UNIVERSITÉ KASDI MERBAH OUARGLA
Faculté des nouvelles technologies de l'information et de la communication
Département D'électronique

Mémoire de Master pour l'obtention
d'une Master Académique

Domaine : Science et Technologie

Filière : AUTOMATIQUE

Spécialité : AUTOMATIQUE ET SYSTÈM

Thème

Reconnaissance des personnes par 3D palmprint en utilisant LPQ

Réalisé par :

- DEKHIL Mohamed Lamine
- BENZAOUI Ilyas

Encadré par :

M. CHAA Mourad	M.C. A	Encadreur	Université de Ouargla
Mme. Nadia Dahraoui	M.C.B	President	Université de Ouargla
M. Rachid Chlaoua	M.C.B	Examinateur	Université de Ouargla

Année Universitaire : 2023 / 2022

Dédicace

Louange à Dieu, qui nous a accordé la force et la persévérance tout au long de mon parcours d'études.

Je remercie ma famille pour son soutien inconditionnel et ses sacrifices pour réaliser nos rêves.

Je remercie tous nos chers amis pour leur soutien illimité et leur encouragement constant à toutes les étapes.

Nous sommes très reconnaissants envers nos camarades d'études qui ont partagé avec nous des moments difficiles et agréables.

Je remercie le corps professoral et tous les membres du personnel qui ont contribué à fournir un environnement d'apprentissage stimulant et soutenant.

Nous exprimons notre gratitude aux entités qui ont contribué à fournir les ressources et les opportunités nécessaires pour réussir cette thèse.

Je remercie ma famille et mes proches pour leur patience et leur soutien tout au long de la période d'écriture de cette thèse.

Je suis profondément reconnaissant envers tous ceux qui ont contribué à mon parcours académique de différentes manières, et je n'oublierai jamais ces moments précieux.

Enfin, j'exprime ma profonde gratitude à tous ceux qui ont contribué au succès de cette thèse, et j'espère que mon travail aura été utile et contributif dans le domaine des études..

Remerciement

Nous tenons tout d'abord à exprimer notre gratitude envers Dieu, le Tout-Puissant, pour nous avoir donné la force, la patience et la volonté nécessaires pour mener à bien ce travail modeste. Nous souhaitons également remercier nos parents et nos familles pour leur contribution, leur soutien constant, leur patience et leurs encouragements.

Un grand merci à **Monsieur CHAA Mourad**, notre encadrant et enseignant au département d'électronique et de communication, pour son précieux accompagnement. Nous exprimons également notre reconnaissance envers les membres du jury d'avoir accepté d'évaluer et de juger ce travail.

Nous tenons à adresser nos remerciements à l'ensemble du corps professoral et administratif du département d'électronique de l'université **Kasdi Merbah de Ouargla** pour la qualité de leurs enseignements et leurs efforts considérables pour assurer une formation actualisée à leurs étudiants.

Nous voulons exprimer notre sincère reconnaissance à nos amis proches qui nous ont constamment encouragés tout au long de la réalisation de ce mémoire.

Enfin, nous souhaitons remercier chaleureusement toutes les personnes qui ont contribué de près ou de loin à la réalisation de ce travail.

Résumé :

L'utilisation croissante de la 3D palmprint en tant que solution biométrique pour l'identification et la vérification de l'identité des individus renforce la sécurité. Nous travaillons actuellement sur l'amélioration du système d'identification basé sur la 3D palmprint. Notre proposition repose sur l'utilisation du filtre TT(tan et triggs) pour le prétraitement des données, ainsi que sur les techniques d'extraction de caractéristiques telles que LPQ, BSIF et HOG. Enfin, la classification des vecteurs est effectuée à l'aide de l'algorithme KNN en utilisant différentes distances (euclidienne, cosinus, ctb, mahcos). Les résultats obtenus démontrent des performances très encourageantes, avec un taux de reconnaissance atteignant 99,95%.

Mots clés : : 3D **palmprint**, extraction des caractéristiques, biométrie, identification, vérification, KNN.

Abstract:

The increasing use of 3D palmprint as a biometric solution for individual identification and identity verification enhances security. We are currently working on improving the 3D palmprint-based identification system. Our proposal is based on using the TT filter for data preprocessing, as well as feature extraction techniques such as LPQ, BSIF, and HOG. Finally, vector classification is performed using the KNN algorithm with different distances (Euclidean, cosine, ctb, mahcos). The results obtained demonstrate highly promising performance, with a recognition rate reaching 99.95%.

Keywords: Palmprint, feature extraction, biometrics, identification, identity,KNN.

ملخص:

الاستخدام المتزايد لنظام بصمة اليد ثلاثي الأبعاد كحلاً بيومتريًا لتحديد وتأكيد هوية الأفراد يعزز الأمان. نحن حاليًا نعمل على تحسين نظام التحقق المبني على بصمة اليد ثلاثية الأبعاد. اقتراحنا يعتمد على استخدام مرشح TT لمعالجة البيانات، بالإضافة إلى تقنيات استخراج الميزات مثل LPQ وBSIF وHOG. وأخيرًا، يتم تصنيف الميزات باستخدام خوارزمية KNN باستخدام مسافات مختلفة (الأبعاد الاقليدية ، الكوسين، CTB، ماهكوس). أظهرت النتائج التي تم الحصول عليها أداءً مشجعًا للغاية، حيث بلغ معدل التعرف 99.95%.

الكلمات المفتاحية: بصمة الكف، استخراج الخصائص، البيو مترية، التحديد، الهوية

CHAPITRE I : SYSTEMES BIOMETRIQUES

Chapitre III : Mise en œuvre et Evaluation

Liste des figures

Liste des tableaux

Acronymes

BD : Base des données ("Data Base")

BSIF : ("Binarized Statistical Image Features")

CMC :(" Cumulative Match Characteristic")

DoG : ("Difference of Gaussians")

LPQ :(Local Phase Quantization)

EER : Taux d'erreurs égales ("Equal Error Rate")

FAR : Taux de Fausses Acceptations ("False Acceptance Rate")

FKP : Empreintes des articulations des doigts ("Finger-Knuckle-Print")

FRR : Le taux de Faux Rejets ("False Rejection Rate")

GAR : Taux des véritables clients ("Genuine Accept Rate ")

HOG : Histogrammes d'orientation de Gradient ("Histogram of Oriented Gradient")

KNN: K plus proches voisines ("k-nearest neighbors")

LBP : Motif binaire local ("Local Binary Patterns")

LDA : Analyse Discriminante Linéaire ("Linear Discriminate Analysis")

PCA : Analyse en composantes principales ("Principal Component Analysis")

ROC: Courbe représentant les taux d'erreur ("Receiver Operating Characteristic").

ROI: Région d'intérêt ("Region Of Interest")

SVM: Machine à vecteurs de support ("Support Vector Machine")

TER : La totale erreur rate ("Total Error Rate")

Introduction générale

La reconnaissance des individus a pris une importance croissante dans la vie quotidienne de l'homme. Elle garantit la sécurisation des transactions effectuées par les personnes dans divers domaines. Au cours des dernières années, l'utilisation des systèmes de reconnaissance était principalement limitée à des secteurs d'envergure tels que le secteur militaire, ainsi qu'à d'autres secteurs nécessitant de nombreuses applications, comme la protection de l'accès à un ordinateur, à un téléphone portable, à une clé USB, à des installations ou à des cartes bancaires.

De nombreuses technologies biométriques ont été développées, toutes basées sur des identifiants biométriques physiologiques et comportementaux tels que l'iris [1], la voix[2], les empreintes digitales[3], le visage[4], la signature, etc. Ces technologies sont considérées comme plus fiables que les systèmes classiques tels que les clés ou les mots de passe, car elles sont difficiles à falsifier. Elles permettent une reconnaissance précise et unique d'une personne en se basant sur des caractéristiques biométriques uniques à chaque individu. C'est la raison pour laquelle les systèmes biométriques connaissent actuellement une demande croissante. Dans le cas de la reconnaissance Palmprint, que ce soit dans des contextes civils, commerciaux ou courants, il s'agit essentiellement d'un processus de comparaison de deux images d'empreintes complètes de qualité contrôlée. La similarité entre le Palmprint et les empreintes digitales a incité les chercheurs à exploiter les concepts et les approches conçus pour la reconnaissance des empreintes digitales. Dans cette étude, nous avons choisi un système de reconnaissance basé sur le Palmprint. Ce système utilise la forme de la partie intérieure de la main pour extraire les caractéristiques biométriques permettant l'identification des individus. Ces caractéristiques sont permanentes et stables tout au long de la vie, et elles sont uniques pour chaque individu[5]. Le résumé mentionne l'utilisation croissante de la 3D palmprint en tant que solution biométrique pour l'identification et la vérification de l'identité des individus, ce qui renforce la sécurité. L'objectif actuel est d'améliorer le système d'identification basé sur la 3D palmprint en utilisant différentes techniques.

Le prétraitement des données est effectué à l'aide du filtre TT, qui permet de préparer les données pour une meilleure extraction des caractéristiques. Ensuite, les caractéristiques sont extraites en utilisant des techniques telles que LPQ (Local Phase Quantization), BSIF (Binarized Statistical Image Features), et HOG (Histogram of Oriented Gradients). Ces

techniques permettent d'extraire des informations spécifiques et discriminantes à partir des empreintes palmprint en 3D.

Pour la classification, l'algorithme KNN (k plus proches voisins) est utilisé. Il permet de classer les vecteurs d'empreintes palmprint en fonction de leur similarité. Différentes distances sont utilisées pour mesurer la similarité, notamment la distance euclidienne, la distance cosinus, la distance ctb (City Block) et la distance mahcos (Mahalanobis cosine).

Les résultats obtenus montrent des performances très encourageantes, avec un taux de reconnaissance atteignant 99,95%. Cela indique que le système d'identification basé sur la 3D palmprint, en utilisant les techniques mentionnées, est très précis et efficace dans la reconnaissance et la vérification de l'identité des individus.

Notre travail est divisé en trois chapitres distincts :

Le premier chapitre : Dans ce chapitre, nous avons défini le concept de biométrie ainsi que les caractéristiques et les modalités biométriques, qu'elles soient physiologiques ou comportementales. Nous avons également abordé les évaluations d'un système biométrique, en fournissant un aperçu des différentes méthodes utilisées pour évaluer les performances et la fiabilité d'un système biométrique.

Le deuxième chapitre : Dans ce chapitre, nous avons examiné l'état de l'art des méthodes d'extraction de caractéristiques pour la 3D Palmprint. Nous avons étudié les différentes approches et techniques utilisées pour extraire les caractéristiques uniques et discriminantes des empreintes Palmprint en 3D. Cela nous a permis de comprendre les méthodes existantes et les avancées récentes dans ce domaine.

Le troisième chapitre : Dans ce dernier chapitre, nous avons présenté en détail la méthode que nous avons utilisée pour représenter les empreintes Palmprint en 3D. Nous avons décrit les différentes étapes de notre méthode, y compris le prétraitement des données, l'extraction des caractéristiques à l'aide de techniques spécifiques telles que LPQ, BSIF et HOG, et enfin, la classification des vecteurs à l'aide de l'algorithme KNN avec différentes distances. Nous avons également présenté les expériences que nous avons menées dans le cadre de notre travail, en fournissant des résultats et une analyse détaillée.

I.1. Introduction

Ce chapitre consiste à un survol sur les différentes modalités biométriques de la main et l'architecture d'un système biométrique. Ceci est pour les deux modes authentification et identification. Également, quelques concepts et lexiques très utilisés dans le système biométrique ont été discutés.

I.2. La biométrie

La biométrie consiste à identifier une personne à partir de ses caractéristiques physiologiques ou comportementales uniques. Les caractéristiques physiologiques peuvent inclure l'iris, l'empreinte digitale, Palmprint, les empreintes des articulations des doigts, les géométries de la main et le visage, tandis que les caractéristiques comportementales incluent la voix, la signature et la démarche. On peut classer les modalités biométriques en deux catégories, à savoir physiologiques et comportementales **[6].**

I.3.Caractéristiques biométriques

Les caractéristiques biométriques par lesquelles il est possible de vérifier l'identité d'un individu sont appelées modalités biométriques. Ces modalités sont basées sur l'analyse des données liées à l'individu et sont généralement classées en deux catégories :

- ✓ Biométrie physiologiques
- ✓ Biométrie comportementale

Pratiquement, n'importe quelle caractéristique physiologiques ou comportementale peut être considérée comme une caractéristique biométrique , dans la mesure ou elle satisfait les propriétés suivantes :

- **Universalité :** Chaque personne doit avoir la caractéristique biométrique
- **Unicité :** toute deux personnes ne devraient pas avoir la même caractéristique.
- **La permanence :** La caractéristique biométrique ne doit pas changer avec le temps.
- **Collectabilité :** l'information doit être colletable et mesurable afin d'être utilisée pour

les comparaisons.

- **Protection contre la falsification :** la caractéristique doit être difficilement falsifiable afin d'éviter une utilisation frauduleuse du système[6].

I.4. Modalités biométriques

Les modalités biométriques sont des moyens de vérification de l'identité basés sur des caractéristiques physiologiques uniques d'une personne, telles que les empreintes digitales, la reconnaissance faciale, l'iris, la signature manuscrite, la reconnaissance vocale, etc. Les modalités biométriques sont souvent utilisées dans les systèmes de sécurité pour l'authentification de l'utilisateur**.[7]**

I.4.1 Les modalités physiologiques

Les modalités physiologiques sont des caractéristiques uniques d'une personne qui peuvent être utilisées pour identifier ou vérifier son identité. Elles incluent des caractéristiques telles que les empreintes digitales, la reconnaissance faciale, la reconnaissance irienne, la reconnaissance vocale, la signature manuscrite, etc. Les modalités physiologiques sont souvent utilisées dans les systèmes de sécurité pour assurer l'authentification de l'utilisateur :

I.4.1.1Empreint digitale

Les empreintes digitales sont des motifs uniques formés par les ridules et les creux sur la surface de la peau qui recouvre les doigts. Elles sont souvent utilisées comme modalité biométrique pour l'authentification d'une personne, car elles sont considérées comme stables et fiables. Les empreintes digitales sont capturées à l'aide d'un capteur et comparées à une base de données d'empreintes digitales enregistrées pour vérifier l'identité de la personne. Les empreintes digitales sont souvent utilisées dans les systèmes de sécurité pour les transactions financières, l'accès à des installations sensibles, etc. la figure 01 montre un exemple d'empreint digitale :

Figure 1: Empreint digitale[3]

Avantages

- Le coût est abordable.
- Le lecteur biométrique a une taille compacte.
- La configuration du système est simple.
- Il est facile à utiliser.

Inconvénients

- La participation de toutes les parties impliquées dans l'inscription peut être problématique si la maladie est de nature physique ou psychologique.

I.4.1.2Visage

La reconnaissance faciale est une modalité biométrique qui utilise des algorithmes pour comparer des caractéristiques uniques d'un visage à une image ou une vidéo enregistrée pour vérifier l'identité d'une personne. Les caractéristiques comparées incluent des éléments tels que la forme du visage, la distance entre les yeux, le nez, la bouche, etc.. La reconnaissance faciale peut être utilisée pour l'authentification en temps réel, par exemple pour déverrouiller un appareil mobile ou pour contrôler l'accès à un bâtiment. Elle est également utilisée dans les systèmes de surveillance et de reconnaissance d'images pour trouver des personnes recherchées ou pour surveiller les foules. Cependant, la reconnaissance faciale peut susciter des préoccupations en matière de vie privée et de protection des données. **La figure 02** présente un exemple de visage :

Figure 2 :Exemple deVisage

Avantages

- Cette technique est bien acceptée par le public.
- Son fonctionnement est simple et efficace.
- Elle est économique et peut utiliser l'équipement d'acquisition d'images existant.

Inconvénients

- Il est difficile de distinguer les vrais jumeaux.
- Les changements physiques peuvent induire en erreur le système.
- La technique est très sensible aux variations d'éclairage ou d'angle de l'appareil photo, etc.

I.4.1.3Iris

L'iris est la partie colorée de l'œil, entourant la pupille. La reconnaissance irienne est une modalité biométrique qui utilise des algorithmes pour capturer et analyser les caractéristiques uniques de l'iris d'une personne pour vérifier son identité. L'iris est considéré comme l'une des modalités les plus fiables pour l'identification biométrique, car il est difficile de falsifier ou de reproduire les caractéristiques de l'iris. La reconnaissance irienne est souvent utilisée pour les applications de sécurité à haut niveau, telles que l'accès à des installations sensibles ou à des systèmes de stockage de données confidentielles.

Figure 3 :Image de l’iris

Avantages

- Les vrais jumeaux sont facilement distinguables.
- Les caractéristiques de l'iris restent constantes tout au long de la vie.
- L'iris contient une grande quantité d'informations.

Inconvénients

- L'acquisition d'images nécessite une formation et une pratique spécifiques.
- - La fiabilité diminue à mesure que la distance entre l'œil et la caméra augmente.
- - Les individus ont des difficultés à accepter cette méthode de biométrie.

1.4.1.4 Empreintes des articulations des doigts (FKP) :

Les empreintes des articulations des doigts (Friction Ridge Pattern, FKP) sont les motifs uniques formés par les ridules et les creux sur la surface de la peau qui recouvre les jointures des doigts. Elles sont souvent considérées comme une modalité biométrique plus fiable que les e empreintes digitales traditionnelles, car elles sont plus difficiles à falsifier ou à reproduire. Les empreintes des articulations des doigts sont capturées à l'aide d'un capteur et comparées à une base de données d'empreintes des articulations des doigts enregistrées pour vérifier l'identité d'une personne. Les empreintes des articulations des doigts sont souvent utilisées dans les systèmes de sécurité pour les transactions financières, l'accès à des installations sensibles [8], etc. la figure 4 montre empreintes des articulations des doigts (FKP).

