC sont représentées dans la figure (3.13) et (3.14) respectivement.

| Mode identification    | Mode verification |        |          |            |
|------------------------|-------------------|--------|----------|------------|
|                        | ROR               | EER(%) | (1%) FAR | (0.1%) FAR |
| <b>LIF-RIF</b>         | 91.41             | 2.83   | 95.35    | 90.10      |
| <b>RMF-LMF</b>         | 94.24             | 2.63   | 96.77    | 93.54      |
| <b>RIF-RMF</b>         | 93.03             | 1.69   | 97.17    | 91.72      |
| <b>LIF-LMF</b>         | 92.83             | 2.24   | 95.96    | 93.13      |
| <b>LIF-RMF</b>         | 93.64             | 2.41   | 96.97    | 93.64      |
| <b>LMF-RIF</b>         | 94.24             | 2.23   | 97.07    | 93.94      |
| <b>LIF-RIF-LMF-RMF</b> | 98.69             | 0.59   | 99.49    | 98.69      |

TABLE 3.5 – Résultats de ROR et EER de LPQ du Système multimodal.

D'après le tableau, nous concluons que la performance la plus haute est obtenue dans le cas de la fusion de quatre modalités (LIF, RIF, RMF et LMF), où le taux de reconnaissance du rang 1 (ROR) est 98.69%. Les valeurs de performance relatives à chaque combinaison de modalité mentionnée dans le tableau, mettent en évidence la supériorité de la combinaison entre les quatre modalités (LIF, RIF, RMF et LMF) en termes de précision. La figure (3.14) présente la courbe CMC pour les différentes modalités notamment (LIF, LMF, RIF et RMF ), ces courbes démontrent visuellement l'efficacité et la performance de notre système pour chaque combinaisons.

De plus, nous avons également évalué les performances de notre système en mode de vérification, où le système donne une haute précision dans le cas de la fusion de quatre modalités (LIF, RIF, RMF et LMF par rapport aux autres combinaisons.

Une minimale erreur EER égal à 0.59% est ainsi obtenue pour la combinaison (LIF, RIF, LMF, RMF). En outre, les restes des combinaisons (LIF-RIF), (LMF-RMF), (RIF-RMF), (LIF-LMF), (LIF-RMF) et (LMF-RIF) donnent respectivement un EER égal à 2.83%, 2.63%, 1.69%, 2.24%, 2.41% et 2.23%.

La figure (3.13) présente les résultats de comparaison entre les sept combinaisons sous forme de la courbe ROC. Ces derniers graphique montre bien la haute performance de la combinaison de quatre modalités (LIF, RIF, RMF et LMF) de couleur jaune.

Ces observations mettent en évidence l'importance de la combinaison de quatre modalités (LIF, RIF, RMF et LMF) dans la reconnaissance et la vérification des FKPs, tandis que les autres combinaisons présentent des performances comparables mais légèrement inférieures.

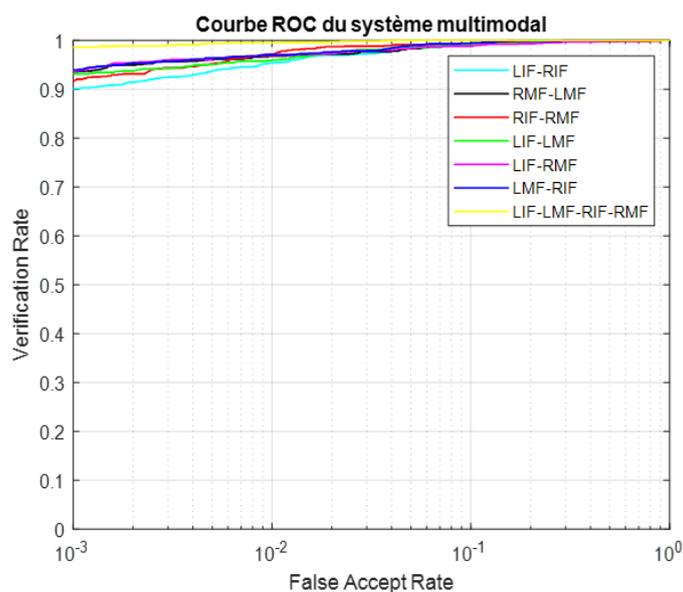


FIGURE 3.13 – Courbe ROC de la méthode LPQ du système multimodal.

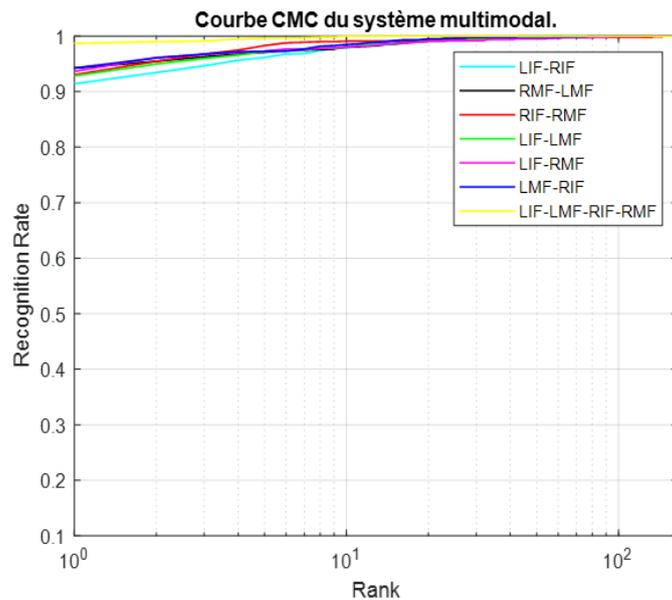


FIGURE 3.14 – Courbe CMC de la méthode LPQ du système multimodal.

- **Expérimentation 06 :**

| Extraction de caractéristique | Reduction de dimension | Classification |
|-------------------------------|------------------------|----------------|
| HOG                           | LDA                    | K-NN           |

Le tableau ci-dessous représente Les mesures (évaluation) de performances pour différents type de doigts (LIF, RIF, LMF, RMF) de cette expérimentation pour les deux modes (identification/vérification) et les courbes ROC et CMC sont représentées dans la figure (3.15) et (3.16) respectivement.

| Mode identification    | Mode verification |        |          |            |
|------------------------|-------------------|--------|----------|------------|
|                        | ROR               | EER(%) | (1%) FAR | (0.1%) FAR |
| <b>LIF-RIF</b>         | 93.03             | 3.03   | 95.76    | 92.83      |
| <b>RMF-LMF</b>         | 93.84             | 2.04   | 97.17    | 94.24      |
| <b>RIF-RMF</b>         | 94.75             | 1.92   | 97.27    | 94.95      |
| <b>LIF-LMF</b>         | 93.23             | 3.03   | 95.66    | 93.64      |
| <b>LIF-RMF</b>         | 93.64             | 3.24   | 96.46    | 94.04      |
| <b>LMF-RIF</b>         | 93.84             | 2.55   | 95.96    | 94.04      |
| <b>LIF-RIF-LMF-RMF</b> | 99.60             | 0.19   | 99.90    | 99.60      |

TABLE 3.6 – Résultats de ROR et EER de HOG du Système multimodal.

D'après le tableau, nous concluons que la performance la plus haute est obtenue dans le cas de la fusion de quatre modalités (LIF, RIF, RMF et LMF), où le taux de reconnaissance du rang 1 (ROR) est 99.60%. Les valeurs de performance relatives à chaque combinaison de modalité mentionnée dans le tableau, mettent en évidence la supériorité de la combinaison entre les quatre modalités (LIF, RIF, RMF et LMF) en termes de précision. La figure (3.16) présente la courbe CMC pour les différentes modalités notamment (LIF, LMF, RIF et RMF), ces courbes démontrent visuellement l'efficacité et la performance de notre système pour chaque combinaisons.

De plus, nous avons également évalué les performances de notre système en mode de vérification, où le système donne une haute précision dans le cas de la fusion de quatre modalités (LIF, RIF, RMF et LMF) par rapport aux autres combinaisons. Une minimale erreur EER égal à 0.19% est ainsi obtenue pour la combinaison (LIF, RIF, LMF, RMF). En outre, les restes des combinaisons (LIF-RIF), (LMF-RMF), (RIF-RMF), (LIF-LMF), (LIF-RMF) et (LMF-RIF) donnent respectivement un EER égal à 3.03%, 2.04%, 1.92%, 3.03%, 3.24% et 2.55%.

La figure (3.15) présente les résultats de comparaison entre les sept combinaisons sous forme de la courbe ROC. Ces derniers graphique montre bien la haute performance de la combinaison de quatre modalités (LIF, RIF, RMF et LMF) de couleur jaune.

Ces observations mettent en évidence l'importance de la combinaison de quatre

modalités (LIF, RIF, RMF et LMF) dans la reconnaissance et la vérification des FKPs, tandis que les autres combinaisons présentent des performances comparables mais légèrement inférieures.

