الجمهورية الجزائرية الديمقراطية الشعبية
Republique Algerienne Democratique et Populaire
وزارة التعليم العالي والبحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
جامعة الشهيد الشيخ العربي التبسي – تبسة
Université Echahid Cheikh Larbi Tébessi – Tébessa
Faculté des Sciences et de la Technologie
Département de d'Électronique et Télécommunications

MEMOIRE

Présenté pour l'obtention du **diplôme** de **Master Académique**

Filière : Télécommunications

Spécialité : Réseaux et Télécommunications

Par: - ZERGUI Aymen
- KABOUR Kheireddine

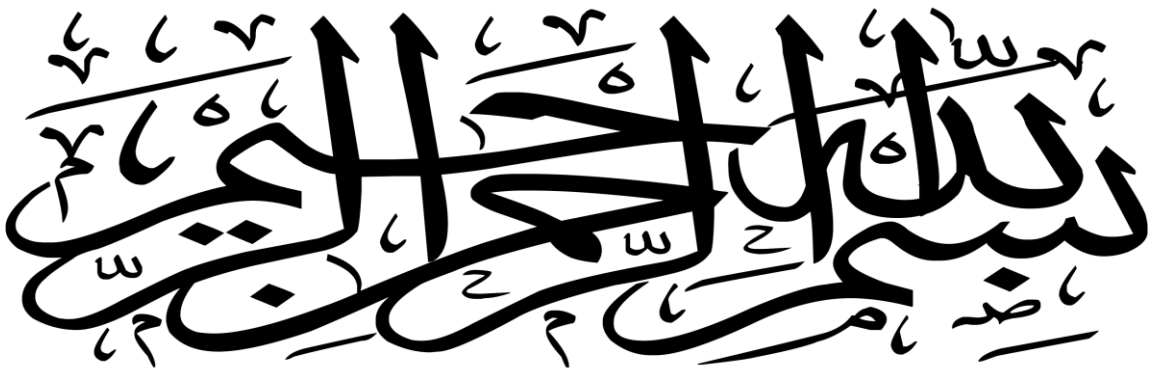
THEME

Reconnaissance des personnes utilisant la multi-représentation de l'empreinte palmaire

Présenté et évalué, le 27/06/2024, par le jury composé de :

Nom et prénom		Grade	Qualité
Dr.	Lotfi HOUAM	MCB	Président
Dr.	Mohamed SAIGAA	MCB	Rapporteur
Mme.	Malika OUACIFI	MAA	Examinatrice

Promotion : 2023/2024



"قَالُوا سُبْحَانَكَ لَا عِلْمَ لَنَا إِلَّا
مَا عَلَّمْتَنَا ۖ إِنَّكَ
أَنْتَ الْعَلِيمُ الْحَكِيمُ"

(صدق الله العظيم)

الآية 32 من سورة البقرة

Remerciements

En préambule à ce mémoire je remercie mon dieu qui m'a aidé et m'a donné la patience et le courage durant ces langues années d'études.

Je souhaite adresser mes remerciements les plus sincères aux personnes qui m'ont apporté leurs aides et qui ont contribué

À l'élaboration de ce mémoire ainsi qu'à la réussite de cette formidable année universitaire.
Ces remerciements vont tout d'abord au corps professoral et administratif du département de l'électronique et télécommunications.

Je tiens à remercier sincèrement mon encadreur Dr. Saigaà de ce mémoire, il était toujours à l'écoute et très disponible tout au long de la réalisation de ce mémoire, ainsi pour l'inspiration, l'aide et le temps qu'elle a bien voulu me consacrer et sans elle ce mémoire n'aurait jamais vu le jour.

Je n'oublie pas mes parents pour leur contribution, leur soutien et leur patience.

Enfin, j'adresse mes plus sincères remerciements à tous mes proches amis, qui m'ont toujours soutenu et encouragé au cours de la réalisation de ce mémoire.

Aymen ZERGUI

Merci

Remerciements

En préambule à ce mémoire je remercie mon dieu qui m'a aidé et m'a donné la patience et le courage durant ces langues années d'études.

Je souhaite adresser mes remerciements les plus sincères aux personnes qui m'ont apporté leurs aides et qui ont contribué

À l'élaboration de ce mémoire ainsi qu'à la réussite de cette formidable année universitaire.
Ces remerciements vont tout d'abord au corps professoral et administratif du département de l'électronique.

Je tiens à remercier sincèrement mon encadreur Dr. Saigaà de ce mémoire, il était toujours à l'écoute et très disponible tout au long de la réalisation de ce mémoire, ainsi pour l'inspiration, l'aide et le temps qu'elle a bien voulu me consacrer et sans elle ce mémoire n'aurait jamais vu le jour.

Je n'oublie pas mes parents pour leur contribution, leur soutien et leur patience.

Enfin, j'adresse mes plus sincères remerciements à tous mes proches amis, qui m'ont toujours soutenu et encouragé au cours de la réalisation de ce mémoire.

Kheireddine KEBBOUR

Merci

Dédicace

Je dédie ce travail à la source de tendresse ma chère maman.

Tout en étant convaincue que mon succès est une récompense pour tous leurs sacrifices, qu'elles trouvent ici l'expression de ma plus profonde gratitude.

A ma sœur.

A mes frères achraf et adlen.

A mes grands-parents, et toute la famille Zergui.

A mes meilleurs amis,

A mes camarades les étudiants de Telecom

A tous ceux que je connais de près ou de loin.

AYMEN

Dédicace

Je dédie ce travail à la source de tendresse que sont mes très chers parents.

Tout en étant convaincue que mon succès est une récompense pour tous leurs sacrifices, qu'ils trouvent ici l'expression de ma plus profonde gratitude.

A ma sœur.

A mon frère.

A mes grands-parents, et toute la famille KEBBOUR et YOUSFI

A mes meilleurs amis

A mes camarades les étudiants de Telecom

A tous ceux que je connais de près ou de loin.

KHEIREDDINE

Résumé

La biométrie, qui se base sur des traits physiologiques et comportementaux spécifiques pour identifier un individu, connaît une croissance de sa popularité dans de nombreuses applications de sécurité gouvernementales, criminelles, militaires et commerciales.

Les empreintes de palme sont une technique physiologique qui est réalisée à partir de la main humaine et qui a démontré sa fiabilité et son acceptabilité par les utilisateurs dans de nombreuses applications de sécurité. Au début de notre travail, nous avons commencé par extraire les caractéristiques en utilisant les méthodes simplifiées HOG et LPQ, puis nous les avons normalisées dans le code MATLAB. La reconnaissance rapide des images d'empreintes palmaires et des caractéristiques est l'objectif principal de ces deux méthodes, car l'extraction des caractéristiques est une étape essentielle dans un système biométrique.

Pour les empreintes palmaires, nous avons également développé des algorithmes de classification et de reconnaissance, et c'est pourquoi nous proposons deux méthodes d'apprentissage automatique à l'aide de SVM et de KNN. Les résultats obtenus montrent de manière évidente que les méthodes d'extraction de caractéristiques et de classification proposées, basées sur l'apprentissage automatique, peuvent être efficaces.

Mots-clés : Biométrie, apprentissage automatique, empreinte palmaire, extraction des caractéristiques, classification.

Abstract

Biometrics, which relies on specific physiological and behavioural traits to identify an individual, is growing in popularity in many government, criminal, military and commercial security applications.

Palmprints are a physiological technique that is made from the human hand and has proven to be reliable and acceptable to users in many security applications. At the start of our work, we first extracted the features using the simplified HOG and LPQ methods, and then normalised them in MATLAB code. Rapid recognition of palmprint images and features is the main objective of both methods, as feature extraction is an essential step in a biometric system.

For palmprints, we have also developed classification and recognition algorithms, so we propose two machine learning methods using SVM and KNN. The results obtained clearly show that the proposed feature extraction and classification methods, based on machine learning, can be effective.

Keywords: Biometrics, machine learning, palmprint, feature extraction, classification.

ملخص

تزداد شعبية القياسات البيو مترية، التي تعتمد تعتمد على سمات فيزيولوجية وسلوكية محددة لتحديد هوية الفرد، في العديد من التطبيقات الأمنية الحكومية والجنائية والعسكرية والتجارية.

بصمات الكف هي تقنية فيزيولوجية من اليد البشرية و أثبتت أنها موثوقة و مقبولة للمستخدمين في العديد من التطبيقات الأمنية، في بداية عملنا قمنا أولا باستخراج الميزات باستخدام طريقتين مبسطتين هما (هوق و أل بي كي) ، ثم قمنا بتطبيعها في كود ماطلاب , إن التعرف السريع على صورة بصمة الكف و ميزاتها هو الهدف الرئيسي لكلتا الطريقتين , حيث أن إستخراج السمات هو خطوة أساسية في نظام القياسات الحيوية .

بالنسبة لبصمات الكف قمنا أيضا باستعمال تقنيات التصنيف والتعرف لذا اقترحنا طريقتين للتعلم الالي باستخدام(اس في ام و كا ان ان) تظهر النتائج التي تم الحصول عليها بوضوح أن طرق استخراج السمات والتصنيف المقترحة بناءا على التعلم الآلي يمكن أن تكون فعالة.

الكلمات المفتاحية: القياسات الحيوية، التعلم الآلي، بصمة اليد، استخلاص السمات، التصنيف.

Sommaire

Chapitre II

Extraction des caractéristiques

Chapitre III

Résultats expérimentaux

Table des figures

Chapitre I
Introduction à la biométrie

Chapitre II
Extraction des caractéristiques

Chapitre III
Résultats expérimentaux

Liste des tableaux

Chapitre III
Résultats expérimentaux

glossaire

ADN	***Acide désoxyribonucléique.***
CMC	*Cumulative Match Characteristic.*
DET	*Detection Error Tradeoff.*
EER	*Taux d'erreur égal.*
FAR	*Taux de fausses acceptations.*
FPR	*Taux de faux positifs.*
FRR	*Taux de faux rejets.*
GAR	*Taux d'acceptation authentique.*
HOG	*Histogram of Oriented Gradients.*
KNN	*k-Nearest Neighbors.*
LPQ	*Local Phase Quantization.*
PLV	*la modalité des veines de la paume.*
RPR	*Rang de reconnaissance parfaite.*
ROC	*Receiver Operating Characteristic.*
ROR	*Reconnaissance au premier rang.*
SVM	*Support Vector Machine.*
TPR	*Taux de vrais positifs.*
2DWFT	*Transformée Discrète de Fourrier à fenêtre à Deux Dimensions.*

Introduction générale

Récemment, tous les pays ont embrassé la transformation numérique dans divers secteurs, la voyant comme une solution miracle pour le développement de leur économie, industrie, santé, services, etc. En réalité, il n'existe pas d'autre alternative que d'adopter ces avancées technologiques pour rester compétitifs face aux pays développés [1]. De nombreux réseaux électroniques, qu'ils soient publics ou privés, se sont unis dans un vaste consortium international de réseaux, connu sous le nom d'Internet. Ce réseau est actuellement le plus populaire, le plus accessible et celui qui transporte le plus d'informations parmi tous les autres réseaux informatiques publics ou privés [2]. Étant donné que la majorité des données sur ce réseau sont vulnérables au vol ou à la fraude, la confiance des utilisateurs devient un élément fondamental et crucial pour la plupart des services en ligne. Par conséquent, la sécurité de l'information est essentielle pour maintenir cette confiance. C'est pourquoi les créateurs de services se sont penchés sur des méthodes de sécurisation de l'information, en introduisant de nouvelles approches basées sur des méthodes biométriques pour l'authentification de l'identité, plutôt que sur les méthodes traditionnelles basées sur la connaissance (mots de passe) ou sur la possession (cartes d'identité) [3].

Le domaine de la biométrie est crucial pour la sécurité de l'information en authentifiant les individus et en contrôlant l'accès aux données sensibles, assurant ainsi l'intégrité des informations dans une société de plus en plus connectée [4]. La technologie biométrique vérifie ou identifie des individus en fonction de leurs caractéristiques uniques, et joue un rôle essentiel dans divers secteurs tels que la sécurité, la santé et le e-commerce. Les applications biométriques vont du contrôle d'accès logique et physique à l'amélioration de la vérification d'identité dans les transactions financières et les documents de voyage [5]. Le domaine de la biométrie continue de progresser, avec des recherches visant à améliorer la précision de l'identification et à explorer de nouvelles modalités. En effet, la biométrie est un outil indispensable pour renforcer la sécurité,

l'authentification et la gestion de l'identité dans divers domaines technologiques et sociétaux. Généralement, dans un système biométrique, l'étape d'extraction des caractéristiques (ou extraction du vecteur d'observations) est la plus cruciale du processus de reconnaissance [6]. Les différentes méthodes proposées dans la littérature pour cette étape ont montré que l'image (par exemple, l'empreinte palmaire) contient principalement trois types d'informations : la texture, les lignes et l'apparence. Un vecteur de caractéristiques représente les traits discriminants de l'image avec, en général, une dimension réduite par rapport à l'image originale. Ce vecteur peut être directement utilisé pour la reconnaissance en mesurant la similarité entre le vecteur de test et celui de référence.