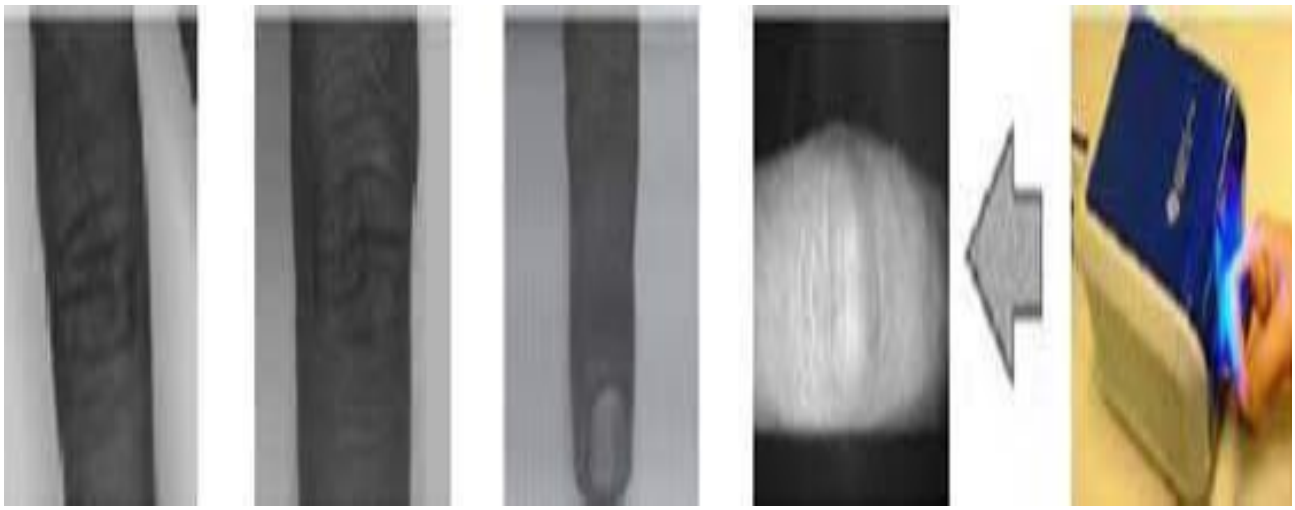

Figure 4: Empreintes des articulations des doigts (FKP)[8]

Avantages :

- Les FKP offrent une différenciation précise des individus en raison de la disposition unique des articulations des doigts.
- Les FKP sont relativement stables au fil du temps, ce qui signifie que les empreintes peuvent être utilisées pour l'identification à long terme.
- Les FKP sont moins susceptibles d'être altérées par des blessures ou des modifications physiques que d'autres caractéristiques biométriques, comme les empreintes digitales.
- Les FKP sont généralement bien acceptées par le public, car elles sont moins intrusives que certaines autres méthodes biométriques.

Inconvénients :

- L'acquisition précise des empreintes des articulations des doigts peut nécessiter des équipements et des techniques spécifiques, ce qui peut rendre le processus d'acquisition plus complexe que celui des empreintes digitales.
- Les FKP peuvent être sensibles à l'orientation de la main et des doigts lors de l'acquisition, ce qui peut rendre la capture d'empreintes cohérentes plus difficile.
- Les dispositifs d'acquisition des empreintes des articulations des doigts peuvent être coûteux, ce qui peut limiter leur adoption dans certaines applications.
- Les FKP peuvent nécessiter un échantillon plus grand pour une identification précise, ce qui peut ralentir le processus d'authentification dans certaines situations.

I.4.1.5 Palmprint:

Palmprint est un modèle unique formé par les lignes et les creux sur la surface de la paume de la main. Elle est souvent utilisée comme modalité biométrique pour vérifier l'identité d'une personne en comparant l'empreinte capturée à une base de données Palmprint enregistrées. La reconnaissance de Palmprint est considérée comme fiable, car elles sont difficiles à falsifier ou à reproduire. Palmprint sont souvent utilisées dans les systèmes de sécurité pour les transactions financières, l'accès à des installations sensibles [8], etc.la figure 5 montre palmprint :

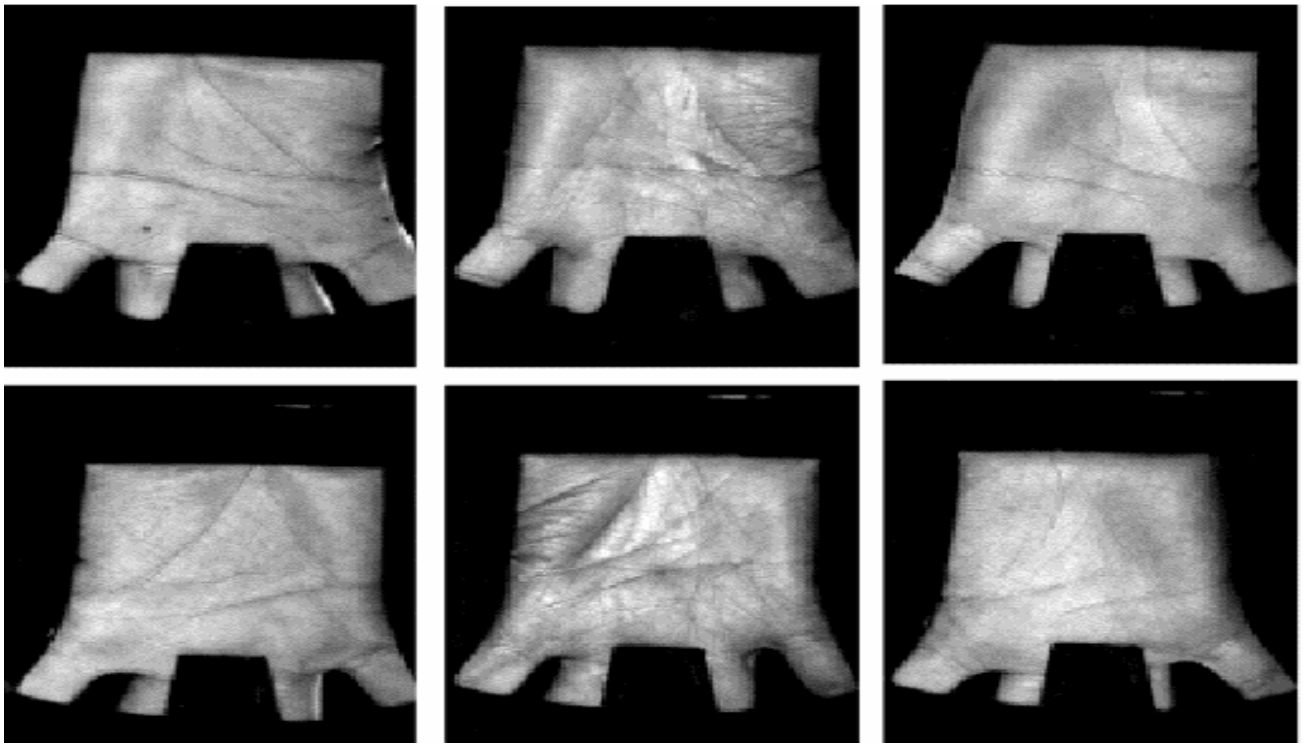

Figure 5 :exemple de Palmprint [8]

Avantages :

- Palmprint offrent une plus grande surface d'information que les empreintes digitales, ce qui permet de capturer plus de détails et de caractéristiques uniques.
- Palmprint sont généralement stables au fil du temps, ce qui permet une utilisation à long terme pour l'identification biométrique.
- Palmprint permettent une différenciation précise entre les individus en raison des caractéristiques uniques présentes, telles que les lignes, les plis et les motifs des veines.

Inconvénients :

- L'acquisition précise de palmprint peut nécessiter des dispositifs d'imagerie spécifiques et des techniques d'alignement appropriées, ce qui peut rendre le processus d'acquisition plus complexe et potentiellement plus lent.

- Lorsque les bases de données de palmprint sont volumineuses, la recherche d'une correspondance peut être plus lente et nécessiter plus de ressources de traitement.

I.4.1.6 Géométrie de la main:

Cette méthode mesure les caractéristiques telles que la forme, la taille et la morphologie de la main pour identifier une personne [10].la figure 6 montre exemple de Géométrie de la main :

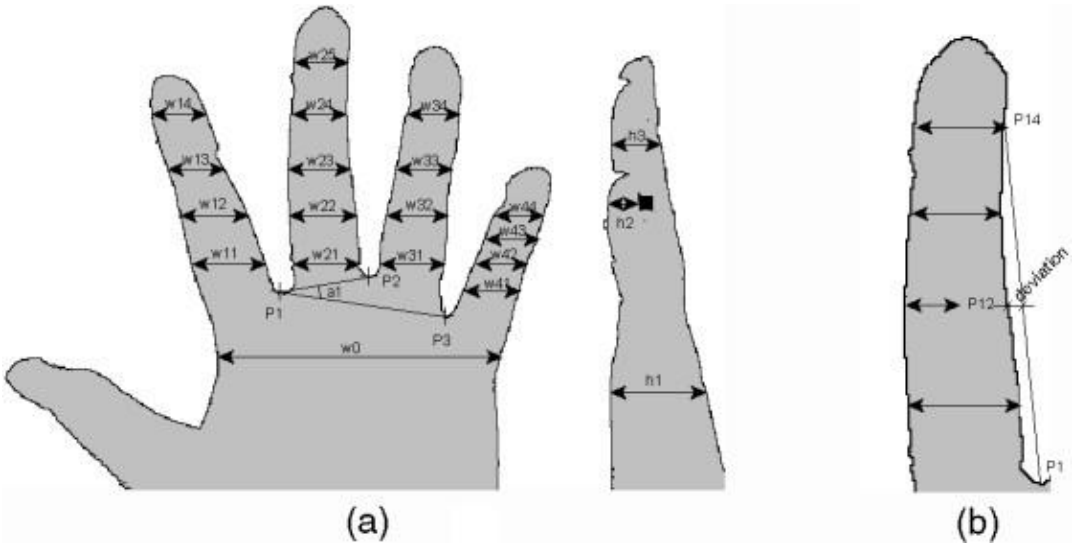

Figure 7 :Exemple deGéométrie de la main[10]

Avantages :

- La géométrie de la main peut être acquise de manière relativement facile à l'aide de caméras ou de scanners spécifiques, sans nécessiter de contact direct avec le dispositif.
- La géométrie de la main offre une différenciation précise entre les individus en se basant sur les caractéristiques uniques telles que la taille, la forme et la disposition des doigts, des paumes et des articulations.
- Les caractéristiques géométriques de la main ont tendance à rester relativement stables au fil du temps, permettant une utilisation à long terme pour l'identification biométrique.

Inconvénients :

- La géométrie de la main peut être sensible aux variations de position et d'orientation lors de l'acquisition, ce qui peut nécessiter une coopération active de l'utilisateur pour obtenir des résultats précis.
- Comparée à certaines autres modalités biométriques, la géométrie de la main peut avoir

une précision légèrement inférieure, ce qui peut conduire à un taux d'erreur légèrement plus élevé lors de l'identification.

- Bien que la géométrie de la main soit relativement stable, elle peut être affectée par des changements physiques tels que les blessures, les maladies ou les interventions chirurgicales, ce qui peut altérer la précision et la fiabilité de l'identification.

I.4.1.7 Signatures manuelles :

Ce système utilise la façon unique de bouger les mains et les doigts pour identifier une personne [11]. La figure 7 montre signatures manuelles :

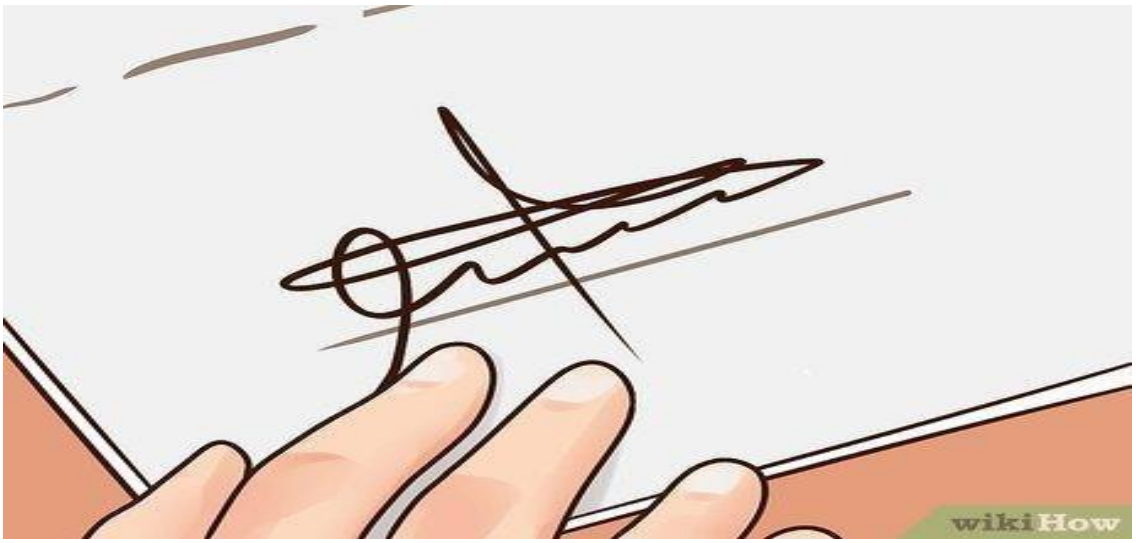

Figure 8: Signatures manuelles[11]

I.4.2. Les modalités comportementales

Les modalités comportementales sont des caractéristiques uniques d'une personne qui reflètent ses habitudes, ses comportements et ses capacités, et qui peuvent être utilisées pour identifier ou vérifier son identité. Elles incluent des éléments tels que la frappe au clavier, la manière de tenir et de déplacer un appareil mobile, la signature vocale, la reconnaissance de la signature manuscrite, etc. Les modalités comportementales sont souvent utilisées en complément des modalités physiologiques pour renforcer la sécurité des systèmes d'authentification [12].

I.4.2.1 La voix

La reconnaissance vocale est une modalité comportementale qui utilise des algorithmes pour analyser les caractéristiques uniques de la voix d'une personne, telles que la tonalité, le rythme et les pauses, pour vérifier son identité. La reconnaissance vocale peut être utilisée pour déverrouiller un appareil mobile, pour contrôler l'accès à un système ou à une application, ou

pour effectuer des transactions financières. Cependant, la reconnaissance vocale peut être influencée par des facteurs tels que le bruit environnant, les maladies de la gorge, etc., ce qui peut affecter la précision de l'identification. La reconnaissance vocale peut également susciter des préoccupations en matière de vie privée et de protection des données. La figure 8 donné exemple de La voix :

Figure 9 :La voix[2]

Avantages :

- La voix est une caractéristique naturelle et familière pour les individus, ce qui rend la reconnaissance vocale facile à utiliser et à adopter.
- La reconnaissance vocale permet une authentification à distance, sans nécessiter la présence physique de l'utilisateur, ce qui peut être avantageux dans certains scénarios d'accès à distance.

Inconvénients :

- La reconnaissance vocale peut être sensible aux bruits environnants et à la qualité du microphone, ce qui peut affecter la précision de la capture et de la reconnaissance de la voix**.**
- L'utilisation de la reconnaissance vocale nécessite souvent l'enregistrement et le stockage des empreintes vocales, ce qui soulève des questions de confidentialité et de sécurité des données.

I.4.2.2 Frappe dynamique sur le clavier :

La frappe dynamique sur le clavier est une modalité comportementale qui utilise des algorithmes pour analyser les caractéristiques uniques de la manière dont une personne tape sur un clavier[7]. telles que la vitesse, la pression et la durée des touches, pour vérifier son identité. La reconnaissance de la frappe dynamique sur le clavier peut être utilisée pour déverrouiller un ordinateur, un appareil mobile ou pour contrôler l'accès à un système ou une application.

Cependant, la reconnaissance de la frappe dynamique sur le clavier peut être influencée par des facteurs tels que la fatigue, les blessures, etc., ce qui peut affecter la précision de l'identification [9].la figure 9 présente exemple de Frappe dynamique sur le clavier :

Figure 9: Frappe dynamique sur le clavier [9]

Avantages :

- La frappe dynamique sur le clavier est basée sur des caractéristiques individuelles, telles que la vitesse de frappe, le rythme, la pression des touches, etc. Cela permet une identification précise des utilisateurs**.**
- Étant donné que la frappe dynamique se base sur l'utilisation naturelle du clavier, elle est souvent facile à adopter pour les utilisateurs.

Inconvénients :

- Les conditions environnementales, telles que le bruit de fond ou la fatigue de l'utilisateur, peuvent influencer la frappe dynamique, ce qui peut affecter la précision de l'identification.
- La mise en œuvre précise de la frappe dynamique peut nécessiter des algorithmes et des techniques sophistiqués pour capturer et analyser les données de frappe de manière précise et fiable.

1.4.2.3 Démarche :

La reconnaissance de la démarche est une modalité comportementale qui utilise des algorithmes pour analyser les caractéristiques uniques de la manière dont une personne marche, telles que la vitesse, le rythme et les mouvements des jambes, pour vérifier son identité. La reconnaissance de la démarche peut être utilisée pour contrôler l'accès à un système ou une installation, pour surveiller la sécurité dans un environnement public, etc. Cependant, la reconnaissance de la démarche peut être influencée par des facteurs tels que la fatigue, les blessures[19], etc., ce qui peut affecter la précision de l'identification. La reconnaissance de la démarche peut également susciter des préoccupations en matière de vie privée et de protection des données .la figure 10montre exemple de la démarche [10] :

Figure 10 : Démarche [19]

Avantages :

- La démarche humaine est une caractéristique individuelle qui peut être utilisée pour l'identification biométrique, car chaque personne a un style de marche distinctif.
- La démarche peut être capturée et analysée à distance, ce qui permet une identification sans nécessiter la proximité physique de l'utilisateur.
- La collecte des données de démarche peut se faire de manière non intrusive, sans nécessiter de contact physique direct avec l'utilisateur.

Inconvénients :

- La démarche peut être influencée par des facteurs externes tels que la surface de marche, l'environnement, les chaussures portées, etc. Cela peut rendre la collecte des données et l'analyse plus complexes.
- La démarche peut varier en fonction de différents facteurs tels que la fatigue, les

blessures, les changements de poids, etc. Cela peut affecter la stabilité et la fiabilité de l'identification biométrique basée sur la démarche.