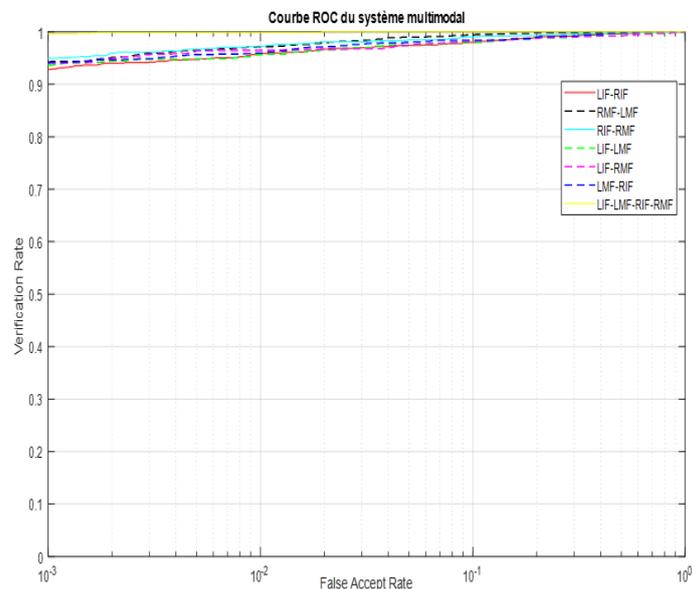


FIGURE 3.15 – Courbe ROC de la méthode HOG du système multimodal.

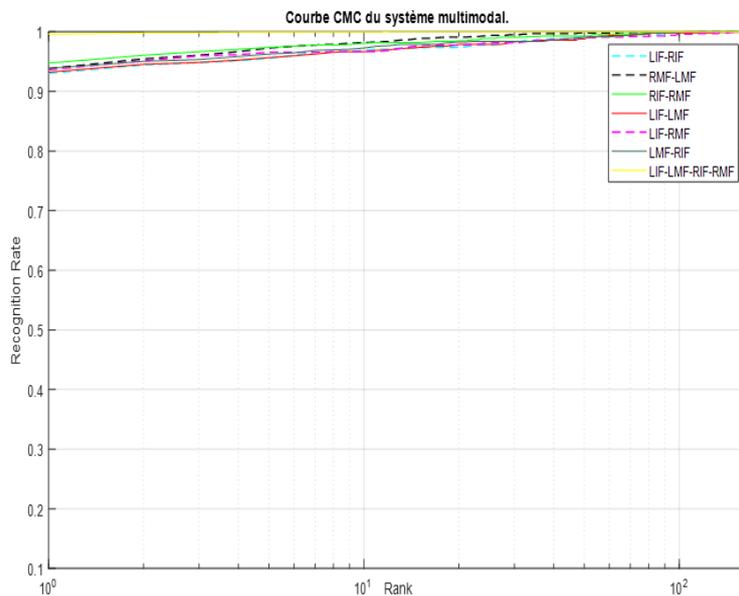


FIGURE 3.16 – Courbe CMC de la méthode HOG du système multimodal.

■ Etude comparative entre les méthodes :

| <i>Modalités</i><br><i>Méthodes</i> | LMF    | RMF    | LIF    | RIF    |
|-------------------------------------|--------|--------|--------|--------|
| Gabor Bank                          | 93.33% | 91.31% | 93.03% | 93.23% |
| LPQ                                 | 85.86% | 85.56% | 84.95% | 83.94% |
| HOG                                 | 79.70% | 80.10% | 76.50% | 76.77% |

TABLE 3.7 – Comparaison ROR de 3 descripteurs pour le système monomodale

| <i>Modalités</i><br><i>Méthodes</i> | LMF   | RMF   | LIF   | RIF   |
|-------------------------------------|-------|-------|-------|-------|
| Gabor Bank                          | 2.92% | 2.94% | 3.53% | 3.94% |
| LPQ                                 | 3.80% | 4.04% | 3.96% | 5.20% |
| HOG                                 | 7.68% | 9.10% | 9.09% | 9.89% |

TABLE 3.8 – Comparaison EER de 3 descripteurs pour le système monomodale

| <i>Modalités</i><br><i>Méthodes</i> | LIF RIF | RMF LMF | RIF RMF | LIF LMF | LIF RMF | RIF LMF | LIF<br>RIF<br>LMF<br>RMF |
|-------------------------------------|---------|---------|---------|---------|---------|---------|--------------------------|
| Gabor Bank                          | 98.18%  | 98.18%  | 98.78%  | 98.28%  | 98.08%  | 98.59%  | 99.89%                   |
| LPQ                                 | 91.41%  | 94.24%  | 93.03%  | 92.83%  | 93.64%  | 94.24%  | 98.69%                   |
| HOG                                 | 93.03%  | 93.84%  | 94.75%  | 93.23%  | 93.64%  | 93.84%  | 99.60%                   |

TABLE 3.9 – Comparaison ROR de 3 descripteurs pour le système multimodale

| <i>Modalités</i><br><i>Méthodes</i> | LIF RIF | RMF LMF | RIF RMF | LIF LMF | LIF RMF | RIF LMF | LIF<br>RIF<br>LMF<br>RMF |
|-------------------------------------|---------|---------|---------|---------|---------|---------|--------------------------|
| Gabor Bank                          | 0.81%   | 0.60%   | 0.45%   | 0.90%   | 0.71%   | 0.32%   | 0.01%                    |
| LPQ                                 | 2.83%   | 2.63%   | 1.69%   | 2.24%   | 2.41%   | 2.23%   | 0.59%                    |
| HOG                                 | 3.03%   | 2.04%   | 1.92%   | 3.03%   | 3.24%   | 2.55%   | 0.19%                    |

TABLE 3.10 – Comparaison l'EER de 3 descripteurs pour le système multimodale

- Les tableaux (3.7) et (3.9) montrent les taux de reconnaissance (ROR) alors que les tableaux (3.8) et (3.10) montrent le taux d'égale erreur (EER) obtenus par chaque descripteur dans un système unimodal et multimodal.
- D'après les résultats des tableaux ci-dessus, on constate que le filtre Gabor Bank fournit les meilleurs taux de reconnaissance et offre aussi un taux d'égale erreur (EER) plus faible par rapport aux autres descripteurs dans le système unimodale et multimodal.
- Les descripteurs HOG et LPQ donnent presque les mêmes résultats avec une légère différence en mode monomodal et en mode multimodal.
- Sur la base des résultats expérimentaux présentés dans les tableaux et la courbe ROC et CMC présentées dans les figures (3.17) et (3.18) respectivement, on peut voir que l'algorithme du filtre de Gabor Bank atteint le meilleur taux de reconnaissance avec un minimum taux d'égale erreur (EER) dans un système multimodal par rapport au même algorithme dans un système monomodal, également pour les autres descripteurs HOG et LPQ, les meilleurs résultats ont été obtenus dans un système multimodal.
- On peut conclure que le système multimodal de toutes les modalités (LIF, LMF, RIF et RMF) avec Gabor Bank est le meilleur par rapport aux autres systèmes proposés.

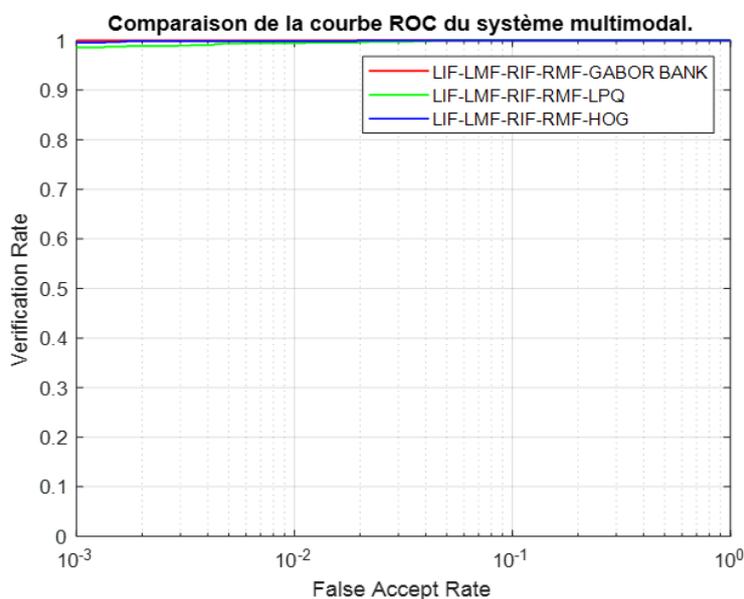


FIGURE 3.17 – Comparaison ROC entre les 3 descripteurs dans un système multimodal.

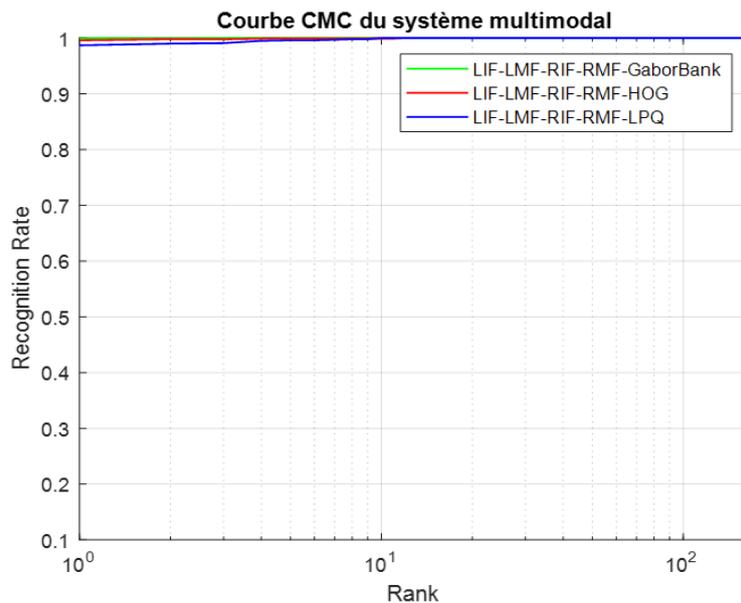


FIGURE 3.18 – Comparaison CMC entre les 3 descripteurs dans un système multimodal.