Les systèmes unimodaux d'authentification biométrique, qui reposent sur une seule caractéristique biométrique, présentent certaines contraintes. L'une des principales limitations réside dans la possibilité d'usurpation ou de contournement du système en utilisant des techniques de contrefaçon ou de copie de la caractéristique biométrique. Par exemple, il est possible de reproduire une empreinte digitale à partir d'une trace laissée sur une surface, ou d'utiliser une image du visage pour tromper un système de reconnaissance faciale. C'est là qu'intervient l'authentification biométrique multimodale [7]. Les systèmes d'authentification multimodale combinent différentes caractéristiques biométriques telles que l'empreinte digitale, la reconnaissance faciale et la voix pour renforcer la sécurité et améliorer la précision de l'identification. En intégrant plusieurs modalités (ou représentations), il devient possible de réduire les limitations propres à chaque modalité individuelle. L'authentification biométrique multimodale présente de nombreux avantages. Tout d'abord, elle accroît la précision de l'identification en utilisant plusieurs sources de données pour vérifier l'identité d'une personne. En croisant les caractéristiques biométriques, elle minimise les risques d'erreurs d'identification. De plus, l'utilisation de méthodes variées renforce la résistance aux tentatives de contournement et de fraude. L'objectif de ce mémoire est de concevoir un système permettant d'identifier de manière fiable l'identité des individus à partir de leurs empreintes palmaires. Ce système biométrique utilise des classifiers : les k plus proches voisins (K-Nearest Neighbors-KNN) et machines à vecteurs de support (Support Vector Machines-SVM). Ces classifiers prennent en entrée des vecteurs de caractéristiques extraits des empreintes palmaires à l'aide de deux méthodes bien établies: l'histogramme de gradient orienté (Histogram of Oriented Gradients-HOG) [8] et les caractéristiques statistiques des images binarisées (Local Phase Quantization Features-LPQ) [9].

Pour atteindre notre objectif, cette thèse est organisée en trois chapitres :

Le premier chapitre présente un aperçu général de la biométrie, couvrant en détail les différentes modalités biométriques ainsi que la structure et le fonctionnement des systèmes biométriques.

Dans le deuxième chapitre, nous examinerons le système de reconnaissance biométrique utilisant les empreintes palmaires. Ce chapitre explore la fusion de données, en abordant différents scénarios et niveaux de fusion, en particulier la fusion au niveau des scores.

La mise en œuvre des méthodes étudiées est présentée dans le troisième chapitre ainsi que les résultats expérimentaux qui sont exprimé par des systèmes biométriques unimodaux et multimodaux.

Enfin, une conclusion générale incluant les perspectives que nous envisagerons est donnée à la fin de ce mémoire.

1.1.Introduction

Dans un monde où la sécurité des informations et des accès est devenue une priorité absolue, les technologies biométriques jouent un rôle crucial en offrant des solutions d'identification et de vérification d'identité plus sûres et plus fiables que les méthodes traditionnelles. La biométrie, qui repose sur des caractéristiques physiques et comportementales uniques telles que les empreintes digitales, la reconnaissance faciale, l'iris et la voix, est devenue une technologie clé dans de nombreux domaines, allant des services financiers à la sécurité nationale.

1.2.Biométrie

On peut définir la biométrie comme l'exploitation de caractéristiques biologiques spécifiques afin d'identifier et de vérifier les individus. Des éléments tels que les empreintes digitales, la reconnaissance faciale, les traits de la rétine, la forme de la main ou de la paume, la voix, ou encore les modèles de frappe au clavier peuvent être inclus dans ces caractéristiques.

La biométrie repose sur l'idée que chaque personne possède des caractéristiques physiques ou comportementales qui la différencient des autres personnes. On enregistre ces caractéristiques à l'aide de systèmes de capture spécifiques, comme des scanners d'empreintes digitales, des caméras de reconnaissance faciale ou des systèmes de reconnaissance vocale [01].

Les caractéristiques biométriques sont difficiles à falsifier ou à reproduire, ce qui permet d'identifier les individus de manière fiable et précise. Elle présente des bénéfices tels qu'une protection accrue, une utilisation simple et une diminution des fraudes.

1.3.Modalités biométriques

Les caractéristiques physiques ou comportementales utilisées dans le domaine de la biométrie pour l'identification et l'authentification des personnes sont appelées modalités biométriques. Différents types de modalités biométriques existent, chacune étant liée à des caractéristiques particulières [03].

1.3.1. Modalités biométriques physiques

La biométrie utilise les modalités biométriques physiques pour identifier et authentifier les individus en utilisant des caractéristiques anatomiques distinctives. Ces modalités reposent sur des caractéristiques physiques uniques et propres à chaque personne. Incluent les empreintes digitales, les traits du visage, les iris, la rétine, la géométrie de la main, la forme de l'oreille et la vascularisation de la main ou du doigt. Chacune de ces approches présente des caractéristiques

Spécifiques qui les rendent adaptées à l'identification biométrique [03]. Cependant, l'emploi des modalités biométriques physiques comporte aussi quelques désavantages. En premier lieu, leur installation et leur entretien peuvent entraîner des dépenses importantes. Ensuite, elles peuvent prendre du temps et demander une procédure laborieuse lors de leur usage. Ensuite, leur utilisation dans des environnements spécifiques peut être plus difficile, comme dans des conditions de faible luminosité ou des environnements bruyants.

- **Empreinte palmaire** : Les traces de la paume sont des traces particulières qui se retrouvent sur la surface de la paume de la main d'un individu et qui sont propres à chaque personne. On utilise ces caractéristiques pour repérer et confirmer l'identité d'une personne [03].

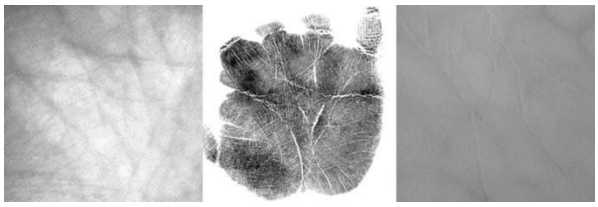


Figure 1.1. *Empreinte palmaire*

- **Reconnaissance de l'iris :** La reconnaissance de l'iris est une technique biométrique qui tire parti des particularités de l'iris de l'œil d'un individu afin de l'identifier. Elle consiste à prendre une photo de l'iris et à la comparer avec une base de données d'iris préalablement enregistrée. Les applications de sécurité utilisent fréquemment la reconnaissance de l'iris, comme le contrôle d'accès et la prévention de la fraude [04].

Figure 1.2. *Empreinte de l'iris*

- **Reconnaissance des empreintes digitales :** La méthode biométrique de reconnaissance des empreintes digitales utilise les motifs caractéristiques présents sur les crêtes des doigts d'une personne afin de l'identifier. Son objectif est de numériser l'empreinte digitale d'une personne et de la comparer à une base de données d'empreintes digitales préalablement enregistrées [04].

Figure 1. 3. *Empreinte digitale*

- **Reconnaissance faciale :** L'identification faciale est une technique biométrique qui utilise les traits caractéristiques du visage afin d'identifier une personne. Elle fonctionne en confrontant en temps réel les caractéristiques faciales d'une personne présente dans une image ou une vidéo à une base de données de visages connus. Il est fréquent d'utiliser la reconnaissance faciale dans des applications de sécurité comme le contrôle d'accès et la détection de fraudes [03]**.**

Figure 1.4. *Empreinte Faciale*

- **Empreinte de doigt :** L'empreinte de doigt est un motif unique créé par les papilles de la surface des doigts, qui est utilisé pour l'identification et la vérification biométrique dans différents domaines tels que la sécurité, la criminalistique et les technologies de reconnaissance. Elle utilise les particularités dermatoglyphiques pour assurer une identification précise et fiable des individus [05].

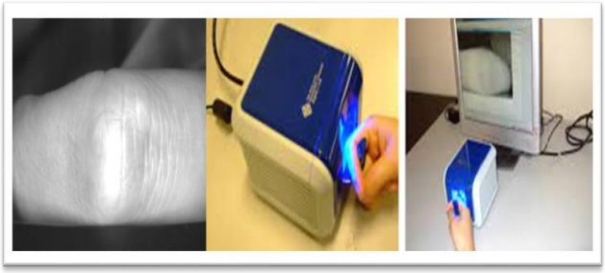


Figure 1.5. *Empreinte de doigt*

- **Reconnaissance géométrique de la main :** La reconnaissance géométrique de la main est une technologie biométrique qui utilise la taille, la forme et d'autres caractéristiques uniques de la main d'une personne pour l'identifier. Elle fonctionne en scannant la main d'une personne et en la comparant à une base de données de mains connues. La reconnaissance de la géométrie de la main est souvent utilisée dans des applications de sécurité, telles que le contrôle d'accès et la prévention de la fraude [04].

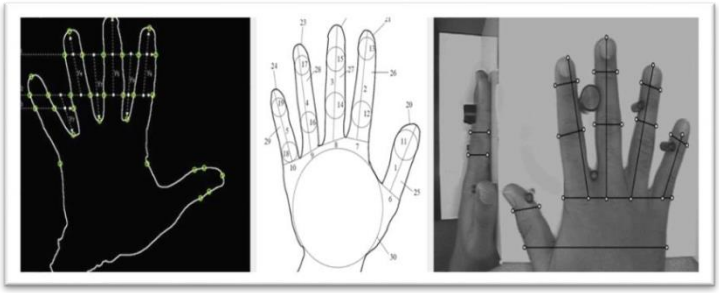


Figure 1.6. *Empreinte de la géométrie de la main*

- **Balayage rétinien :** La technique du balayage rétinien est une méthode biométrique qui exploite les motifs spécifiques des vaisseaux sanguins de la rétine d'un individu afin de l'identifier. Son fonctionnement repose sur le scanner de la rétine d'un individu et sa comparaison avec une base de données de rétines connues. Les applications de sécurité utilisent fréquemment le balayage rétinien, comme le contrôle d'accès et la prévention de la fraude [04].

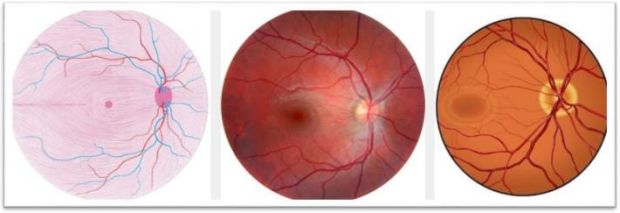


Figure 1.7. *Empreinte rétinienne*

1.3.2. Modalité biométrique comportementale

La modalité biométrique comportementale consiste à utiliser des modèles de comportement spécifiques pour identifier une personne. Il peut s'agir de traits comme la manière dont une personne marche, la manière dont elle tape ou la manière dont elle communique. Les applications de sécurité utilisent fréquemment la biométrie comportementale, comme le contrôle d'accès et la prévention de la fraude [06].

- **Dynamique de la frappe** : Aussi appelée reconnaissance de la frappe au clavier ou frappe au clavier dynamique, la dynamique de la frappe est une méthode biométrique comportementale qui permet de mesurer et d'analyser les caractéristiques individuelles de la façon dont une personne tape sur un clavier. Les modèles de pression, de timing et de style de frappe d'un individu sont utilisés dans cette méthode afin d'identifier et d'authentifier l'utilisateur [06].

Figure 1.8. *Dynamique de frappes*

- **Reconnaissance vocale :** La reconnaissance vocale est une méthode comportementale biométrique qui évalue la manière dont une personne parle. Elle peut comprendre des éléments tels que la taille, le ton et le rythme de la voix d'un individu. Il est possible d'utiliser la reconnaissance vocale afin d'identifier des individus avec une grande précision [06].

Figure 1.9. *Reconnaissance vocale*

- **Analyse de la démarche :** L'étude de la marche est une méthode biométrique comportementale qui évalue la manière dont une personne se déplace. Son contenu peut englober des éléments tels que la vitesse, la longueur de la foulée et la vitesse de marche d'un individu. On peut utiliser l'analyse de la démarche pour repérer des individus avec une grande précision [06].

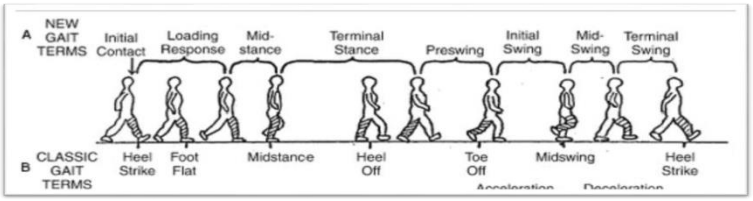


Figure 1.10. *Analyse de démarche*

1.3.3. Modalité biométrique biologie

Ce genre de biométrie repose sur l'étude des singularités biologiques de chaque individu, comme l'odeur, l'ADN et les signaux physiologiques. L'idée principale est que ces informations biologiques peuvent être utilisées comme une signature personnelle. Toutefois, cette méthode n'est pas fréquemment employée pour le contrôle d'accès logique ou physique, et nous ne fournirons pas d'informations supplémentaires à ce sujet [04].

- ADN : L'ADN, également connu sous le nom d'acide désoxyribonucléique, est une substance qui se trouve dans toutes les cellules vivantes. Dans la biologie, l'ADN est une modalité biométrique qui permet d'identifier et d'authentifier les individus en se basant sur leur code génétique unique. Chaque individu possède un ADN unique qui lui est propre, sauf les jumeaux monozygotes. Les gènes et les régions non codantes de l'ADN sont composés de séquences de nucléotides (A, T, C, G). Les différences génétiques entre les individus sont déterminées par les variations dans ces séquences et leur arrangement particulier [04]

Figure 1.11. *ADN*

1.4.Système biométrique

Les informations biométriques d'une personne sont recueillies et stockées dans une base de données sécurisée, et elles sont comparées à chaque fois qu'elle essaie d'accéder au système ou de s'identifier. Les applications telles que le contrôle d'accès physique, la sécurité des données, les transactions bancaires, les passeports biométriques et les systèmes de vote en ligne font de plus en plus appel aux systèmes biométriques [05].