1.4.2.4 Signature manuscrite :

La reconnaissance de la signature manuscrite est une modalité comportementale qui utilise des algorithmes pour analyser les caractéristiques uniques de la signature d'une personne, telles que la forme, la vitesse et les mouvements, pour vérifier son identité. La reconnaissance de la signature manuscrite peut être utilisée pour authentifier des signatures sur des documents officiels, des formulaires de demande, etc. Cependant, la reconnaissance de la signature manuscrite peut être affectée par des facteurs tels que la fatigue [13], le blessures, etc., ce qui peut affecter la précision de l'identification. La reconnaissance de la signature manuscrite peut également susciter des préoccupations en matière de vie privée et de protection des données. La figure 11montre le Signature manuscrite :

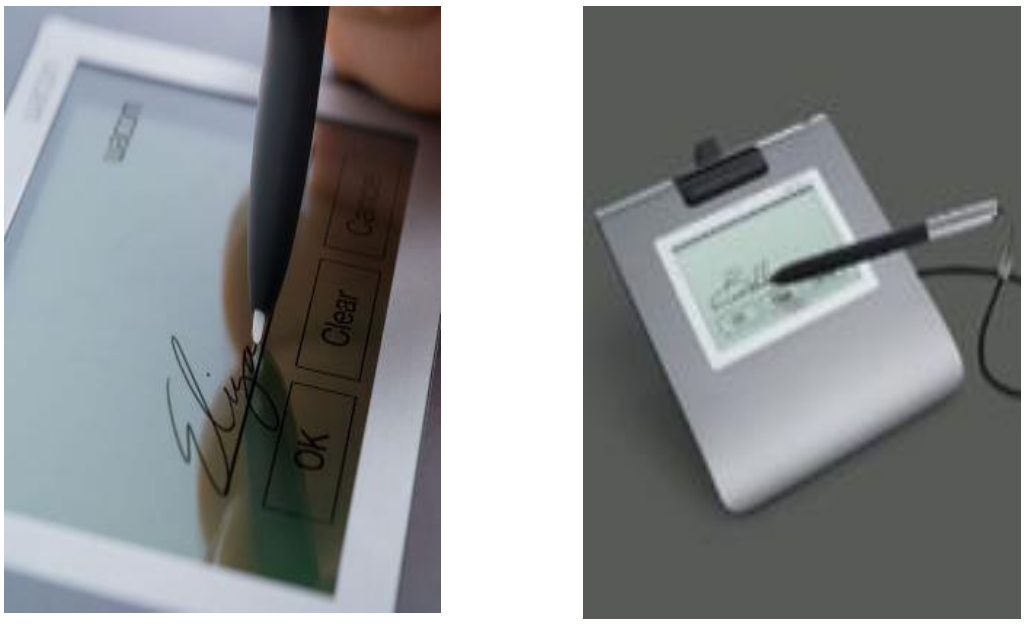

Figure 11: Signature manuscrite [13]

Avantages :

- Chaque signature manuscrite est unique, reflétant le style et les traits distinctifs de l'individu, ce qui permet une identification précise et fiable.

- La capture d'une signature manuscrite peut être réalisée facilement à l'aide d'un stylo et de papier, ou de manière électronique avec des dispositifs de capture spécifiques.
- Comparativement à certaines autres méthodes biométriques, l'utilisation de la signature manuscrite peut être moins coûteuse en termes d'équipement et d'infrastructure

nécessaires.

Inconvénients :

- Les signatures manuscrites peuvent être contrefaites ou imitées, ce qui peut compromettre la sécurité et l'authenticité des transactions.
- L'interprétation des signatures manuscrites peut être subjective et varier d'une personne à l'autre, ce qui peut entraîner des erreurs de reconnaissance ou des divergences d'opinions lors de la vérification.

1.4.2.5 Thermographie

Cette méthode utilise les caractéristiques uniques de la température de la main pour Identifier une personne.

Chacune de ces modalités a ses propres avantages et inconvénients en termes de fiabilité, de coût et de facilité d'utilisation, et peut être utilisée seule ou en combinaison avec d'autres méthodes pour améliorer la sécurité [14]. La figure 12 montre exemple de thermographie :

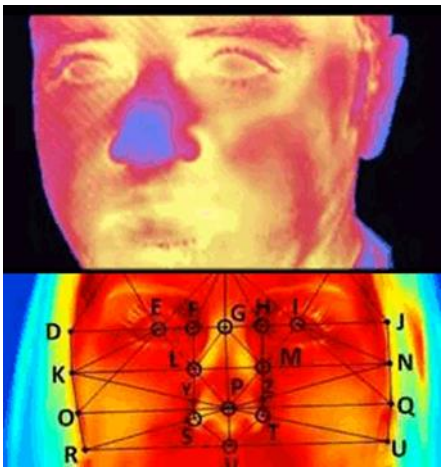

Figure 12: Thermographie[14]

Avantages :

- La thermographie permet de prendre des mesures de température rapidement et facilement, ce qui est particulièrement utile dans des situations où des contrôles rapides sont nécessaires, comme dans les aéroports, les installations de santé, etc.
- La thermographie peut être utilisée pour surveiller les températures corporelles à distance, ce qui peut être bénéfique dans des environnements à haut risque ou pour des situations nécessitant une surveillance à distance.

Inconvénients :

- La précision de la thermographie peut être affectée par des facteurs tels que les conditions environnementales, les mouvements de l'individu, les variations individuelles de température, ce qui peut entraîner des mesures moins précises.

1.5. Architecture d'un système biométrique

Un système biométrique comprend généralement les éléments suivants illustré par la figure13

- Capteur biométrique : il s'agit de l'appareil qui mesure la caractéristique biométrique, telle que les empreintes digitales, la reconnaissance faciale, la reconnaissance vocale, etc.
- Module extraction des caractéristiques : ce module analyse les données biométriques captées par le capteur pour extraire les caractéristiques utilisées pour l'identification.
- Base de données d'utilisateurs : cette base de données stocke les modèles biométriques associés à chaque utilisateur autorisé
- Comparaison des données biométriques : le système compare les données biométriques captées avec les modèles stockés dans la base de données pour déterminer l'identité de l'utilisateur [14]. L'architecture d'un système biométrique illustré sur la figure 13 :

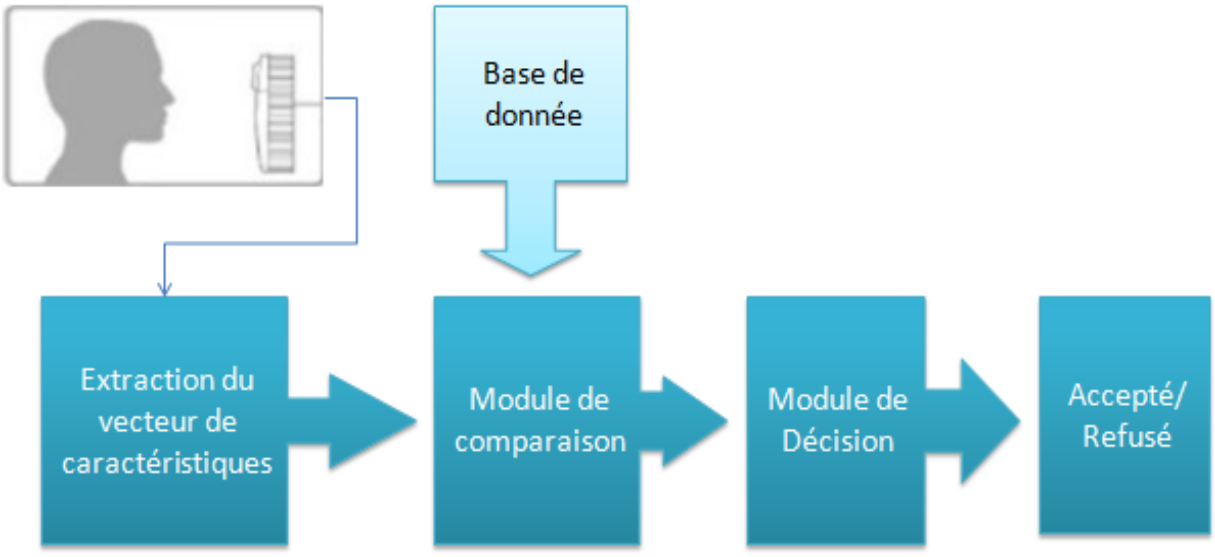

Figure 13 :Architecture d'un système biométrique

I.5.1 Mode vérification

Le mode de vérification dans un système biométrique est le processus qui permet de vérifier l'identité d'un utilisateur en comparant les données biométriques captées avec celles stockées dans la base de données. Il se déroule généralement de la manière suivante :

Prise d'une donnée biométrique : l'utilisateur fournit une donnée biométrique à travers le capteur biométrique, comme par exemple une empreinte digitale ou une image de son visage.

Extraction des caractéristiques biométriques : le logiciel de traitement d'image analyse la donnée biométrique captée et extrait les caractéristiques utilisées pour l'identification.

Comparaison avec les données stockées : les caractéristiques biométriques extraites sont comparées aux modèles biométriques stockés dans la base de données pour déterminer si elles correspondent à une entrée existante [14]. La figure 14 montre le mode vérification :

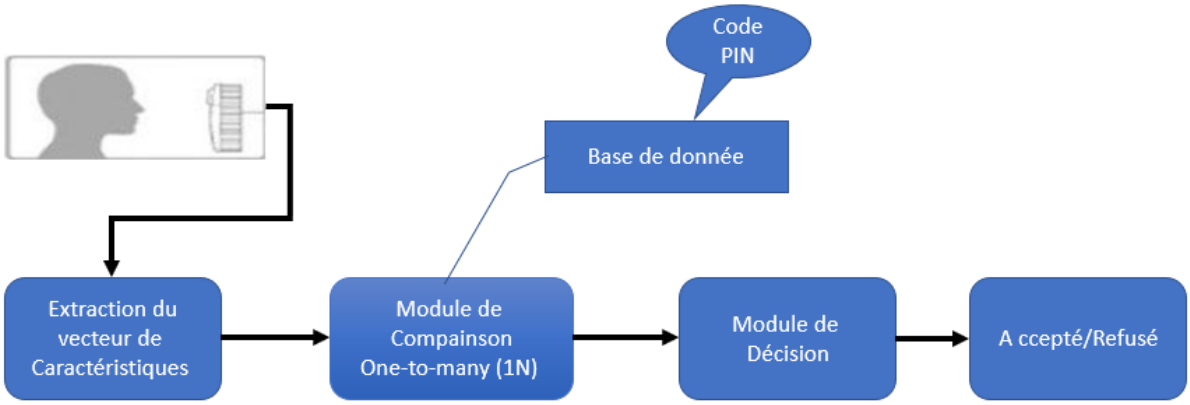

Figure 14: Mode vérification

I.5.2 Mode identification

Détermination de l'identité : si la correspondance est trouvée, l'utilisateur est considéré comme authentifié et son identité est déterminée. Sinon, l'accès est refusé.

Notification de résultat : l'interface utilisateur affiche le résultat de la vérification pour informer l'utilisateur de son statut d'authentification [14]. La figure 15 montre le mode

identification :

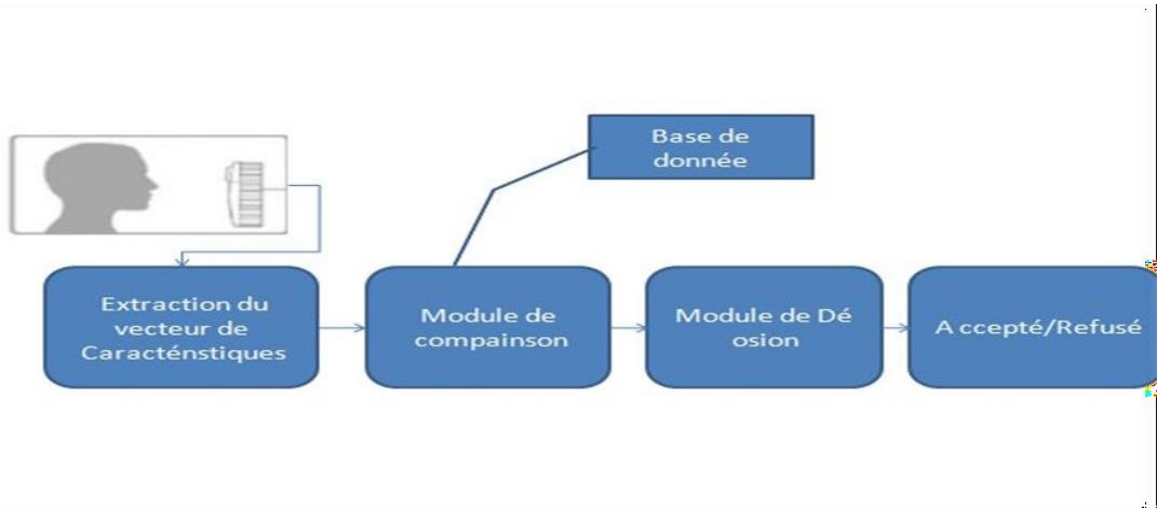

Figure 15: Mode identification

1.6. Système uni-modal:

Un système biométrique uni modal est un système qui utilise une seule méthode biométrique pour l'identification et l'authentification des utilisateurs. Les systèmes biométriques uni modaux sont généralement plus simples et moins désignés à mettre en œuvre que les systèmes biométriques multimodaux. Ils sont également plus faciles à utiliser et à gérer. Les systèmes biométriques uni modaux peuvent être basés sur des caractéristiques physiques telles que l'empreinte digitale, la reconnaissance faciale, la reconnaissance vocale, l'iris et la rétine. Ils peuvent également être basés sur des caractéristiques comportementales telles que la signature, le mouvement et le comportement. Les systèmes biométriques uni modaux sont généralement plus précis et plus fiables que les systèmes biométriques multimodaux.

Cependant, ils sont également plus vulnérables aux contrefaçons et aux attaques. Par exemple, une empreinte digitale peut être contrefaite à l'aide d'un moulage ou d'une photo. De même, une photo peut être utilisée pour contrefaire une reconnaissance faciale. Les systèmes biométriques uni-modaux sont généralement utilisés pour des applications à faible risque, telles que l'accès à des bâtiments ou à des systèmes informatiques. Ils sont également utilisés pour des applications à haut risque, telles que l'accès à des comptes bancaires ou à des systèmes de sécurité.

Les systèmes biométriques uni modaux sont généralement plus faciles à mettre en œuvre et à gérer que les systèmes biométriques multimodaux. Ils sont également moins requis et plus faciles à utiliser. Cependant, ils sont plus vulnérables aux contrefaçons et aux attaques. Par conséquent, ils ne sont pas toujours adaptés aux applications à haut risque [15].

1.7. Système biométrique multimodal

Un système biométrique multimodal est un système de reconnaissance d'identité qui utilise plusieurs modalités biométriques simultanément pour vérifier l'identité d'une personne. Par exemple, un système biométrique multimodal peut utiliser à la fois une empreinte digitale et un scan de la rétine pour vérifier l'identité d'une personne.

Les systèmes biométriques uni modaux sont généralement plus faciles à mettre en œuvre et à gérer que les systèmes biométriques multimodaux. Ils sont également moins requis et plus faciles à utiliser. Cependant, ils sont plus vulnérables aux contrefaçons et aux attaques. Par conséquent, ils ne sont pas toujours adaptés aux applications à haut risque [15].

1.7. Système biométrique multimodal

L'utilisation de plusieurs modalités biométriques offre plusieurs avantages par rapport à l'utilisation d'une seule modalité. Tout d'abord, cela améliore la fiabilité du système en utilisant plusieurs caractéristiques biométriques pour vérifier l'identité d'une personne. Deuxièmement, cela peut réduire les erreurs de reconnaissance en combinant les forces et les faiblesses de différentes modalités. Enfin, cela peut également offrir une plus grande flexibilité en permettant à l'utilisateur de choisir parmi plusieurs options pour vérifier son identité.[15] La figure 16 présenté le systèmes biométriques multimodaux :

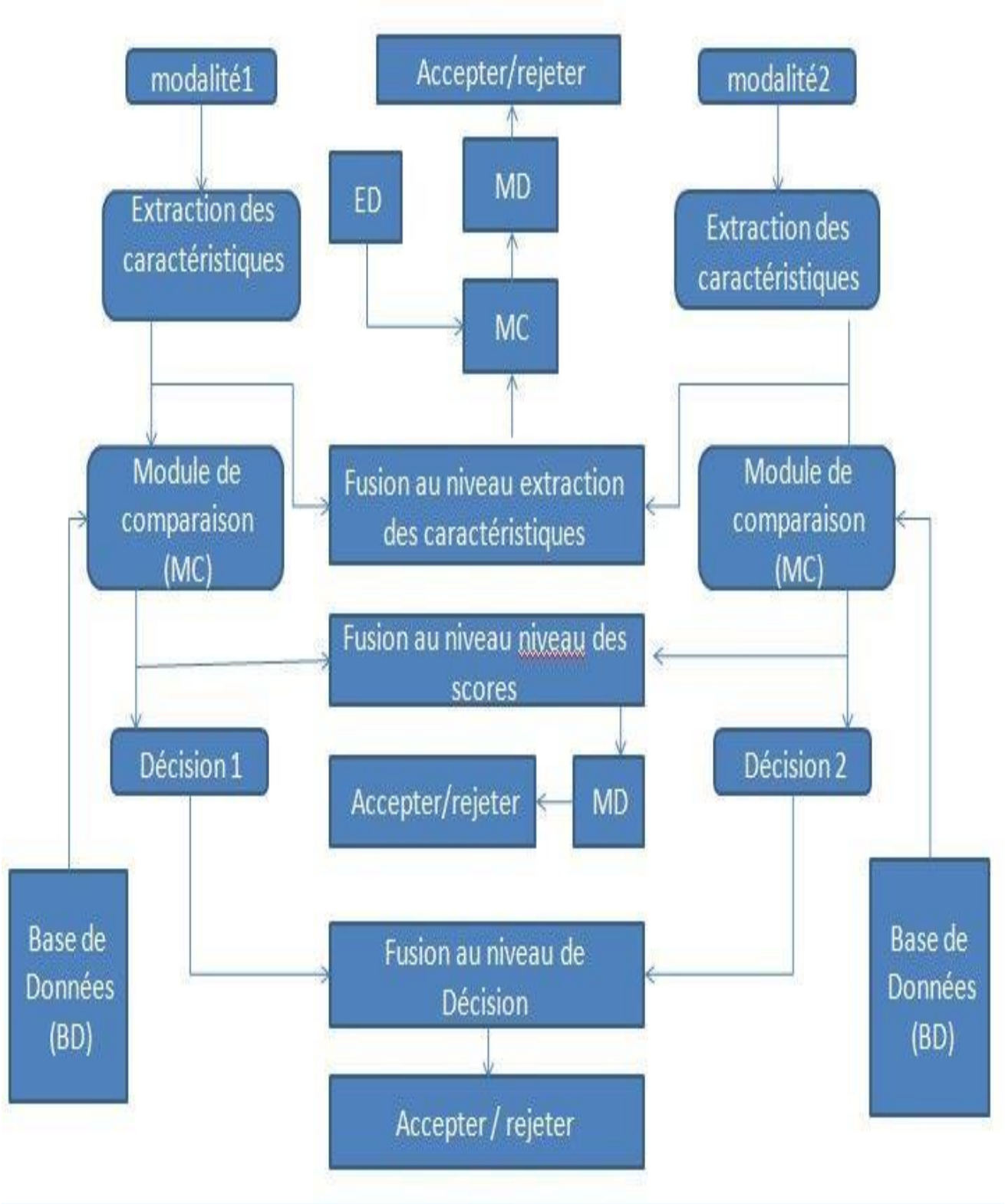

Figure 16: Systèmes biométriques multimodaux

1.8. Evaluation d'un système biométrique

L'évaluation d'un système biométrique implique l'analyse de ses performances pour déterminer sa qualité et sa fiabilité. Les critères importants pour évaluer un système biométrique incluent

Taux de reconnaissance : il s'agit de la capacité du système à identifier correctement une personne. Les taux de reconnaissance correcte et incorrecte sont importants pour évaluer la fiabilité du système.