#### ■ Comparaison des ROR avec certains travaux dans la littérature :

La comparaison de ROR (%) de notre système multimodal avec ROR des autres systèmes présentés dans la littérature est portée dans le tableau ci dessous (3.11).

Les résultats expérimentaux obtenues démontrent que la méthode proposés basée sur l'algorithme Gabor Bank a aboutit un résultat meilleur à l'exception de la méthode donnée dans [83].

| Méthodes                             | Combinaison     | ROR [%]       |
|--------------------------------------|-----------------|---------------|
| <b>DFB + LDA + Norm [84].</b>        | LMF-LIF         | 95.55%        |
| <b>DFB + LDA + Norm [84].</b>        | LMF+LIF+RMF+RIF | 99.29%        |
| <b>Encoding LBP [83].</b>            | LMF-LIF         | 99.09%        |
| <b>Encoding LBP [83].</b>            | LMF+LIF+RMF+RIF | 100%          |
| <b>Intensity + Gabor [85].</b>       | LMF-LIF         | 95.56%        |
| <b>Intensity + Gabor [85].</b>       | LMF+LIF+RMF+RIF | 96.56%        |
| <b>Gabor + PCA + LDA [55].</b>       | LMF-LIF         | 92.12%        |
| <b>Gabor + PCA + LDA [55].</b>       | LMF+LIF+RMF+RIF | 98.79%        |
| <b>Méthode proposée (Gabor Bank)</b> | LMF-LIF         | <b>98.28%</b> |
| <b>Méthode proposée (Gabor Bank)</b> | LMF+LIF+RMF+RIF | <b>99.89%</b> |

TABLE 3.11 – Comparaison des ROR avec certains travaux dans la littérature.

## 3.5 Interface :

### 3.5.1 Description de l'interface :

Notre interface de reconnaissance des empreintes d'articulation des doigts sous Matlab est un système interactif conçu pour identifier les individus en utilisant les caractéristiques uniques de leurs empreintes digitales articulaires. Elle repose sur des algorithmes avancés de traitement d'images et de reconnaissance de motifs pour extraire les caractéristiques des empreintes d'articulation des doigts et les comparer aux empreintes enregistrées dans la base de données.

Les utilisateurs peuvent interagir avec le système en utilisant des boutons et des zones de texte pour effectuer des actions sur des images telles que la rotation, le niveau de gris, changement des dimensions, la comparaison des empreintes, et l'affichage des résultats.

L'interface contient des :

**Boutons :** Pour télécharger l'image, les rotations, identification, mettre l'image au niveau de gris, changer la taille, un bouton pour annuler les modifications apportées et un autre pour effacer tout.

**Sliders :** Un pour le changement de luminosité et l'autre permet d'augmenter le contraste.

**Zone des textes :** Pour entrer des paramètres ou bien pour afficher des messages aux utilisateurs.

### 3.5.2 Objectif de l'interface :

Les objectifs de notre interface sont les suivants :

1. Facilité d'utilisation : L'interface vise à offrir une expérience intuitive aux utilisateurs, en réduisant la complexité de l'utilisation du système. Les fonctionnalités sont accessibles de manière claire et les actions sont faciles à comprendre et à exécuter.
2. Faciliter la navigation : L'interface est conçue de manière à ce que les utilisateurs puissent naviguer facilement entre les différentes fonctionnalités et les étapes du processus de reconnaissance des empreintes d'articulation. Les sliders et les boutons sont organisés de manière logique.
3. Informations claires et concises : L'interface fournit des informations pertinentes aux utilisateurs de manière claire et concise. Les messages d'instructions, les résultats de la reconnaissance et les indicateurs d'état sont présentés de manière compréhensible.

4. Contrôle des paramètres : L'interface offre aux utilisateurs la possibilité de régler certains paramètres du système, tels que la taille, le niveau de gris ou la résolution de l'image.
5. Temps de réponse : L'interface est optimisée pour offrir une réactivité rapide et des temps de réponse courts. Cela permet aux utilisateurs d'interagir avec le système de manière fluide et sans délai perceptible.

### 3.5.3 Utilisation de l'interface :

#### ■ Guide d'utilisation :

La figure (3.19) montre l'interface d'utilisateur est les différents composants (les boutons, les sliders ...), et pour aider les utilisateurs à tirer le meilleur parti des fonctionnalités de l'application, voici la description de certains composants couramment utilisés :

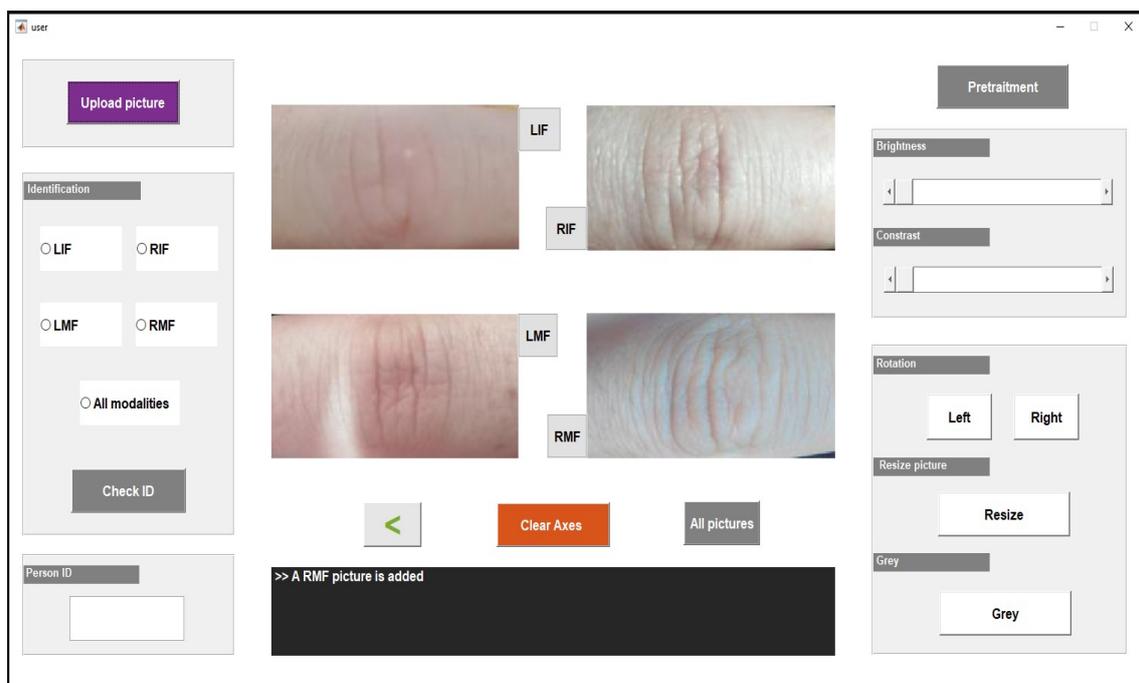


FIGURE 3.19 – Interface d'utilisateur

- **Boutons** : Les boutons sont des éléments interactifs permettant aux utilisateurs d'effectuer différentes actions. Voici une explication comment chaque bouton est utilisé dans l'application :
  - Bouton "Upload picture" : Permet aux utilisateurs de sélectionner une image d'empreinte digitale à analyser.

