

République Algérienne Démocratique et Populaire
Ministère de l'enseignement supérieur et de la recherche scientifique
Université 8Mai 1945 – Guelma
Faculté des sciences et de la Technologie
Département d'Electronique et Télécommunications



**Mémoire de fin d'étude
Pour l'obtention du diplôme de Master Académique**

Domaine : **Sciences et Technologie**
Filière : **Electronique**
Spécialité : **Instrumentation**

Identification palmaire par la représentation multi-échelle

Présenté par :

Feraga Abdelhak

Sous la direction de :

Dr. Doghmane Hakim

Juillet 2019

Dédicace

Je dédie ce modeste travail

A mes chères parentes pour tous leurs sacrifices, leur amour, leur tendresse, leur soutien et leurs prières tout au long de mes études,

A mes très beaux frères : LOTFI et ABD EL AZIZ

A toute ma famille Feraga

A tous mes amis : RIYAD MOHAMED SALEH REZAK FAOUZI ACHREF MOUDJIB OSEMA YOUNES et MOHAMED pour leur appui et leur encouragement,

Sans oublier tous les enseignants et les professeurs qui m'ont orienté durant toute ma carrière d'étude.

Remerciements

J'ai l'honneur d'être dirigé par mon Professeur Dr. Dougheman, dans la présente recherche.

Je vous remercie énormément mon professeur pour avoir encadré et suivi ce travail.

Merci beaucoup pour votre disponibilité, pour les nombreuses et intéressantes discussions scientifiques, pour les remarques et orientations constructives, pour les nombreux conseils avisés, pour vos encouragements quotidiens, pour ne pas avoir cessé, pour le soutien permanent, pour votre compréhension, pour la confiance que vous avez accordée et qu'il a toujours témoignée à mon égard, pour votre écoute et tout simplement pour votre gentillesse.

Je tiens à exprimer tout au fond de mon cœur mes reconnaissances à département d'électronique et télécommunication pour toutes les années de spécialité et ce que je pris de la science et de la connaissance.

Résumé

Au cours des dernières années, l'identification automatique des individus devient une exigence importante pour une variété d'applications telles que le contrôle d'accès et les systèmes de surveillance. Les systèmes biométriques offrent une identification automatique de l'identité, basés sur des mesures physiologiques et/ou comportementales de l'individu. Nous nous sommes intéressés dans cette étude à la modalité biométrique paume de la main (palmprint).

La reconnaissance par palmprint possède plusieurs avantages par rapport aux autres technologies; elle est non-intrusive et facile à utiliser. Cependant, une identification rapide et précise par palmprint présente toujours un certain nombre de défis et de difficultés, particulièrement dans les environnements non-contrôlés.

Dans le cadre de ce travail, nous utilisons une approche d'extraction des caractéristiques basée principalement sur une représentation multi-échelle par l'utilisation de l'ondelette de Gabor, dans le but d'identifier les individus à partir des images d'intensités 2D de palmprints dans des conditions non-contrôlées. En effet, quatre étapes sont réalisées pour générer le vecteur caractéristique : i) prétraitement et extraction de la région d'intérêt (ROI), ii) Gabor Wavelet, iii) le descripteur LPQ est utilisé, iv) La méthode SPH (Spatial Pyramid Histogram) décomposition. De plus, le classifieur K-NN est utilisé avec la distance intersection dans la phase de classification. Pendant cette étude des expérimentations sont réalisées sur la base de données de palmprint PolyU.

Mots-clés: Palmprint, ondelette de Gabor, SPH, WLDA.

Abstract

In recent years, automatic identification of individuals has become an important requirement for a variety of applications such as access control and surveillance systems. Biometric systems offer automatic identification of identity, based on physiological and/or behavioural measures of the individual. We were interested in this study in the biometric palmprint modality.

Palmprint recognition has several advantages over other technologies; it is non-intrusive and easy to use. However, rapid and accurate identification by palmprint still

presents a number of challenges and difficulties, especially in uncontrolled environments.

In this work, we use a feature extraction approach based mainly on a multi-scale representation using the Gabor wavelet, in order to identify individuals from 2D intensity images of palmprints under uncontrolled conditions. Indeed, four steps are performed to generate the characteristic vector: i) pre-treatment and extraction of the region of interest (ROI), ii) Gabor Wavelet, iii) the LPQ descriptor is used, iv) The SPH (Spatial Pyramid Histogram) decomposition method. In addition, the K-NN classifier is used with the distance intersection in the classification phase. During this study, experiments are carried out on the PolyU palmprint database.

Keywords: Palmprint, Gabor wavelet, SPH, WLDA

ملخص:

في السنوات الأخيرة ، أصبح التحديد التلقائي للأفراد مطلبًا مهمًا لمجموعة متنوعة من التطبيقات مثل أنظمة التحكم في الوصول والمراقبة. توفر الأنظمة الحيوية التعرف التلقائي للهوية ، بناءً على القياسات الفسيولوجية أو السلوكية للفرد. ونحن مهتمون في هذه الدراسة براحة اليد (Palmprints)

التعرف على كف اليد لديه العديد من المزايا على التقنيات الأخرى ؛ انها غير تدخلية وسهلة الاستخدام. ومع ذلك ، فإن التحديد السريع والدقيق بواسطة راحة اليد يمثل دائمًا عددًا من التحديات والصعوبات ، لا سيما في البيئات غير المنضبطة.

كجزء من هذا العمل ، نستخدم نهجًا لاستخراج المعالم يعتمد أساسًا على تمثيل متعدد المقاييس باستخدام الموجات غابور ، من أجل تحديد الأفراد من الصور الكثيفة 2D palmprints. في ظل ظروف غير المنضبطة. في الواقع ، يتم تنفيذ أربع خطوات لإنشاء المتجه المميز (i) :المعالجة واستخراج المنطقة ذات الاهتمام (ROI) ، (ii) Gabor Wavelet ، (iii) استخدام واصف LPQ ، (iv)طريقة SPH الهرم المكاني المدرج التكراري (التحلل. بالإضافة إلى ذلك ، يتم استخدام المصنف K-NN مع مسافة التقاطع في مرحلة التصنيف. خلال هذه الدراسة ، يتم إجراء تجارب على قاعدة بيانات PolyU palmprint.

كلمات مفتاحية: Palmprint ، Gabor Wavelet ، SPH ،

Sommaire

Remerciement.....	i
Dédicace.....	ii
Résumé.....	iv
Liste des figures.....	viii
Liste des tableaux.....	xi
Liste des acronymes.....	xii
Introduction générale.....	1

Chapitre 1

1.1 Introduction	2
1.2 Définition de la biométrie.....	2
1.2.1 Les caractéristiques biométriques	2
1.2.2 Les modèles biométriques.....	4
1.2.3 Les modalités biométriques.....	5
1.2.4 Utilisation de la biométrie.....	9
1.2.5 La biométrie et les méthodes d'authentification traditionnelle.....	10
1.2.6 Les applications de la biométrie.....	11
1.3. Systèmes biométriques.....	12
1.3.1 Modes de fonctionnement.....	12
1.3.2 Architecture d'un système biométrique.....	14
1.3.3 Les types de systèmes biométriques.....	15
1.3.3.1 Les systèmes multimodaux.....	16
1.3.3.2 L'architecture des systèmes multimodaux.....	19
1.3.4 Les niveaux de fusion.....	20

1.3.4.1 La fusion pré-classification.....	21
1.3.4.2 La fusion post-classification.....	22
1.3.5 Principe de fonctionnement d'un système biométrique.....	24
1.3.6 Performance d'un système biométrique.....	24
1.4. Les avantages et les limites de la biométrie.....	26
1.4.1 Les avantages de la biométrie.....	26
1.4.2 Les limites de la biométrie.....	26
1.5 Conclusion.....	28

Chapitre 2

2.1. Introduction.....	30
2.2. Palmaire	30
2.2.1. Les Caractéristiques de palmaire	30
2.2.1.1. Caractéristiques géométriques	30
2.2.1.2. Les lignes principales de palmaire	31
2.2.1.3. Les caractéristiques de rides	32
2.2.1.4. Points de référence	32
2.2.1.5. Les caractéristiques de minutie	32
2.2.2. Reconnaissance de palmaire 3D	33
2.2.2.1. Motivations de l'utilisation palmaire 3D	33
2.2.2.2. Acquisition des images de palmaire 3D	33
2.2.2.3. Algorithmes des représentations des images de palmaire 3D.....	34
2.2.3. Algorithmes d'extraction des caractéristiques et classification des images palmaire (2D et 3D)	36
2.3. Palmaire multi spectrales	37
2.3.1. Le dispositif d'acquisition des images palmaire multi spectrales	38

2.3.2. Algorithmes d'extraction des caractéristiques et classification des images de palmaire multi spectrales	40
2.4. Conclusion	42

Chapitre 3 :

3.1 Introduction	44
3.2 Représentation palmaire par DGLSPH.....	44
3.2.1 La méthode de la décomposition spatiale pyramidale (SPH).....	48
3.2.2 La méthode d'analyse discriminante linéaire blanchie (WLDA).....	49
3.2.3 Etape de classification.....	49
3.3 Etude Expérimentale.....	50
3.3.1 La base de données PolyU.....	50
3.3.1.1 Expérimentation 1.....	51
3.3.1.2 Expérimentation 2.....	52
3.4 Conclusion.....	54
Conclusion générale.....	55
Bibliographie	56