Taux de faux positifs et faux négatifs : Le taux de faux positifs mesure le nombre d'identifications erronées, tandis que le taux de faux négatifs mesure le nombre d'identifications non reconnues.

Rapidité : Le temps nécessaire pour vérifier l'identité d'une personne est important pour évaluer la commodité d'utilisation du système.

Coût : le coût des équipements, des dispositifs et des services associés au système biométrique est important pour évaluer sa faisabilité économique. Flexibilité : La capacité du système à s'adapter à différentes conditions d'utilisation, telles que les différences d'éclairage ou les variations du nombre de personnes à vérifier, est importante pour évaluer sa flexibilité [16].

Sécurité : la sécurité du système, notamment la protection des données biométriques et la prévention des fraudes, est importante pour évaluer la fiabilité du système.

FAR: « False Acceptance Rate » c'est le taux de Fausses Acceptations: défini comme le nombre de Fausses Acceptations (FA) divisé par le nombre d'imposteursdans la base N i . FAR est calculé selon l'équation[16] :

$$FAR(T) = \frac{FA(T)}{N_i} \qquad (1)$$

FRR : « False Reject Rate » c'est le taux de Faux Rejetés indique le nombre de Faux Rejets (FR) divisé par le nombre de clients dans la base N c [30] . FRR est calculé par :

$$FRR(T) = \frac{FR(T)}{N_c} \qquad (2)$$

GAR : «GenuineAccept Rate» c'est le taux des véritables clients acceptés par le système

biométrique [16]. GAR est calculé par l'équation :

$$GAR(T) = 1 - FRR(T) \qquad (3)$$

EER :« EqualError Rate » c'est le taux d'erreur égale du système, qui correspond au taux d'erreur pour lequel FAR est égal à FRR.

ROC :(Receiver Operating Characteristic). Cette courbe représente les valeurs de FRR en termes de FAR. Ceci est obtenu en calculant le couple (FAR, FRR) ou chaque valeur du seuil de décision. Celui-ci diffère de la plus petite valeur obtenue à une valeur supérieure. Cette courbe peut être décomposée en trois zones : zone de haute sécurité, zone de compromis et zone de basse sécurité[16]. La figure 17montre exemple de la courbe ROC :

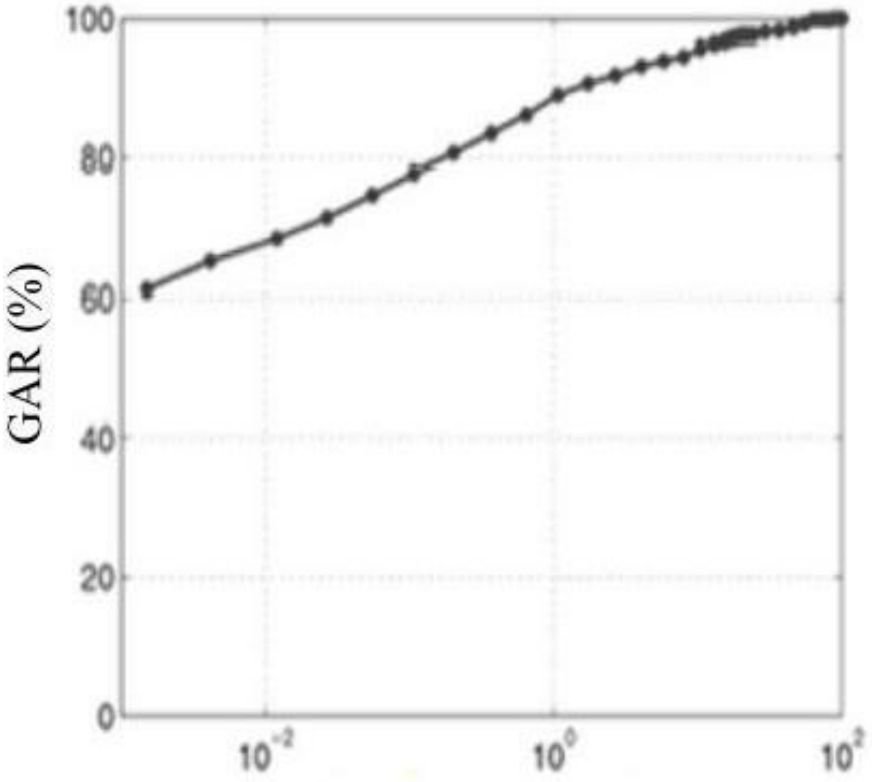

Figure 17 :exemple de la courbe ROC

CMC : En anglais on dite (Cumulative Match Characteristic) si l'identité correcte d'un utilisateur correspond à la plus haute correspondance (score le plus élevé parmi tous les scores de N matchs), nous dirons que l'utilisateur a été identifié au premier rang[34]. Le Rang-1 est calculé par:

$$Rang - 1 = \frac{N_i}{N} . 100(\%) \qquad (4)$$

Où Ni représente le nombre d'images attribuées avec succès à l'identité correcte (bien classées) et N représente le nombre total d'images essayant d'assigner une identité. Le taux d'identification de rang-n pour différentes valeurs de n peut être résumé en utilisant la courbe CMC Où n varie de 1 à N. N est le nombre d'utilisateurs dans la base de données. La figure 18 montre un exemple de la courbe CMC :

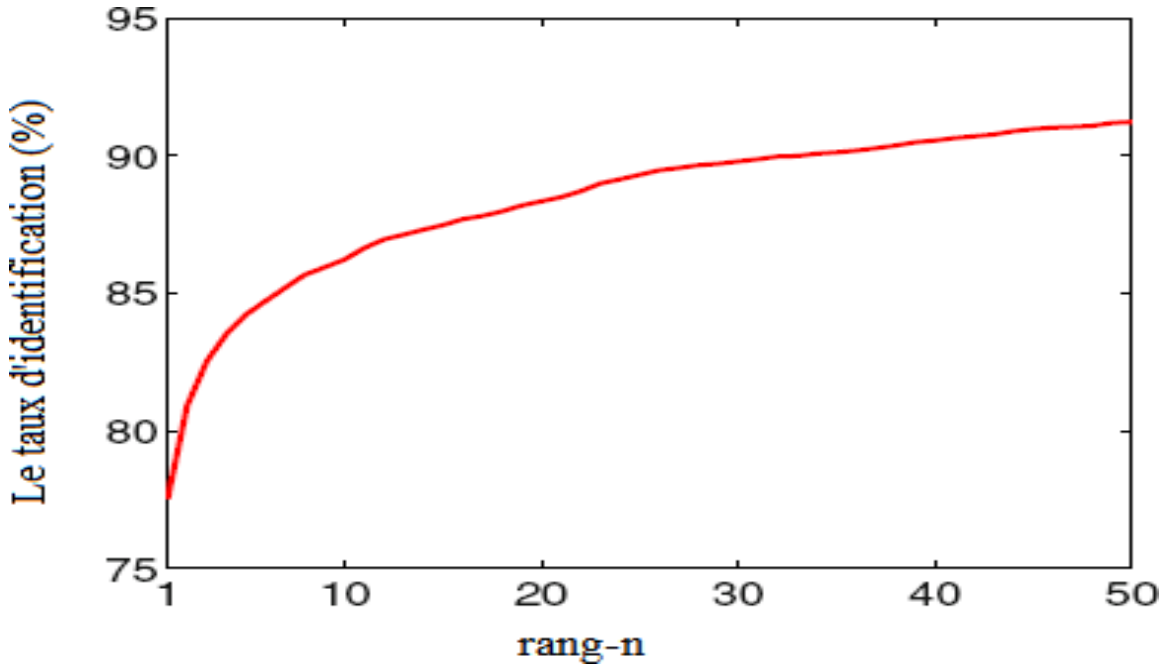

Figure 18 :exemple de La courbe CMC[13]

En général, une évaluation complète du système biométrique doit prendre en compte tous ces critères pour déterminer son appropriable pour une application donnée.

I.9 Conclusion

Dans ce chapitre, nous avons présenté quelques modalités biométriques avec leurs défis rencontrés dans les systèmes biométriques. Nous avons évoqué aussi les types et

L'architecture d'un système biométrique avec leur application dans la vie réelle et enfin Nous avons discuté l'évaluation d'un s système biométrique.

II.1 Introduction

L'état de l'art pour la reconnaissance des Palmprint en 3D utilise généralement des algorithmes de vision par ordinateur et d'apprentissage automatique pour extraire des caractéristiques distinctives des Palmprint en 3D. Ces caractéristiques sont ensuite utilisées pour identifier Palmprint et pour les comparer à une base de données Palmprint connues [17].

II .2 Définition de palmprint:

La paume de la main est la partie intérieure de la main (non visible lorsque celle-ci est fermée) allant du poignet aux racines des doigts, comme le montre la figure 19. Le palmprint est l'image de l'impression de la paume de la main obtenue par la pression de celle-ci sur une surface donnée. En d'autres termes, il s'agit du modèle de la paume de la main illustrant les caractéristiques physiques du motif de la peau, telles que les lignes (principales et les rides), les points, les minuties et la texture [18].

L'identification palmaire peut être vue comme la capacité d'identifier une personne unique à travers un algorithme approprié exploitant les caractéristiques du palmprint. La figure 19 montre quelques caractéristiques fondamentales du palmprint :

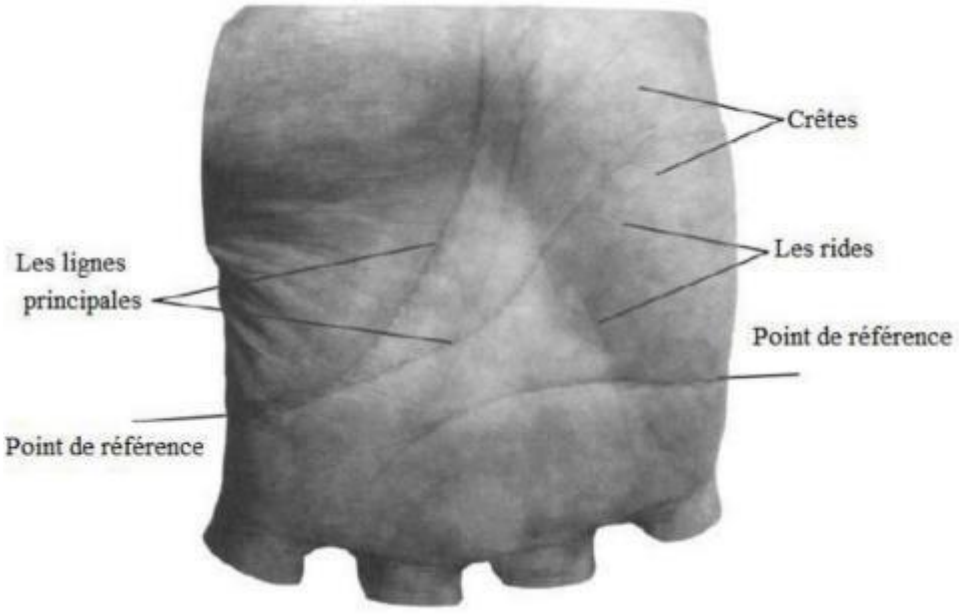

Figure 19 :Quelques caractéristiques fondamentales du palmprint[18]

Le palmprint en 3D est une méthode biométrique qui utilise les caractéristiques tridimensionnelles de la paume de la main d'une personne pour l'identification. Contrairement à la reconnaissance d'empreintes digitales ou faciales, qui se base sur des caractéristiques en 2D, la reconnaissance du palmprint en 3D offre des avantages supplémentaires en termes de précision et de fiabilité.

Voici comment fonctionne généralement un système de reconnaissance du palmprint en 3D :

Acquisition de l'image 3D de la paume de la main : Un dispositif de capture d'image, tel qu'un scanner ou une caméra 3D, est utilisé pour capturer l'image tridimensionnelle de la paume de la main de l'individu. Ce processus peut impliquer l'illumination de la paume à l'aide de lumières structurées ou la projection de motifs pour obtenir une représentation précise de la surface de la main.

Extraction des caractéristiques : Une fois que l'image 3D de la paume de la main est acquise, des algorithmes sont utilisés pour extraire les caractéristiques distinctives de la paume. Cela peut inclure la forme globale de la paume, les plis de la peau, les lignes principales, les textures et d'autres détails spécifiques.

Création d'un modèle biométrique : Les caractéristiques extraites sont utilisées pour créer un modèle biométrique unique pour chaque individu. Ce modèle est généralement représenté sous forme d'empreinte numérique ou de vecteur de caractéristiques qui peut être comparé avec d'autres empreintes pour l'identification.

Comparaison et identification : Lorsqu'une personne souhaite être identifiée, son palmprint en 3D est comparé aux modèles biométriques enregistrés dans la base de données. Les algorithmes de correspondance sont utilisés pour calculer la similarité entre les modèles et déterminer si une correspondance est trouvée.

La reconnaissance du palmprint en 3D présente plusieurs avantages par rapport aux méthodes biométriques traditionnelles en 2D. Elle offre une meilleure résistance aux attaques de contrefaçon et de falsification, car la nature tridimensionnelle de la paume de la main rend plus difficile la reproduction précise. De plus, les palmprints en 3D peuvent fournir des informations supplémentaires telles que la taille de la main, la profondeur des plis et d'autres détails structurels, ce qui améliore la précision de l'identification.

Cependant, il convient de noter que la reconnaissance du palmprint en 3D nécessite des équipements spécifiques pour l'acquisition des images, ce qui peut rendre son déploiement plus

coûteux et moins pratique que d'autres systèmes biométriques plus largement utilisés.

II.3 Avantages et inconvénients de reconnaissance de palmprint

II.3.1 Les avantages

- Traitement d'image à basse résolution.
- Peu de risqué d'intrusion.
- Les traits des lignes sont stables.
- Taux élevé d'acceptation par les utilisateurs.

II.3.2 Les désavantages

Il est difficile d'obtenir un bon taux de reconnaissance en utilisant uniquement les lignes principales en raison de leur ressemblance entre différents individus. (Note: "height" n'a pas de contexte dans cette phrase et ne nécessite donc pas de traduction.)[19]

II.4 Pourquoi utiliser le 3D palmprint

Des problèmes, des limitations et des cas d'usurpation d'identité ont été observés dans le système de reconnaissance 2D palmprint, même s'il a été largement testé sur de vastes bases de données. Afin de résoudre ces problèmes, l'utilisation de la reconnaissance 3D palmprint est proposée pour fournir des informations supplémentaires sur la profondeur et la courbure des lignes et des rides à la surface de la paume de la main. De plus, pour améliorer les performances, les chercheurs ont intégré les systèmes de reconnaissance 2D et 3D palmprint et ont exploré différentes stratégies de fusion, ce qui a donné une indication de la capacité d'adaptation du système[19].

II.5 Prétraitement

L'état de l'art en matière de prétraitement des Palmprint 3D comprend plusieurs techniques pour nettoyer, normaliser et préparer les données brutes avant l'analyse. Voici quelques algorithmes et techniques couramment utilisés dans le prétraitement des Palmprint 3D :

- ➔ **Filtrage et lissage :** Cette technique consiste à éliminer le bruit de fond et à lisser les données en utilisant des filtres tels que le filtre différence de gaussien(DOG), le filtre de la placient et le filtre médian[14].

- ➔ **Extraction regioninteret** :L'extraction de la région d'intérêt (ROI) est une technique de traitement d'images qui consiste à extraire une partie spécifique d'une image qui

contient les informations les plus pertinentes pour l'analyse ou la reconnaissanc d'objet. Cette technique est couramment utilisée en vision par ordinateur pour réduire la quantité de données à traiter, améliorer la précision de la reconnaissance et accélérer le processus de traitement.

Le processus d'extraction de ROI peut être réalisé manuellement ou automatiquement à l'aide de techniques de segmentation d'image. Les techniques de segmentation d'image permettent de délimiter automatiquement les zones d'intérêt en se basant sur des caractéristiques telles que la couleur, la texture, la forme ou la taille des objets dansl'image.

L'extraction de ROI est utilisée dans de nombreuses applications, notamment la reconnaissance faciale, la reconnaissance de plaques d'immatriculation, la reconnaissance de caractères, la détection d'objets et la reconnaissance de motifs[14].

Normalisation : La normalisation est un processus important pour rendre les données comparables et standardisées. Les techniques de normalisation couramment utilisées incluent la normalisation par min max,la normalisation par la moyenne et l'écart type..[14].

II.5.1 Technique de normalisation Tan et Triggs

La technique TT a été introduite par Tan et Triggs dans le domaine de la reconnaissance Palmprint Ici, la technique TT a été utilisée pour augmenter le contraste des régions sombres dans l'image et pour atténuer celui des régions lumineuses, pour supprimer le bruit et les gradients d'illumination et normaliser le contraste [15].

II .5.2 Différence de gaussien(DOG) :

La différence de gaussiennes (Dog) est une technique de traitement d'image utilisée pour détecter les contours et les bords d'une image. La technique consiste à soustraire une image gaussienne floue à une autre image gaussienne floue avec un écartement de variance (ou d'échelle) différente. Plus précisément, la différence de gaussiennes est obtenue en soustrayant l'image floue G(x,y) générée à partir d'une fonction gaussienne avec une variance σ, de l'image floue G(x,y) générée à partir d'une fonction gaussienne avec une variance kσ, où k est un facteur d'échelle. Cette différence de gaussiennes est une approximation de la La placien de Gaussienne, qui est une mesure de la seconde dérivée de l'image. La technique de la différencede gaussiennes est souvent utilisée dans les tâches de détection de caractéristiques d'images telles que la détection de contours, les coins ou les points d'intérêt, la détection de bordures, etc. Elle est également utilisée dans les applications de vision par ordinateur telles que la reconnaissance faciale, la détection d'objets, la segmentation d'images, etc[14]. La figure 20 montre (a) images de palmprint. (b) Leur images filtrées par un filtre DoG :

$$Ip(x,y) = DOG * I(x,y) \qquad (5)$$

Le filtre DoG est calculé par l'équation :

$$DOG = \frac{1}{2\pi\sigma_L^2}\, e^{\frac{x^2+y^2}{2\pi\sigma\sigma_L^2}} - \frac{2}{2\pi\sigma_H^2} e^{-\frac{x^2+y^2}{2\sigma_H^2}} \qquad (6)$$

La figure 20 montre (a) images de palmprint. (b) Leur images filtrées par un filtre DoG :

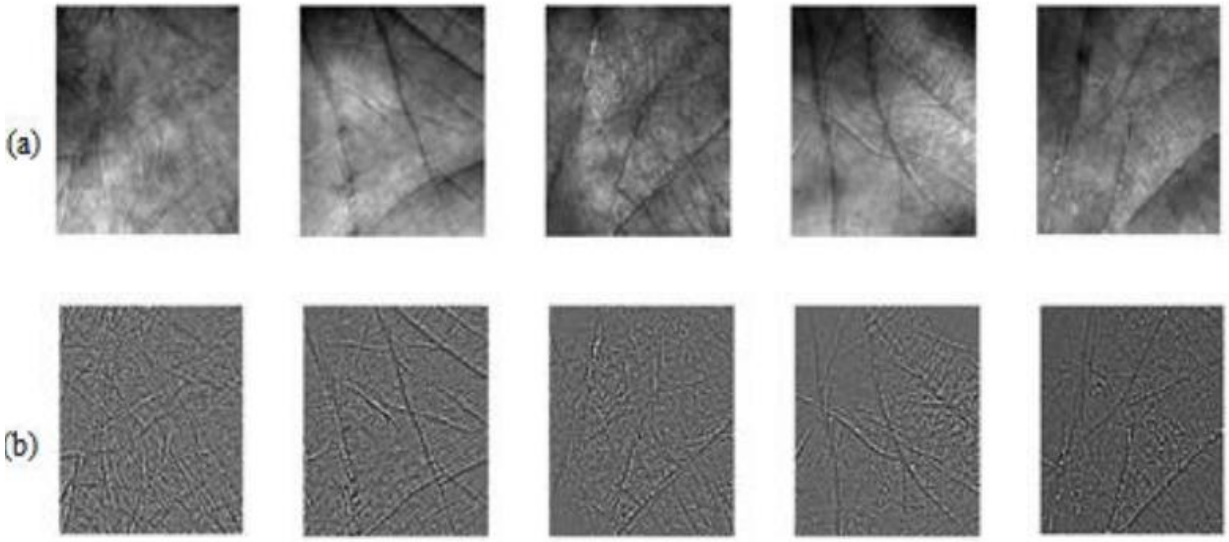

Figure 20:(a) images de palmprints. (b) Leur images filtrées par un filtre DoG

II.6 Les méthodes de l'extraction de caractéristiques

II .6.1 Les méthodes locales :

En traitement d'image et en vision par ordinateur, les caractéristiques locales sont des régions d'une image qui ont une apparence ou une structure distincte par rapport à leur voisinage. Ces caractéristiques sont souvent utilisées pour la détection, la description et la reconnaissance d'objets ou de formes dans une image.