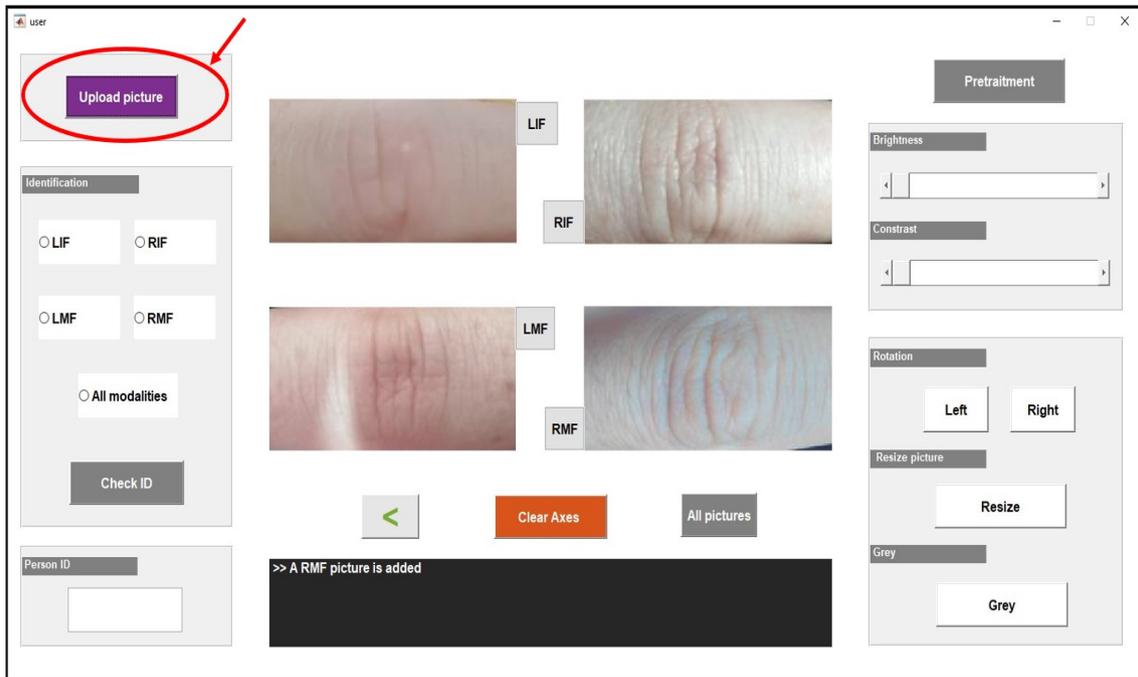


FIGURE 3.20 – Bouton charger image

- Bouton "Check ID" : Lance le processus de reconnaissance des empreintes d'articulation des doigts.

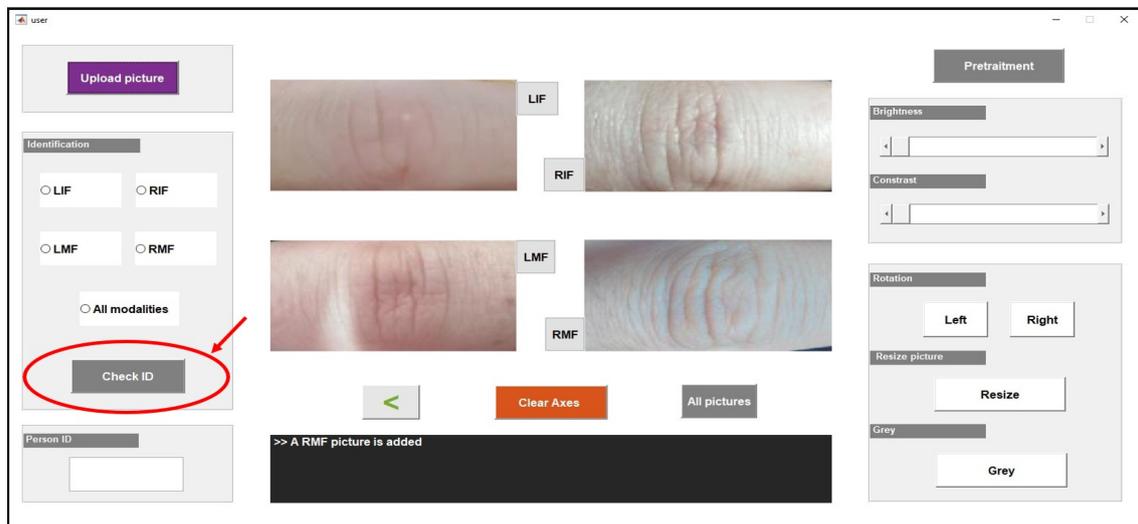


FIGURE 3.21 – Bouton identification

- Bouton "Clear Axes" : Réinitialise l'interface en supprimant les résultats précédents et en initialisant les paramètres.

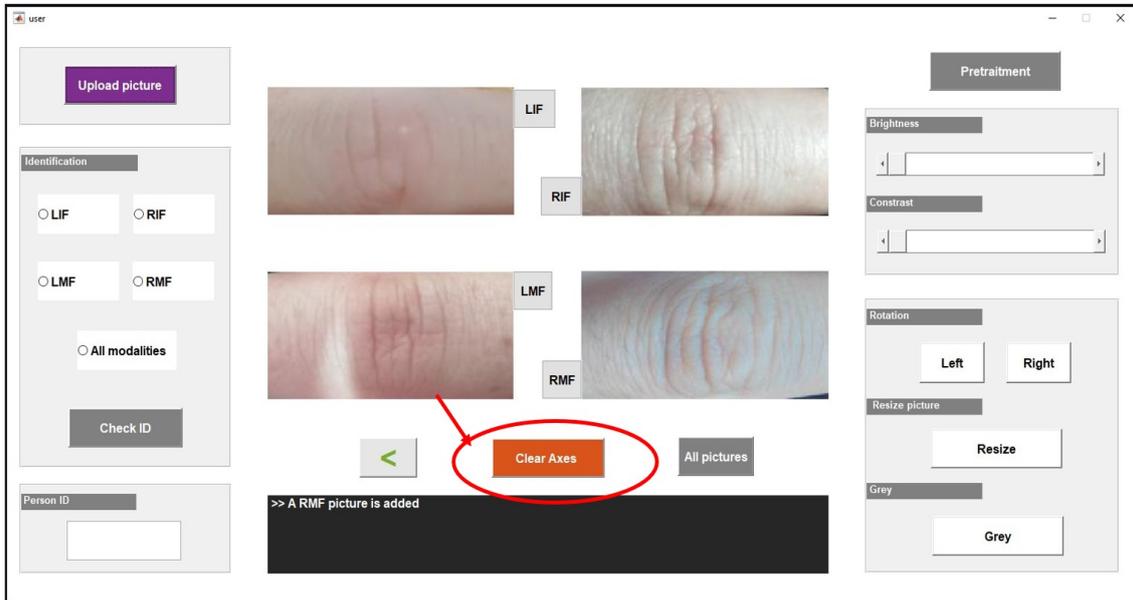


FIGURE 3.22 – Bouton effacer tout

- Des Boutons pour la sélection des images soit une par une ou bien à la fois en cliquant sur "All pictures".



FIGURE 3.23 – Buttons de sélection

- Boutons "Left" et "Right" : permettent de faire la rotation de 90 degrés gauche et droite.
- Bouton "Grey" : dans le prétraitement il est nécessaire de convertir l'image en niveau de gris, le bouton Grey prend en charge de cette tâche.

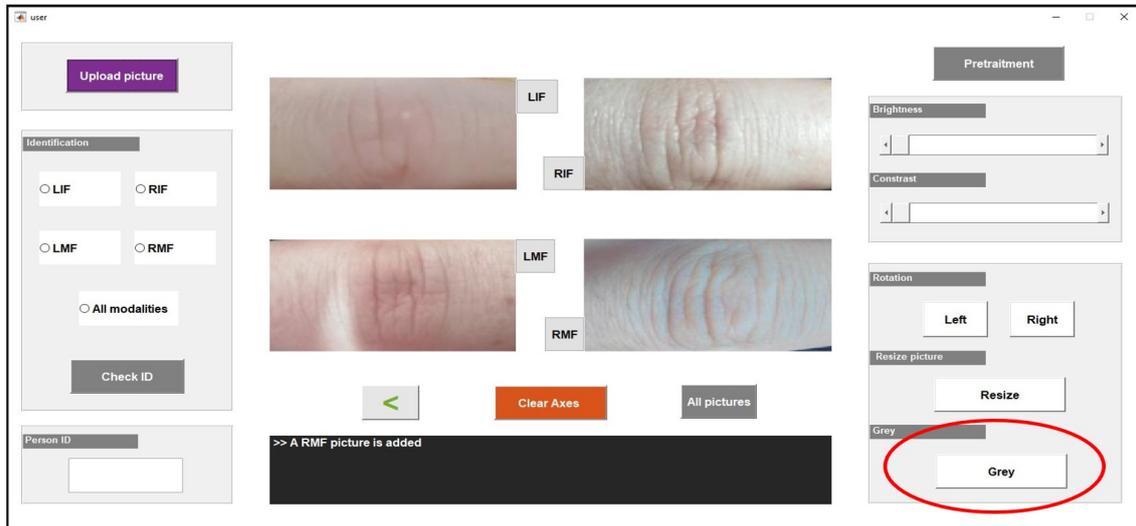


FIGURE 3.24 – Bouton de niveau gris

- Bouton "Resize" : rendre l'image en 220 pixels en largeur et 110 pixels en hauteur.