Listes de figures

Les figures de chapitres 1

Figure.1.1 Quelques modalités biométriques.	4
Figure.1.2 Quelques exemples de modèles biométriques. De gauche à droite, de haut en bas : minuties extraites d'une empreinte, Iris code, graphe d'un visage utilisant les points d'intérêt, signal vocal et signal de dynamique de frappe au clavier.	5
Figure.1.3 Images de l'empreinte digitale	6
Figure.1.4 Géométrie de la main	6
Figure.1.5 L'iris	7
Figure.1.6 La rétine.....	7
Figure.1.7 La voix.....	8
Figure.1.8 Visage	8
Figure.1.9 Parts de marché des techniques biométriques en 2009.....	10
Figure.1.10 Enrôlement d'une personne dans un système biométrique.....	12
Figure.1.11 Authentification d'un individu dans un système biométrique.....	13
Figure.1.12 Identification d'un individu dans un système biométrique	14
Figure.1.13 Architecture générique d'un système biométrique (extrait de l'Organisation Internationale de Normalisation ISO/IEC 19795-1 [5]).	15
Figure.1.14 Systèmes multi algorithmes	16
Figure.1.15 Systèmes multi échantillons	17
Figure.1.16 Systèmes multi capteurs	17
Figure.1.17 Systèmes multi instances.....	18
Figure.1.18 Systèmes multi caractères.....	18
Figure.1.19 Architecture de fusion en parallèle.....	19
Figure.1.20 Architecture de fusion en série (incrémentale ou séquentielle)	20

Figure.1.21 Les différents niveaux de fusion	20
Figure.1.22 Schéma de fusion au niveau du capteur	21
Figure.1.23 Schéma de fusion au niveau de l'extraction des caractéristiques	22
Figure.1.24 Schéma de fusion au niveau de la décision.....	23
Figure.1.25 Schéma de fusion au niveau de scores	23
Figure.1.26 Illustration du FRR et du FAR	25

Les figures de chapitres 2

Figure 2.1 Caractéristiques géométriques de palmaire	31
Figure 2.2 Les quatre principales lignes de l'image de palmaire.....	31
Figure 2.3 Les rides, les crêtes et les points de référence sur l'image de palmaire.....	32
Figure 2.4 Minuties de palmaire.....	33
Figure 2.5 Un dispositif d'acquisition d'images 3D basé sur la lumière et un exemple image de palmaire 3 D	34
Figure 2.6 1ere ligne les ROI 3D images de palmaire.....	36
Figure 2.7 La structure interne d'un dispositif d'acquisition d'image palmaire multi spectrale	38
Figure 2.8 la structure externe d'un dispositif d'acquisition d'image palmaire multi spectrale	39
Figure 2.9 la plate-forme et la fixation de la main	39

Les figures de chapitre 3

Figure 3.1 Schéma de principe de la méthode utilisée.....	45
Figure 3.2 Illustration de la représentation palmaire DGLSPH	46
Figure 3.3 Illustration de détection de la région d'intérêt (ROI) palmaire.	47
Figure 3.4 Partie réelle de l'ondelette de Gabor avec deux échelles et quatre orientations. (a) Taille de la fenêtre est de 4x4, (b) Taille de la fenêtre est de 8x8.....	48

Figure 3.5 Les stratégies de décomposition verticale en plusieurs sous-blocs.....	49
Figure 3.6 Quelques ROIs extraits des images palmaires de la base de données PolyU (a) Première session, (b) Seconde session.....	51
Figure 3.7 Taux d'erreur d'identification palmaire sur la base de données poly	53
Figure 3.8 Courbes CMC sur la base de données PolyU.....	54

Liste des tableaux

Tableau 1.1 : Comparaison entre les techniques biométriques.....	4
Tableau 1.2: Comparaison entre l'authentification biométrique et par mot de passe/clé.....	11
Tableau 3.1 : Taux d'identifications utilisant la représentation DGLSPH sur la base de données PolyU.....	52
Tableau 3.2: Taux d'identifications utilisant la représentation GLSPH sur la base de données PolyU.....	52
Tableau 3.3: Différents protocoles d'identification des empreintes palmaires utilisés dans les bases de données PolyU et PolyU 2D/3D.....	52
Tableau 3.4: Etude comparative de la méthode proposée avec les méthodes de codage sur la base de données PolyU.....	53

Liste des acronymes

ADN : Acide Désoxyribo Nucléique

BD : Base des données ("Data Base")

CCD: Récepteurs à transferts de charge (" charge coupled device")

CR: La représentation collaborative

DET: Courbes représentant les taux d'erreurs en échelle logarithmique

("Detection Error Trade-off curve")

DFB : la banque de filtres directionnels ("Directional Filter Bank")

DWT: La transformée en ondelettes discrète ("Discrete Wavelet Transform")

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 ")

GCI : Image de courbure gaussienne ("Gaussian curvature image")

HTER : Taux d'erreur moyenne ("Half Total Error Rate ")

HMM : Modèle de Markov caché ("Hidden Model Markov")

IBLDA: Image-Based Linear Discriminant Analysis

ICA : Analyse en composantes indépendantes ("Independent Component Analysis")

ICP : Iterative Closest Point

KLDA : Analyse Discriminante Linéaire à noyau ("kernel Linear Discriminate Analysis")

KPCA : Analyse en composantes principales à noyau ("kernel Principal Component Analysis")

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

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

LBP-HF: Local Binary Pattern Histogram Fourier Features

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

LIF : Index du doigt gauche ("Left Index Finger")

LGIC: Local-Global Information combination

LGBP: Local Gabor Binary Patterns

LMF : Milieu du doigt gauche ("Left Middle Finger")

MAD : Median Absolute Deviation

MCI : Une image de courbure moyenne ("Mean curvature image")

MLE : Maximum de vraisemblance ("Maximum Likelihood Estimation")

MMDA : Multi-manifold discriminant analysis

MSLBP: Modèle binaire local à multiéchelles ("the Multi-scale Shift Binary") Pattern

NIR: Near-infrared

OLOF: Orthogonal Line Ordinal Feature

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

PIN : Numéro d'Identification Personnel ("Personnal Identification Number")

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

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

RIF : Index du doigt droit ("Right Index Finger")

RMF : Milieu du doigt droit ("Right Middle Finger")

SIFT : Scale Invariant Feature transform

SR-KDA : Spectral regression kernel discriminant analysis

ST: Surface Type

TFR : Le taux de faux rejet ("False Reject Rate" ou FRR)

TFA: Le taux de fausse acceptation (“False Accept Rate” ou FAR)

TPTSR: Two-Phase Test Sample Representation

WLDA : La méthode d'analyse discriminante linéaire blanchie

Introduction générale

Durant tout le XX siècle, le mot « biométrie » a été utilisé quasi exclusivement dans le sens très large de « étude quantitative des êtres vivants », notamment à l'aide des méthodes statistiques. C'est dans cette optique que la revue Biométrie paraît depuis 1901 et que Société internationale de Biométrie (The International Biométrie Society) a été fondée en 1947.

La reconnaissance des individus a connu plus d'importance dans la vie humaine quotidienne. Elle assure les transactions des personnes en différents domaines afin d'assurer une sécurité pertinente. Dans les dernières années, la pratique des systèmes de reconnaissance reste limitée aux grands secteurs tels que le secteur militaire et d'autres secteurs nécessitant de nombreuses applications telles que la protection de l'accès à un ordinateur, un téléphone portable, une clé USB, un établissement, des cartes bancaires.... De nombreuses technologies biométriques ont été développées, toutes basées sur les identificateurs biométriques physiologiques et comportementales telles que : l'iris, la voix, les empreintes digitales, le visage, la signature.... Ces derniers sont plus fiables que les systèmes classiques (clé, mot de passe. . .) dans la reconnaissance d'une personne car ils sont difficilement falsifiables. C'est la raison pour laquelle les systèmes biométriques sont actuellement de plus en plus sollicités.

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

Dans cette étude, on a choisi un système de reconnaissance par les empreintes palmaires. Ce système utilise la forme de la partie intérieure de la main pour l'extraction des caractéristiques biométriques d'identification des individus. Ces caractéristiques sont permanentes et stables durant toute la vie, aussi uniques pour chacun. Notre travail est articulé sur trois chapitres :

Le premier chapitre : nous avons défini la biométrie ainsi que les différentes techniques biométriques utilisées. Ce chapitre est finalisé par un aperçu sur les principaux domaines d'application de la biométrie.

Le deuxième chapitre : on décrit l'état de l'art des méthodes d'extraction des caractéristiques palmaires.

Le troisième chapitre : explique en détails la méthode utilisée pour la représentation palmaire et les différentes expériences réalisées dans le cadre de ce travail.

Chapitre 1

1.1 Introduction :

Un système biométrique est essentiellement un système de reconnaissance de formes qui utilise les données biométriques d'un individu. Les systèmes biométriques sont de plus en plus utilisés depuis quelques années. L'apparition de l'ordinateur et sa capacité à traiter et à stocker les données ont permis la création des systèmes biométriques informatisés. Nous introduirons dans ce chapitre quelques notions et définitions de base liées à la biométrie. Nous donnerons le principe de fonctionnement des systèmes biométriques ainsi que les outils utilisés pour mesurer leurs performances. Nous insisterons surtout sur la place de la reconnaissance faciale parmi les autres techniques biométriques, car elle constitue l'objectif de ce thème.

1.2 Définition de la biométrie :

Il existe trois façons génériques pour vérifier ou déterminer l'identité d'un individu :

- ce que l'on sait (code PIN, mot de passe, etc.)
- ce que l'on possède (badge, carte à puce, etc.)
- ce que l'on est ou ce que l'on sait faire (empreinte digitale, dynamique de frappe au clavier, etc.)

Ce dernier point fait référence à la biométrie.

La biométrie consiste à vérifier ou déterminer l'identité d'un individu à partir de ses caractéristiques biologiques (comme l'ADN), comportementales (comme la voix) ou morphologiques (comme l'empreinte digitale).