Les caractéristiques locales sont souvent détectées à l'aide de descripteurs tels que le LBP (Local Binary Pattern), le HOG (Histogram of Oriented Gradients). Ces descripteurs extraient des informations à partir de zones de l'image qui ont des variations significatives de couleurs, de textures ou d'orientations.

Une fois que les caractéristiques locales ont été extraites, elles peuvent être utilisées pour la reconnaissance d'objets, la segmentation d'images, la détection de mouvement ou pour d'autres tâches de vision par ordinateur. Les caractéristiques locales peuvent également être utilisées en conjonction avec des algorithmes de classification tels que les SVM (Support Vector Machines) ou les réseaux de neurones pour améliorer la précision de la classification [14].

II .6.1.1 HOG (Histogram of Oriented Gradients)

N. Dalal et al ont proposé "Histogramme des gradients orientés" (HOG) comme un descripteur très puissant. Initialement développé pour la détection humaine, HOG a depuis été étendu et appliqué à divers autres problèmes de vision par ordinateur HOG capture l'apparence et la forme locale d'un objet dans une image en utilisant la distribution des gradients[14]

Etape 1: Diviser l'image (x, y) en N cellules régulières (N petites régions) et des blocs. Les valeurs de gradient sont calculées pour chaque pixel en utilisant un filtre dérivatif 1-D centré, dans les directions horizontales et verticales. Pour cela les masques suivants sont utilisés:

$$\boldsymbol{Dx} = [\mathbf{-1\ 0\ 1}] \qquad (7)$$

$$\boldsymbol{Dy} = \begin{bmatrix} \mathbf{1} \\ \mathbf{0} \\ \mathbf{-1} \end{bmatrix} \qquad (8)$$

$$\begin{cases} \boldsymbol{Gx(x,y) = I(x,y) * Dx} \\ \boldsymbol{Gy(x,y) = (x,y) * Dy} \end{cases} \qquad (9)$$

Caractéristiques résultant représente les caractéristiques de l'image.Le calcul du HOG implique les étapes suivantes :

- **Calcul des gradients de l'image :** Les gradients de l'image sont calculés en utilisant des filtres tels que les filtres de Sobel. Les gradients représentent la direction et la magnitude du changement de luminosité dans l'image.
- **Division de l'image en cellules :** L'image est divisée en cellules de taille fixe (par exemple, 8x8 pixels). Les gradients dans chaque cellule sont utilisés pour calculer un histogramme de directions.
- **Normalisation des blocs :** Les blocs de cellules sont normalisés pour améliorer la robustesse du descripteur au bruit et aux variations d'éclairage.
- **Concaténation des descripteurs de blocs :** Les descripteurs de blocs normalisés sont concaténés pour former un vecteur de caractéristiques final qui peut être utilisé pour la classification.

Le HOG est particulièrement utile pour la reconnaissance d'objets car il peut détecter les contours et les formes des objets dans l'image, indépendamment de la couleur et de l'éclairage de l'image. Cependant, il est sensible aux variations de taille et de rotation des objets. Des variantes du HOG ont été proposées pour améliorer sa robustesse à ces variations, telles que le HOG multi-échelle et le HOG rotational [14]. La figure 21montre exemple de le (Histogram of Oriented

Gradients) :

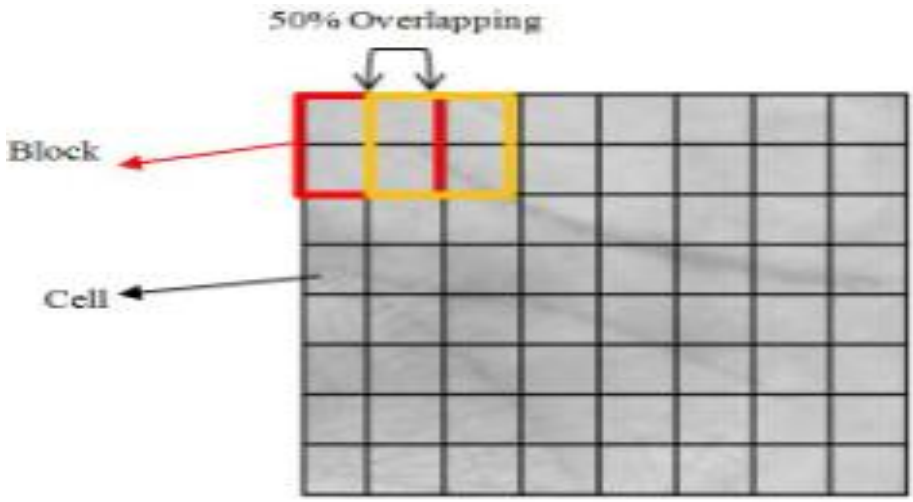

Figure 21 :Example de le HOG Histogram of Oriented Gradients

II .6.1.2. Binarized Statistical Image Features (BSIF)

Le descripteur local BSIF est une méthode récente utilisée pour reconnaître des textures. Il a été initialement introduit par J. Kannala et E. Rahtu en 2012 . Ce descripteur repose sur un ensemble de filtres linéaires de taille fixe. Lorsqu'il est appliqué à une image donnée I de dimensions N x N pixels, les filtres φi de taille N x N génèrent des réponses ri qui sont ensuite binarisées. Dans leur étude, J. Kannala et E. Rahtu ont formé un ensemble de filtres φi N x N en utilisant un ensemble d'images naturelles (comme décrit dans) (voir Figure 22). Ces filtres sont estimés en maximisant l'indépendance statistique des réponses ri à l'aide de l'ICA (Analyse en Composantes Indépendantes). Dans notre travail, nous avons également utilisé des filtres open-source qui ont été appris à partir de 13 images naturelles différentes . La réponse du filtre est obtenue de la manière suivante[14] . la figure 22 montre images naturelles utilisées pour l'apprentissage des filtres dans le descripteur BSIF :

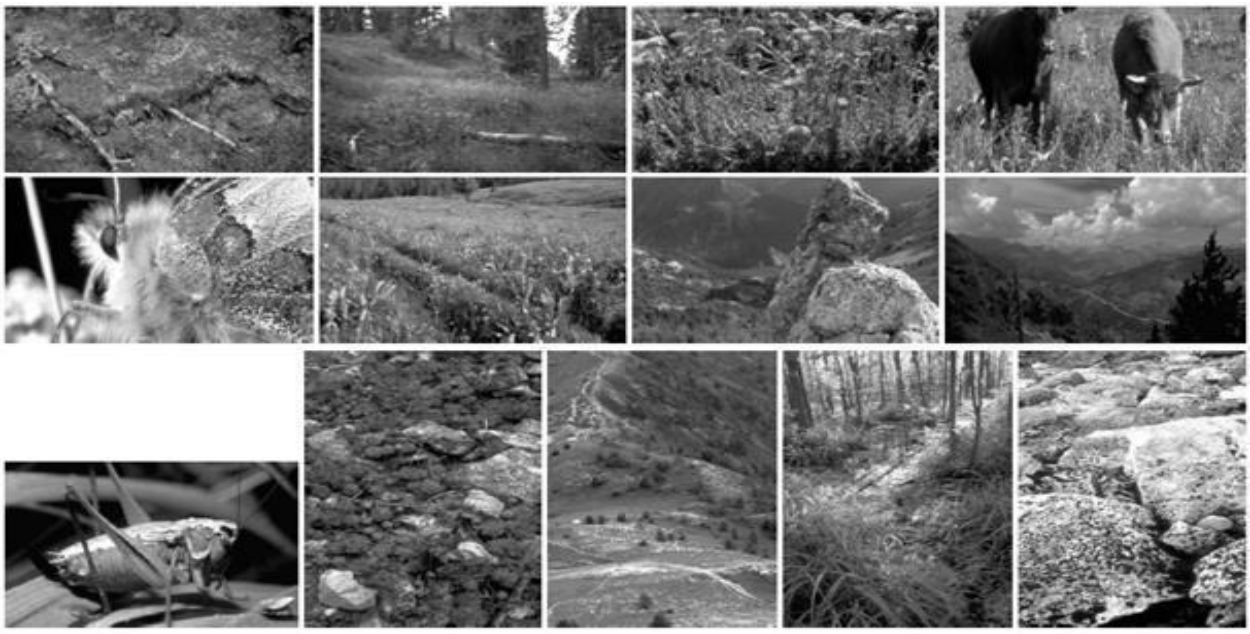

Figure 22 : Les 13 images naturelles utilisées pour l'apprentissage des filtres dans le descripteur BSIF

$$ri = \sum_{x,y} \varphi_i^{N*N}\ (x,y) I(x,y) \qquad (10)$$

Dans cette nouvelle formulation, la phrase est légèrement réorganisée et certaines expressions sont modifiées pour améliorer la clarté et la compréhension :

Les filtres linéaires φi de taille N, où i = {1, 2... n}, représentent le nombre de filtres statistiquement indépendants dont les réponses peuvent être calculées ensemble et binarisées. La binarisation est obtenue en utilisant la règle suivante :

$$bi = \begin{cases} 1\ si\ ri\ > 0 \\ 0 si\ ri\ \leq 0 \end{cases} \qquad (11)$$

II.6.1.3 Motif binaire local (LBP)

L'opérateur d'analyse de texture LBP, introduit par Ojala et al , repose sur le principe de comparer le niveau de gris d'un pixel à ceux de ses voisins. Si le niveau de gris du voisin est supérieur ou égal à celui du pixel courant, il prendra une valeur de 1, sinon il prendra la valeur de 0. Les pixels ainsi définis par ce motif binaire sont ensuite multipliés par des poids et sommés pour obtenir un code LBP pour le pixel courant. LBP est un descripteur de texture puissant, connu pour ses propriétés discriminantes et sa simplicité de calcul, ce qui en fait un choix populaire dans les applications pratiques[20].

Le calcul du descripteur LBP implique les étapes suivantes :

- Choix d'un rayon et d'un nombre de points : Le descripteur LBP est basé sur un cercle de rayon r centré sur chaque pixel de l'image. Le nombre de points choisi sur le cercle détermine la dimension du motif binaire local.
- Comparaison des niveaux de gris : Pour chaque point du cercle, la différence entre le niveau de gris du pixel central et celui du point est calculée et comparée à un seuil. Si la différence est supérieure ou égale au seuil, le point est marqué comme "1" dans le motif binaire local, sinon il est marqué comme "0".
- Calcul de l'histogramme : Les motifs binaires locaux sont utilisés pour calculer un histogramme de fréquence des motifs.

Le descripteur LBP est souvent utilisé en combinaison avec des classificateurs tels que les SVM ou les réseaux de neurones pour la reconnaissance d'objets ou la segmentation d'image.

$$\boldsymbol{LBP\,(xc\,,yc\,) = \sum_{i=0}^{p-1} f(x)\,(gi\; -\; gc\,) * 2^i} \qquad (12)$$

la fonction de seuillage, donnée par :

$$\boldsymbol{f(x) = \begin{cases} 1\ si\ x \geq 0 \\ 0 \quad\ x < 0 \end{cases}} \qquad (13)$$

Il est robuste aux variations de luminosité et de contraste, ainsi qu'aux variations géométriques telles que la rotation et l'échelle [20]. La figure 23montre exemple de (Motif binaire local) :

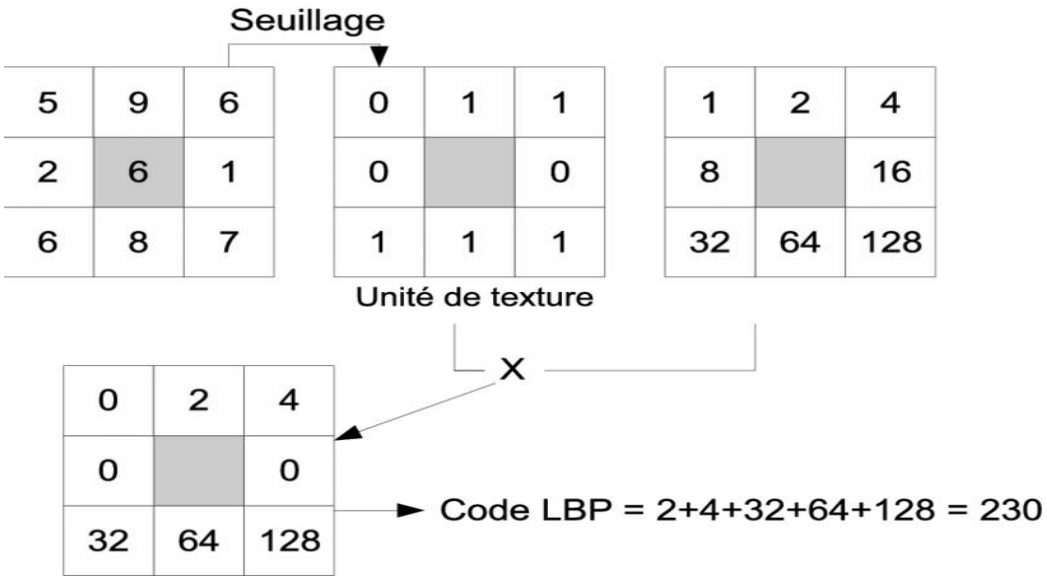

Figure 23: exemple de (Motif binaire local) [20]

II .6.1.4 LPQ (Local Phase Quantization)

LPQ (Local Phase Quantization) est une méthode de traitement d'images utilisée pour extraire des caractéristiques locales à partir d'images. Cette méthode est particulièrement utile pour la reconnaissance de textures.

LPQ se base sur la quantification de la phase de l'image locale, c'est-à-dire la différence de phase entre les pixels voisins. Cette quantification est effectuée à l'aide de la transformée de Fourier locale. LPQ calcule ensuite un histogramme de la distribution des valeurs quantifiées pour chaque image.[14]

Les caractéristiques obtenues par LPQ sont invariantes par translation, rotation et échelle, ce qui les rend robustes aux variations dans l'image. De plus, la méthode est relativement simple à implémenter et ne nécessite pas d'apprentissage préalable.

LPQ a été utilisé avec succès dans des applications telles que la reconnaissance de visages, la reconnaissance de textures, la détection de changements dans les images, et la détection de défauts dans les matériaux. La figure 24 montre local phase quantization (LPQ) :

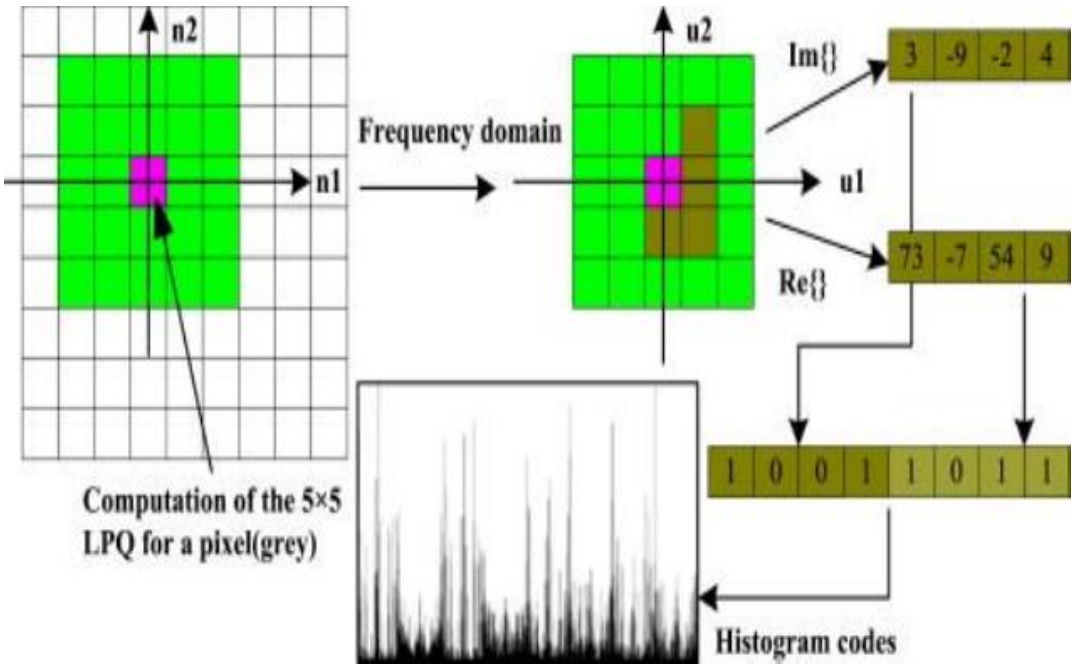

Figure 24 :LPQ (Local Phase Quantization [18]

II.6.2 Les méthodes globales

Les caractéristiques globales sont des descripteurs d'image qui représentent une image entière plutôt que des régions locales. Contrairement aux caractéristiques locales telles que le LBP ou le HOG, les caractéristiques globales sont calculées à partir de l'ensemble de l'image et fournissent une représentation globale de ses propriétés. Les caractéristiques globales sont

souvent utilisées pour la classification ou la reconnaissance d'images, en particulier lorsque les caractéristiques locales ne sont pas suffisantes ou ne sont pas adaptées au problème considéré [14].