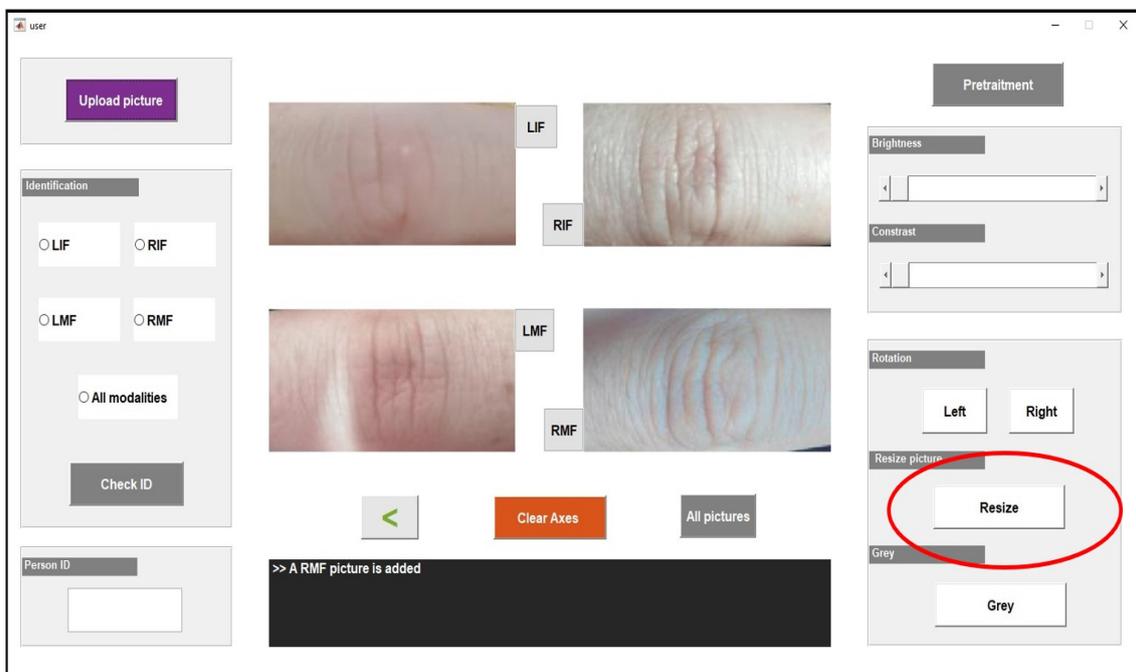


FIGURE 3.25 – Bouton Redimensionnement

- **Sliders** : Les sliders sont des contrôles permettant aux utilisateurs de régler des paramètres spécifiques. La description de la fonction de chaque slider est comme la suivante :
  - Slider "Brightness" : Permet aux utilisateurs d'ajuster la luminosité de l'image.



FIGURE 3.26 – Slider de luminosité (Brightness)

- Slider "Contrast" : Permet aux utilisateurs de définir et modifier le contraste de l'image entrée.

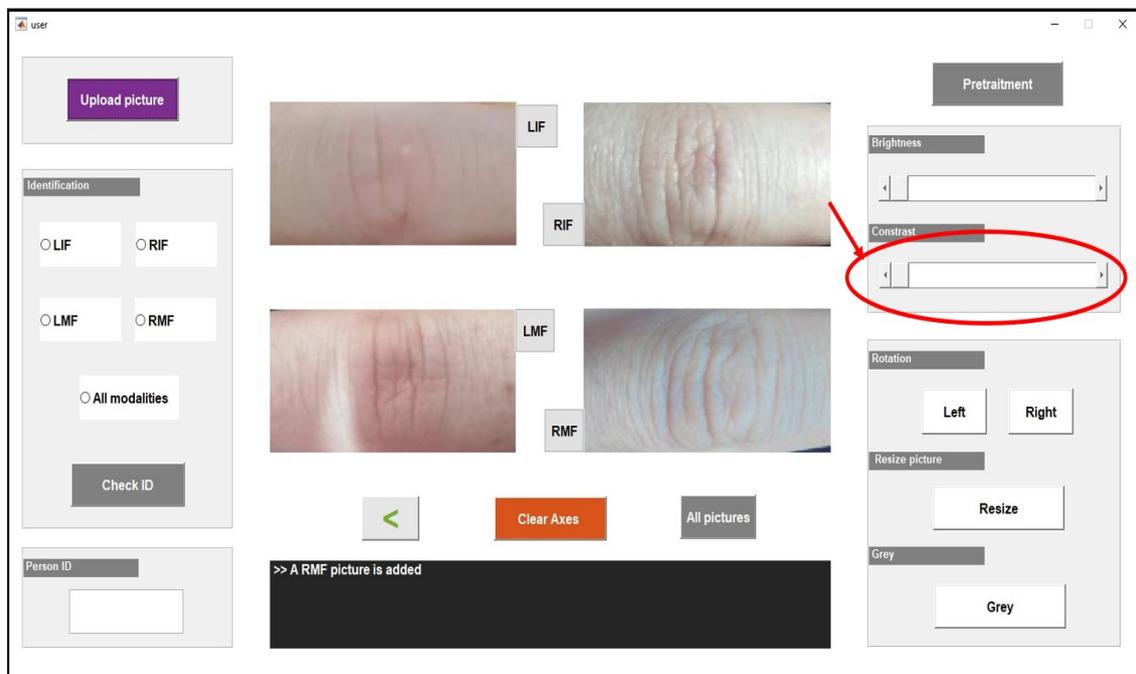


FIGURE 3.27 – Slider de contraste

- **Zone d'affichage** : L'axe d'affichage est l'espace où les images, et les résultats graphiques sont affichés. L'axe est utilisé pour présenter les images d'empreintes, à chaque traitement et visualiser les données pertinentes.
- **Zone de texte** : il y a deux types des zones de texte :
  - **Texte statique** : Les textes statiques sont des éléments utilisés pour afficher des informations importantes aux utilisateurs comme des messages tels que les messages d'erreurs et les suggestions.



FIGURE 3.28 – Zone des messages

- **Edit texte** : est utilisé pour montrer le résultat de l'identification et afficher le ID de la personne.

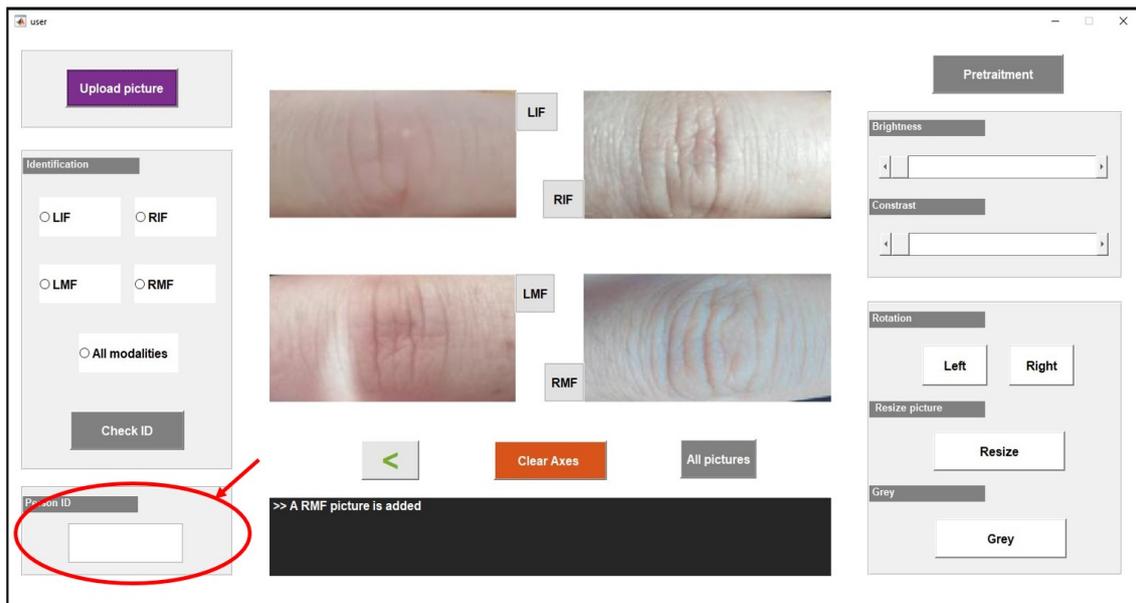


FIGURE 3.29 – Zone de résultat

Ce guide a pour objectif d'aider les utilisateurs à comprendre et à exploiter pleinement les fonctionnalités de notre interface. Pour faciliter leur expérience, nous présenterons un schéma d'utilisation qu'il guidera à travers les différentes étapes pour effectuer la reconnaissance des empreintes d'articulation des doigts.

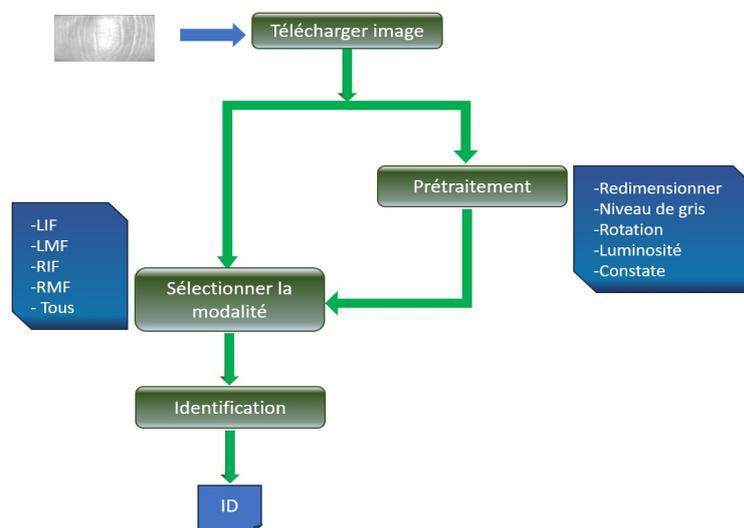


FIGURE 3.30 – Schéma d'utilisation de l'interface

Le processus d'identification multimodale de l'interface de reconnaissance des empreintes d'articulation des doigts repose sur un schéma. Tout d'abord, si l'image téléchargé est prétraitée alors il est possible de passer directement à l'identification en appuyant sur le bouton " Check ID" après avoir sélectionné la modalité

correspond à l'image. Cela permet une identification rapide et efficace sans nécessiter de prétraitements supplémentaires.