1.2.1 Les caractéristiques biométriques :

Les caractéristiques biométriques par lesquelles il est possible de vérifier l'identité d'un individu sont appelées modalités biométriques. La figure 1 illustre un exemple de quelques modalités biométriques. Ces modalités sont basées sur l'analyse des données liées à l'individu et sont généralement classées en trois catégories: biométrie biologique, comportementale et morphologique. La biométrie biologique se base sur l'analyse des données biologiques liées à l'individu (salive, ADN, etc.). La biométrie comportementale se base sur l'analyse de comportements d'un individu (manière de marcher, dynamique de frappe au clavier, etc.). La biométrie morphologique se base sur les traits physiques particuliers qui, pour toutes personnes, sont permanents et

uniques (empreinte digitale, visage, etc.). Pratiquement, n'importe quelle caractéristique morphologique ou comportementale peut être considérée comme une caractéristique biométrique, dans la mesure où elle satisfait les propriétés suivantes [1]

- **Universalité** : toutes les personnes à identifier doivent la posséder ;
- **Unicité** : l'information doit être aussi dissimilaire que possible entre les différentes personnes.
- **Permanence** : l'information collectée doit être présente pendant toute la vie d'un individu.
- **Collectabilité** : l'information doit être collectable et mesurable afin d'être utilisée pour les comparaisons.
- **Acceptabilité** : le système doit respecter certains critères (facilité d'acquisition, rapidité, etc.) afin d'être employé.

Les caractéristiques biométriques ne possèdent pas toutes ces propriétés, ou les possèdent mais à des degrés différents. Le tableau 1, extrait de [2], compare les principales modalités biométriques selon les propriétés suivantes : universalité, unicité, permanence, Collectabilité, acceptabilité et performance. Ce tableau montre qu'aucune caractéristique n'est donc idéale et qu'elles peuvent être plus ou moins adaptées à des applications particulières. Par exemple, l'analyse basée sur l'ADN est une des techniques les plus efficaces pour vérifier l'identité d'un individu ou l'identifier [3]. Néanmoins, elle ne peut pas être utilisée pour le contrôle d'accès logique ou physique pour des raisons de temps de calcul, mais aussi, parce que personne ne serait prêt à donner un peu de sang pour faire la vérification. Le choix de la modalité est ainsi effectuée selon un compromis entre la présence ou l'absence de certaines de ces propriétés selon les besoins de chaque application. A noter que le choix de la modalité biométrique peut aussi dépendre de la culture locale des usagers. En Asie, les méthodes nécessitant un contact physique comme les empreintes digitales sont rejetées pour des raisons d'hygiène alors que les méthodes sans contact sont plus répandues et acceptées.

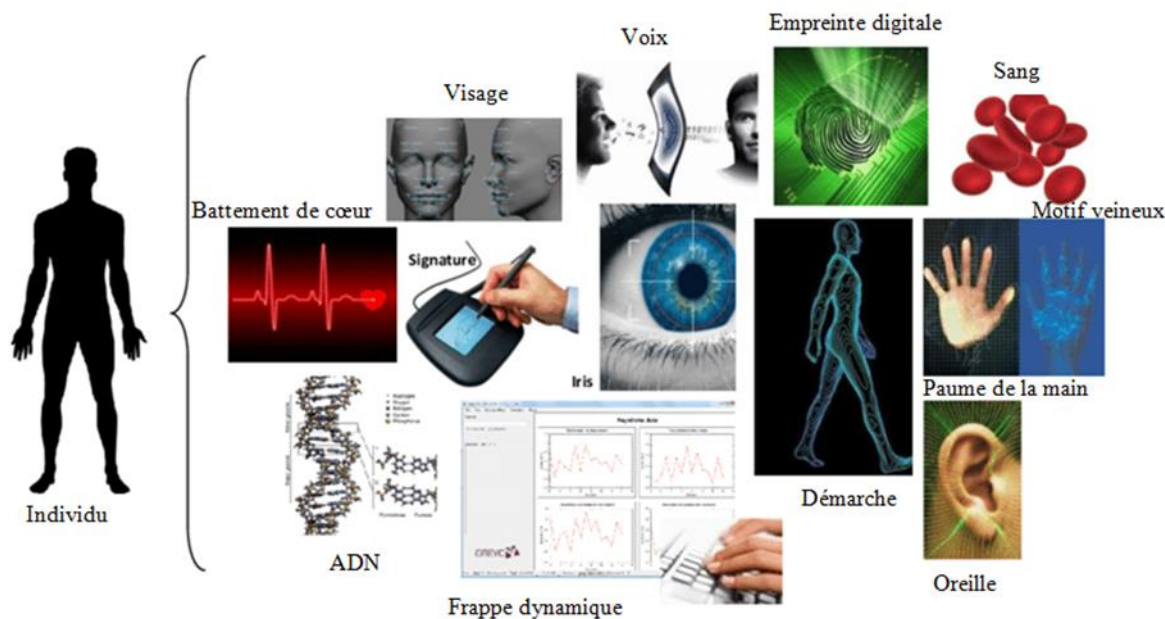


Figure 1.1 : Quelques modalités biométrie

biométrie	Universalité	Unicité	Permanence	Mesurabilité	Performance	Acceptabilité	Circonvention
DNA	Haute	Haute	Haute	Faible	Haute	Faible	Faible
Oreille	Moyenne	Moyenne	Haute	Moyenne	Moyenne	Haute	Moyenne
Visage	Haute	Faible	Moyenne	Haute	Faible	Haute	Haute
Thermo Visage	Haute	Haute	Faible	Haute	Moyenne	Haute	Haute
Empreinte	Moyenne	Haute	Haute	Moyenne	Haute	Moyenne	Moyenne
Démarche	Moyenne	Faible	Faible	Haute	Faible	Haute	Moyenne
Géométrie Main	Moyenne	Moyenne	Moyenne	Haute	Moyenne	Moyenne	Moyenne
Veine Main	Moyenne	Moyenne	Moyenne	Moyenne	Moyenne	Moyenne	Faible
Iris	Haute	Haute	Haute	Moyenne	Haute	Faible	Faible
Frappe Clavier	Faible	Faible	Faible	Moyenne	Faible	Moyenne	Moyenne
Odeur	Haute	Haute	Haute	Faible	Faible	Moyenne	Faible
Rétine	Haute	Haute	Moyenne	Faible	Haute	Faible	Faible
Signature	Faible	Faible	Faible	Haute	Faible	Haute	Haute
Voix	Moyenne	Faible	Faible	Moyenne	Faible	Haute	Haute

Tableau 1: Comparaison entre les techniques biométriques [2].

1.2.2 Les modèles biométriques :

Un modèle biométrique (appelé aussi gabarit ou Template) est l'ensemble des données utilisées pour représenter un utilisateur. Les caractéristiques biométriques acquises ne sont pas enregistrées et utilisées telles quelles. Une phase de traitement est

effectuée pour réduire les données biométriques brutes et produire ainsi le modèle biométrique. La figure 2 illustre quelques exemples de modèles biométriques. Pour le stockage de ces modèles, il existe quatre emplacements principaux que sont le l'EUSB, la base centralisée, la machine individuelle de travail et le capteur biométrique. Chacun de ces emplacements présente des avantages et faiblesses en termes de temps de traitement, confidentialité et respect de la vie privée. En France, l'utilisation de la base centralisée est proscrite pour un nombre d'individus élevé par la Commission Nationale Informatique et Libertés (CNIL).

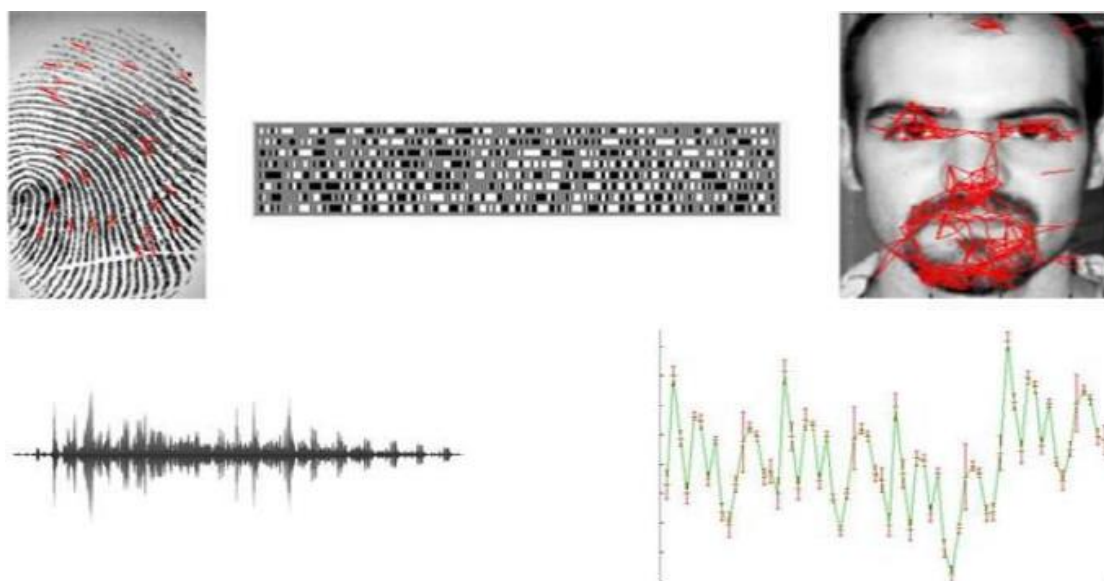


Figure 1.2: Quelques exemples de modèles biométriques. De gauche à droite, de haut en bas : minuties extraites d'une empreinte, Iris code, graphe d'un visage utilisant les points d'intérêt, signal vocal et signal de dynamique de frappe au clavier.

1.2.3 Les modalités biométriques

La multitude des caractères biométriques de l'être humain a donné naissance à plusieurs systèmes d'authentification, chacun repose sur un caractère morphologique ou comportemental, parmi ces systèmes il y a ceux qui ont prouvé leur fiabilité et leurs cours d'évolution.

-Les systèmes morphologiques : Ce type de systèmes est basé sur l'identification de traits physiques particuliers qui, pour toute personne, sont uniques et permanents. Cette catégorie regroupe la reconnaissance des empreintes digitales, de la forme de la main, de la forme du visage, de la rétine, de l'ADN et de l'iris de l'œil.

- **Les Empreintes digitales** : Il s'agit d'une des premières biométries utilisées dans des machines d'authentification, La formation des empreintes dépend des conditions initiales développement embryogénique, ce qui les rend uniques à chaque personne et même à chaque doigt.