Voici quelques exemples de caractéristiques globales couramment utilisées en vision par ordinateur :

II.6.2.1 Analyse en composantes principales (PCA)

La méthode PCA est largement utilisée en reconnaissance de visage et en biométrie pour projeter les données dans un nouvel espace de représentation. L'objectif est de trouver une nouvelle base de données obtenue par combinaison linéaire de la base originale. Cette représentation a été appliquée pour la première fois au visage en 1991 par MattiewTurk Le but est de trouver une transformation linéaire dans un espace de dimension réduite qui maximise la variance des projections des échantillons originaux. Pour q images d'entraînement, la méthode PCA consiste à trouver les vecteurs propres de la matrice de covariance formée par les différentes images de la base [21]. la figure 25montre (analyse en composantes principales) :

Etape1

$$X_T = \begin{pmatrix} a_{11} & a_{21} & \dots & a_{q1} \\ a_{12} & a_{22} & \dots & a_{q2} \\ \vdots & \vdots & \dots & \vdots \\ a_{1m} & a_{2m} & \dots & a_{qm} \end{pmatrix} = (X_1, X_2, \dots, X_q) \qquad (14)$$

Etape2 :

$$\mu = \frac{1}{q}\sum_{j=1}^{q} X_J \qquad (15)$$

Etape3:

$$\bar{\phi}_j = X_j - \mu \qquad (16)$$

Etape4:

$$C = AA^T OuA = [\emptyset_1 \emptyset_2 \dots \emptyset_q] \qquad (17)$$

Etape5:

$$C = A^T AOuA = [\emptyset_1 \emptyset_2 \dots \emptyset_q] \qquad (18)$$

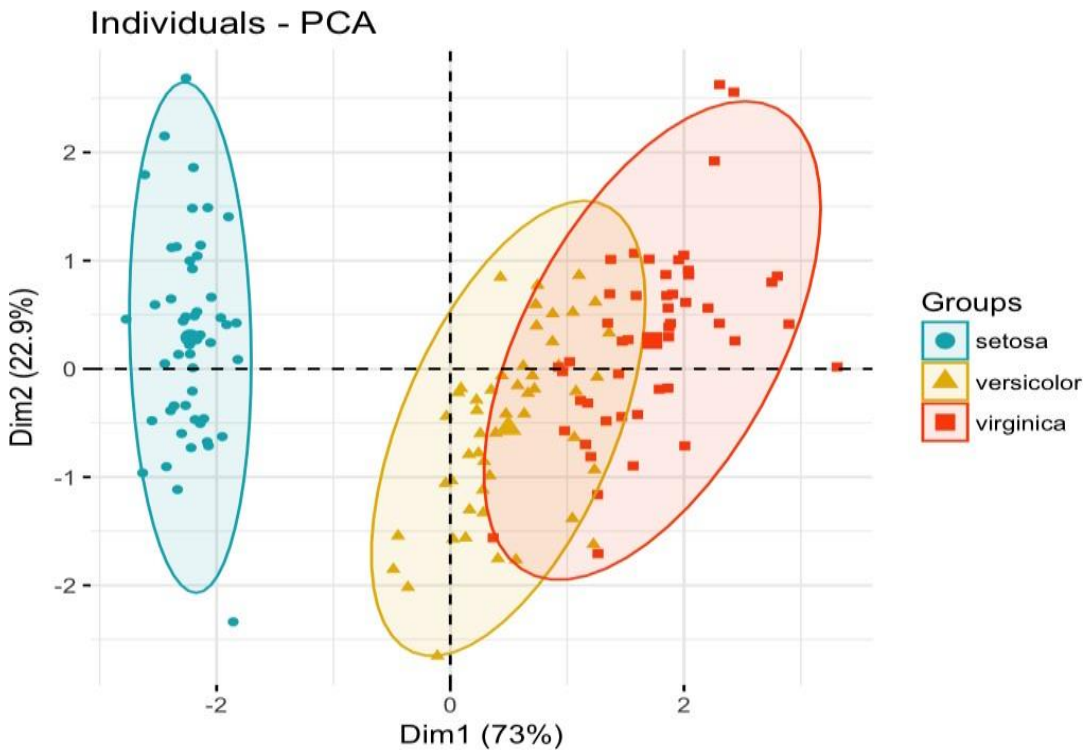

Figure 25 Analyse en composantes principales (PCA)

II.6.2.2 LDA (L'Analyse Discriminante Linéaire)

L'analyse discriminante linéaire (LDA), également appelée « Linear Discriminate Analysis » en anglais, est une méthode populaire pour trouver une combinaison linéaire de caractéristiques qui permet de mieux séparer les classes d'objets. Les combinaisons résultantes peuvent être utilisées comme un classificateur linéaire ou pour réduire les caractéristiques avant la classification. Les combinaisons linéaires sont obtenues à l'aide de la formule de Fisher palm T(w) (équation). LDA est une technique qui recherche les directions pour discriminer les données.[22]

Soit la matrice d'entraînement $\boldsymbol{XT}$ = [$X1$, $X2$, ..., Xq]. Xj désigne le vecteur caractéristique de l'image (j), où chaque Xj appartient à l'une des N classes (1, 2, ..., C) avec $1 \leq j \leq q$. Un sous-espace LDA a été construit de manière à minimiser la variance intra-classe SB (matrice de dispersion inter-classes) et à maximiser la variance inter-classe SW (matrice de dispersion intra-classes):

$$\boldsymbol{S_B = \sum_{i=1}^{N} ni(u_i - u)(u_i - u)^T} \qquad \boldsymbol{(19)}$$

$$\boldsymbol{S_w = \sum_{i=1}^{N} \sum_{X_j \in C_i} (x_j - u_i)(x_j - u_i)^T} \qquad \boldsymbol{(20)}$$

ni représente le nombre d'échantillons dans la i-ème classe, μi désigne la moyenne des données

d'apprentissage appartenant à la i-ème classe, N est le nombre de classes et μ représente la moyenne globale de toutes les données d'entraînement. Ensuite, nous dérivons la matrice de transformation W qui maximise le critère discriminant de Fisher.

$$T(W) = W_{opt} = arg_W max \frac{|w^T S_B W|}{|W^T S_W W|} = [W_1 W_2 \cdots W_d \qquad (21)$$

La solution optimale à ce problème d'optimisation est donnée par la résolution du problème généralisé des vecteurs propres

$$S_B W = \gamma S_W W \qquad (22)$$

La figure 26 montre exemple de l'analyse discriminante linéaire (LDA) :

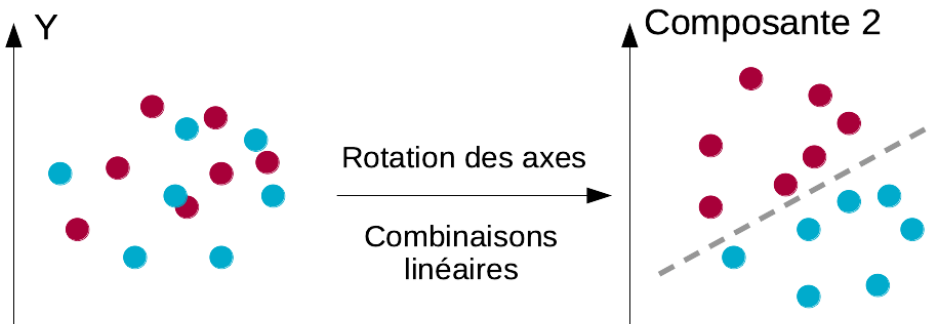

Figure 26: LDA (L'Analyse Discriminante Linéaire)[20]

II.6.3 Les méthodes de classification

La classification est une tâche importante en apprentissage automatique qui consiste à attribuer une étiquette à une donnée d'entrée en fonction de ses caractéristiques. En d'autres termes, il s'agit de trouver une fonction qui prend en entrée des caractéristiques et produit en sortie une étiquette qui représente la catégorie ou la classe à laquelle appartient la donnée.

Il existe plusieurs méthodes de classification, telles que la classification supervisée et la classification non supervisée. Dans la classification supervisée, le modèle est entraîné sur un ensemble de données étiquetées, c'est-à-dire un ensemble de données pour lequel on connaît les étiquettes associées à chaque donnée. Le modèle apprend ainsi à associer des caractéristiques à des étiquettes en utilisant un algorithme d'apprentissage supervisé, tel que les SVM, les réseaux de neurones, etc.

Dans la classification non supervisée, le modèle n'est pas entraîné sur un ensemble de données étiquetées mais cherche plutôt à regrouper les données en fonction de leurs caractéristiques similaires. Les algorithmes de clustering, tels que K-means, DBSCAN, etc. sont des exemples de techniques de classification non supervisée.La classification est utilisée dans de nombreux domaines, tels que la reconnaissance d'images, la classification de documents, la détection de spam, la classification de signaux biomédicaux, etc[14].

II.6.3.1 KNN (k-Nearest Neighbors)

La méthode des k plus proches voisins, également appelée k-NN (Nearest-Neighbor), fait partie des algorithmes d'apprentissage automatique (machine learning). L'idée de l'apprentissage automatique n'est pas récente, car le terme "machine learning" a été utilisé pour la première fois par l'informaticien américain Arthur Samuel en 1959. Les algorithmes d'apprentissage automatique ont connu un regain d'intérêt important au début des années 2000, notamment grâce à la disponibilité de grandes quantités de données sur Internet.

La méthode des plus proches voisins consiste à déterminer, pour chaque nouvelle personne que l'on souhaite classer, la liste des k plus proches voisins parmi les individus déjà classés. L'individu est ensuite attribué à la classe qui contient le plus grand nombre d'individus parmi ces plus proches voisins. Le choix du nombre de voisins à prendre en compte est important. Cette méthode est non-paramétrique et supervisée, et elle est souvent performante. De plus, son apprentissage est relativement simple, car il s'agit d'un apprentissage par cœur, c'est-à-dire que l'on conserve tous les exemples d'apprentissage. Cependant, le temps de prédiction est généralement long, car il nécessite le calcul de la distance avec tous les exemples, mais il existe des heuristiques permettant de réduire le nombre d'exemples à considérer.

Le principe de cet algorithme de classification est très simple. On lui fournit un ensemble de données d'apprentissage D, une fonction de distance d et un entier k. Pour chaque nouveau point de test x, pour lequel une décision doit être prise, l'algorithme recherche dans D les k points les plus proches de x selon la distance d, puis attribue x à la classe la plus fréquente parmi ces k voisins [24]. La figure 28 présenté la méthode de KNN (k-Nearest Neighbors) :

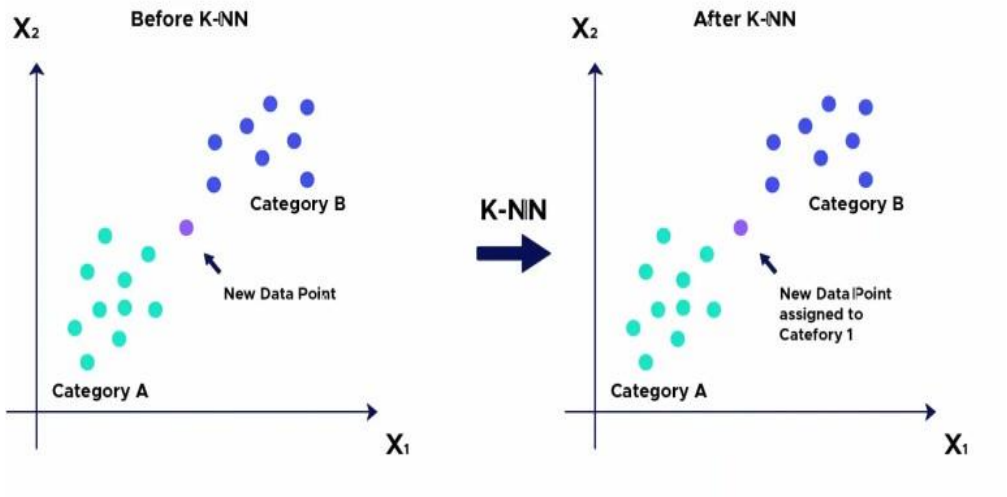

Figure 27 :KNN (k-Nearest Neighbors[22]

Ce travail focalise sur l'utilisation de quatre distances métriques qui sont :

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

$$d(x,y) = \sqrt{\sum_{i=1}^{n}(xi - yi)^2} \qquad (23)$$

- **Distance Manhattan (City block)** : La distance de Manhattan, également connue sous le nom de distance "city-block" ou métrique absolue, est définie comme la somme des valeurs absolues des différences entre les coordonnées de deux points.

$$d(x,y) = \sum_{i=1}^{n} |xi - yi| \qquad (24)$$

- **Distance de Mahalanobis** : En deux dimensions, la distance de Mahalanobis et la distance euclidienne sont égales. Cependant, la forme de la boule associée à la distance de Mahalanobis est elliptique, tandis que la boule associée à la distance euclidienne est un cercle.

  La distance mahalanobis donné par cette équation :

$$d(x,y) = \sqrt{(x-y) * cov(d)' * (x-y)'} \qquad (25)$$

- La distance Cosinus (Cos) est donnée par :

$$d(x,y) = \left(1 - \frac{XiYj^T}{\sqrt{XiYi^T)(YjYj^T}}\right) \qquad (26)$$

II.6.3.2 SVM (Support Vector Machine)

Est un algorithme de classification supervisée populaire en apprentissage automatique. L'idée de base de l'algorithme est de trouver un hyperplan qui sépare les données d'entraînement en deux classes en maximisant la marge entre les deux classes.
L'algorithme SVM peut être utilisé pour résoudre des problèmes de classification linéaire ou non linéaire en utilisant des fonctions de noyau qui permettent de projeter les données dans un espace de caractéristiques de dimension supérieure. Les SVM peuvent également être utilisés pour résoudre des problèmes de régression en modélisant les données de sortie continue à l'aide d'une fonction linéaire ou non linéaire.

L'algorithme SVM peut être utilisé avec différents types de fonctions de coût et de noyau, qui peuvent être choisis en fonction des données et du problème de classification spécifique. Les SVM ont plusieurs avantages, notamment leur capacité à gérer des données de grande dimensionnalité, leur robustesse aux données bruyantes et leur capacité à gérer des données non linéaires.

Cependant, l'algorithme SVM peut être sensible à la sélection des hyper paramètres, tels que le choix de la fonction de coût, la fonction de noyau et les paramètres associés. De plus, l'entraînement d'un SVM peut être relativement lent pour les grands ensembles de données[25].

La figure 29 montre le support vector machine(SVM) :

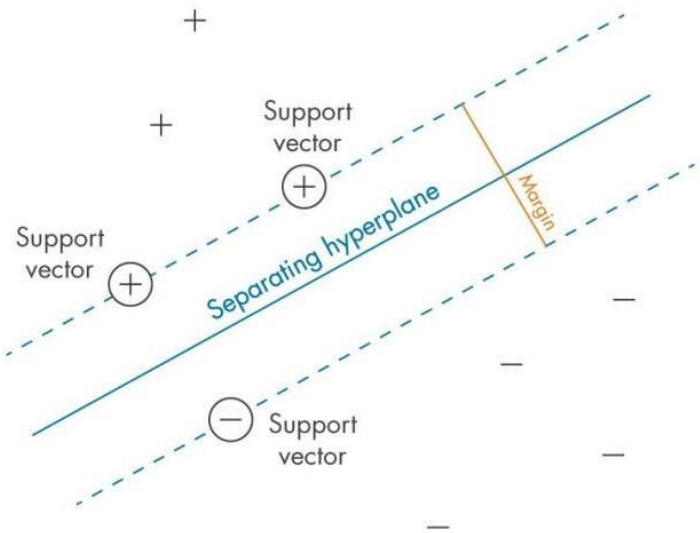

Figure 28:SVM Support Vector Machine[23]

II.7 Conclusion

Dans ce chapitre. Nous avons examiné l'algorithme de prétraitement TT . et nous avons parlé aussi des quelques algorithmes utilisés dans le domaine de la biométrie pour le prétraitement l'extraction des caractéristiques et pour la classification. Dans le prochain chapitre, nous allons approfondir la façon dont ces algorithmes sont appliqués dans la pratique. Nous discuterons de l'utilisation concrète de ces algorithmes, ainsi que des filtres associés, afin d'améliorer les performances et la précision des systèmes biométriques.

III.1 Introduction

L'étude expérimentale de ce projet est basée sur la reconnaissance de personnes par leurs Palmprint 3D en utilisant les principes décrits dans le chapitre précédent. Ensuite, nous avons abordé la base de données utilisée et le protocole de test. À la fin de ce chapitre, nous avons introduit la partie expérimentale qui contient les résultats que nous avons obtenus à partir de notre expérience.

III.2 Protocole De Test

Dans cette section, nous discutons des expériences sélectionnées confondit pour la reconnaissance palmprint 3D. Toutes les expériences ont été menée sur la base de données publique palmprint PolyU 3D . L'environnement expérimental comprend un PC:

- CP U: Intel core i7 4th.
- RAM : 8 GB
- GP U: (NVIDIA GeForce, GTX 1650).
- Le programme utilisé : MATLAB R2018

III.3 Principe de la méthode proposé

Cette section présente en détail le système de reconnaissance automatique de Palmprint 3D proposé. Le système repose sur l'utilisation d'un descripteur BSIF, HOG et LPQ de l'algorithme TT. La méthode proposée pour la reconnaissance automatique de Palmprint 3D se compose de deux étapes distinctes : l'enrôlement et l'identification/authentification. L'étape d'enrôlement consiste à acquérir les images de Palmprint 3D et à extraire les caractéristiques à l'aide du les descripteurs BSIF, HOG et LPQ. Le descripteur BSIF permet de représenter de manière compacte les informations discriminantes de Palmprint 3D. Ces caractéristiques extraites sont ensuite utilisées pour créer un modèle de référence de Palmprint de chaque individu enregistré dans le système. L'étape d'identification/authentification est réalisée lorsqu'une Palmprint 3D est soumise au système pour une vérification. Les caractéristiques de Palmprint sont également extraites à l'aide du leur descripteur. Ensuite, l'algorithme TT est utilisé pour comparer le

caractéristiques de Palmprint soumise aux modèles de référence stockés dans le système. Une correspondance est recherchée et une décision d'identification ou d'authentification est prise en fonction de la similarité entre les caractéristiques.

En résumé, le système de reconnaissance automatique de Palmprint 3D proposé utilise le descripteur BSIF, HOG et LPQ a partir de l'algorithme TT pour extraire et comparer les caractéristiques de Palmprint. Il se divise en deux étapes distinctes : l'enrôlement, où les modèles de référence sont créés, et l'identification/authentification, où Palmprint soumises sont comparées aux modèles de référence pour prendre une décision [26].