Les systèmes biométriques ont l'avantage de fournir des données biométriques uniques pour chaque individu, ce qui rend difficile leur imitation ou leur vol. Néanmoins, les systèmes biométriques comportent aussi des dangers en termes de sécurité, car les données biométriques sont des informations personnelles sensibles qui nécessitent un stockage et une protection adéquats. Il est primordial de mettre en œuvre des mesures de sécurité solides afin de préserver la vie privée et la sécurité des individus face aux attaques et aux vulnérabilités des systèmes biométriques [05].

1.4.1. Structure d'un système biométrique

Les différents éléments d'un système biométrique sont interconnectés et jouent un rôle crucial dans la reconnaissance et l'authentification des individus. Les principales parties d'un système biométrique sont les suivantes.

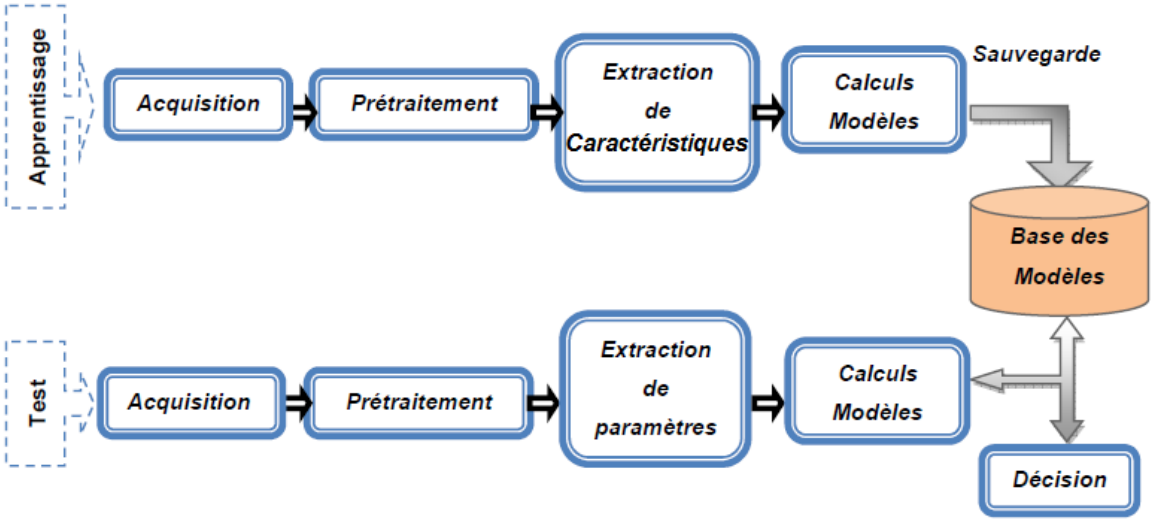


Figure 1.12. *Structure d'un système biométrique*

- **Acquisition** : L'appareil d'acquisition des données biométriques est chargé de collecter les informations biométriques d'une personne à partir d'un dispositif de capture, comme une caméra, un scanner ou un microphone. Par la suite, les informations biométriques collectées sont converties en format numérique et enregistrées dans une base de données [05].

- **Prétraitement :** Les informations biométriques non traitées peuvent présenter des fluctuations et des défauts susceptibles d'influencer les performances du système de reconnaissance. Les données biométriques sont nettoyées et normalisées par le composant de prétraitement, qui utilise des méthodes de filtrage, de normalisation et d'optimisation afin d'améliorer leur qualité [05].

- **Extraction de caractéristiques :** Cette partie est chargée de l'identification et de l'authentification des individus avec l'extraction des caractéristiques les plus pertinentes et distinctives des données biométriques. Ces caractéristiques sont souvent extraites en utilisant des techniques avancées comme la reconnaissance de motifs et l'apprentissage automatique [05].

- **Comparaison et décision :** Ce module a pour fonction de comparer les informations biométriques de l'utilisateur actuel avec celles stockées dans la base de données et de décider de l'authentification en fonction de la similarité des données. On utilise fréquemment des algorithmes avancés comme les réseaux de neurones et les machines à vecteurs de support pour cette étape [05].

1.4.2. Fonctionnement d'un système biométrique

Le système biométrique fonctionne en trois étapes principales : l'enregistrement, la vérification et l'identification. Voici une explication approfondie de chaque étape :

- **Enrôlements :** L'objectif de cette étape est de recueillir les informations biométriques d'un individu et de les conserver dans une base de données. Les informations peuvent comprendre des photos du visage, des empreintes digitales, des modèles d'iris, des schémas de veines de la paume, et ainsi de suite. Il est également possible d'externaliser les données afin de minimiser les fluctuations causées par les conditions d'acquisition.
- **Vérification :** Pour vérifier l'identité d'un individu, le système biométrique compare les données biométriques d'un individu avec celles enregistrées dans la base de données d'enrôlement. On utilise le procédé de vérification pour authentifier une personne qui prétend être la personne qu'elle prétend être. En cas de réussite de la vérification, l'individu peut accéder au système ou à une zone sécurisée.
- **Identification :** À la différence de la vérification, l'identification ne requiert pas l'enregistrement préalable de l'individu dans la base de données. L'identification de la personne est réalisée en comparant les caractéristiques biométriques de l'individu avec toutes les données stockées dans la base de données. Le procédé d'identification peut servir à repérer une personne inconnue ou à rechercher une personne précise dans une grande base de données. En cas de réussite de l'identification, le système fournira l'identité de la personne concernée [05].
- Globalement, le fonctionnement d'un système biométrique est complexe et demande une combinaison de méthodes d'acquisition de données, de traitement de données et d'algorithmes de reconnaissance afin de générer des résultats précis et fiables.

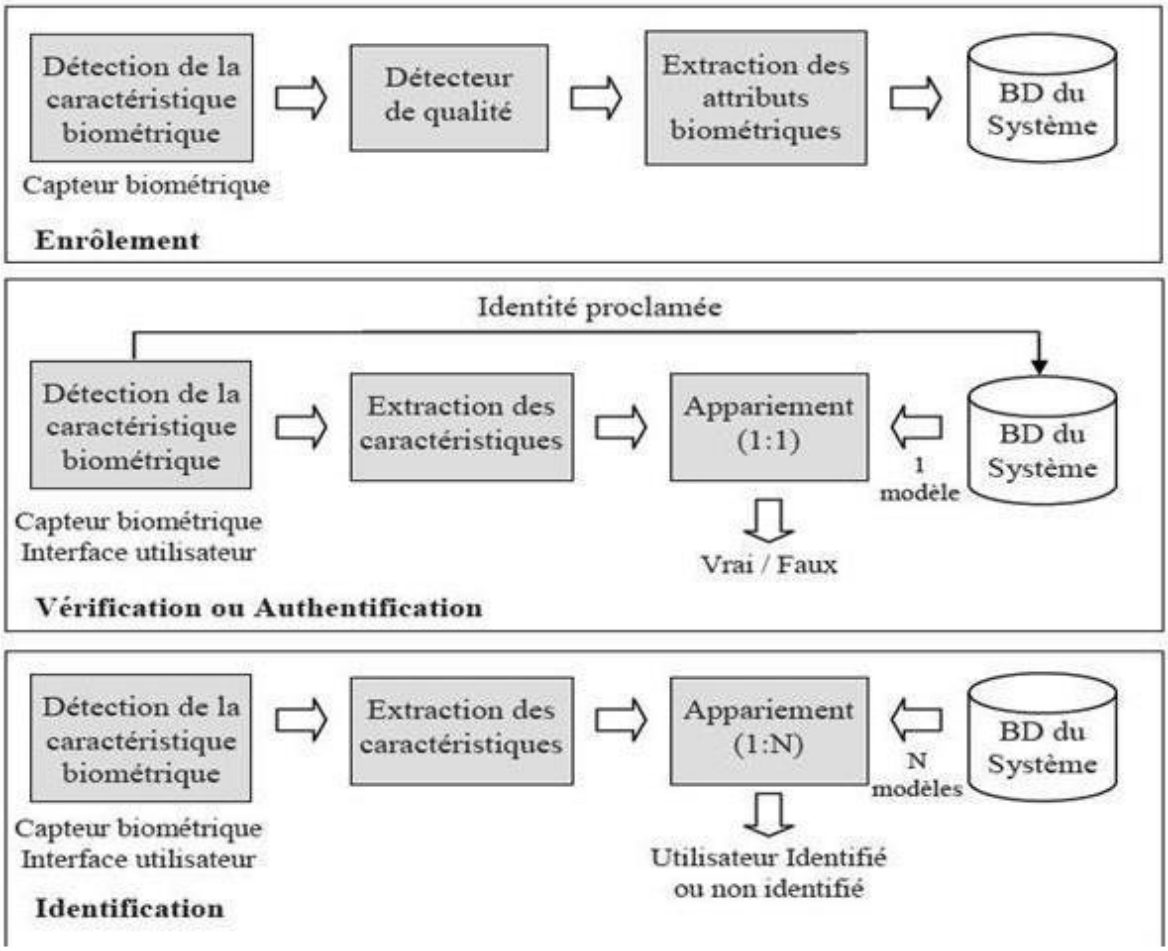


Figure 1.13. *Les étapes d'un système biométrique*

1.5.Évaluation d'un système biométrique

La conception d'un système de vérification/identification biométrique implique une évaluation des performances d'un système biométrique. Dans cette partie, nous abordons les différentes méthodes de test d'un système biométrique et examinons différentes statistiques et graphiques de performances qui sont utilisés pour la visualisation. Il y a deux types d'applications biométriques, comme nous l'avons vu plus haut, la vérification et l'identification. Il est pertinent de les différencier ici car ils influenceront la décision concernant l'évaluation des performances [06].

1.5.1. Mesures du taux d'erreur

Plusieurs métriques sont généralement employées dans le cadre de la conception et de l'évaluation de systèmes biométriques. Certaines d'entre elles sont utilisées dans l'application de vérification, tandis que d'autres sont utilisées dans celle d'identification (ensemble ouvert/ensemble fermé). Ci-dessous, nous présentons les métriques les plus fréquemment utilisées.

- **Taux de fausses acceptations (FAR)** : Correspond à la probabilité où un système biométrique autorise à tort une personne non autorisée. Cela survient lorsque le système, la solution ou l'application biométrique fait correspondre de façon erronée une entrée biométrique à un modèle stocké, ce qui entraîne une correspondance erronée et permet à une personne non autorisée d'accéder [06].
- **Taux de faux rejets (FRR) :** On peut définir le comme le contraire du FAR, c'est-à-dire la probabilité de cas où un système biométrique refuse involontairement l'accès à une personne autorisée. Il arrive que le système, la solution ou l'application biométrique ne parvienne pas à faire correspondre l'entrée biométrique avec un modèle stocké, ce qui entraîne une erreur de no match et refuse l'accès à une personne autorisée. Le FRR, également connu sous le nom de FAR, est une mesure cruciale utilisée pour évaluer les performances d'un système biométrique [06].
- **Taux d'erreur égal (EER)** : Taux auquel FAR est égal à FRR. Cependant, leur différence subtile est que FAR et FRR sont des erreurs au niveau du système qui incluent des échantillons qui n'ont pas pu être acquis ou comparés [06].

1.5.2. Courbes de performance

- **Courbe DET :** La courbe DET (Detection Error Tradeoff) est une représentation graphique du taux de fausses acceptations (FAR) et du taux de faux rejets (FRR) d'un système biométrique. La courbe DET est un outil utile pour comparer les performances des systèmes biométriques [01].

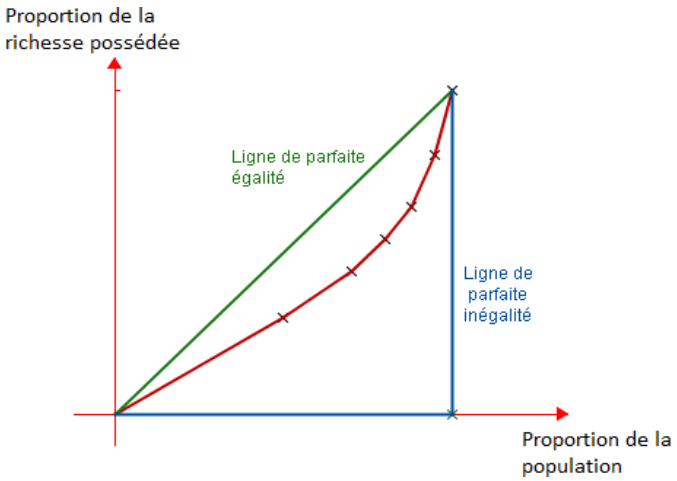


Figure 1.14. *Courbe DET*

- **Courbe ROC :** La courbe ROC (Receiver Operating Characteristic) est une représentation graphique du taux de vrais positifs (TPR) et du taux de faux positifs (FPR) d'un système biométrique. La courbe ROC est un outil utile pour comparer les performances de différents systèmes biométriques [01].

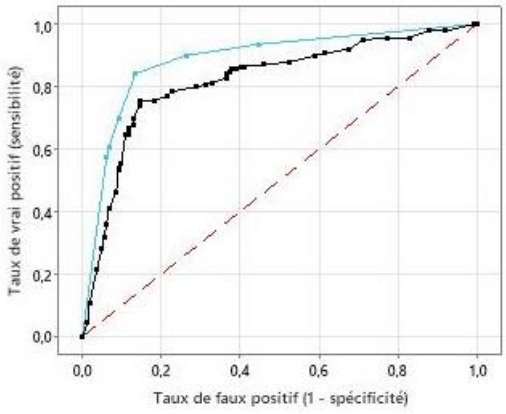


Figure 1.15. *Courbe ROC*

- **Courbe CMC :** La courbe CMC (Cumulative Match Characteristic) est une représentation graphique des scores ordonnés de toutes les correspondances possibles entre une sonde et une galerie. La courbe CMC est un outil utile pour évaluer les performances d'un système biométrique à différents niveaux de précision [01].