Figure 1.3 : Images de l'empreinte digitale

- **Géométrie de la main** : Il consiste à mesurer plusieurs caractéristiques de la main (jusqu'à 90) telle que la forme de la main, longueur et largeur des doigts, formes des articulations, longueurs inter articulations, &etc. La technologie associée à cela est principalement de l'imagerie infrarouge.



Figure 1.4 : Géométrie de la main

- **L'iris** : est la membrane colorée de l'œil. Une caméra proche des infrarouges photographie une tranche de l'iris, elle relève les caractéristiques particulières du relief.

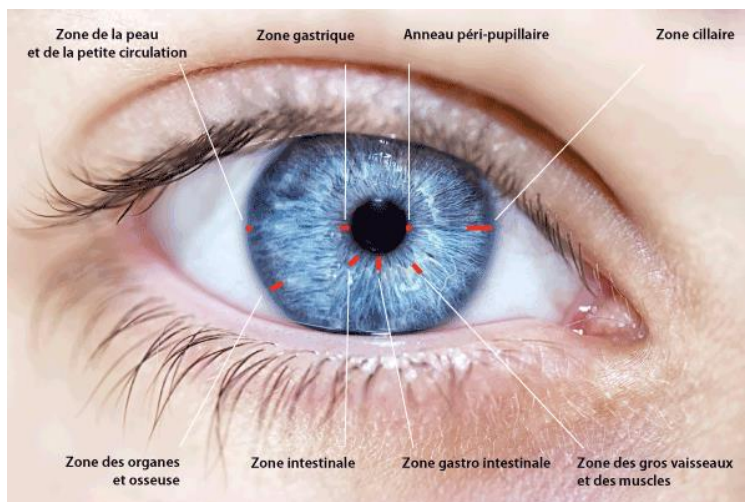
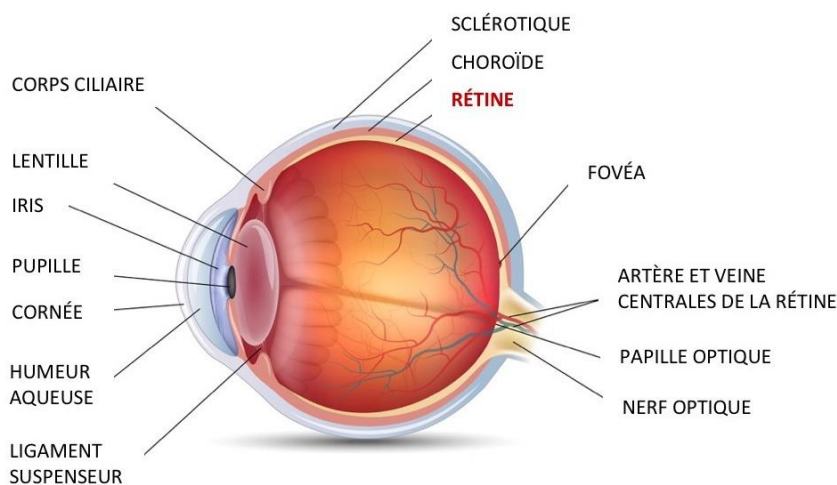


Figure 1.5 : L'iris

- **La rétine** : Il a été montré que chaque S'il possède en sa rétine un vaisseau sanguin. La technique basée sur la rétine utilise la texture de ces vaisseaux. L'identification consiste à éclairer le fond de l'œil par un faisceau lumineux de faible intensité.



© Copyrighted - translated by Pro Visu

Figure 1.6 : La rétine

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

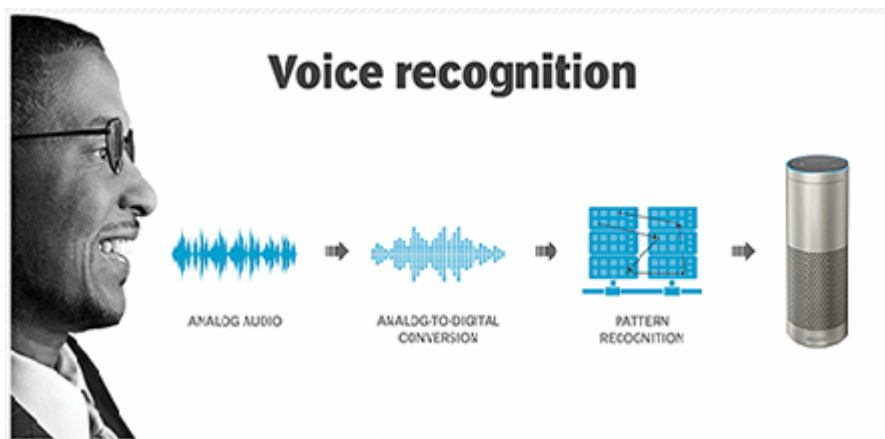


Figure 1.7 : La voix

- **Le visage** : Il s'agit de capter la forme du visage d'un individu et d'en extraire certaines informations jugées évidentes pour l'authentification.

Selon le système utilisé, l'individu doit être positionné devant l'appareil où peut-être en mouvement à une certaine distance. Les données biométriques qui sont obtenues sont par la suite comparées au fichier référence. Au début des années 1970, la reconnaissance par le visage était principalement basée sur des attributs faciaux mesurables comme l'écartement des yeux, des sourcils, des lèvres, la position du menton, la forme, & etc. Depuis les années 1990, les différentes technologies utilisées exploitent toutes les découvertes effectuées dans le domaine du traitement d'image et de l'analyse de données.

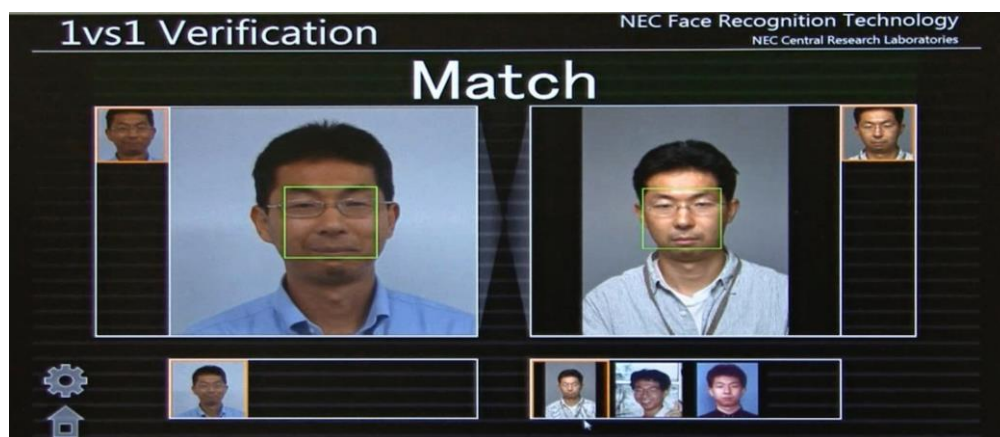


Figure 1.8 : Visage

Les systèmes comportementaux : Ce type de systèmes se base sur l'analyse de certains comportements d'une personne comme le tracé de sa signature, sa démarche et sa façon de taper sur un clavier.

Les modalités biologiques : Elle est basée sur l'identification de traits biologique particuliers.

- ADN
- Odeur
- Salive
- Urine
- Cheveux
- Veines de la main

1.2.4 Utilisation de la biométrie

Le champ d'application de la biométrie est très vaste. En effet, tous les domaines qui nécessitent de vérifier ou d'déterminer l'identité de personnes sont concernés. On retrouve ainsi des applications de la biométrie pour gérer l'accès à des ressources physiques (comme l'accès à des lieux sécurisés) et logiques (comme le commerce électronique). La biométrie intéresse aussi plusieurs pays (l'Europe, les Etats-Unis, etc.) afin de produire des titres d'identité plus sûres, telle que la carte nationale d'identité ou le passeport biométrique. A noter qu'en France, le passeport biométrique est désormais d'employé. Il intègre une puce RFID qui contient au moins deux informations biométriques : une empreinte digitale et une image du visage numérisée. Enfin, la biométrie n'a pas que des applications à vocation sécuritaire, mais également des applications qui facilitent le quotidien des usagers. Ainsi, la biométrie est utilisée dans certains aéroports permettant aux clients réguliers de ne pas perdre de temps lors de l'embarquement. La figure 9, réalisée d'après les chiffres d'International Biométrie Group [4], montre les parts de marché des principales méthodes biométriques en 2009. Les empreintes digitales sont toujours les plus utilisées, suivies par la reconnaissance faciale. Ces deux modalités représentent les trois quarts du marché de la biométrie.

Parts de marché des procédés biométriques

Source : International Biometric Group, 2009

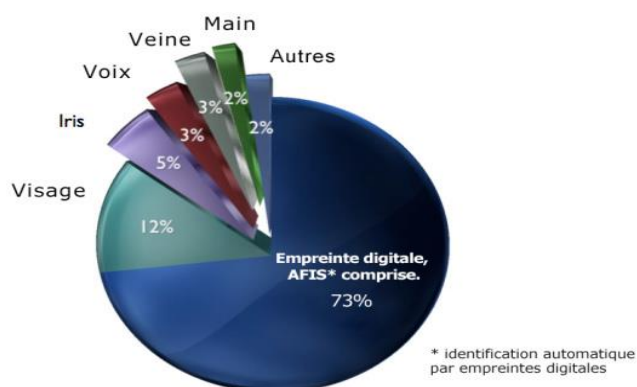


Figure 1.9 : Parts de marché des techniques biométriques en 2009 [4]

1.2.5 La biométrie et les méthodes d'authentification traditionnelles :

Puisque la biométrie fait appel à ce que l'on est, elle comporte un avantage primordial sur les méthodes traditionnelles, dans le sens où elle évite l'usage d'un grand nombre de mots de passe complexes, de badges, etc. Le tableau 2 présente un parallèle entre la biométrie et les méthodes d'authentification traditionnelles. Ce tableau montre que les systèmes biométriques facilitent le processus d'authentification et résistent aux différentes attaques existantes sur les systèmes basés sur un secret ou une possession. Cependant, ces systèmes présentent plusieurs inconvénients concernant le respect de la vie privée et l'incertitude de l'information biométrique. Une comparaison de ces techniques est détaillée par O'Gorman [5].