La figure 30 donné l'architecture d'un système d'identification de palmprint 3D :

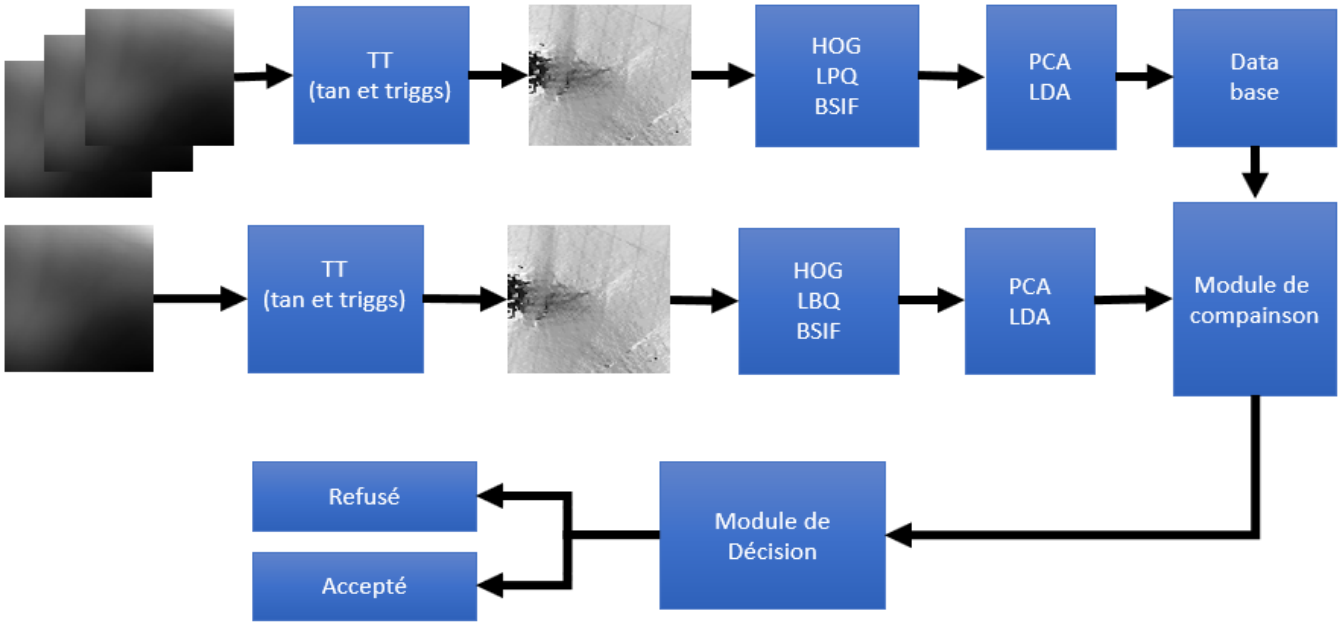

Figure 29: Architecture d'un système d'identification de palmprint 3D

III.3.1 Extraction de la région d'intérêt (ROI)

Li et al. [10] ont développé un appareil permettant d'acquérir des données d'empreintes digitales 3D à l'aide de la technologie de lumière structurée. Cet appareil est capable de capturer simultanément des informations d'empreintes digitales 3D et 2D à partir d'une paume. Le processus d'extraction de la région d'intérêt (ROI) est illustré à la Figure 30. Initialement, l'image d'origine subit un lissage gaussien, suivi d'une binarisation à l'aide d'une valeur de seuil, notée T (voir Figures 30 et b). Les valeurs de seuil sont calculées automatiquement à l'aide de la méthode d'Otsu et appliquées pour convertir l'image en niveaux de gris en une image binaire. Ensuite, un algorithme de suivi de frontière est utilisé pour extraire les contours de l'image binaire (Figure 30). L'image de contour résultante est

ensuite traitée pour déterminer les points P1 et P2, qui sont utilisés pour localiser le motif de la ROI en 2D. En utilisant les coordonnées de Y1 et Y2, un rectangle est tracé pour indiquer la zone de la ROI (Figure 30), et ensuite la ROI en 2D est extraite (Figure 30). De plus, les Figures 2f et g montrent respectivement l'image d'empreinte digitale 3D et la ROI 3D obtenue. La ROI 3D est générée en regroupant les points de nuage correspondant aux pixels de la ROI 2D, en suivant la méthode décrite dans [27].

La figure 31montre les étapes d'extraction de la région d'intérêt (ROI) de l'image de palmprint 3D :

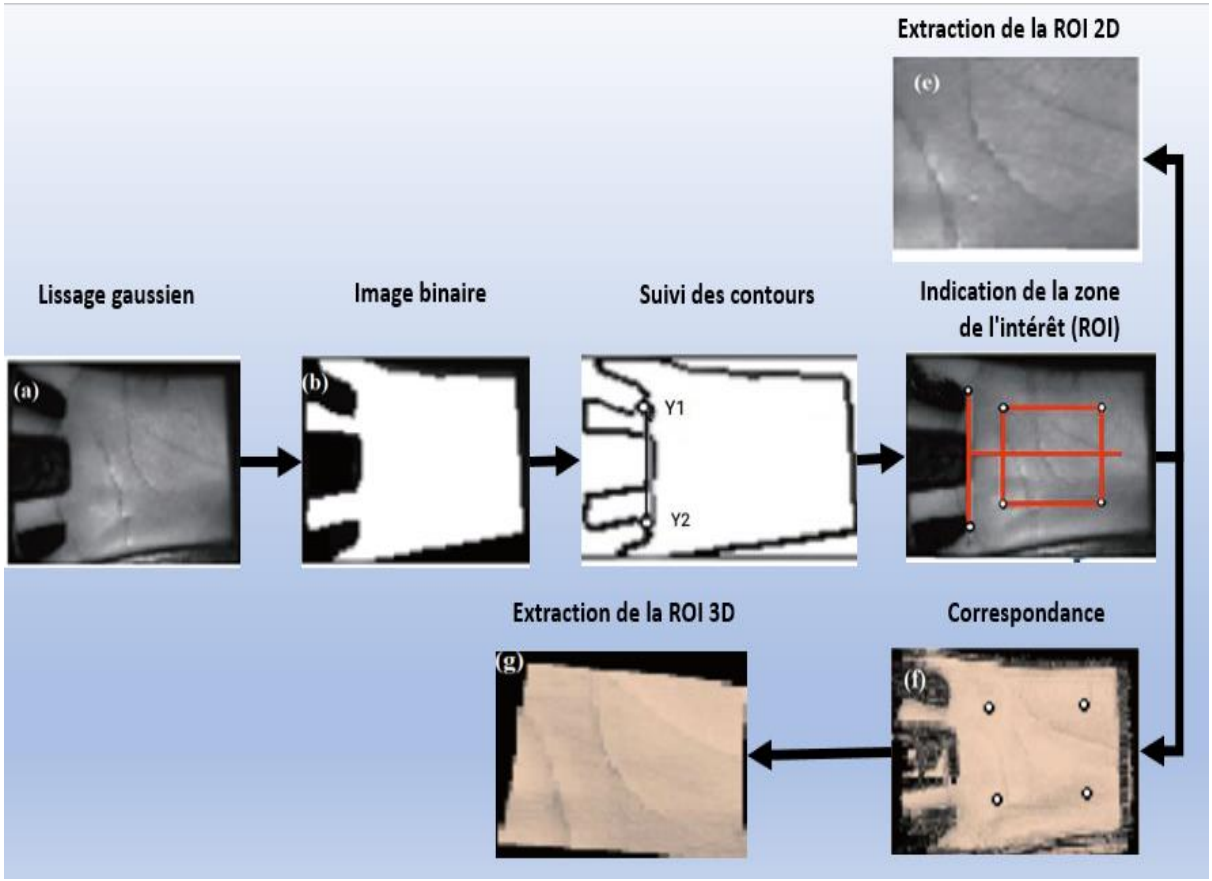

Figure 30 :Étapes d'extraction de la région d'intérêt (ROI) de l'image de palmprint 3D

III.3.2 Base de données

Afin d'évaluer les performances de notre approche, nous avons utilisé des données palmprint 3D disponibles au public et collectées par l'université polytechnique de Hong Kong (PolyU). Cet ensemble de données [30] contient 8000 échantillons provenant de 400 paumes différentes (classes) correspondant à 200 sujets (136 hommes et 64 femmes), avec 20 paumes différentes pour chaque classe. Les images de palmprint 3D ont été capturées lors de deux séances. Lors de chaque séance, 10 images ont été enregistrées à partir des

paumes gauche et droite de la personne. L'intervalle de temps moyen entre deux séances est de 1 mois.

III.3.3 Séparation de base de données

Pour évaluer et tester notre système, nous avons divisé l'ensemble des images de la base de données 3D palmprint en deux parties : l'ensemble d'apprentissage et l'ensemble de test. Lors de nos séries de tests, nous avons effectué la division de la base de données de la manière suivante :

- **Images d'apprentissages** : 10 images pour chaque personne servent pour la phase d'apprentissage.
- **Images Tests** : 10 images pour chaque personne vont servir pour la réalisation des différents tests

Nous évaluons les performances de notre système en utilisant le taux de reconnaissance. Le taux de reconnaissance mesure la capacité de notre système à identifier correctement les images de la main gauche dans l'ensemble de test.

III.3.4 Résultats et discussion

Pour évaluer les performances de l'algorithme utilisé, nous avons effectué des tests en comparant chaque vecteur de l'image de test avec tous les vecteurs présents dans la base de référence. Si les deux vecteurs appartiennent à la même classe (c'est-à-dire à la même personne), nous considérons cela comme une correspondance positive, ce qui signifie que le système a correctement reconnu la personne. En revanche, si les vecteurs appartiennent à des classes différentes, nous les considérons comme une correspondance négative, indiquant que le système n'a pas réussi à reconnaître correctement la personne.

Le taux de reconnaissance est calculé en comparant le nombre total de correspondances positives avec le nombre total de correspondances (positives + négatives). Ce protocole de test nous permet de mesurer la précision du système dans la reconnaissance des images de palmprint en 3D et d'évaluer son efficacité.

III.3.4.1 Les résultats obtenus par la méthode BSIF

Dans cette première expérience, nous avons appliqué l'algorithme TT pour le prétraitement des données, puis nous avons utilisé le filtre BSIF pour l'extraction des caractéristiques.

Enfin, nous avons utilisé l'algorithme KNN avec différentes distances pour la classification. **Le tableau 1** présente les résultats obtenus pour différentes valeurs de paramètres (taille et longueur) du filtre BSIF.

Les meilleurs résultats ont été obtenus avec un filtre BSIF de taille (17×17) et une longueur de 10 bits (lorsque on a fixé la valeur de variation a 0.2). Dans ce cas, nous avons obtenu un taux de reconnaissance Rank-1 de 81% pour le mode d'identification et un taux d'erreur Equal Error Rate (EER) de 4.97% pour le mode de vérification.

Ces résultats démontrent l'efficacité du filtre BSIF de taille (17×17) et de longueur 10 bits pour la tâche de reconnaissance des caractéristiques étudiées dans cette expérience.

Tableau 1 EER/Rang-1 pour les différentes tailles du filtre

		Identification	**Vérification**			
Taille	**longueur**	**Rank-1 (%)**	**EER (%)**	**The minimal half total EER (%)**	**VR at 1% FAR (%)**	**VR at 0.1% FAR (%)**
17×17	12	62.25%	9.53%	9.12%	76.68%	60.82%
17×17	11	78.97%	6.05%	5.48%	88.13%	79.03%
17×17	10	81.00%	4.97%	4.60%	90.70%	82.40%
17×17	9	78.42%	5.30%	4.95%	89.58%	80.13%
17×17	8	65.63%	7.99%	7.58%	80.17%	62.25%
17×17	7	47.77%	13.58%	13.39%	59.08%	38.35%
17×17	6	25.80%	25.06%	24.33%	31.53%	16.40%
17×17	5	2.10%	45.34%	43.36%	5.70%	1.02%
15×15	12	53.42%	11.57%	11.20%	68.75%	51.13%
15×15	11	70.47%	7.69%	7.24%	82.70%	69.17%
15×15	10	75.90%	6.23%	5.89%	87.13%	76.65%
15×15	9	73.67%	6.18%	5.65%	87.45%	74.08%
15×15	8	62.20%	8.25%	7.84%	77.03%	59.40%
15×15	7	44.85%	15.63%	15.04%	54.05%	34.20%
15×15	6	16.48%	33.81%	32.64%	19.15%	8.77%
15×15	5	1.25%	47.45%	44.13%	4.80%	1.08%
13×13	12	39.88%	15.01%	14.39%	56.70%	36.88%
13×13	11	60.85%	9.42%	8.86%	76.30%	59.75%
13×13	10	66.77%	7.65%	7.20%	82.13%	67.92%
13×13	9	65.70%	7.64%	7.27%	82.47%	67.18%

13×13	8	56.43%	9.38%	8.97%	74.58%	55.05%
13×13	7	43.10%	11.25%	10.81%	65.15%	41.02%
13×13	6	15.35%	32.34%	31.43%	19.67%	8.67%
13×13	5	11.97%	23.59%	23.49%	25.50%	10.45%
11×11	12	23.43%	19.09%	18.83%	39.30%	19.95%
11×11	11	43.97%	12.92%	12.35%	62.63%	42.52%
11×11	10	54.43%	9.96%	9.61%	73.20%	54.35%
11×11	9	53.30%	9.08%	8.86%	75.25%	54.23%
11×11	8	47.50%	11.29%	10.87%	67.05%	45.57%
11×11	7	20.97%	31.37%	29.78%	22.25%	9.00%
11×11	6	11.75%	36.06%	34.99%	15.28%	6.43%
11×11	5	1.88%	46.87%	44.20%	4.75%	1.15%
9×9	12	11.45%	25.97%	25.74%	22.65%	8.55%
9×9	11	26.38%	18.52%	18.17%	43.85%	23.22%
9×9	10	35.43%	13.89%	13.59%	56.77%	33.85%
9×9	9	37.52%	12.76%	12.39%	61.93%	37.35%
9×9	8	35.20%	13.79%	13.48%	57.25%	33.58%
9×9	7	5.53%	42.29%	40.89%	7.15%	2.12%
9×9	6	16.15%	19.80%	19.75%	33.38%	13.65%
9×9	5	7.52%	25.77%	25.67%	20.83%	6.55%
7×7	12	5.00%	31.69%	31.42%	12.50%	3.67%
7×7	11	13.48%	25.56%	24.95%	26.40%	10.95%
7×7	10	22.40%	19.26%	18.90%	40.25%	20.03%
7×7	9	23.55%	17.02%	16.78%	45.95%	22.70%
7×7	8	22.38%	19.95%	19.52%	39.52%	18.43%
7×7	7	18.45%	19.21%	18.94%	37.70%	17.73%
7×7	6	2.17%	45.43%	44.26%	4.27%	1.15%
7×7	5	1.07%	47.65%	45.58%	3.17%	0.90%
5×5	12	2.38%	37.03%	36.67%	6.95%	1.65%
5×5	11	6.60%	30.52%	30.36%	16.07%	4.83%
5×5	10	11.85%	25.23%	24.98%	25.00%	9.72%
5×5	9	14.35%	21.89%	qwq21.73%	32.23%	12.00%
5×5	8	13.43%	22.91%	22.57%	29.85%	12.02%
5×5	7	4.32%	43.95%	42.61%	4.65%	1.18%

5×5	6	1.13%	47.29%	45.72%	3.05%	0.35%
5×5	5	0.47%	47.40%	46.01%	2.52%	0.70%
3×3	8	9.22%	26.58%	26.40%	22.72%	7.50%
3×3	7	6.45%	33.94%	33.43%	12.48%	3.90%
3×3	6	1.15%	47.14%	45.64%	2.92%	0.60%
3×3	5	0.40%	48.18%	46.74%	2.35%	0.25%

En fixant la taille du filtre BSIF à (17x17) et une longueur de 10 bits, nous avons ensuite varié la valeur de variation de l'algorithme TanTriggs de 0.1 à 2.5. Les résultats correspondants sont présentés dans le tableau 2.

Veuillez noter que **le tableau 2** présente les résultats obtenus en fonction des différentes valeurs de variation de TanTriggs.

Tableau 2 EER/Rang-1 en fonction des différentes valeurs de variation de TanTriggs.

Taille	**Longueur**	**Variance**	**Rank-1 (%)**	**EER (%)**	**Mht EER(%)**	**VR at 1% FAR**	**VR at 0.1% FAR**
17×17	10	0.1	54.63%	11.78%	11.28%	69.50%	52.02%
17×17	10	0.2	62.25%	9.53%	9.12%	76.68%	60.82%
17×17	10	0.3	62.75%	9.69%	9.23%	76.73%	61.12%
17×17	10	0.4	63.45%	9.76%	9.32%	76.77%	61.95%
17×17	10	0.5	62.98%	9.54%	9.02%	76.83%	62.15%
17×17	10	0.6	66.17%	8.83%	8.14%	79.42%	65.53%
17×17	10	0.7	68.05%	8.56%	8.12%	79.42%	66.70%
17×17	10	0.8	70.11%	8.04%	7.78%	80.11%	68.34%
17×17	10	0.9	71.92%	7.64%	7.20%	82.58%	71.08%
17×17	10	1	72.47%	7.53%	6.89%	83.73%	72.10%
17×17)	10	1.1	74.42%	7.17%	6.55%	85.22%	73.55%
17×17	10	1.2	75.52%	7.05%	6.30%	85.55%	75.02%
17×17	10	1.3	77.10%	6.74%	6.18%	86.42%	77.20%
17×17	10	1.4	77.85%	6.42%	5.91%	87.00%	78.20%
17×17	10	1.5	79.35%	5.90%	5.53%	88.45%	78.72%
17×17	10	1.6	79.90%	5.64%	5.24%	88.98%	79.75%
17×17	10	1.7	80.60%	5.65%	5.18%	89.02%	80.00%

17×17	10	1.8	81.35%	5.67%	5.11%	89.15%	81.27%
17×17	10	1.9	81.47%	5.46%	5.07%	89.52%	82.42%
17×17	10	2	82.88%	5.38%	5.02%	89.88%	83.13%
17×17	10	2.1	83.78%	3.49%	3.17%	93.77%	86.83%
17×17	10	2.2	84.08%	3.63%	3.35%	93.65%	87.02%
17×17	10	2.3	84.47%	3.47%	3.28%	93.97%	87.55%
17×17	10	2.4	85.63%	3.31%	3.07%	94.38%	89.00%
17×17	10	2.5	83.00%	4.19%	3.81%	92.77%	85.70%

Commentaires

D'après le tableau, nous avons observé que l'utilisation d'un filtre BSIF avec une taille de (17x17) et une longueur de 10 bits, ainsi qu'une valeur de variation de TanTriggs égale à 2.4, a donné de bons résultats en termes de taux de reconnaissance de rang 1 (85,63 %) et d'erreur plus faible par rapport aux autres tailles (3,31 %).