- **Courbe de distribution des scores clients et des imposteurs :** La courbe de distribution des scores des clients et des imposteurs est une représentation graphique de la distribution des scores pour les correspondances authentiques (clients) et les correspondances imposteurs. La courbe peut être utilisée pour évaluer les performances d'un système biométrique à différents niveaux de confiance [01].

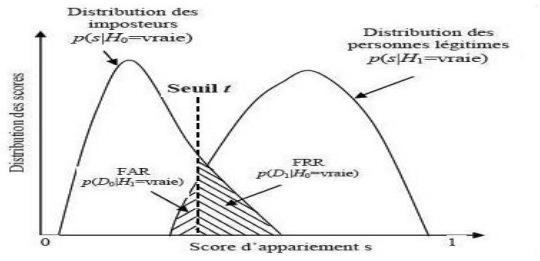


Figure 1. 16.. *Courbe de distribution des scores des clients et des imposteurs*

- **Courbe de taux d'erreur :** La courbe du taux d'erreur est une représentation graphique du taux d'erreur d'un système biométrique en fonction du seuil de décision. La courbe peut être utilisée pour évaluer les performances d'un système biométrique à différents niveaux de sécurité [01].

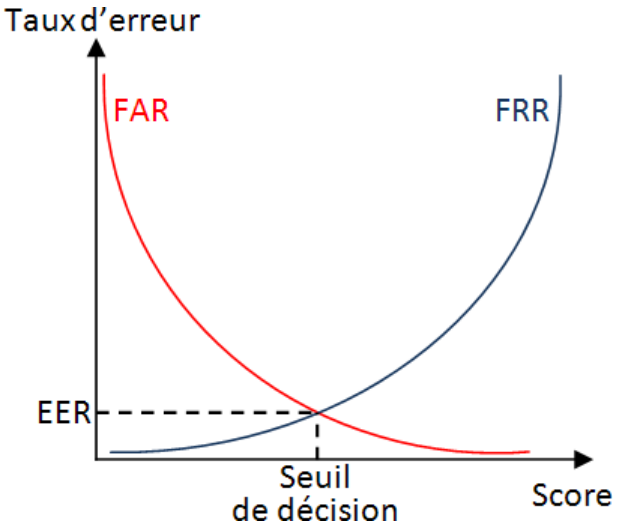


Figure 1.17. *Courbe taux d'erreur*

1.6.Application de la biométrie

La biométrie a gagné en popularité dans de nombreux secteurs tels que la sécurité, la surveillance, la gestion des identités et des accès, la santé, la banque et les transactions financières, ainsi que la gestion des frontières et des voyageurs. Les méthodes traditionnelles d'identification et d'authentification, comme les mots de passe, les cartes d'identité et les clés, peuvent présenter des avantages considérables par rapport aux systèmes biométriques.

1.6.1. Sécurité

Les systèmes de reconnaissance faciale, les empreintes digitales et les scanners de rétine sont fréquemment employés dans le domaine de la sécurité afin de surveiller l'accès aux bâtiments, aux ordinateurs et aux données sensibles. Dans les aéroports, les gares et les ports, ces systèmes peuvent aussi servir à repérer les individus à risque et à empêcher l'entrée de personnes non autorisées [09].

1.6.2. Surveillance

Dans le domaine de la surveillance, les systèmes biométriques peuvent être utilisés pour identifier les suspects lors d'enquêtes criminelles et pour prévenir les fraudes et les vols. Les

systèmes de reconnaissance faciale peuvent être utilisés pour surveiller les zones publiques, telles que les centres commerciaux et les gares afin d'identifier les personnes recherchées ou de détecter les comportements suspects [09].

1.6.3. Gestion des identités et des accès

Les systèmes biométriques peuvent être employés dans la gestion des identités et des accès afin de garantir la sécurité des données confidentielles et de l'infrastructure des entreprises. Les empreintes digitales, les scans de rétine et les reconnaissances vocales peuvent être employés afin de garantir que les informations confidentielles ne sont accessibles qu'aux personnes autorisées [09].

1.6.4. Santé

Les systèmes biométriques peuvent être utilisés pour garantir que les patients reçoivent les soins appropriés et que leurs dossiers médicaux sont correctement identifiés. Les scans de rétine et les empreintes digitales peuvent être utilisés pour garantir que les soins sont administrés à la bonne personne [09].

1.6.5. Banques et les transactions financières

Lessystèmesbiométriquespeuventêtreutiliséspourrenforcerlasécuritédestransactions.Lessystèmes de reconnaissance vocale, de reconnaissance faciale et de scan de rétine peuvent être utilisés pour authentifier les utilisateurs et empêcher les fraudes financières [09].

I.7. Conclusion

La biométrie consiste à identifier les individus en se basant sur leurs particularités physiques ou comportementales. Les applications des systèmes biométriques comprennent le contrôle d'accès, le suivi des horaires et des présences, ainsi que la détection des fraudes.
Les empreintes digitales, la reconnaissance faciale et la reconnaissance de la paume sont les traits biométriques les plus fréquents. Les empreintes digitales sont les données biométriques les plus couramment employées, car elles sont relativement simples à prendre et peuvent servir à identifier des individus même s'ils portent des gants ou ont les mains sales.

La reconnaissance faciale gagne en popularité, car il s'agit d'une méthode non invasive pour identifier les personnes. La caractéristique biométrique la plus précise est la reconnaissance de l'iris, mais elle est également la plus coûteuse à mettre en place.

2.1.Introduction

L'extraction de caractéristiques biométriques consiste à identifier et analyser des caractéristiques physiques ou comportementales uniques dans le but de reconnaissance et d'authentification. Ce processus capture des attributs distinctifs tels que les empreintes digitales, les structures faciales, les motifs de l'iris et les dynamiques vocales, les transformant en données numériques pouvant être utilisées pour vérifier les identités individuelles.

En s'appuyant sur des algorithmes avancés et des technologies de capteurs, l'extraction de caractéristiques biométriques offre une méthode hautement sécurisée et efficace pour la vérification de l'identité, jouant un rôle crucial dans diverses applications allant des systèmes de sécurité aux appareils personnels.

2.2.Caractéristiques de l'image

Les caractéristiques extraites des images d'empreintes jouent un rôle crucial dans leur utilisation efficace pour la reconnaissance biométrique. Voici les points essentiels à considérer :

2.2.1. Intérêts des caractéristiques extraites

Les caractéristiques extraites des empreintes offrent plusieurs avantages et intérêts :

- **Unicité** : Elles captent des aspects uniques de l'empreinte de chaque individu, permettant ainsi une identification précise même parmi un grand nombre d’individus.
- **Stabilité** : Les caractéristiques sont robustes aux variations intra-personnelles (changements mineurs dans l'empreinte au fil du temps) tout en étant sensibles aux variations inter-personnelles (différences entre individus).
- **Compatibilité avec les systèmes existants** : Elles sont conçues pour être utilisées avec différents algorithmes de reconnaissance biométrique, ce qui facilite leur intégration dans des systèmes existants et leur utilisation à grande échelle.

2.2.2. Propriétés des caractéristiques extraites

Les caractéristiques biométriques extraites des empreintes doivent posséder les propriétés suivantes :

- **Discrimination élevée** : Elles doivent pouvoir différencier de manière fiable entre les empreintes palmaires de différents individus, même lorsque les conditions d'acquisition des images varient (par exemple, différentes bandes spectrales ou conditions d'éclairage).

- **Invariantes aux transformations** : Elles doivent être robustes aux variations telles que les rotations, les changements d'échelle et les déformations mineures de l'empreinte, tout en maintenant leur capacité à identifier de manière précise l'individu.
- **Taille** : La taille des images biométriques est une propriété cruciale qui influence directement la précision et l'efficacité des systèmes de reconnaissance et d'authentification. En général, les images biométriques telles que les scans de visage, d'iris ou d'empreintes digitales sont capturées avec une résolution et une taille spécifique pour assurer la captation précise des détails distinctifs. Par exemple, les images faciales doivent souvent être de haute résolution pour détecter les traits caractéristiques du visage avec précision [10]. De même, les scans d'iris nécessitent une résolution élevée pour distinguer les motifs uniques de l'iris. En outre, la taille des images biométriques influe sur les exigences en matière de stockage, de transmission et de traitement des données, ce qui est crucial pour garantir l'efficacité et la sécurité des systèmes biométriques. Ainsi, la sélection appropriée de la taille des images biométriques est essentielle pour optimiser les performances tout en répondant aux exigences spécifiques des applications biométriques.
- **Temps de calcul** : Le temps de calcul est une propriété critique dans le domaine des images biométriques, influençant directement la rapidité et l'efficacité des processus de reconnaissance et d'authentification. Les algorithmes utilisés pour extraire et comparer les caractéristiques biométriques, tels que les empreintes digitales, les scans de visage ou d'iris, nécessitent souvent des calculs intensifs pour garantir la précision et la fiabilité des résultats. Par exemple, les techniques avancées de reconnaissance faciale basées sur la comparaison de multiples points caractéristiques peuvent exiger des ressources de calcul considérables pour traiter les images en temps réel [5]. De même, les systèmes de reconnaissance d'iris utilisent des algorithmes complexes pour identifier et comparer les motifs uniques, impactant directement le temps nécessaire à l'authentification [6]. La gestion efficace du temps de calcul est donc essentielle pour optimiser les performances des systèmes biométriques tout en répondant aux exigences de temps réel dans diverses applications.

2.3.Méthodes d’extractions de caractéristiques

Les méthodes d'extraction de caractéristiques biométriques jouent un rôle essentiel dans la précision et la fiabilité des systèmes de reconnaissance, en permettant la capture et l'analyse précises des attributs distinctifs.

L'extraction de caractéristiques se décompose en trois catégories, caractéristique liée aux lignes comme les lignes, caractéristique liée aux textures et caractéristique liées aux formes.

Les approches basées sur les lignes regroupent les approches structurelles qui sont basées spécifiquement sur les lignes principales [21], les rides, la crête et le point caractéristique.

En reconnaissance de l'apparence, l'apparence est décrite en fonction de la position et de la direction simplement comme une courbe connectée dans un champ 2D. Les caractéristiques de l'apparence peuvent être utilisées pour des applications médicales, par exemple pour la classification des cellules cervicales ou pour les systèmes de récupération d'images basés sur le contenu où les caractéristiques de couleur ne sont pas utiles [9].

La texture est une caractéristique utilisée pour partitionner et classer les images en zones d'intérêt. Il offre des données dans la structure spatiale de couleur ou d'intensité d'une image . La texture d'un point ne peut pas être décrite. Elle est définie par la répartition spatiale des taux d'intensité du voisinage. La résolution à laquelle une image est identifiée définit l'échelle de perception de la texture.

Dans notre nous utilisons deux techniques d'extraction de caractéristiques basé sur la texture de l'image, la 1ère c'est l'Histogramme d'Orientations de Gradients (HOG) et la 2nd la Quantification de phase Locale (LPQ).

2.3.1. Histogramme d'Orientations de Gradients (HOG)

L'histogramme de gradient orienté (Histogram of Oriented Gradients-HOG) [7] est une technique puissante de description de caractéristiques, largement utilisée en vision par ordinateur et en traitement d'images, en particulier pour la détection d'objets. Il décrit la distribution des gradients d'intensité locaux (variations des valeurs de pixels) au sein d'une image. Les caractéristiques HOG agissent comme une représentation cartographique des contours, capturant à la fois les détails sur l'amplitude du gradient et les positions des contours dans des cellules spécifiques. Supposons que l'entrée soit une fenêtre **I** de dimensions $\mathbf{H} \times \mathbf{W}$ d'une image en niveaux de gris, ou même l'image entière, pour créer une fonction HOG [14], nous suivons les étapes suivantes :

a) **Calcul des gradients :** Déterminer les composantes du gradient (I_x, I_y) par :

$$\begin{cases} I_x(i,j) = I(i,j+1) - I(i.j-1) \\ I_y(i,j) = I(i-1,j) - I(i+1,j) \end{cases} i = 1 \dots H\ ,\ j = 1 \dots W \qquad (2.1)$$

Le gradient est ensuite transformé en coordonnées polaires avec un angle limité entre 0° et 180° degrés pour identifier les gradients opposés.

$$\begin{cases} \mu = \sqrt{I_x^2 + I_y^2} \\ \theta = \frac{180}{x} \left(\tan^{-1}(I_x, I_y)\right) mod\pi \end{cases} \quad (2.2)$$

Où $\tan^{-1}$ est la tangente inverse, qui donne des valeurs comprises entre -π et π, et μ et θ désignent respectivement l'amplitude et la direction (angle) du gradient de chaque pixel.

b) **Histogrammes d'orientation des cellules :** La fenêtre est divisée en cellules voisines de taille $c \times c$ qui ne se chevauchent pas. Ensuite, pour chaque cellule, un histogramme des directions de gradient est calculé et trié dans B bins. Les bins sont numérotées de 0 à $B - 1$ et chacune a une largeur de $\omega = \frac{180}{B}$.

c) **Normalisation des blocs :** Pendant cette étape, les cellules sont disposées en blocs de pixels superposés de taille $2c \times 2c$ avec un décalage vertical et horizontal de c pixels. Ensuite, les histogrammes des quatre cellules de chaque bloc sont fusionnés en un seul bloc, qui est ensuite normalisé en utilisant la norme euclidienne.

$$b_k = \left[h_{(i,j)}, h_{(i,j+1)}, h_{(i+1,j)}, h_{(i+1,j+1)}\right] \quad (2.3)$$

Où b_k désigne la caractéristique du bloc k et $h_{(i,j)}$, l'histogramme de la cellule *(i, j)*. Ces caractéristiques de bloc est normalisée comme suit :

$$\widetilde{b_k} = \frac{b_k}{\sqrt{\|b_k\|^2 + \epsilon}} \quad (2.4)$$

Où ∈ est une petite constante positive qui empêche la division par zéro dans des blocs sans gradient.