Authentification Biométrique	Authentification par mot de passe\ Clé
Basée sur des mesures morphologiques, comportementales ou biologiques	Basée sur l'on sait ou que l'on possède
Utilisation facile (pas de secrets à retenir)	Pouvant être plus compliquée (mot de passe complexe)
Authentifie l'individu	Il peut être perdu, vole ou oubliée
L'information est en relation étroite à l'utilisation de façon permanente	Exacte : utilise une comparaison
Probabiliste : utilise une comparaison	L'information ne varie pas, elle est sûre
L'information biométrique peut être modifiée	Moindre impact sur la vie privée
Problème de respect de la vie privée	Changement aisé
Difficile à révoquer l'information	Authentifie l'individu

Tableau 2 : Comparaison entre l'authentification biométrique et par mot de passe/clé.
[5]

1.2.6 Les applications de la biométrie :

Trois secteurs sont particulièrement concernés par l'utilisation de la biométrie

- **Application judiciaires :**

C'est certainement le premier secteur où l'identification biométrique a été appliquée : Identification de criminels, de terroristes, de cadavres, enfants disparus, etc...

- **Application gouvernementales :**

La biométrie peut éviter un usage frauduleux de documents (ex : passeport, permis de conduire, etc...).

- **Contrôle d'accès physique et logique :**

- Le contrôle d'accès logique (contrôle d'accès à un ordinateur, login d'ouverture de session réseaux, accès distants connexions VPN,...).

- Le contrôle d'accès physique à des locaux (salle informatique, service de recherche, site sensible,...), serrures électroniques,...

1.3. Systèmes biométriques :

Un système biométrique est essentiellement un système de reconnaissance de formes qui utilise les données biométriques d'un individu. Les systèmes biométriques sont de plus en plus utilisés depuis quelques années. L'apparition de l'ordinateur et sa capacité à traiter et à stocker les données ont permis la création des systèmes biométriques informatisés.

1.3.1 Modes de fonctionnement :

Les systèmes biométriques fonctionnent selon trois modes que sont l'enrôlement, la vérification d'identité et l'identification :

- Enrôlement :

L'enrôlement est la première phase de tout système biométrique. Il s'agit de l'étape pendant laquelle un utilisateur est enregistré dans le système pour la première fois. Elle est commune à la vérification et l'identification. Pendant l'enrôlement, la caractéristique biométrique est mesurée en utilisant un capteur biométrique afin d'extraire une représentation numérique. Cette représentation est ensuite réduite, en utilisant un algorithme d'extraction bien défini, afin de réduire la quantité de données à stocker pour ainsi faciliter la vérification et l'identification. Dépendant de l'application et du niveau de sécurité souhaité, le modèle biométrique retenu, est stocké soit dans une base de données centrale soit sur un élément personnel propre à chaque personne.

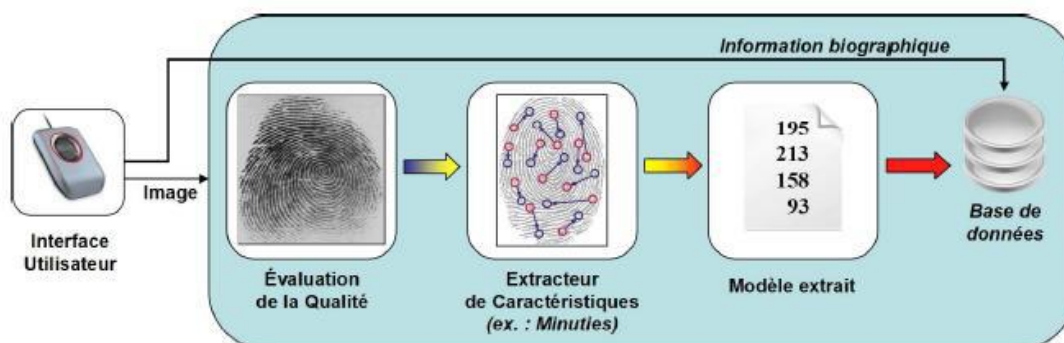


Figure 1.10 : Enrôlement d'une personne dans un système biométrique.

- **Vérification (Authentication) :**

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

Le système doit alors répondre à la question suivante "Suis-je réellement la personne que suis-je entrain de proclamer?" [6].

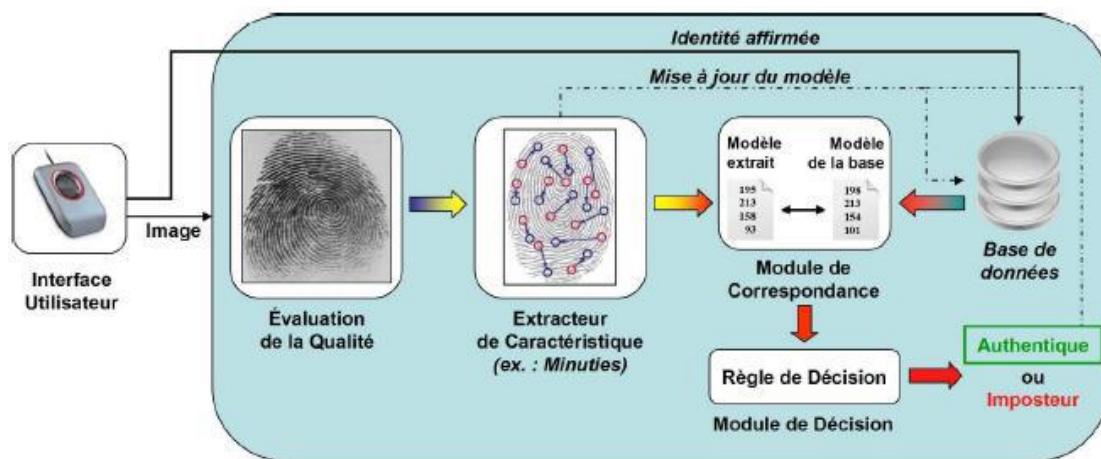


Figure 1.11 : Authentification d'un individu dans un système biométrique.

- **Identification :**

Le système identifie un individu en cherchant les signatures (Template) de tous les utilisateurs dans la base de données. Par conséquent, le système conduit plusieurs comparaisons 1-à-N pour établir l'identité d'un individu [7]. En résumé, un système biométrique opérant en mode identification répond à la question "Suis-je bien connu du système ?".

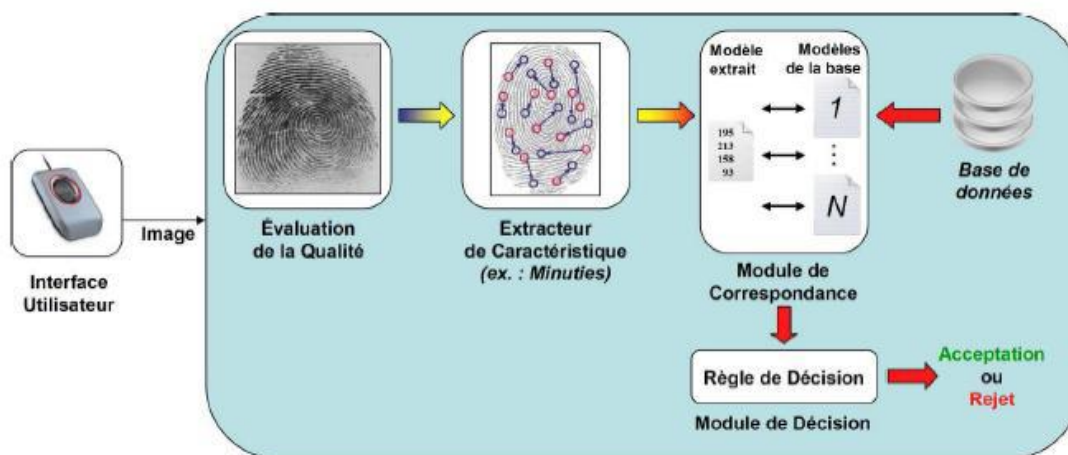


Figure 1.12 : Identification d'un individu dans un système biométrique.

1.3.2 Architecture d'un système biométrique :

L'architecture d'un système biométrique contient 5 modules :

- Le module de capture qui consiste à acquérir les données biométriques afin d'extraire une représentation numérique. Cette représentation est ensuite utilisée pour l'enrôlement, la vérification ou l'identification. Il s'agit d'un capteur biométrique qui peut être de type sans ou avec contact [8].
- Le module de traitement du signal qui permet de réduire la représentation numérique extraite afin d'optimiser la quantité de données à stocker lors de la phase d'enrôlement, ou pour faciliter le temps de traitement pendant la phase de vérification et l'identification.

Ce module peut avoir un test de qualité pour contrôler les données biométriques acquises.

- Le module du stockage qui contient les modèles biométriques des utilisateurs enrôlés du système.
- Le module de similarité qui compare les données biométriques extraites par le module d'extraction de caractéristiques à un ou plusieurs modèles probablement enregistrés. Ce module détermine ainsi le degré de similarité (ou de divergence) entre deux vecteurs biométriques.

- Le module de décision qui détermine si l'indice de similarité retourné est suffisant pour déterminer l'identité d'un individu.