III.3.4.2 Les résultats obtenus par la méthode LPQ

Dans cette deuxième expérience, nous avons utilisé l'algorithme TT pour prétraiter les données et le filtre LPQ pour extraire les caractéristiques. Ensuite, nous avons appliqué l'algorithme KNN avec différentes distances pour effectuer la classification. Les résultats obtenus pour différentes tailles de fenêtre du descripteur LPQ sont récapitulés dans **le tableau 3**.

Les performances les plus élevées ont été obtenues avec une taille de fenêtre de 19. À cette valeur, nous avons obtenu un taux de reconnaissance Rank-1 de 99,85% pour le mode d'identification et un taux d'erreur Equal Error Rate (EER) de 0,00% pour le mode de vérification.

Ces résultats démontrent l'efficacité du filtre LPQ avec une taille de fenêtre de 19 pour la tâche de reconnaissance des caractéristiques étudiées dans cette expérience. De plus, un EER de 0,00% pour le mode de vérification indique qu'aucune erreur de classification n'a été commise lors de la vérification des identités, ce qui est un résultat excellent. Par conséquent, la taille de fenêtre 19 a été sélectionnée pour la suite des expérimentations.

Tableau 3 Rank -1/EER pour les différentes tailles de la fenêtre de LPQ descripteur

Tf	Rank-1	EER	The minimal half total error rate equals	The verification rate at 1% FAR equals (%)	The verification rate at 0.1% FAR equals (%)
5	92.38%	1.12%	1.10%	98.78%	96.00%
7	97.35%	0.38%	0.38%	99.83%	99.45%
9	99.15%	0.10%	0.07%	99.98%	99.90%
11	99.65%	0.10%	0.06%	100.00%	99.90%
13	99.83%	0.02%	0.02%	100.00%	100.00%
15	99.70%	0.04%	0.01%	100.00%	100.00%
17	99.60%	0.00%	0.00%	100.00%	100.00%
19	99.85%	0.00%	0.00%	100.00%	100.00%

TB= tailles de bloc, MhTEER (%)=The minimal half total error rate equals

Le tableau 04 présente les résultats de Rank-1/EER pour différentes tailles de blocs d'image. En maintenant la taille de fenêtre à 19, nous avons varié les tailles de blocs d'image et observé les performances. Les meilleures performances ont été obtenues avec une taille de bloc de 15. Dans ce cas, nous avons obtenu un taux de reconnaissance Rank-1 de 99,92% pour le mode d'identification et un taux d'erreur Equal Error Rate (EER) de 0,02% pour le mode de vérification.

Ces résultats mettent en évidence l'efficacité du filtre LPQ avec une taille de bloc de 15 pour la tâche de reconnaissance des caractéristiques étudiées dans cette expérience. De plus, un EER de 0,02% pour le mode de vérification indique qu'aucune erreur de classification n'a été commise lors de la vérification des identités, ce qui est un résultat excellent. Par conséquent, la taille de bloc de 15 a été déterminée comme le paramètre optimal dans notre approche.

Tableau 4 Rank -1/EER pour les différentes tailles de bloc d'image

TB	RANK-1(%)	EER(%)	MHTEER (%)	VR at 1% FAR (%)	VR at 0.1% FAR (%)
[18 18]	99.88%	0.00%	0.00%	100.00%	100.00%
[17 17]	99.90%	0.02%	0.02%	100.00%	100.00%
[16 16]	99.90%	0.00%	0.00%	100.00%	100.00%
[15 15]	99.92%	0.02%	0.01%	100.00%	100.00%

Le tableau 05 présente les résultats de Rank-1/EER pour différentes tailles de bordure. En maintenant la taille de bloc à 15, nous avons fait varier les tailles de bordure et évalué les performances. Les meilleures performances ont été obtenues avec une taille de bordure de [2]. Dans ce cas, nous avons obtenu un taux de reconnaissance Rank-1 de 99,92% pour le mode d'identification et un taux d'erreur Equal Error Rate (EER) de 0,00% pour le mode de vérification.

Ces résultats démontrent l'efficacité du filtre LPQ avec une taille de bordure de [2] pour la tâche de reconnaissance des caractéristiques étudiées dans cette expérience. De plus, un EER de 0,00% pour le mode de vérification indique qu'aucune erreur de classification n'a été commise lors de la vérification des identités, ce qui est un excellent résultat. Par conséquent, la taille de bordure de [2] a été déterminée comme le paramètre optimal dans notre approche.

Tableau 5 Rank -1/EER pour la taille de la bordure

TB	RANK-1(%)	EER(%)	MHTEER (%)	VR at 1% FAR (%)	VR at 0.1% FAR (%)
[1 1]	99.90%	0.00%	0.00%	100.00%	100.00%
[2 2]	99.92%	0.00%	0.00%	100.00%	100.00%
[4 4]	99.85%	0.00%	0.00%	100.00%	100.00%
[6 6]	99.79%	0.00%	0.00%	100.00%	100.00%
[8 8]	99.85%	0.00%	0.00%	100.00%	100.00%

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

- ✓ la taille de fenêtre : 19
- ✓ la taille de bloc : [15 15]
- ✓ la taille de la bordure : [2 2]

III.3.4.3 Les résultats obtenus par la méthode HOG

Le tableau 06 présente les résultats de Rank-1/EER pour différentes tailles de cellule. Nous avons modifié les tailles de cellule et évalué les performances. Les meilleures performances ont été obtenues avec une taille de [8]. Dans ce cas, nous avons obtenu un taux de reconnaissance Rank-1 de 79,40% pour le mode d'identification et un taux d'erreur Equal Error Rate (EER) de 4,20% pour le mode de vérification.

Ces résultats mettent en évidence l'efficacité du filtre HOG avec une taille de cellule de [8] pour la tâche de reconnaissance des caractéristiques étudiées dans cette expérience. Par conséquent, la taille de cellule de [8] a été déterminée comme le paramètre optimal dans notre approche.

Tableau 6 Rank -1/EER pour différentes Taille de cellule

TC	RANK-1(%)	EER(%)	MHTEER (%)	VR at 1% FAR (%)	VR at 0.1% FAR (%)
[8 8]	79.40%	4.20%	3.92%	91.63%	82.58%
[16 16]	71.45%	5.84%	4.95%	87.40%	70.60%
[32 32]	58.90%	9.15%	8.74%	75.50%	53.37%

Le tableau 07 présente les résultats de Rank-1/EER pour différentes tailles de blocs. Nous avons modifié les tailles de blocs et évalué les performances. Les meilleures performances ont été obtenues avec une taille de [2]. Dans ce cas, nous avons obtenu un taux de reconnaissance

Rank -1 de 80,89% pour le mode d'identification et un taux d'erreur Equal Error Rate (EER) de 4,13% pour le mode de vérification.

Ces résultats mettent en évidence l'efficacité du filtre HOG avec une taille de bloc de [2] pour la tâche de reconnaissance des caractéristiques étudiées dans cette expérience. Par conséquent, la taille de bloc de [2] a été déterminée comme le paramètre optimal dans notre approche.

Tableau 7 Rank -1/EER pour différentes Tailles de bloc

Tb	RANK-1(%)	EER(%)	MHTEER (%)	VR at 1% FAR (%)	VR at 0.1% FAR (%)
[2 2]	80.89%	4.13%	3.89%	91.45%	84.22%
[4 4]	80.33%	4.17%	4.12%	91.65%	82.53%
[6 6]	77.13%	4.85%	4.65%	89.90%	79.45%
[8 8]	80.74%	4.30%	4.10%	91.00%	83.66%

Le tableau 08 présente les résultats de Rank-1/EER pour différents chevauchements de blocs. En maintenant les tailles de blocs et de cellules fixées aux valeurs optimales, nous avons varié le chevauchement des blocs et évalué les performances. Les meilleures performances ont été obtenues avec un chevauchement de blocs de [1 1]. Dans ce cas, nous avons obtenu un taux de reconnaissance Rank-1 de 81,15% pour le mode d'identification et un taux d'erreur Equal Error Rate (EER) de 4,12% pour le mode de vérification.

Par conséquent, la taille de chevauchement de blocs de [1 1] a été déterminée comme le paramètre optimal dans notre approche.

Tableau 8 Rank -1/EER pour différentes chevauchement de bloc

Chevauchement de bloc	RANK-1(%)	EER(%)	MHTEER (%)	VR at 1% FAR (%)	VR at 0.1% FAR (%)
[1 1]	81.15%	4.12%	3.85%	92.00%	84.15%
[2 2]	74.69%	5.69%	4.78%	90.21%	81.44%

Le tableau 09 présente les résultats de Rank-1/EER pour différents nombres de classes. En utilisant les résultats optimaux obtenus précédemment, nous avons évalué les performances pour différentes configurations de nombres de classes. Les meilleures performances ont été obtenues avec un nombre de classe de [19]. Dans cette configuration, nous avons obtenu un

taux de reconnaissance Rank-1 de 81,33% pour le mode d'identification et un taux d'erreur Equal Error Rate (EER) de 4,10% pour le mode de vérification.

Par conséquent, le nombre de classe [19] a été déterminé comme le paramètre optimal dans notre approche.

Tableau 9 Rank -1/EER pour différentes nombre de classes

Nombre de classes	RANK-1(%)	EER(%)	MHTEER (%)	VR at 1% FAR (%)	VR at 0.1% FAR (%)
9	79.40%	4.20%	3.92%	91.63%	82.58%
12	79.72%	4.44%	4.26%	91.25%	82.45%
15	80.33%	4.06%	3.83%	91.70%	83.70%
16	78.95%	4.44%	4.10%	92.00%	83.80%
17	80.50%	4.06%	3.95%	92.30%	84.30%
18	81.15%	4.12%	3.85%	92.00%	84.15%
19	81.33%	4.10%	3.86%	92.15%	84.22%

III.3.4.5 Distances :

Dans le tableau 10 Dans le tableau 10, nous constatons que le taux de reconnaissance Rank-1 (%) est le même et égal à 87,75 % pour toutes les configurations. Cependant, il y a eu une erreur lors de la modification du taux d'erreur Equal Error Rate (EER) dans la méthode BSIF.

Tableau 10 Performances des méthodes proposées en utilisant différentes distances.

Method	Mahcos		cos		Ctb		Euc	
	Rank-1(%)	EER	Rank-1(%)	EER	Rank-1(%)	EER	Rank-1(%)	EER
HOG	87.75%	2.80%	88.70%	2.60%	84.75%	3.34%	86.70%	2.95%
BSIF	87.75%	4.05%	88.70%	3.85%	84.75%	5.60%	86.70%	4.72%
LPQ	87.75%	2.80%	88.70%	2.60%	84.75%	3.34%	86.70%	2.95%

III.3.4.6 Méthode proposée de palmprint multi spectrale

Le tableau 11 présente une méthode de reconnaissance de personnes basée sur le palmprint multi-spectral en utilisant les filtres de HOG, BSIF et LPQ. Trois méthodes ont été proposées et les résultats expérimentaux démontrent leur supériorité par rapport aux méthodes existantes dans la littérature en termes de performances. De plus, il a été confirmé que les systèmes biométriques multimodaux surpassent les systèmes monomodaux.

La configuration qui a donné les meilleurs résultats est celle de la somme pondérée. Dans cette configuration, un taux de reconnaissance Rank-1 de 99,95 % et un taux d'erreur Equal Error Rate (EER) de 0,02 % ont été obtenus. Il est important de noter qu'aucune erreur de classification n'a été observée lors de la vérification des identités, ce qui est un résultat remarquable.

Tableau 11 Rank -1/EER pour différentes méthodes

	Rank-1	**EER**	**MHT EER**	**VR1%FAR(%)**	**VR0.1%FAR(%)**
Somme	99.87%	0.05%	0.04%	100.00%	99.98%
Max	98.55%	0.33%	0.33%	99.83%	98.88%
Min	98.80%	0.07%	0.06%	100.00%	99.95%
Somme pondérée	99.95%	0.02%	0.01%	100.00%	100.00%

III.7 Conclusion

Dans ce chapitre, nous avons développé un système d'identification des personnes basé sur la reconnaissance 3D palmprint. Pour ce faire, nous avons proposé plusieurs systèmes biométriques, comprenant à la fois des systèmes monomodaux et multimodaux. L'objectif était d'améliorer le taux d'identification des modalités lors des processus d'identification et de vérification.

En testant ces systèmes sur une base de données comprenant 400 personnes, nous avons observé une amélioration significative du taux d'identification, atteignant 99,95 %. Ces résultats démontrent l'efficacité de notre travail dans la reconnaissance 3D palmprint et confirment leur potentiel pour des applications biométriques.

Conclusion générale

En conclusion, ce mémoire a présenté un système de reconnaissance des personnes basé sur les 3D palmprint. Différentes approches biométriques, tant monomodales que multimodales, ont été proposées pour améliorer le taux d'identification et de vérification. Les résultats expérimentaux ont démontré l'efficacité de ces approches, avec des performances supérieures à celles des méthodes existantes dans la littérature.

Le système de reconnaissance des 3D palmprints en a atteint un taux de reconnaissance Rank-1 de 99.95% et un taux d'erreur Equal Error Rate (EER) de 0.02% lors du mode de vérification. De plus, aucune erreur de classification n'a été observée lors de la vérification des identités, ce qui souligne la fiabilité et l'exactitude du système.

Ces résultats démontrent le potentiel et l'applicabilité de 3D palmprint en tant que modalité biométrique pour la reconnaissance des personnes. Les avancées réalisées dans ce domaine ouvrent la voie à des applications pratiques dans des domaines tels que la sécurité, le contrôle d'accès et la surveillance.

Il convient de souligner que ce mémoire n'est qu'une étape dans la recherche continue sur la reconnaissance des personnes par 3D palmprint. Des améliorations supplémentaires peuvent être envisagées, telles que l'utilisation de techniques d'apprentissage en profondeur ou l'exploration de nouvelles caractéristiques biométriques.

En fin de compte, ce mémoire contribue à l'avancement des systèmes de reconnaissance des personnes et ouvre des perspectives intéressantes pour des développements futurs dans le domaine de la biométrie.

Références bibliographiques

1. E. Krichen, “Reconnaissance des personnes par l’iris en mode dégradé,” Ph.D. dissertation, Evry, Institut national des télécommunications, 2007
2. S.Boudjelial, " detection et identification d’individu par méthode biométrique ".UMMTO.2014
3. Détection directe des minuties en niveaux de gris dans les empreintes digitales,”Transactions IEEE sur l’analyse de modèles et l’intelligence artificielle, vol. 19, pp. 27–40.
4. A.Murhula, " Conception et mise en place d'une plateforme de sécurisation par synthese et reconnaissance biométrique de documents de traffic ". Polytechnique_INITELEMATIQUE_BURUNDI - Ingénieur Civil en Informatique et télécommunications 2015.
5. F.Perronnin, J. Dugelay, “An Introduction to Biometrics Audio and Video-Based Person Authentification ”. Volume 19 – n4,2002.
6. M.Moulay, M.Arbaoui, "authentification des personnes par l’articulation du doigt " UNIVERSITE KASDI MERBAH OUARGLA.2015
7. Martin, A., Sellen, A., & Whittaker, S. (2016). Understanding typing behavior: A comparative analysis of typing dynamics across different input devices. In Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (pp. 3698-3709). ACM.
8. M.Moulay, M.Arbaoui, "authentification des personnes par l’articulation du doigt " UNIVERSITE KASDI MERBAH OUARGLA.2015.
9. A.Meraoumia, "Modèle de Markov caché applique à la multi biométrie " USTHB. 2014.
10. Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2009). Handbook of fingerprint

recognition. Springer Science & Business Media.

11. Jain, A.K., Ross, A., & Nandakumar, K. (2016). Introduction to Biometrics. Springer. https://doi.org/10.1007/978-0-387-77326-3

12. John Daugman, "How Iris Recognition Works", IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 21-30, Jan. 2004

13. "Joint Fingerprint Recognition: A Review" de Muhammad Sharif et al., publié dans la revue IEEE Access en 2018 : cet article propose une revue des travaux de recherche sur la reconnaissance des empreintes des articulations des doigts, avec une présentation des différentes techniques utilisées et de leurs performances"Palmprint Recognition: A Review" par Mayank Vatsa, Richa Singh, Afzel Noore, et Ajay Kumar, publié dans IEEE Transactions on Systems, Man, and Cybernetics: System en 2014

14. CHAA, Mourad. Système de reconnaissance de personne par des techniques biométriques. 2017. PhD Thèses. Université Ferhat Abbas.

15. . ACHRAF, B. E. N.; FOUZIA MANEL, CHAIBI. Système de reconnaissance des personnes par 3D palmprint. mémoire. UNIVERSITY OF KASDI MERBAH OUARGLA.

16. . ELMECHRI, ADJAINE; ABDELKARIM, BENSLIMAN; MZ TIDJANI, MK BENSID. Authentification et Identification biométrique des personnes par les empreintes palmaires.

17. BERREDJEM, Achref. La re connaissance des individus par leur empreinte des articulations des doigts. 2019.

18. ALATISE, Mary B.; HANCKE, Gerhard P. A review on challenges of autonomous mobile robot and sensor fusion methods. IEEE Access, 2020, 8: 39830-39846.

19. ZAHOUA, BAMBARA; RACHA, ZITOUN. Reconnaissance biométrique de

personnes par les empreintes palmaires 3D et l'apprentissage profond. mémoire. Université Kasdi Merbah OUARGLA.

20. BOUTELBA, Adem; BOUMELIHA, Hemza; BOUATMANE, Sabrina Encadreur. Reconnaissance de visages par les formes locales binaires LBP. 2018. PhD Thesis. Université de Jijel.

21. BERGER, Jean-Louis. Analyse factorielle exploratoire et analyse en composantes principales: guide pratique. 2021.

22. NABILA, MERAMRIA. Reconnaissance de visages par Analyse Discriminante Linéaire (LDA). Mémoire de master, Université Badji Mokhtar Annaba, 2016.

23. . TOUAHRI, ISLAM. Détection et Classification des Véhicules par Réseaux de Neurones à Convolution CNN. 2020.

24. STEINBACH, Michael; TAN, Pang-Ning. kNN: k-nearest neighbors. In: The top ten algorithms in data mining. Chapman and Hall/CRC, 2009. p. 165-176.

25. NOBLE, William S. What is a support vector machine?. Nature biotechnology, 2006, 24.12: 1565-1567.

26. Zhang, D., Lu, G., Li, W., et al.: 'Three dimensional palmprint recognition using structured light imaging'. IEEE 2008 2nd IEEE Int. Conf. on Biometrics: Theory, Applications and Systems (BTAS 2008), Arlington, USA, 2008.