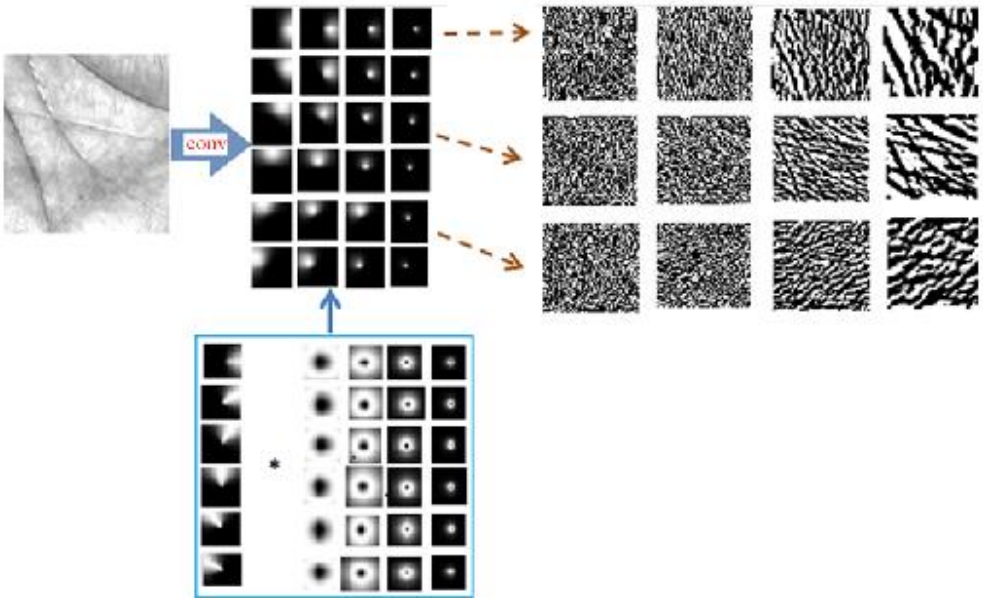


Figure 2.1. Génération d'images filtrées.

d) **Vecteur de Caractéristique HOG :** Enfin, pour représenter l'intégralité de la caractéristique de la fenêtre, toutes les caractéristiques de bloc normalisées ($\widetilde{b_k}$) sont concaténées pour produire un vecteur de caractéristiques HOG ($\mathcal{H}$), comme indiqué ci-dessous :

$$\mathcal{H} = [\widetilde{b_1}, \widetilde{b_2}, \ldots, \widetilde{b_k}, \ldots, \widetilde{b_p}] \quad (2.5)$$

Où p est le nombre de blocs dans la fenêtre. Enfin, la fonction HOG résultante est également normalisée à l'aide de l'équation (2.2).

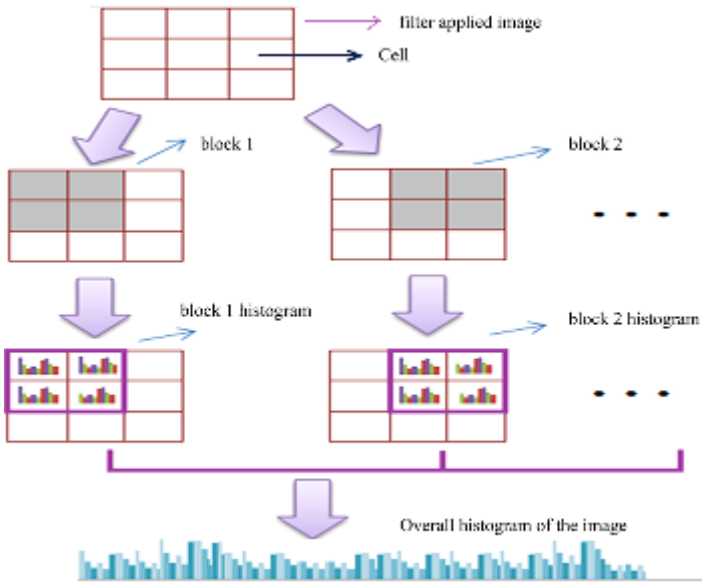


Figure 2.2. Génération d'un histogramme global.

2.3.2. Quantification de phase Locale (LPQ)

L'informations de LPQ (Local Phase Quantization) peut être extraite en utilisant la transformée discrète de Fourrier à fenêtre à deux dimensions (2DWFT).

$$Fu(x) = \sum h(m - x) f(m) e - j\pi u\, T\, m = Eu\, Tfx, m \epsilon N \quad (2.6)$$

Où EuT, de taille = 1 ×M², est un vecteur de base de 2DWFT avec la fréquence u, etfx, taille = M² × N, est un vecteur contenant les valeurs des pixels d'image dans Nx à chaque position x. La fonction fenêtre, h (x) est une fonction rectangulaire [15].

La transformation est calculée à quatre valeurs de la fréquence, u = [u0, u1, u2, u3] où u0= $[a, 0]$ T , u1= $[0, a]$ T , u2 = $[a, a]$ T et u3 = $[a, -a]$ T . La valeur a est la plus haute fréquence scalaire pour laquelle $\boldsymbol{Hui} > 0$. Ainsi, seuls quatre fonctions complexes comme un banc de filtres sont nécessaires pour produire huit images résultantes, composées de 4 images de la partie réelle et 4

images de la partie imaginaire de la transformée. Chaque pixel de l'image complexe résultant peut être codé en une valeur binaire représentée dans l'équation (2.2) en appliquant (the quadrant bit coding) [8].

$$\underset{Bui}{Re} = \begin{cases} 1 \; SiFui\,(x) > 0 & Re \\ 0 \; SiFui\,(x) \leq 0 & Re \end{cases} \quad \underset{Bui}{Im} = \begin{cases} 1 \; SiFui\,(x) > 0 & Im \\ 0 \; SiFui\,(x) \leq 0 & Im \end{cases} \tag{2.7}$$

Ce procédé de codage attribue deux bits pour chaque pixel pour représenter le quadrant dans lequel se trouve l'angle de phase [9]. En fait, il fournit également la quantification de la fonction de phase de Fourier. En général, LPQ est une chaîne binaire, présentée dans l'expression (2.7), obtenue pour chaque pixel par la concaténation des codes quadrant bits réelles et imaginaires des huit coefficients de Fourier de ui [16].

$$LPQ\,(x) = [\,B_{u0}(x)\,, B_{u0}(x)\,, \ldots . B_{u3}(x)\,, B_{u3}(x)\,] \tag{2.8}$$

La chaîne binaire est convertie en nombre décimal par l'expression (2.9) pour produire une étiquette de LPQ.

$$LPQ(x) = B_{u0}(x) + B_{u0}(x)x2^{1} + \cdots . + B_{u3}(x)x2^{K-1} + B_{u3}(x)x2^{k} \tag{2.9}$$

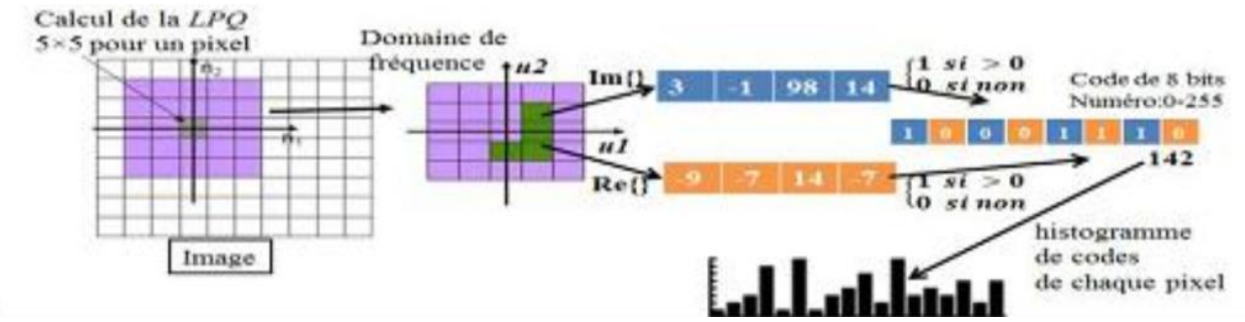


Figure 2.3. Organigramme de l'ensemble des étapes nécessaire à la construction du descripteur LPQ

2.4.Classificateurs

Les classifieurs SVM (Support Vector Machine) et kNN (k-Nearest Neighbors) sont deux algorithmes populaires utilisés dans le domaine de l'apprentissage automatique pour la classification de données.

2.4.1. Machine a vecteurs de support (SVM)

Un Support Vector Machine (SVM) est une méthode d'apprentissage supervisé couramment utilisée dans les problèmes de machine Learning. Cette méthode est principalement utilisée pour les problèmes de classification et de régression. Elle fonctionne en créant une équation pour une ligne qui sépare les points d'entraînement en deux ensembles. Cette ligne est appelée la frontière de décision. De plus, un classifieur SVM peut avoir plusieurs équations pour les frontières de décision [17].

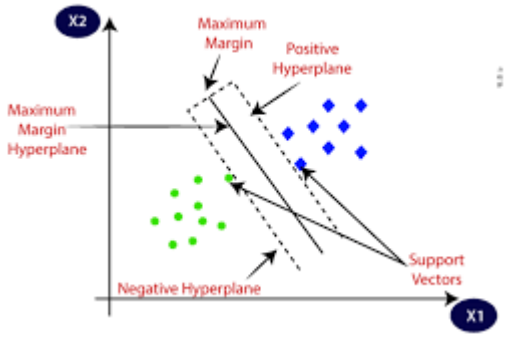


Figure 2.4. Algorithme SVM

a) **Principe de Séparation** : Le classifier SVM cherche à trouver un hyperplan dans un espace *n*-dimensionnel qui sépare les données en deux classes (dans le cas de la classification binaire). Cet hyperplan est défini comme $w \cdot x + b = 0$, où w est le vecteur de poids et b est le biais (ou l'intercept).

b) **Marges et Vecteurs de Support** : La marge est la distance entre l'hyperplan et les points de données les plus proches de chaque classe. SVM cherche à maximiser cette marge, car elle favorise une meilleure généralisation du modèle. Les points de données qui touchent cette marge maximale sont appelés vecteurs de support. Ils sont essentiels pour déterminer l'hyperplan optimal et sont ceux qui influencent directement la position de l'hyperplan.

c) **Optimisation de l'Hyperplan** : L'objectif de SVM est de trouver l'hyperplan qui maximise la marge tout en minimisant l'erreur de classification. Cela se formule souvent comme un problème d'optimisation quadratique, où l'on cherche à minimiser $\frac{1}{2}\|w\|^2$ sous des contraintes données par $y_i(w \cdot x_i + b) \geq 1y\_i$ pour chaque paire de données (x_i, y_i), avec y_i étant l'étiquette de classe $\{-1,1\}$.

2.4.2. K plus proches voisins (KNN)

Le K-Nearest Neighbour (KNN) est un algorithme d'apprentissage supervisé couramment utilisé dans les problèmes de classification en machine Learning. Cet algorithme classe un échantillon en examinant les points les plus proches de cet échantillon, appelés voisins. Le nombre de voisins examinés est défini par la valeur k. Lors de la classification, l'algorithme examine les k voisins les plus proches et classe l'échantillon en fonction de la catégorie représentée majoritairement par les voisins [18].

a) **Principe :** KNN est basé sur l'idée que les points de données similaires ont tendance à se regrouper dans des zones de l'espace des caractéristiques. Pour classer un nouvel exemple, KNN cherche les k voisins les plus proches dans l'ensemble d'apprentissage et attribue la classe majoritaire parmi ces voisins au nouvel exemple.

b) **Paramètre K :** k est un paramètre crucial dans KNN, déterminant le nombre de voisins à considérer pour la classification. Un choix de K trop petit peut conduire à une sensibilité au bruit, tandis qu'un K trop grand peut engendrer une généralisation excessive.

c) Étapes de fonctionnement

Distance : KNN utilise des mesures de distance pour calculer la similarité entre les points de données dans l'espace des caractéristiques.

Classification : Une fois les k voisins les plus proches identifiés, KNN attribue la classe majoritaire parmi ces voisins au nouvel exemple. Par exemple, si la majorité des voisins sont de la classe A, alors le nouvel exemple est classé comme appartenant à la classe A.

2.5.Biométrie Multimodale

La biométrie multimodale combine plusieurs modalités biométriques telles que les empreintes digitales, la reconnaissance faciale, l'analyse de l'iris, la reconnaissance vocale, etc., En intégrant plusieurs sources de données biométriques, cette approche vise à compenser les limitations individuelles de chaque modalité tout en exploitant les avantages de chacune. un système biométrique peut offrir une sécurité accrue et une meilleure performance dans des conditions variables telles que l'éclairage ou la qualité des données. Les recherches récentes ont montré que l'intégration de plusieurs modalités peut non seulement améliorer la précision de l'identification, mais aussi augmenter la résistance aux tentatives de fraude ou de contournement des systèmes de

sécurité [05]. Cependant, la biométrie multimodale pose également des défis en termes de gestion des données, de complexité algorithmique et de coût d'implémentation, nécessitant une intégration et une optimisation minutieuses pour maximiser ses avantages.