Dans le cas où l'image n'est pas prétraitée il est nécessaire d'effectuer certaines étapes de prétraitement tel que le redimensionnement, mettre l'image en niveau de gris et la rotation, le changement de la luminosité et de contraste, l'utilisateur a la possibilité d'effectuer ces prétraitements manuellement en utilisant les commandes fournies ou de les réaliser automatiquement en appuyant sur le bouton "Prétraitement".

Après avoir cliquer sur le bouton " Check ID", à ce stade, le système fait appel au modèle correspond à la modalité pour identifier la personne. Le numéro identificateur de la personne sera affiché dans la zone de texte dédiée.

La figure suivante résume les étapes d'utilisation de l'interface et tester le modèle que nous avons proposé

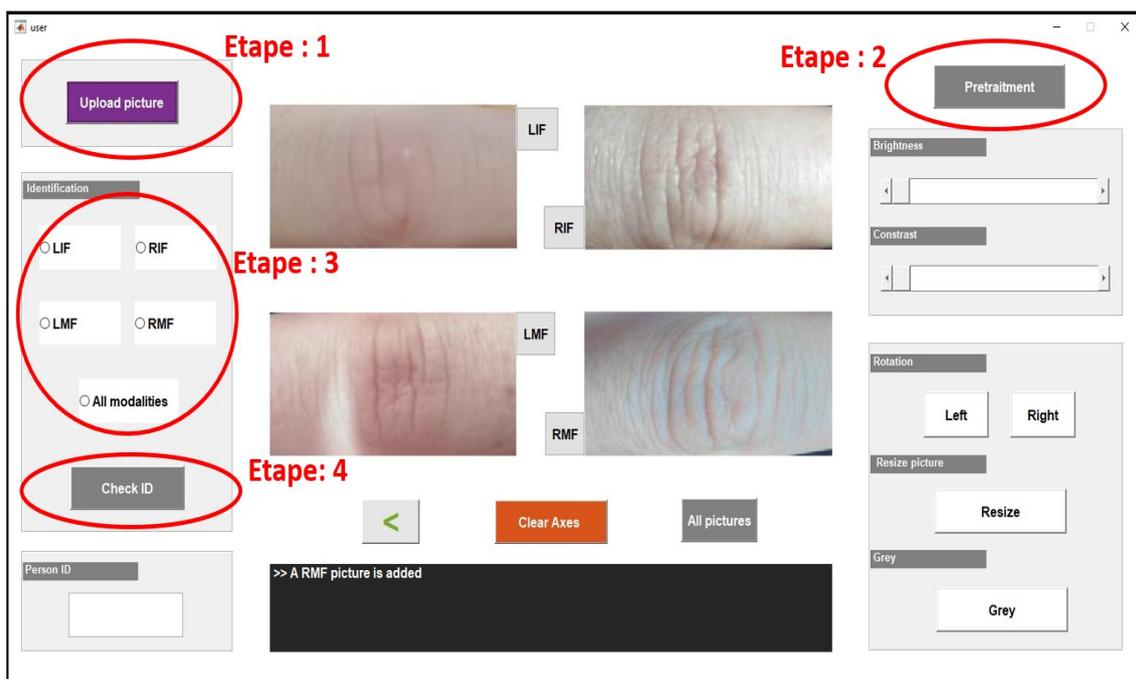


FIGURE 3.31 – Les étapes d'utilisation de l'interface

Lorsqu'un utilisateur télécharge une image pour effectuer l'identification après avoir choisi la modalité correspondant à l'image téléchargée, le système fait appel au modèle approprié parmi les 5 modèles créés. Par exemple, si un utilisateur entre une image de l'index du doigt droit (RIF), le système comparera cette image avec le modèle RIF créé. La même procédure est appliquée pour toutes les modalités, y compris les quatre images simultanément. Le schéma suivant montre le fonctionnement du système.

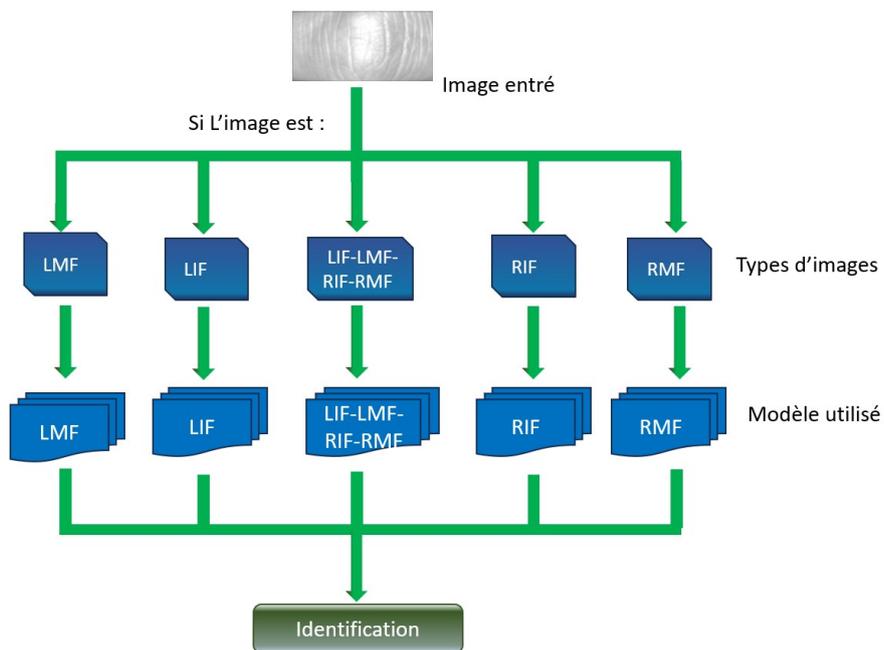


FIGURE 3.32 – Le fonctionnement de l'interface

### 3.5.4 Les avantages et les limites de l'interface :

- **Avantages :** L'interface présente plusieurs avantages significatifs, tel que la sécurité car l'utilisation des empreintes d'articulation des doigts comme modalité biométrique offre un niveau élevé de sécurité. Ces empreintes sont uniques à chaque individu, ce qui rend difficile leur reproduction ou leur falsification. Aussi la précision du modèle offre une identification fiable et rapide. De plus la simplicité de l'interface d'utilisateur rend l'utilisation facile pour les utilisateurs non techniques.
- **Limitations :** Malgré les avantages et les performances prometteuses de l'application certaines limitations doivent être prises en compte, les limitations liées à la qualité des images, les images de mauvaise qualité peuvent affecter l'exactitude de l'identification.

Une autre limitation réside dans l'incapacité de l'interface à extraire la région d'intérêt (FKP) des images entrées.

Enfin, elle est limitée à la reconnaissance des empreintes d'articulation des doigts et ne peut pas être utilisée pour d'autres modalités biométriques. Cela signifie qu'elle ne peut pas être utilisée pour la reconnaissance d'autres parties du corps, telles que le visage ou la voix.

## 3.6 Conclusion

Dans ce chapitre, nous avons présenté la méthode FKP et discuter ses résultats expérimentaux. Nos expérimentations ont révélé que notre système multimodal surpassait le système monomodal en termes de performances. Notamment, nous avons observé que l'algorithme de filtrage Gabor Bank présentait les meilleures performances parmi tous les algorithmes testés. Ces résultats expérimentaux confirment la valeur ajoutée de la multimodalité dans un système biométrique.

De plus, nous avons mis en place une interface permettant de tester notre système. Cette interface offre aux utilisateurs la possibilité de soumettre différentes modalités des empreintes d'articulation des doigts. En conclusion, quelle que soit l'algorithme ou la méthode utilisée dans un système biométrique, l'utilisation de la multimodalité s'avère plus avantageuse que l'utilisation d'un système monomodal.

# Conclusion générale

Dans ce mémoire nous nous sommes intéressés au système biométrique multimodal dans le but d'améliorer la reconnaissance des individus. À travers une revue de la littérature et une analyse approfondie dans le premier et le deuxième chapitres, nous avons examiné les principes fondamentaux de la biométrie, les différentes techniques de reconnaissance des formes et les méthodes utilisées dans la mise en œuvre de systèmes biométriques.

Nous avons constaté que la biométrie, en particulier la reconnaissance des empreintes d'articulation des doigts, présente un potentiel prometteur pour l'identification et la vérification des individus. Cette approche offre des avantages significatifs tels qu'une précision élevée, une résistance aux fraudes et une facilité d'utilisation. Les systèmes biométriques basés sur les empreintes d'articulation des doigts ont été largement adoptés dans divers domaines. L'objectif de notre mémoire est de développer un système multimodal pour l'identification des personnes en fusionnant plusieurs modalités FKP au niveau d'extraction des caractéristiques.