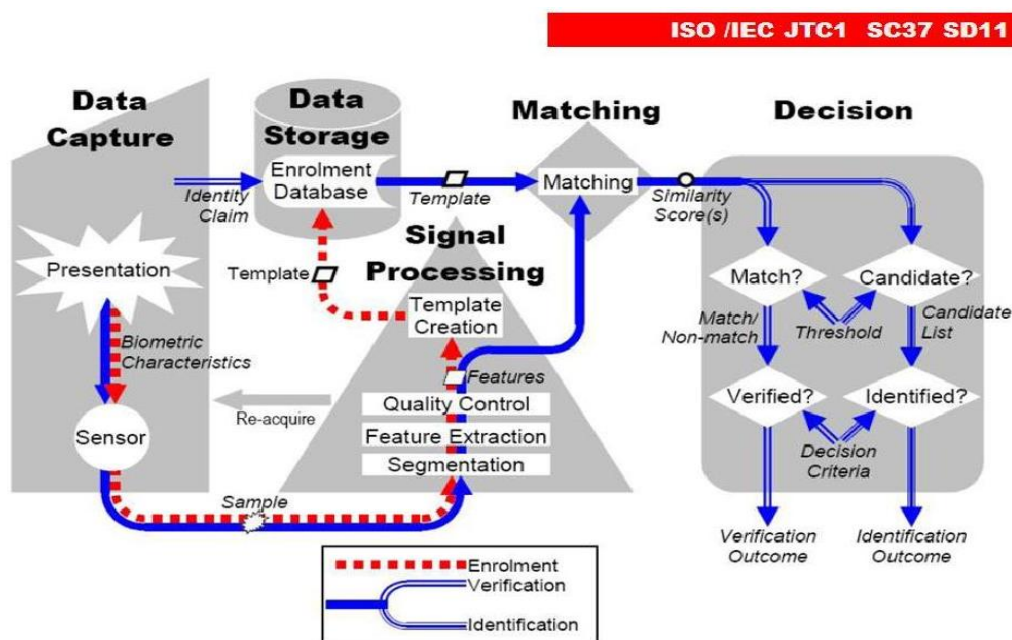


Figure 1.13 : Architecture générique d'un système biométrique (extrait de l'Organisation Internationale de Normalisation ISO/IEC 19795-1 [6]).

1.3.3 Les types de systèmes biométriques :

La multitude des caractères biométriques de l'être humain a donné naissance à plusieurs systèmes d'authentification, chacun repose sur un caractère morphologique ou comportemental, parmi ces systèmes il y a ceux qui ont prouvé leur fiabilité et leurs cours d'évolution.

-Monomodalité :

La biométrie monomodale est une technologie d'authentification de personnes se basant sur une seule modalité biométrique. Avant de procéder à proposer un système biométrique, il est nécessaire de choisir la modalité la plus appropriée l'application.

-Multimodalité :

Elle peut se définir comme l'association de différentes technologies biométriques en vue d'améliorer la précision ou les résultats du système (elle est également appelée «biométrie multi niveaux»). Les systèmes biométriques utilisent au moins deux traits/modalités biométriques de la même personne lors du processus d'établissement

de correspondances. Ces systèmes peuvent travailler de différentes manières, soit en collectant différentes données biométriques avec différents capteurs soit en collectant plusieurs unités des mêmes données biométriques. Certaines études englobent également dans cette catégorie les systèmes qui procèdent à plusieurs lectures des mêmes données biométriques et les systèmes qui utilisent plusieurs algorithmes pour l'extraction de traits du même échantillon biométrique. Parmi les systèmes biométriques multimodaux, on retrouve le passeport électronique au niveau de l'UE ainsi que le système d'identification biométrique US-VISIT aux États-Unis.

1.3.3.1 Les systèmes multimodaux :

Peuvent se référer à de nombreux systèmes différents :

- **Systèmes multi algorithmes:** C'est le type de système le plus classique implicitement utilisé par de nombreuses approches. Les caractéristiques sont extraites via différents algorithmes puis fusionnées. La fusion de caractéristiques extraites via un algorithme analysant les textures et un autre la forme d'un caractère biométrique entre dans ce cadre.

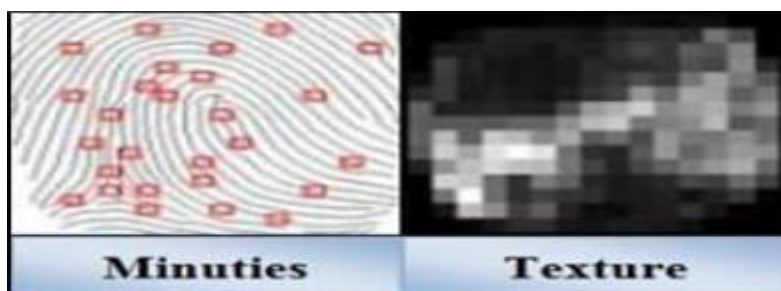


Figure 1.14 : Systèmes multi algorithmes

- **Systèmes multi échantillons:** Un capteur unique peut capturer plusieurs instances du même caractère biométrique dans le but de rendre plus robuste l'extraction des caractéristiques ou d'enrichir le modèle biométrique d'une personne. C'est le cas, par exemple, de plusieurs captures de visage d'une personne sous différents angles. L'utilisation de vidéos entre également dans ce cadre.

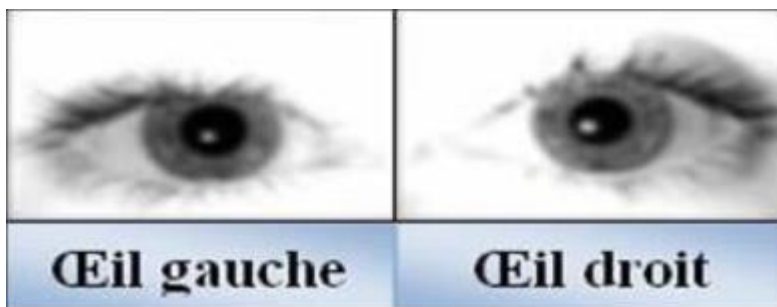


Figure 1.15 : Systèmes multi échantillons

- **Systèmes multi capteurs:** Plusieurs capteurs permettent de capturer le même caractère biométrique sous différents angles. Ainsi la capture d'un visage à l'aide d'une caméra classique et d'une caméra infrarouge entre dans ce scénario. Ce type de système permet notamment la fusion au niveau capteur, ce que ne permettent pas d'autres systèmes comme les systèmes multi caractères.



Figure 1.16 : Systèmes multi capteurs

-**Systèmes multi instances:** Ce type de système permet de capturer plusieurs instances du même caractère biométrique. L'acquisition de plusieurs empreintes digitales via le même capteur est l'exemple typique de ce type de système. Ces systèmes n'entraînent pas de surcoût de capteurs, ni le développement de nouveaux algorithmes. À ne pas confondre avec les systèmes multi échantillons.



Figure 1.17 : Systèmes multi instances

-Systèmes multi caractères: Ce type de système combine différents traits biométriques d'un individu. Les fusions visage iris, ou visage empreinte digitale font partie de ce type d'approche. Ces systèmes nécessitent différents capteurs ainsi que des algorithmes dédiés à chaque caractère biométrique. Ce type de système a comme principale caractéristique que les caractères biométriques considérés peuvent être plus décorrélés que pour les systèmes multi capteurs.



Figure 1.18 : Systèmes multi caractères

La fusion de données issues de visages capturés via une caméra en lumière visible et une autre en lumière infrarouge entre dans le cadre des systèmes multi capteurs, où il est considéré que les deux captures sont issues de modalités différentes. Même si les deux captures sont sensiblement décorrélés (la chaleur émise par un visage n'est pas visible en lumière visible), la fermeture des yeux d'un individu est visible sur les deux modalités. À noter la présence des systèmes hybrides combinant plusieurs scénarios. Une revue de nombreux systèmes biométriques multimodaux développés peut être trouvée dans [9].

1.3.3.2 L'architecture des systèmes multimodaux :

Les systèmes multimodaux associent plusieurs systèmes biométriques et nécessitent donc l'acquisition et le traitement de plusieurs données. L'acquisition et le traitement peuvent se faire successivement, on parle alors d'architecture en série, ou simultanément, on parle alors d'architecture en parallèle. L'architecture est en réalité surtout liée au traitement. En effet, l'acquisition des données biométriques est en général séquentielle pour des raisons pratiques. Il est difficile d'acquérir en même temps une empreinte digitale et une image d'iris dans de bonnes conditions. Il existe cependant certains cas où les acquisitions peuvent être faites simultanément lorsque les différentes données utilisent le même capteur par exemple les capteurs d'empreintes multi-doigts qui permettent d'acquérir plusieurs doigts simultanément ou même les empreintes palmaires. L'architecture est donc en général liée au traitement et en particulier à la décision. En effet la différence entre un système multimodal en série et un système multimodal en parallèle réside dans le fait d'obtenir un score de similarité à l'issue de chaque acquisition (fusion en série) ou de procéder à l'ensemble des acquisitions avant de prendre une décision (fusion en parallèle). L'architecture en parallèle (figure 19) est la plus utilisée car elle permet d'utiliser toutes les informations disponibles et donc d'améliorer les performances du système. En revanche, l'acquisition et le traitement d'un grand nombre de données biométriques est coûteux en temps et en matériel, et réduit le confort d'utilisation. C'est pour cela que l'architecture en série (figure 19) peut être privilégiée dans certaines applications ; par exemple si la Multimodalité est utilisée pour donner une alternative pour les personnes ne pouvant pas utiliser l'empreinte digitale. Pour la majorité des individus seule l'empreinte est acquise et traitée mais pour ceux qui ne peuvent pas être ainsi authentifiés on utilise un système à base d'iris alternativement.