2.5.1. Nécessité

La nécessité de la biométrie multimodale réside dans sa capacité à améliorer la fiabilité et la sécurité des systèmes d'identification et d'authentification biométriques. En intégrant plusieurs modalités biométriques telles que les empreintes digitales, la reconnaissance faciale, l'analyse de l'iris, et parfois la reconnaissance vocale ou la dynamique de frappe, cette approche permet de surmonter les limitations individuelles de chaque méthode. Par exemple, alors que la reconnaissance faciale peut être affectée par des conditions d'éclairage variables, les empreintes digitales offrent une fiabilité accrue dans des environnements poussiéreux ou humides. L'utilisation conjointe de plusieurs modalités augmente non seulement la précision de l'identification, mais renforce également la résistance aux tentatives de fraude et aux fausses identifications.

Des recherches récentes soulignent que la biométrie multimodale offre une meilleure robustesse et une réduction des taux d'erreurs comparé à l'utilisation de méthodes biométriques individuelles [05]. De plus, elle permet une adaptation plus flexible aux divers scénarios d'application, tels que la sécurité des frontières, les systèmes de paiement sécurisés, et les dispositifs d'accès aux entreprises.

2.5.2. Fusion des données

La fusion des données en biométrie désigne le processus de combinaison de plusieurs sources d'informations biométriques pour améliorer la précision et la fiabilité des systèmes d'identification ou d'authentification. Elle exploite différentes modalités biométriques (telles que les empreintes digitales, la reconnaissance faciale, les scans d'iris) afin de compenser les limitations individuelles et renforcer la sécurité globale du système. La fusion peut intervenir à différents niveaux : en combinant les caractéristiques extraites (fusion au niveau des caractéristiques), en fusionnant les scores de similarité (fusion au niveau des scores), ou en intégrant les décisions finales (fusion au niveau des décisions). Cette approche améliore la précision, la robustesse et l'adaptabilité des applications biométriques, optimisant les performances en utilisant des données complémentaires provenant de sources diverses [19].

2.5.3. Scénarios de fusion

La fusion de modalités dans les systèmes biométriques multimodaux peut être réalisée de différentes manières en fonction des besoins spécifiques et des scénarios d'application. Voici quelques scénarios courants de fusion de modalités Figure 2.5.

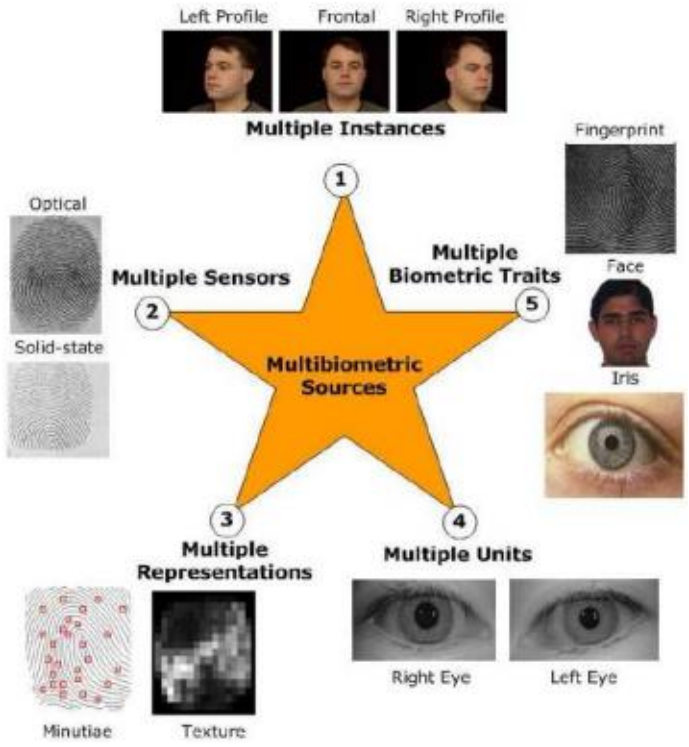


Figure 2.5. Sources de multiples éléments de preuve d'identité dans les systèmes biométriques multimodaux

a) **Fusion au niveau de la décision**

Vote majoritaire : Chaque modalité fournit une décision indépendante et la décision finale est prise en fonction du vote majoritaire parmi toutes les modalités.

Vote pondéré : Chaque modalité contribue à une décision finale avec un poids spécifique attribué en fonction de la fiabilité ou de la pertinence de la modalité dans un contexte donné.

b) Fusion au niveau des traits

Caractéristiques conjointes : Les caractéristiques extraites de différentes modalités sont combinées pour créer un vecteur de traits biométriques plus riche et robuste.

Caractéristiques complémentaires : Les caractéristiques extraites de différentes modalités sont utilisées de manière complémentaire pour améliorer la représentation globale de l'identité.

c) Fusion au niveau des scores

Score de décision : Les scores de confiance ou de similarité provenant de chaque modalité sont agrégés pour former un score global qui est ensuite utilisé pour la décision d'authentification ou d'identification.

Score adaptatif : Les scores de différentes modalités sont adaptativement pondérés en fonction des conditions de l'environnement ou de la qualité des données pour optimiser la performance du système.

d) Fusion au niveau des décisions :

Fusion hiérarchique : Une décision est d'abord prise indépendamment par chaque modalité, puis ces décisions sont fusionnées pour arriver à une décision finale.

Fusion séquentielle : Les modalités sont utilisées dans un ordre spécifique où chaque modalité est activée séquentiellement jusqu'à ce qu'une décision finale soit atteinte ou qu'un seuil de confiance soit satisfait.

e) Fusion au niveau des contextes :

Contexte adaptatif : La modalité à utiliser est sélectionnée en fonction du contexte spécifique de l'application ou de l'environnement dans lequel la vérification ou l'identification est réalisée.

Contexte dynamique : La sélection des modalités peut varier dynamiquement en réponse à des changements dans l'environnement ou dans les conditions de l'utilisateur.

Chaque scénario de fusion peut être adapté en fonction des exigences de sécurité, de performance et de convivialité du système biométrique multimodal dans différents domaines tels que la sécurité physique, la gestion des identités, les transactions financières, etc.

2.5.4. Fusion au niveau des scores

Kittler et al. [Kitt 98] ont développé un cadre théorique pour combiner les informations d'identification obtenues à partir de plusieurs classifieurs en utilisant des schémas tels que la règle somme (“sum rule”), la règle "produit" (“product rule”), la règle maximum (“max rule”), la règle minimum (“min rule”), règle somme pondéré (“sum_pondéré rule”)et la règle médiane (“median rule”).

a) **Fusion par somme :** Dans la fusion par somme, les scores de similarité ou de confiance obtenus à partir de chaque modalité sont simplement additionnés pour obtenir un score global.

Formule : Soit S_i le score de similarité de la modalité i, alors le score global S_{global} est calculé comme :

$$S_{global} = \sum_{i=1}^{n} S_i$$

où n est le nombre de modalités.

b) **Fusion par produit :** Dans la fusion par produit, les scores de similarité de chaque modalité sont multipliés pour obtenir un score global.

Formule : Soit S_i le score de similarité de la modalité i, alors le score global S_{global} est calculé comme :

$$S_{global} = \prod_{i=1}^{n} S_i$$

où n est le nombre de modalités.

c) **Fusion par minimum** : La fusion par minimum consiste à sélectionner le score le plus bas parmi les scores de similarité ou de confiance obtenus à partir de chaque modalité. La décision finale est alors basée sur ce score minimal.

Formule : Soit S_i le score de similarité de la modalité i, alors le score global S_{global} est calculé comme :

$$S_{global} = min(S_1, S_2 \dots \dots, S_n)$$

où n est le nombre de modalités.

d) **Fusion par maximum** : La fusion par minimum consiste à sélectionner le score le plus bas parmi les scores de similarité ou de confiance obtenus à partir de chaque modalité. La décision finale est alors basée sur ce score minimal.

Formule : Soit S_i le score de similarité de la modalité i, alors le score global S_{global} est calculé comme :

$$S_{global} = max(S_1, S_2 \dots \dots, S_n)$$

où n est le nombre de modalités.

e) **Fusion par somme pondérée :** Dans la fusion par somme pondérée, les scores de similarité ou de confiance obtenus à partir de chaque modalité sont additionnés en utilisant des poids spécifiques attribués à chaque modalité en fonction de sa fiabilité, de sa précision ou d'autres critères pertinents.

Formule : Soit le score de similarité de la modalité i, et w_i le poids attribué à la modalité i , alors le score global S_{global} est calculé comme :

$$S_{global} = \prod_{i=1}^{n} w_i \cdot S_i$$

2.6.Conclusion

La fusion des données biométriques représente une approche cruciale pour améliorer la précision, la fiabilité et la sécurité des systèmes d'identification et d'authentification. En intégrant différentes modalités biométriques telles que les empreintes digitales, la reconnaissance faciale et l'iris, la biométrie multimodale utilise des techniques comme la somme, le produit et la concaténation pour maximiser les avantages complémentaires des données. Ces méthodes permettent de renforcer la robustesse des systèmes en compensant les limitations individuelles des modalités biométriques et en réduisant les taux d'erreurs.

3.1.Introduction

La reconnaissance de la paume est une technologie qui a connu des améliorations significatives ces dernières années grâce à l'utilisation de données massives d'images et de vidéos pour entraîner des algorithmes d'apprentissage. De ce fait, l'empreinte palmaire est reconnue Cette technologie est devenue mature et largement utilisée dans de nombreux domaines, offrant des perspectives prometteuses pour de nombreuses applications futures.

Ce chapitre débutera par un aperçu des bases de données utilisées dans l'étude. Ensuite, nous passerons en revue le processus et les différentes méthodes que nous avons évaluées pour extraire les caractéristiques de paume de chaque individu.

3.2.Description de l'ensemble de données

La base de données d'empreintes palmaires multispectrales PolyU est une collection de données précieuse pour la recherche en biométrie. Voici les points clés de cette base de données [27] :

Nombre d'images

- Elle comprend 6000 images au total.
- Ces images sont obtenues à partir de 500 paumes différentes.

Bandes spectrales

- Les images sont recueillies à partir de quatre bandes spectrales différentes : rouge, vert, bleu et NIR (proche infrarouge).

Capture des images

- Les images sont capturées à l'aide d'un dispositif conçu par des chercheurs de l'Université polytechnique de Hong Kong.
- Chaque session de collecte d'images est effectuée à un intervalle d'environ deux mois.
- Chaque personne fournit 6 images par paume lors de chaque session, ce qui totalise 12 images par personne pour les deux sessions.

Nombre total d'images par personne

- Pour chaque paume et pour chaque bande spectrale, il y a 12 images par personne (6 par session).

Intervalle de collecte

- L'intervalle moyen entre la première et la deuxième session est d'environ neuf jours.

Caractéristiques des images

- Toutes les images sont en basse résolution, spécifiquement à 150 dpi.
- Elles sont en niveaux de gris (8 bits par bande).
- Les dimensions de chaque image sont de 128x128 pixels.

Cette base de données est utile pour les études qui nécessitent des empreintes palmaires multispectrales, notamment pour développer et tester des algorithmes de reconnaissance ou d'identification biométrique.

3.3.Protocole de test

Nous avons utilisé 12 images par classe (personne) pour le processus d'enrôlement. De ces 12 images, 3 ont été sélectionnées aléatoirement pour construire la base de données du système et les 9 images restantes de chaque classe pour les tests authentiques, Il y a 300 classes dans la base de données, donc nous avons réalisé 2400 comparaisons authentiques (clients) (9 images par classe * 300 classes). Pour les tests imposteurs, nous avons comparé chaque ensemble de 9 images avec toutes les autres classes de la base de données. Cela a donné un total de 358800 comparaisons imposteurs (9 images * 300 classes * 299 autres classes).

3.4.Métriques pour l'évaluation de la performance

Lors de l'évaluation de la performance d'un système biométrique, plusieurs métriques et courbes sont utilisées pour analyser son efficacité et son adéquation à l'usage prévu. Voici un résumé des principaux éléments et concepts associés à cette évaluation :

3.4.1. Métriques clés pour l'évaluation de la performance

a) Taux de fausse acceptation (FAR) :

- Indique la probabilité qu'un imposteur soit accepté par le système comme un utilisateur authentique.
- Mesure la sécurité du système ; plus le FAR est faible, plus le système est sécurisé contre les imposteurs.

b) Taux de faux rejet (FRR) :

- Indique la probabilité qu'un utilisateur légitime soit rejeté par le système.
- Mesure l'accessibilité du système ; plus le FRR est faible, moins les utilisateurs légitimes sont rejetés à tort.

c) Taux d'erreur égal (EER) :

- Correspond au point où le FAR est égal au FRR.
- Fournit une mesure globale de la précision du système ; un EER plus bas indique une meilleure performance globale du système.

d) Taux d'acceptation authentique (GAR) :

- Mesure l'efficacité du système à identifier correctement les utilisateurs légitimes.
- Souvent utilisé dans les systèmes d'identification pour évaluer la capacité du système à authentifier les utilisateurs corrects.

3.4.2. Courbes de performance

a) Courbe ROC (Receiver Operating Characteristic):

- Utilisée principalement en identification à jeu ouvert.
- Visualise le compromis entre le FAR et le FRR pour différentes valeurs de seuil de décision.
- Aide à choisir le meilleur point de fonctionnement en ajustant le seuil en fonction des besoins de sécurité et d'accessibilité.

b) Courbe CMC (Cumulative Match Characteristic):

- Utilisée en identification à jeu fermé.