Dans le cadre de ce travail, nous avons rencontré un certain nombre d'options et de pistes afin d'arriver à l'objectif.

Le troisième chapitre montre le chemin, les expériences, les expérimentations et les choix faits durant la création et la conception de notre solution proposée. Enfin les résultats obtenus confirment que le modèle créé est vraiment performant et que l'interface va faire une reconnaissance et une identification multimodale fiable et répondre aux besoins de l'utilisateur.

Nous espérons que cette étude servira de base solide pour de futures recherches et développements dans le domaine de la reconnaissance des empreintes d'articulation des doigts,

et qu'elle contribuera à l'avancement de la technologie et à l'amélioration de la sécurité et de l'identification des individus.

# Bibliographie

- [1] Ichallalene Katia and Amara Fatma. *Développement d'un système biométrique pour la reconnaissance de visages basé sur l'approche LBP, ses variantes et un réseau neuronal*. PhD thesis, Université Mouloud Mammeri, 2019.
- [2] Zalix Biométrie. Zalix biométrie - veinaccess - système de contrôle d'accès biométrique- réseau veineux. <https://www.dailymotion.com/video/ximdk5>, 2011. Dernier accée le 01/2023.
- [3] Winston Maxwell et David Bounie. Pour la reconnaissance faciale à distance ou locale, les enjeux éthiques ne sont pas les mêmes. <https://www.telecom-paris.fr/reconnaissance-faciale-distance-locale-enjeux-ethiques>, mars 2020. Dernier accée le 02/2023.
- [4] DANIEL ICHBIAH. <https://www.futura-sciences.com/tech/dossiers/technologie-tendances-biometrie-965/page/2/>. <https://www.futura-sciences.com/tech/dossiers/technologie-tendances-biometrie-965/page/2/>, Avril 2012. Dernier accée le 01/2023.
- [5] Pauline Gravel. La biométrie, un outil fiable mais vulnérable. <https://www.ledevoir.com/societe/184557/la-biometrie-un-outil-fiable-mais-vulnérable>, avril 2008. Dernier accée le 01/02/2023.
- [6] Didier Guillerm. Rétine. <https://www.biometrie-online.net/technologies/retine>, 1990-2023. Dernier accée le 01/02/2023.
- [7] Julian Ashbourn. *Guide to Biometrics for Large-Scale Systems*, volume 8. Springer, 2011.

- 
- [8] Davide Maltoni, Dario Maio, Anil K Jain, Salil Prabhakar, et al. *Handbook of fingerprint recognition*, volume 2. Springer, 2009.
- [9] Ruud M Bolle, Jonathan H Connell, Sharath Pankanti, Nalini K Ratha, and Andrew W Senior. *Guide to biometrics*. Springer Science & Business Media, 2013.
- [10] HEC MONTREAL. La reconnaissance vocale : Une technologie qui résonne À travers le marketing numérique. <https://digital.hec.ca/blog/la-reconnaissance-vocale-en-plein-essor/>, Mars 2022. Dernier accée le 03/02/2023.
- [11] Djallal Rafik HAMMOU. *Optimisation des bases de données des applications de la reconnaissance biométrique*. PhD thesis, Université Mustapha Stambouli de Mascara, Département Infor.
- [12] Souhila Guerfi. *Authentification d'individus par reconnaissance de caractéristiques biométriques liées aux visages 2D/3D*. PhD thesis, Université d'Evry-Val d'Essonne, 2008.
- [13] Pim Tuyls and Jasper Goseling. Capacity and examples of template-protecting biometric authentication systems. In *Biometric Authentication : ECCV 2004 International Workshop, BioAW 2004, Prague, Czech Republic, May 15th, 2004. Proceedings*, pages 158–170. Springer, 2004.
- [14] Rohit Kundu. Matrice de confusion : comment l'utiliser et interpréter les résultats. <https://www.v7labs.com/blog/confusion-matrix-guide>, septembre 2022. Dernier accée le 04/2023.
- [15] Jean Gebarowski. Le doigt dans l'œil de la biométrie. <https://www.nextinpact.com/article/68790/le-doigt-dans-lil-biometrie>, 2022. Dernier accée le 02/2023.
- [16] Andrey MURHULA. Technique de detection et verification par reconnaissance des empreintes digitales. [https://www.memoireonline.com/03/15/8967/m\\_Conception-et-mise-en-place-dune-plateforme-de-securisation-par-synthese-et-reconnaissance-biom10.html](https://www.memoireonline.com/03/15/8967/m_Conception-et-mise-en-place-dune-plateforme-de-securisation-par-synthese-et-reconnaissance-biom10.html), 2015. Dernier accée le 06/03/2023.

- 
- [17] Lorène Allano. *La Biométrie multimodale : stratégies de fusion de scores et mesures de dépendance appliquées aux bases de personnes virtuelles*. PhD thesis, Evry, Institut national des télécommunications, 2009.
- [18] Abdallah Meraoumia. *Modèle de Markov caché appliqué à la multi-biométrie*. PhD thesis, Université des sciences et de la technologie Houari Boumediè, 2014.
- [19] Didier Guillerm. Le marché de la biométrie. <https://www.biometrie-online.net/biometrie/le-marche>, 2023. Dernier accée le 04/2023.
- [20] Mr Brahim FAROU. Multimédia mining reconnaissance des formes dans une vidéo. *Université Badji Mokhtar-Annaba*, 1945.
- [21] Shichang Du, Changping Liu, and Delin Huang. A shearlet-based separation method of 3d engineering surface using high definition metrology. *Precision Engineering*, 40 :55–73, 2015.
- [22] MOHAMED NAOUAI. Filtrage d’image. <https://slideplayer.fr/slide/1153263/>, 2009. Dernier accée le 04/03/2023.
- [23] Lionel Augé. médian marginal. <http://vokvince.free.fr/IMAC/TS/marginal.html>, 2011. Dernier accée le 04/03/2023.
- [24] Neha Patil. Bilateral filter. <https://alchetron.com/Bilateral-filter>, 2022. Dernier accée le 03/2023.
- [25] Stephen M Pizer, E Philip Amburn, John D Austin, Robert Cromartie, Ari Geselowitz, Trey Greer, Bart ter Haar Romeny, John B Zimmerman, and Karel Zuiderveld. Adaptive histogram equalization and its variations. *Computer vision, graphics, and image processing*, 39(3) :355–368, 1987.
- [26] JN Kapoor, MP Singh, and AK Misra. A comparative study of image enhancement techniques. In *Proceedings of the 2014 International Conference on Advances in Computing, Communications and Informatics*, pages 1902–1906. ACM, 2014.
- [27] Lijun Ding and Ardeshir Goshtasby. On the canny edge detector. *Pattern recognition*, 34(3) :721–725, 2001.

- 
- [28] Dennis Gabor. Theory of communication. part 1 : The analysis of information. *Journal of the Institution of Electrical Engineers-part III : radio and communication engineering*, 93(26) :429–441, 1946.
- [29] Peter J Burt. *The pyramid as a structure for efficient computation*. Springer, 1984.
- [30] Navneet Dalal and Bill Triggs. Histograms of oriented gradients for human detection. In *2005 IEEE computer society conference on computer vision and pattern recognition (CVPR'05)*, volume 1, pages 886–893. Ieee, 2005.
- [31] Luca Ghiani, Gian Luca Marcialis, and Fabio Roli. Fingerprint liveness detection by local phase quantization. In *Proceedings of the 21st international conference on pattern recognition (ICPR2012)*, pages 537–540. IEEE, 2012.
- [32] Nadia Belaidi. L'apprentissage supervisé : définition et exemples. <https://blent.ai/blog/a/apprentissage-supervise-definition>, Avril 2022. Dernier accée le 07/03/2023.
- [33] Horace B Barlow. Unsupervised learning. *Neural computation*, 1(3) :295–311, 1989.
- [34] David Silver, Thomas Hubert, Julian Schrittwieser, Ioannis Antonoglou, Matthew Lai, Arthur Guez, Marc Lanctot, Laurent Sifre, Dhharshan Kumaran, Thore Graepel, et al. A general reinforcement learning algorithm that masters chess, shogi, and go through self-play. *Science*, 362(6419) :1140–1144, 2018.
- [35] Anis Chaari. *Nouvelle approche d'identification dans les bases de données biométriques basée sur une classification non supervisée*. PhD thesis, Université d'Evry-Val d'Essonne, 2009.
- [36] Max Chassé. La biométrie au québec : Les enjeux. *Commission d'accès à l'information au Québec*, 2002.
- [37] Jean-Luc Dugelay and Antitza Dantcheva. L'Histoire de la Biométrie. CAFE TECHNO, doctorante EURECOM de 2008 à 2011, 2011. Accessed on May 5, 2023.
- [38] Peter Gregory and Michael A Simon. *Biometrics for dummies*. John Wiley & Sons, 2008.
- [39] hossine. Iso. <https://www.iso.org/>, 2015. Dernier accée le 18 février 2023.