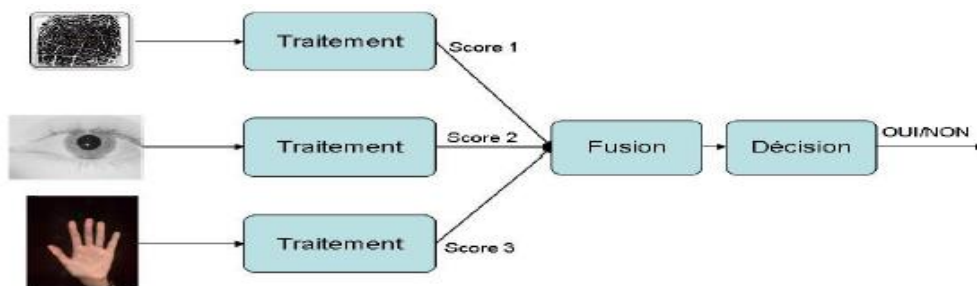


Figure 1.19 : Architecture de fusion en parallèle

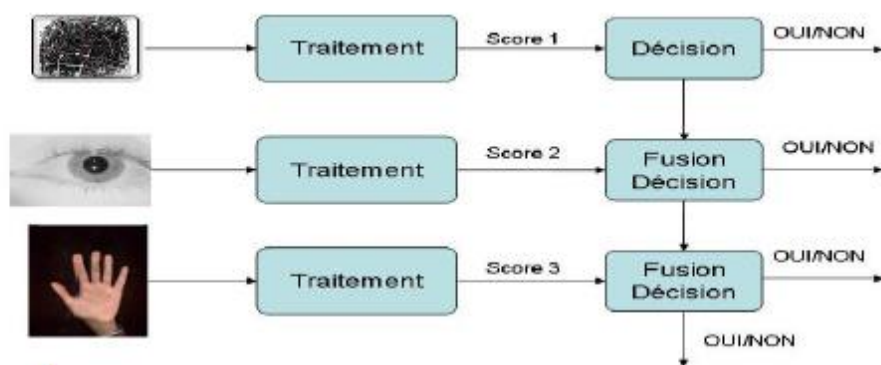


Figure 1.20 : Architecture de fusion en série (incrémentale ou séquentielle)

1.3.4 Les niveaux de fusion :

La combinaison de plusieurs systèmes biométriques peut se faire à quatre niveaux différents: au niveau des données, au niveau des caractéristiques extraites, au niveau des scores issus du module de comparaison ou au niveau des décisions du module de décision (figure 21).

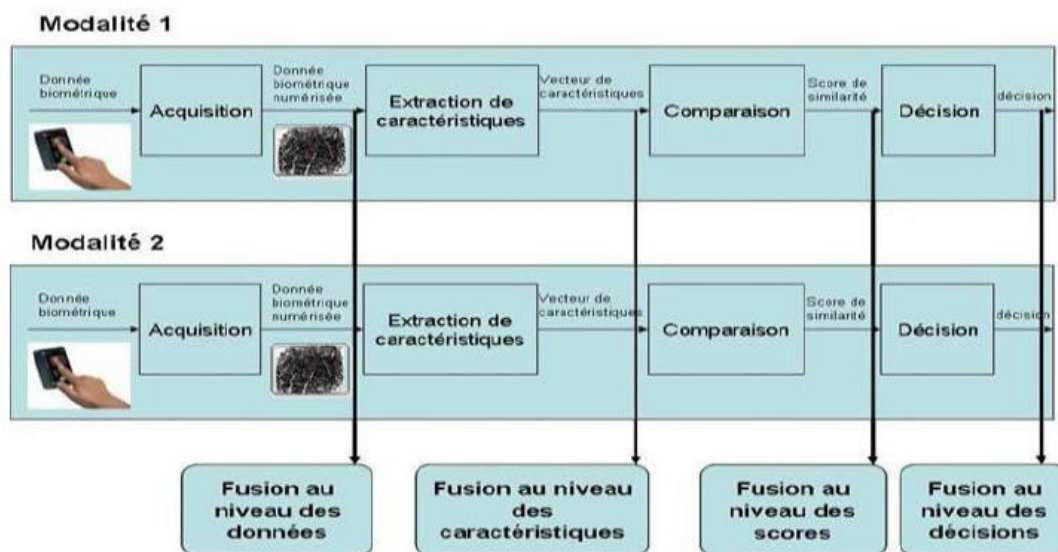


Figure 1.21 : Les différents niveaux de fusion

Ces quatre niveaux de fusion peuvent être classés en deux sous-ensembles :

- la fusion pré-classification (avant comparaison),
- la fusion post-classification (après la comparaison).

1.3.4.1 La fusion pré-classification :

La fusion pré-classification correspond à la fusion des informations issues de plusieurs données biométriques au niveau du capteur (images brutes) ou au niveau des caractéristiques extraites par le module d'extraction de caractéristiques.

- Niveau du capteur (Sensor Level)

La fusion au niveau capteur est relativement peu utilisée car se faire uniquement si les diverses captures sont des instances du même trait biométrique obtenu à partir de plusieurs capteurs compatibles entre eux ou plusieurs instances du même trait biométrique obtenu à partir d'un seul capteur. De plus, les captures doivent être compatibles entre elles et la correspondance entre les points dans les données brutes doit être connue par avance. Par exemple, les images de visage obtenues à partir de plusieurs caméras peuvent être combinées pour former un modèle 3D du visage. Un autre exemple de fusion au niveau capteur consiste à mettre en mosaïque plusieurs images d'empreintes digitales afin de former une image d'empreinte digitale finale plus complexe. La fusion au niveau capteur n'est généralement pas possible si les instances des données sont incompatibles (par exemple, il est peut être difficile de fusionner des images de visages provenant de caméras ayant des résolutions différentes).

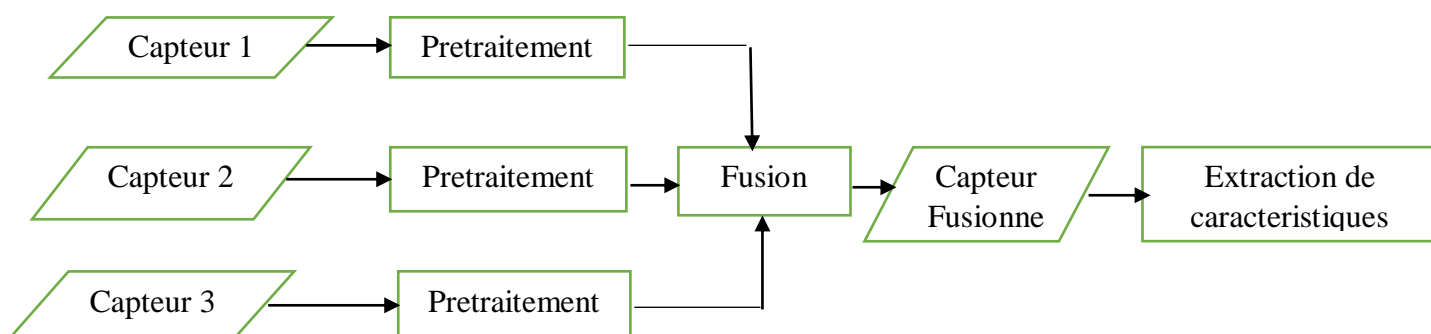


Figure 1.22 : Schéma de fusion au niveau du capteur.

- Niveau Caractéristiques (Feature Level) :

La fusion au niveau des caractéristiques est moins limitée par la nature des données biométriques. Cependant une certaine homogénéité est nécessaire pour la plupart des méthodes de fusion au niveau des caractéristiques comme par exemple la moyenne de

plusieurs "templates" d'empreintes ou de visage. Un exemple de fusion au niveau des caractéristiques qui ne nécessitent pas vraiment d'homogénéité est la concaténation de plusieurs vecteurs de caractéristiques avant le traitement par l'algorithme de comparaison. Par exemple, dans [22], Jing et al proposent une méthode de fusion de caractéristiques pour de la fusion de visage et d'empreinte palmaire. La fusion est effectuée par concaténation d'images obtenues par transformée de Gabor sur les images de visage et d'empreinte de la main. Mais la concaténation pose le problème de la dimension de l'espace de classification qui lorsqu'il augmente, rend plus difficile la tâche de classification. Les méthodes de fusion pré-classification sont assez peu utilisées car elles posent un certain nombre de contraintes qui ne peuvent être remplies que dans certaines applications très spécifiques. En revanche, la fusion post-classification est très étudiée par les chercheurs.

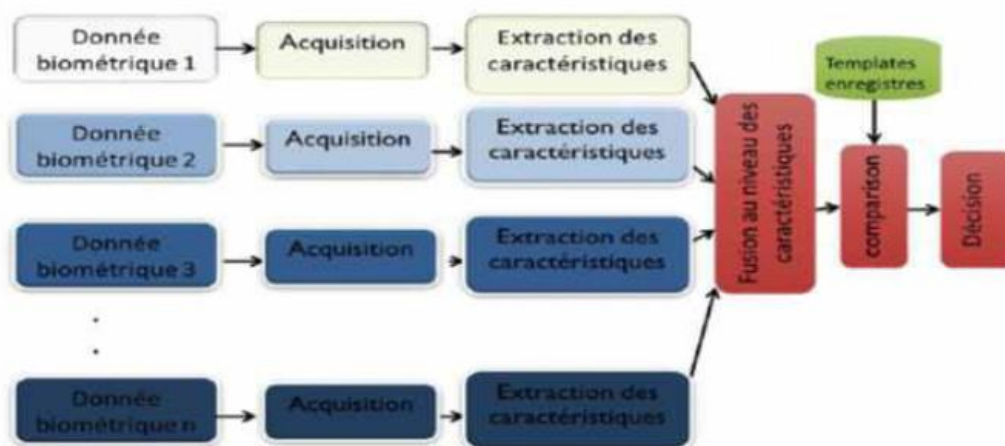


Figure 1.23 : Schéma de fusion au niveau de l'extraction des caractéristiques.

1.3.4.2 La fusion post-classification :

La fusion post-classification peut se faire au niveau des scores issus des modules de comparaison ou au niveau des décisions. Dans les deux cas, la fusion est en fait un problème bien connu de la littérature sous le nom de "Multiple Classifier systems".