- Représente la performance du système en termes de reconnaissance correcte des utilisateurs par rapport au rang de la réponse correcte.
- Permet d'évaluer la performance du système pour différentes positions de classement des réponses correctes.

3.4.3. Mode d'identification

- **Identification à ensemble ouvert :** L'accent est mis sur la capacité à gérer un grand nombre de candidats, avec un équilibre entre sécurité (FAR) et convivialité (FRR) via la courbe ROC.
- **Identification à ensemble fermé :** Se concentre sur la reconnaissance précise des utilisateurs connus, évaluée par des métriques telles que la ROR (reconnaissance au premier rang) et la RPR (rang de reconnaissance parfaite), souvent représentées par la courbe CMC.

3.5.Performances du système biométrique

Dans cette étude comparative des performances d'un système biométrique basé sur la modalité des veines de la paume (PLV), nous avons exploré deux approches distinctes pour le traitement des images : l'analyse de l'image entière et l'analyse basée sur des blocs. L'objectif était d'évaluer comment ces deux méthodes d'extraction de caractéristiques affectent l'efficacité globale du système, en tenant compte à la fois des performances de reconnaissance et des exigences en termes de temps de traitement et d'utilisation de la mémoire.

Pour chaque méthode, nous avons utilisé des ensembles de données spécifiques et avons mesuré les performances à l'aide de métriques standard telles que le taux de reconnaissance correcte (GAR), le taux de fausse acceptation (FAR) et le taux de faux rejet (FRR). Nos résultats ont révélé des différences significatives entre les deux approches : l'analyse de l'image entière a montré une meilleure précision globale dans certains cas, tandis que l'analyse par blocs a pu offrir une efficacité accrue en termes de temps de traitement et de gestion de la mémoire.

En outre, nous avons examiné l'impact de ces méthodes sur la robustesse du système face à des variations telles que l'éclairage et l'angle de capture des images. Cette analyse approfondie nous a permis de formuler des recommandations pratiques pour l'application future de systèmes biométriques PLV, en soulignant les avantages et les limitations de chaque approche et en identifiant des pistes pour des améliorations potentielles.

En raison de l'impact significatif que la représentation des caractéristiques de l'image a sur le taux d'identification du système, et de la dépendance critique des méthodes d'extraction de caractéristiques (HOG et LPQ) à l'égard de paramètres spécifiques, nous avons entrepris un test empirique visant à déterminer les paramètres optimaux susceptibles d'améliorer la précision globale du système et d'optimiser ses performances. Dans ces tests préliminaires, nous avons exploré la sélection du nombre de zones dans le HOG (wh) et la taille ainsi que la largeur de fenêtre LPQ à partir des ensembles de valeurs suivants : wh = {3, 5, 7, 9, 11} et wb = {21, 25, 29, 33,37,} respectivement.

Afin d'observer l'impact des paramètres de HOG sur les performances du système biométrique, nous présentons clairement les résultats du système d'identification ensemble ouvert et fermé (exprimés en termes Equal Error Rate-(EER) et Rank One Recognition-ROR) dans les Fig. 3.1. et 3.2, respectivement pour les systèmes. D'après ces figures en peut tirer quelques observations :

3.5.1. Performance du système biométrique unimodale : Système basé sur le HOG

Pour le système basé sur le HOG avec les deux classificateurs les résultats comme suivant il n'y a pas une optimisation de performance (EER=0%, ROR=100%) dans la majorité des cas

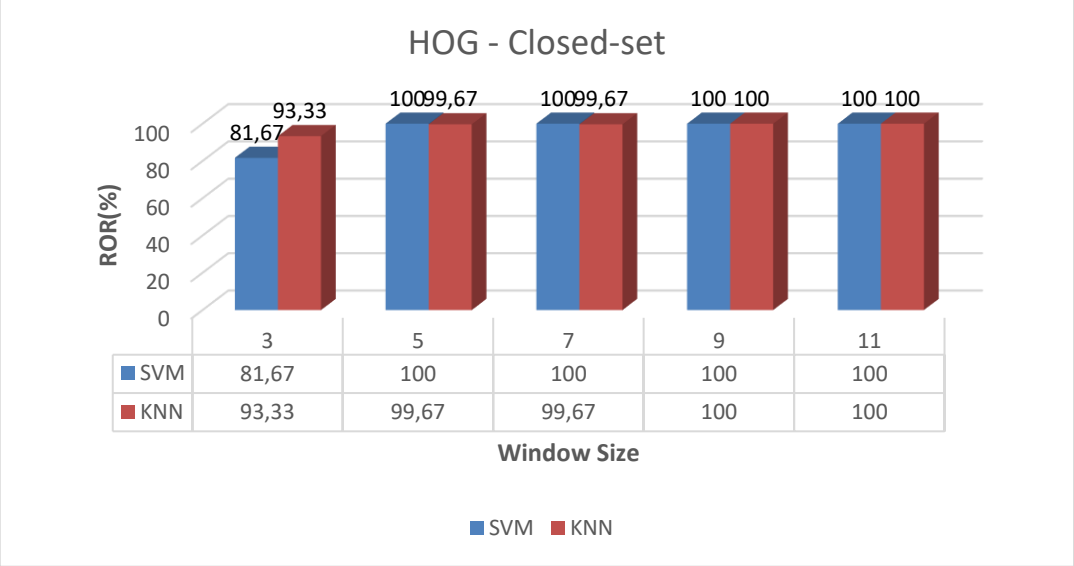


Figure 3. 1. Performance du système biométrique unimodale : Ensemble fermé (HOG)

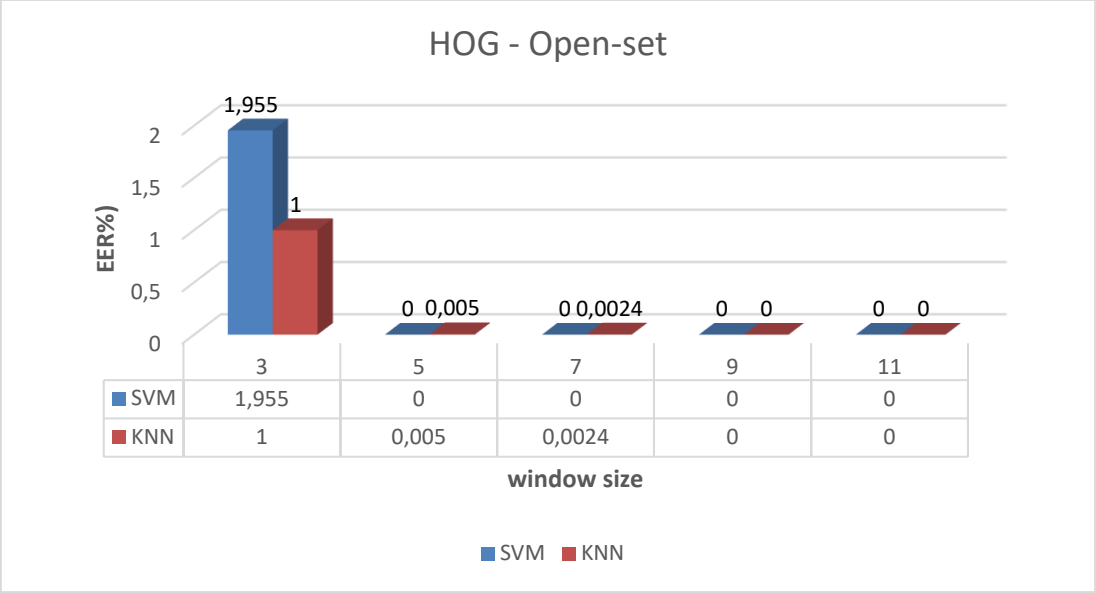


Figure 3. 2. Performance du système biométrique unimodale : Ensemble ouvert (HOG)

3.5.2. Performance du système biométrique unimodale : Système basé sur le LPQ

Pour le système basé sur le LPQ avec les deux classificateurs les résultats comme suivant la différente valeur obtenue dépend des diffèrent taille des blockset voici la variation des EER dans les tableaux suivants :

WIN-SIZE	SVM-LPQ			
	Open-Set		Closed-Set	
	EER (%)	*T0*	ROR (%)	RPR
21	0,7690	0,8127	92,00	18
25	0,3350	0,8098	95,33	20
29	0,3515	0,7835	96,33	55
33	0,3330	0,7567	97,00	52
37	0,6660	0,6902	92,67	102

(a)

WIN-SIZE	KNN-LPQ			
	Open-Set		Closed-Set	
	EER (%)	*T0*	ROR (%)	RPR
21	0,0047	0,9361	99,67	3
25	0,0311	0.9274	99,67	6
29	0,0309	0.8468	99,67	12
33	0,0642	0.7874	99,67	27
37	0,233	0.7083	99,67	68

(b)

Tableau 3.1. : Les performances du système d'identification LPQ

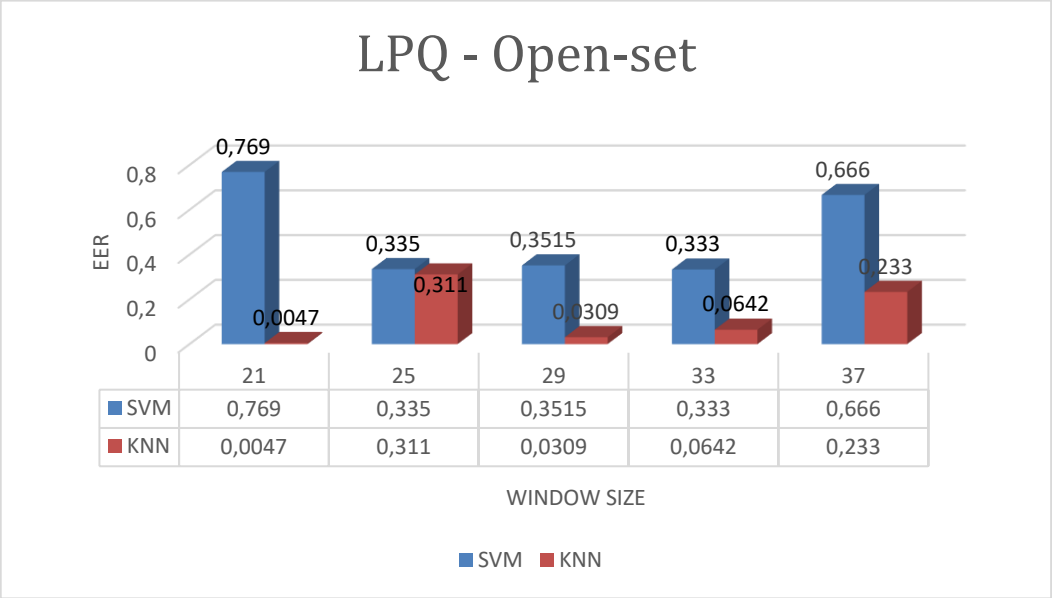


Figure 3. 3. Performance du système biométrique unimodale : Ensemble ouvert (LPQ)

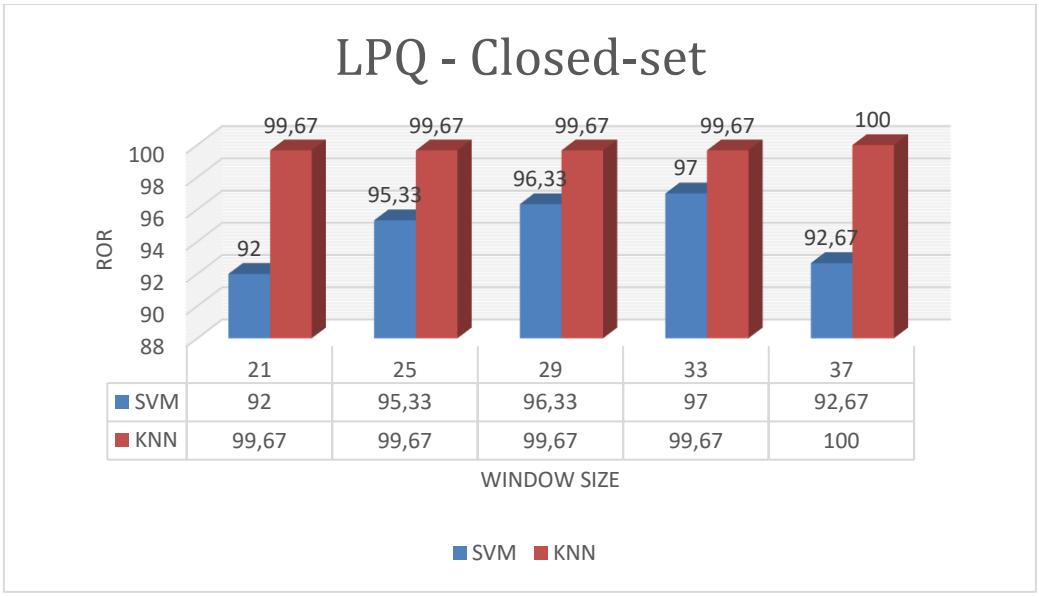


Figure 3. 4. Performance du système biométrique unimodale : Ensemble fermé (LPQ)

3.5.3. Performance du système biométrique multimodale

Les systèmes unimodaux souffrent de certaines limitations et ne peuvent pas fournir des performances de reconnaissance satisfaisantes dans plusieurs cas, comme la possibilité de bruit dans la modalité biométrique et sa non-universalité **[20]**, qui augmente l'erreur du système (EER). La dissimilarité intra-classe, ainsi que la similarité inter-classe, peuvent également avoir un impact sur le système biométrique unimodal et donc sur le résultat de l'identification **[21]**. Un

excellent système d'identification biométrique nécessite une valeur EER très faible, qui peut être atteinte par le système multimodal **[22] [23]**. Un tel système combine plusieurs caractéristiques de chaque modalité à différents niveaux afin d'améliorer les performances du système. La fusion au niveau du score de correspondance est la plus utilisée dans les systèmes biométriques. Dans notre travail, nous fusionnons uniquement les échantillons de l'empreinte palmaire de la base de données (PolyU) au niveau du score de correspondance afin d'améliorer les performances du système.