- [40] Commissariat à la protection de la vie privée du Canada. Des données au bout des doigts : La biométrie et les défis qu'elle pose à la protection de la vie privée. [https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/renseignements-sur-la-sante-renseignements-genetiques-et-autres-renseignements-sur-le-corps/gd\\_bio\\_201102/](https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/renseignements-sur-la-sante-renseignements-genetiques-et-autres-renseignements-sur-le-corps/gd_bio_201102/), Février 2011. Dernière accéle 29/01/2023.
- [41] Anil Jain, Ruud Bolle, and Sharath Pankanti. *Biometrics : personal identification in networked society*, volume 479. Springer Science & Business Media, 1999.
- [42] Talib Hichem Betaouaf. Caractérisation de la rétine pour la reconnaissance biométrique des personnes. 2011.
- [43] RABi HALIMI and Amel SEDDIKI. *Système Biométrique pour la Reconnaissance des Articulations des Doigts et la Méthode de Quantification de phase Local*. PhD thesis.
- [44] Anil K Jain, Arun Ross, and Salil Prabhakar. An introduction to biometric recognition. *IEEE Transactions on circuits and systems for video technology*, 14(1) :4–20, 2004.
- [45] David Zhang. *Automated biometrics : technologies and systems*. Springer Science & Business Media, 2000.
- [46] Karthik Nandakumar, Anil K Jain, and Arun Ross. Fusion in multibiometric identification systems : What about the missing data ? In *Advances in Biometrics : Third International Conference, ICB 2009, Alghero, Italy, June 2-5, 2009. Proceedings 3*, pages 743–752. Springer, 2009.
- [47] Zhenan Sun, Alessandra A Paulino, Jianjiang Feng, Zhenhua Chai, Tieniu Tan, and Anil K Jain. A study of multibiometric traits of identical twins. In *Biometric technology for human identification Vii*, volume 7667, pages 283–294. SPIE, 2010.
- [48] Bastien L. Confusion matrix : l'outil de mesure de performances du machine learning. <https://www.lebigdata.fr/confusion-matrix-definition>, 10 décembre 2018. Dernière accéle 05/05/2023.
- [49] Damon L Woodard and Patrick J Flynn. Finger surface as a biometric identifier. *Computer vision and image understanding*, 100(3) :357–384, 2005.

- [50] Ch Ravikanth and Ajay Kumar. Biometric authentication using finger-back surface. In *2007 IEEE Conference on Computer Vision and Pattern Recognition*, pages 1–6. IEEE, 2007.
- [51] Lin Zhang, Lei Zhang, and David Zhang. Finger-knuckle-print : a new biometric identifier. In *2009 16th IEEE international conference on image processing (ICIP)*, pages 1981–1984. IEEE, 2009.
- [52] A Morales, CM Travieso, MA Ferrer, and JB Alonso. Improved finger-knuckle-print authentication based on orientation enhancement. *Electronics Letters*, 47(6) :1, 2011.
- [53] Lin Zhang, Lei Zhang, David Zhang, and Hailong Zhu. Ensemble of local and global information for finger-knuckle-print recognition. *Pattern recognition*, 44(9) :1990–1998, 2011.
- [54] Lin Zhang, Lei Zhang, David Zhang, and Hailong Zhu. Online finger-knuckle-print verification for personal authentication. *Pattern recognition*, 43(7) :2560–2571, 2010.
- [55] Zahra S Shariatmadar and Karim Faez. A novel approach for finger-knuckle-print recognition based on gabor feature fusion. In *2011 4th International Congress on Image and Signal Processing*, volume 3, pages 1480–1484. IEEE, 2011.
- [56] Chetana Hegde, P Deepa Shenoy, KR Venugopal, and Lalit M Patnaik. Authentication using finger knuckle prints. *signal, image and video processing*, 7 :633–645, 2013.
- [57] Reda Adjoudj. *Reconnaissance des Formes*. ResearchGate, 2006.
- [58] George Nagy. Twenty years of document image analysis in pami. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 22(1) :38–62, 2000.
- [59] Michael D Abràmoff, Peter T Lavin, Michael Birch, Nishant Shah, and James C Folk. Pivotal trial of an autonomous ai-based diagnostic system for detection of diabetic retinopathy in primary care offices. *NPJ digital medicine*, 2(1) :39, 2019.
- [60] Konstantinos Makantasis, Anastasios Doulamis, Nikolaos Doulamis, and Antonios Nikitakis. Real-time multi-camera vehicle detection and tracking using deep learning and manifold clustering. *Expert Systems with Applications*, 131 :240–254, 2019.

- 
- [61] Ali Fathi, Hossein Mehranpour, Ehsan Mohammadi, and Payman Moallem. Automatic solar panel surface defects detection and classification using a multi-level pattern recognition framework. *Solar Energy*, 185 :235–246, 2019.
- [62] Linwei Fan, Fan Zhang, Hui Fan, and Caiming Zhang. Brief review of image denoising techniques. *Visual Computing for Industry, Biomedicine, and Art*, 2(1) :1–12, 2019.
- [63] Yves Usson. *Traitement d’images numériques en microscopie*, 2006.
- [64] Wilhelm Burger and Mark J Burge. *Digital image processing : an algorithmic introduction using Java*. Springer, 2016.
- [65] Isabelle Bloch, Y Gousseau, H Maître, D Matignon, B Pesquet-Popescu, F Schmitt, M Sigelle, and F Tupin. Le traitement des images. *Polycopié du cours ANIM, version*, 5 :12, 2004.
- [66] Metin Sezgin and Bülent Sankur. Survey over image thresholding techniques and quantitative performance evaluation. *Journal of Electronic Imaging*, 13(1) :146–165, 2004.
- [67] Nobuyuki Otsu. A threshold selection method from gray-level histograms. *IEEE Transactions on Systems, Man, and Cybernetics*, 9(1) :62–66, 1979.
- [68] Abderrahmane Kefali, Toufik Sari, and Mokhtar Sellami. Evaluation de plusieurs techniques de seuillage d’images de documents arabes anciens. In *5<sup>ème</sup> symposium international Images Multimédias Applications Graphiques et Environnements*, pages 123–134, 2009.
- [69] Derek Bradley and Greg Roth. Adaptive thresholding using the integral image. *Journal of graphics tools*, 12(2) :13–21, 2007.
- [70] Khairun Saddami, Khairul Munadi, Yuwaldi Away, and Fitri Arnia. Improvement of binarization performance using local otsu thresholding. *International Journal of Electrical & Computer Engineering (2088-8708)*, 9(1), 2019.
- [71] Chao Zhu. *Effective and efficient visual description based on local binary patterns and gradient distribution for object recognition*. PhD thesis, Ecully, Ecole centrale de Lyon, 2012.

- 
- [72] S. A. Kumar, A. R. Jayakumar, K. S. Jayaprakasam, and P. R. Gounder. A review of feature extraction techniques for image classification. *International Journal of Advanced Research in Computer Science and Software Engineering*, 5(9) :1072–1077, Sep 2015.
- [73] Amir Benzaoui, Abdenour Hadid, and Abdelhani Boukrouche. Ear biometric recognition using local texture descriptors. *Journal of electronic imaging*, 23(5) :053008–053008, 2014.
- [74] Amir Benzaoui, Insaf Adjabi, and Abdelhani Boukrouche. Experiments and improvements of ear recognition based on local texture descriptors. *Optical Engineering*, 56(4) :043109–043109, 2017.
- [75] Narimen Saad. *Reconnaissance tridimensionnelle de visage*. PhD thesis, université Mohamed Khider de Biskra, 2018.
- [76] Amitabh Wahi, F Mohamed Athiq, and C Palanisamy. A hybrid feature extraction method-based object recognition by neural network. In *2008 International Conference on Computing, Communication and Networking*, pages 1–5. IEEE, 2008.
- [77] Luis G. Serrano. *Grokking Machine Learning*. Manning Publications, 2019.
- [78] Laurent Candillier. *Contextualisation, visualisation et évaluation en apprentissage non supervisé*. PhD thesis, Université Charles de Gaulle-Lille III, 2006.
- [79] Christopher M Bishop and Nasser M Nasrabadi. *Pattern recognition and machine learning*, volume 4. Springer, 2006.
- [80] Patrenahalli M. Narendra and Keinosuke Fukunaga. A branch and bound algorithm for feature subset selection. *IEEE Transactions on computers*, 26(09) :917–922, 1977.
- [81] Anil K Jain, Robert P. W. Duin, and Jianchang Mao. Statistical pattern recognition : A review. *IEEE Transactions on pattern analysis and machine intelligence*, 22(1) :4–37, 2000.
- [82] Anil K Jain, Patrick Flynn, and Arun A Ross. *Handbook of biometrics*. Springer Science & Business Media, 2007.
- [83] Zahra S Shariatmadar and Karim Faez. Finger-knuckle-print recognition via encoding local-binary-pattern. *Journal of Circuits, Systems and Computers*, 22(06) :1350050, 2013.

- [84] Behnam Zeinali, Ahmad Ayatollahi, and Mohammad Kakooei. A novel method of applying directional filter bank (dfb) for finger-knuckle-print (fkp) recognition. In *2014 22nd Iranian conference on electrical engineering (ICEE)*, pages 500–504. IEEE, 2014.
- [85] Zahra S Shariatmadar and Karim Faez. An efficient method for finger-knuckle-print recognition by using the information fusion at different levels. In *2011 international conference on hand-based biometrics*, pages 1–6. IEEE, 2011.