Dans notre travail on a utilisé la fusion au niveau score par la combinaison des scores issue des algorithmes d'extraction de caractéristiques (HOG) et (LPQ), en appliquant les cinq régles de fusion, à savoir la somme (SUM), le produit (MUL) et la somme pondérée (WHT SUM), le MIN et le MAX. Les performances de notre système d'identification multimodale sont présentées dans les tableaux 3.8 et 3.9. L'analyse des données a montré que les résultats de la fusion multimodale étaient bien meilleurs que ceux des systèmes biométriques unimodaux. Comme le montrent les résultats, l'EER le plus bas de l'identification multimodale a été obtenu en utilisant la combinaison qui sont toujours meilleures que les résultats les plus bas du système unimodal. En outre, les meilleurs résultats ont été obtenus avec un EER = 0.1202 %.

Les meilleurs résultats du système biométrique unimodal étaient de 0,333 % (paramètres extracteur LPQ avec les classificateurs SVM et KNN).

	SUM		**MUL**		**WHT(SUM)**		**MAX**		**MIN**	
	T0	**EER**	**T0**	**EER**	**T0**	**EER**	**T0**	**EER**	**T0**	**EER**
LPQ-SVM-KNN	0.7076	0.2092	0.5347	0.1409	0.7153	0.1601	0.7626	0.3335	0.7142	0.1202

Tableau III.2 : Les performances du système d'identification multimodal

Un excellent système d'identification biométrique nécessite une valeur EER très faible, qui peut être atteinte par le système multimodal **[22]**. Un tel système combine plusieurs caractéristiques de chaque modalité à différents niveaux afin d'améliorer les performances du système.

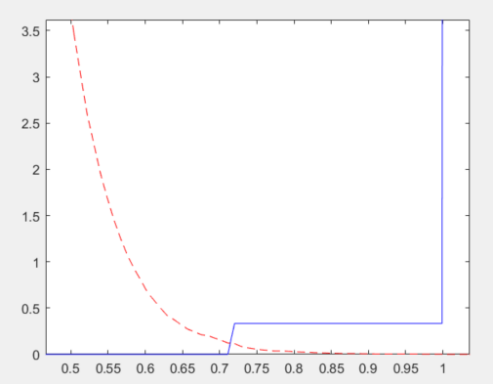


Figure 3.5. *Performance d'un système multimodal après la fusion a règle de MIN*

La fusion au niveau des scores de correspondance est la stratégie de fusion d'informations biométriques la plus couramment utilisée, car les scores de correspondance sont facilement disponibles et conservent suffisamment d'informations.

Pour distinguer la correspondance authentique de la correspondance imposteur. Dans notre travail, nous combinerons (fusionnerons) toutes les échantillons et l'empreinte palmaire NIR au niveau du score correspondant pour améliorer les performances du système. L'expérience a été menée avec cinq méthodes de fusion qui sont la somme des scores (SUM), la somme des scores pondérés (WHT SUM), le produit des scores (MUL), la note maximale (MAX)et la note minimale (MIN), ce dernier qui est le meilleur résultat du test. La figure suivante présente un courbe ROC pour le FAR et le GAR

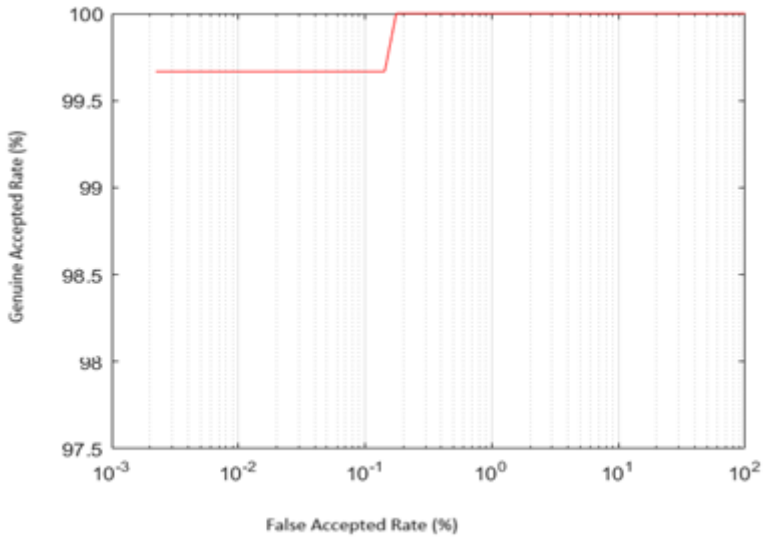


Figure 3. 6. *Résultats des tests du système d'identification biométrique multimodal.*

3.6. Conclusion

Dans ce travail, nous avons proposé des systèmes d'identification unimodaux et multimodaux efficaces pour la reconnaissance rapide des empreintes palmaires. La méthode proposée est basée sur les extracteurs des paramètres HOG et LPQ et nous avons variés les tailles des fenêtres pour chaque algorithme afin de réduire le l'erreur d'identification et d'améliorer la précision de la reconnaissance en résumé, HOG capture des informations sur les formes et les contours, tandis que LPQ capture des informations sur les textures et les motifs dans les images, par conséquent nous avons utilisé les classificateur SVM et KNN

Pour le système multimodal nous utilisons la méthode de fusion des scores de correspondance afin d'améliorer les performances du système unimodal La méthode proposée améliore efficacement la précision de reconnaissance et réduit le nombre de caractéristiques.

De même, le système d'identification multimodale réalisé sur la base de données PolyU offre des optimisations parfaites pour l'identification de l'ensemble ouvert et pour l'identification de l'ensemble fermé. À l'avenir, nous testerons notre méthode proposée avec d'autres grandes bases de données, telles que des images médicales. Nous utiliserons également d'autres techniques de regroupement et de réduction de la dimensionnalité. En outre, nous utiliserons l'unité de traitement graphique (GPU) pour réduire le temps de traitement, qui est un outil très précieux pour accélérer la vitesse de traitement des algorithmes à forte intensité de calcul.

Conclusion Générale

La technologie biométrique est un domaine émergent des technologies de l'information qui reconnaît une personne sur la base d'un vecteur de caractéristiques dérivé de caractéristiques physiologiques ou comportementales spécifiques que la personne possède. Ainsi, parmi plusieurs traits biométriques pouvant être extraits de la main, l'empreinte palmaire est utilisée de manière systématique depuis plusieurs années pour l'identification. Dans ce travail, pour améliorer la capacité de discrimination et la précision du système de classification, nous proposons un système biométrique multimodal où l'empreinte palmaire est analysée en utilisant deux méthodes d'extraction de caractéristiques et est classée avec deux classifiers différents. Ensuite, les résultats obtenus sont combinés par fusion au niveau des scores de correspondance. Dans notre méthode, l'empreinte palmaire est représentée par des caractéristiques extraites à l'aide des méthodes HOG et BSIF, puis classées par les algorithmes KNN et SVM. La méthode proposée est validée pour son efficacité sur la base de données d'empreintes palmaires PolyU disponibles, comprenant 300 utilisateurs.

Les expériences présentées dans ce travail valident la robustesse et l'efficacité de notre proposition. Cependant, des taux d'identification parfaits (EER = 0,000 % et ROR = 100,00 %) ont été obtenus. Pour de futures améliorations, nous envisageons d'explorer d'autres méthodes d'extraction de caractéristiques basées sur l'apprentissage profond telles que les réseaux de neurones convolutifs [24], les machines Boltzmann restreintes [25] et les modèles encodeur-décodeur [26]. De plus, dans biométrie multimodale, nous nous concentrons sur d'autres niveaux de fusion tels que les niveaux de capture, de caractéristiques et de décision pour en améliorer l'efficacité.

Bibliographie

[1] El-Abed, M. (2011). *Évaluation de système biométrique* (Doctoral dissertation, Université de Caen).

[2] Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. *IEEE Transactions on circuits and systems for video technology*, *14*(1), 4-20.

[3] LAMARE, F. (2016). ''OCT en phase pour la reconnaissance biométrique par empreintes digitales et sa sécurisation.''Paris: École doctorale: Informatique. *Télécommunications et Électronique de Paris*..

[4] Massicotte, F. (2007). *La biométrie, sa fiabilité et ses impacts sur la pratique de la démocratie libérale* (Doctoral dissertation, Université du Québec à Montréal).

[5] Meraoumia, A. (2014). *Modèle de Markov caché appliqueé a la multi-biométrie* (Doctoral dissertation, Université des sciences et de la technologie Houari Boumediè).

[6] BENOUAER, A., TAHRINE, S., MERAOUMIA, A., & KORICHI, M. Système biométrique basé sur les motifs locaux binaires orientés (LBP^{θ}).

[7] Zhang, D., Lu, G., & Zhang, L. (2018). *Advanced biometrics*. Springer International Publishing.

[8] Sagar, G. V., Abidali Munna, N. C., Suresh Babu, K., Raja, K. B., & Venugopal, K. R. (2017). Multi scale ICA based iris recognition using BSIF and Hog. *Signal Image Process Int J*, *8*(6), 11-31.

[9] Ojansivu, V., & Heikkilä, J. (2008). Blur insensitive texture classification using local phase quantization. In *Image and Signal Processing: 3rd International Conference, ICISP 2008. Cherbourg-Octeville, France, July 1-3, 2008. Proceedings 3* (pp. 236-243). Springer Berlin Heidelberg.

[10] Aykut, M., & Ekinci, M. (2015). Developing a contactless palmprint authentication system by introducing a novel ROI extraction method. *Image and Vision Computing*, *40*, 65-74.

[11] Wassila, B., & Mohamed, B. Identification Biométrique des Individus par leurs Empreintes Palmaires «Palmprints»: Classification par la Méthode des Séparateurs à Vaste Marge (SVM).

[12] BARKA, K., & BOUKHRIS, Y. (2016). Système d'identification biométrique à base d'un modèle flou.

[13] Zouied, N. (2020). L'empreinte palmaire multispectrale.

[14] Dalal, N., & Triggs, B. (2005, June). Histograms of oriented gradients for human detection. In *2005 IEEE computer society conference on computer vision and pattern recognition (CVPR'05)* (Vol. 1, pp. 886-893). Ieee.

[15] Li, Y., Shan, S., Zhang, H., Lao, S., & Chen, X. (2013). Fusing magnitude and phase Features for robust face recognition. In *Computer Vision–ACCV 2012: 11th Asian Conference on Computer Vision, Daejeon, Korea, November 5-9, 2012, Revised Selected Papers, Part II 11* (pp. 601-612). Springer Berlin Heidelberg.

[16] Chan, C. H., Tahir, M. A., Kittler, J., & Pietikainen, M. (2012). Multiscale local phase quantization for robust component-based face recognition using kernel fusion of multiple descriptors. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *35*(5), 1164-1177.

[17] Boumazza, A. (2023). Identification des personnes par les empreintes palmaires.

[18] Tanvir, K., Jony, A. I., Haq, M. K., Nazera, F., Dass, M., & Raju, V. (2023). Clinical Insights Through Xception: A Multiclass Classification of Ocular Pathologies. *Tuijin Jishu/Journal of Propulsion Technology*, *44*(04), 2023.

[19] Dass, S. C., Nandakumar, K., & Jain, A. K. (2005). A principled approach to score level Fusion in multimodal biometric systems. In *Audio-and Video-Based Biometric Person Authentication: 5th International Conference, AVBPA 2005, Hilton Rye Town, NY, USA, July 20-22, 2005 Proceedings 5* (pp. 1049-1058). Springer Berlin Heidelberg.

[20] Wang, F., & Han, J. (2008). Robust multimodal biometric authentication integrating iris, face and palmprint. *Information technology and control*, *37*(4).

[21] Oloyede, M. O., & Hancke, G. P. (2016). Unimodal and multimodal biometric sensing systems: a review. *IEEE access*, *4*, 7532-7555.

[22] Yang, W., Hu, J., Wang, S., & Chen, C. (2015). Mutual dependency of features in multimodal biometric systems. *Electronics letters*, *51*(3), 234-235.

[23] Kant, C., & Chaudhary, S. (2021). A multimodal biometric system based on finger knuckle print, fingerprint, and palmprint traits. In *Innovations in Computational Intelligence and Computer Vision: Proceedings of ICICV 2020* (pp. 182-192). Springer Singapore.

[24] Patterson, J., & Gibson, A. (2017). *Deep learning: A practitioner's approach*. " O'Reilly Media, Inc.".

[25] Ackley, D. H., Hinton, G. E., & Sejnowski, T. J. (1985). A learning algorithm for Boltzmann Machines. *Cognitive science*, *9*(1), 147-169.

[26] Chandar AP, S., Lauly, S., Larochelle, H., Khapra, M., Ravindran, B., Raykar, V. C., & Saha, A. (2014). An autoencoder approach to learning bilingual word representations. *Advances in neural information processing systems*, *27*.

[27] Zhang, D. (2006). Polyu palmprint database. *Biometric Research Centre, Hong Kong Polytechnic University,(Online) Available from:(http://www. comp. polyu. edu. hk/biometrics/)*.