- Niveau Décision (Decision Level)

La fusion au niveau des décisions est souvent utilisée pour sa simplicité. En effet, chaque système fournit une décision binaire sous la forme OUI ou NON que l'on peut représenter par 0 et 1, et le système de fusion de décisions consiste à prendre une décision finale en fonction de cette série de 0 et de 1. Les méthodes les plus utilisées

sont des méthodes à base de votes telles que le OR (si un système a décidé 1 alors OUI), le AND (si tous les systèmes ont décidé 1 alors OUI) ou le vote à la majorité (si la majorité des systèmes ont décidé 1 alors OUI). On peut également utiliser des méthodes plus complexes qui pondèrent les décisions de chaque sous-système ou qui utilisent des classifieurs dans l'espace de décisions telles que BKS (Behaviour Knowledge Space). Dans [23], Verlinde présente un grand nombre de méthodes de fusion de décision. Ces méthodes de fusion au niveau des décisions sont très simples mais utilisent très peu d'information (0 ou 1).

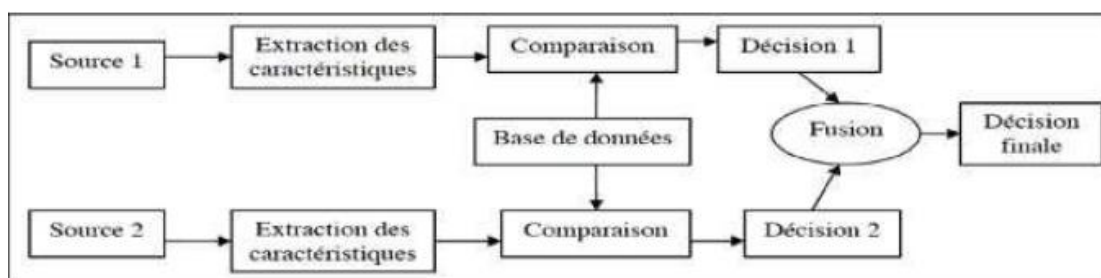


Figure1. 24 : Schéma de fusion au niveau de la décision.

- Niveau Score (Score Level)

La fusion au niveau des scores est le type de fusion le plus utilisé car elle peut être appliquée à tous les types de systèmes (contrairement à la fusion pré-classification), dans un espace de dimension limité (un vecteur de scores dont la dimension est égale au nombre de sous-systèmes), avec des méthodes relativement simples et efficaces mais traitant plus d'information que la fusion de décisions. La fusion de scores consiste donc à la classification : OUI ou NON pour la décision finale, d'un vecteur de nombres réels dont la dimension est égale au nombre de sous-systèmes.

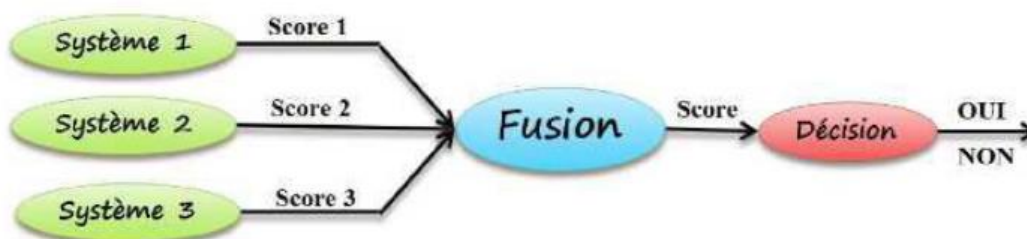


Figure 1.25 : Schéma de fusion au niveau de scores [19].

1.3.5 Principe de fonctionnement d'un système biométrique :

En matière de fonctionnement, tous les systèmes biométriques fonctionnent comme suit :

- Capture des caractéristiques :

Collecte de certaines caractéristiques physiologique, comportementales ou biologiques présentée au moyen d'un terminal de capture biométrique, lequel restitue cette caractéristique sous la forme d'un échantillon biométrique capturé. La qualité du capteur peut grandement influencer les performances du système.

- Extraction de caractéristiques :

Cette phase comprend, en général ; un processus de segmentation visant à localiser l'information de la caractéristique dans l'échantillon biométrique capturé, un processus d'extraction de traits. Seuls les paramètres pertinents sont extraits de l'échantillon biométrique capturé et un processus de contrôle de qualité évalue la validité des échantillons.

- Comparaison :

Compare l'ensemble des caractéristiques extraites avec une ou plusieurs références préalablement stockées et les résultats de comparaison (degrés de correspondance) sont transmis au sous-système de décision. L'identité de l'utilisateur peut correspondre à l'identité recherchée ou pas.

- Décision :

Détermine si l'identité de l'utilisateur correspond ou non à l'identité proclamée (authentification) ou recherchée (identification). L'identification d'une personne est basée sur le degré de similitude entre les caractéristiques extraites et les modèles stockés.

1.3.6 Performance d'un système biométrique :

Les performances d'un système biométrique sont données par la mesure de trois taux d'erreurs :

Le taux de faux rejet (“False Reject Rate” ou FRR) : Ce taux représente le pourcentage d'utilisateurs censés être acceptés mais qui sont rejetés par le système [10].

$$TFR = \frac{\text{nombre des clients rejete (FR)}}{\text{nombre total d'accès de clients}}$$

2. Le taux de fausse acceptation (“False Accept Rate” ou FAR) : Ce taux représente le pourcentage d'utilisateurs censés ne pas être reconnus mais qui sont tout de même acceptés par le système.

$$TFA = \frac{\text{nombre des imposteurs accepté (FA)}}{\text{nombre total d'accès imposteurs}}$$

3. Le taux d'égalé erreur (“Equal Error Rate” ou EER) : Ce taux est calculé à partir des deux premiers critères et constitue un point de mesure de performance courante. Ce Point correspond à l'endroit où $FRR = FAR$, c'est-à-dire le meilleur compromis entre les faux rejets et les fausses acceptations.

Un système fonctionnel aura un FRR le plus bas possible. Un système sûr aura un FAR le plus bas possible.

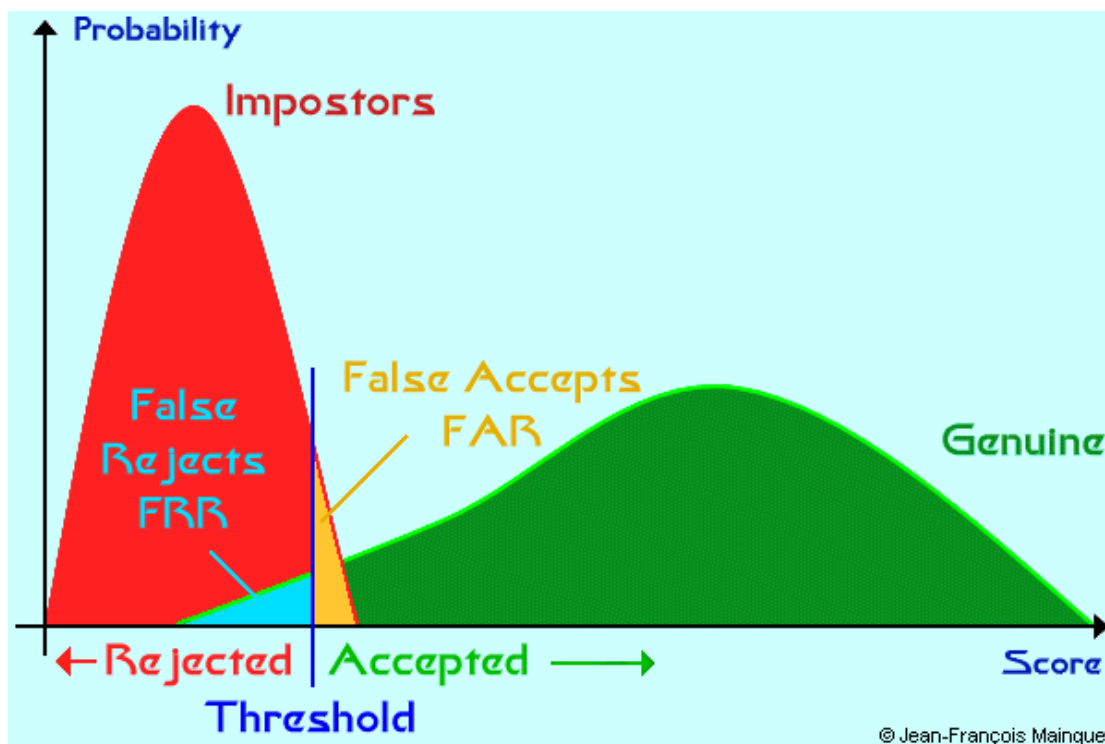


Figure 1.26 : Illustration du FRR et du FAR. [10]

1.4 Les avantages et les limites de la biométrie :

1.4.1 Les avantages de la biométrie :

La biométrie est une technologie récente et commence à être adoptée par de grands constructeurs de matériel informatique.

L'usage de la biométrie est un complément de l'utilisation des méthodes d'authentification comme des mots de passe, des badges, des cartes à puce.-

Suppression des mots de passe, Suppressions des clés :

Au lieu de retaper son mot de passe dès que le PC se met en veille, une simple pression de l'empreinte digitale sur le capteur suffit et permet facilement de changer la session d'utilisateur.- Utilisation d'une signature biométrique: Grande sécurité, intransmissible à une autre personne. Une identité vérifiée (Le destinataire est bien la personne autorisée à visualiser ou à utiliser les données).Lors de transactions financières, il est capital de savoir quel moyen de paiement du consommateur est le plus sûr. La biométrie constitue le chaînon manquant dans la triade des problèmes de sécurité :

- Diminution de la fraude.
- Rehaussement de l'intégrité des informations et la sécurité.
- Réduction des attaques à l'égard des programmes gouvernementaux.
- Croissance de la confiance envers les systèmes de sécurité.
- Diminution des frais administratifs.
- Accélération des services.

1.4.2 Les limites de la biométrie:

La biométrie présente malheureusement un certain nombre d'inconvénients parmi eux le problème de la qualité de l'authentification. Ces méthodes ne sont en effet pas toujours fiables à 100%, ce qui empêche des utilisateurs de bonne foi d'accéder à leur système. Car il s'agit bien là d'une des caractéristiques majeures de tout organisme vivant: on s'adapte à l'environnement, on vieillit, on subit des traumatismes plus ou moins importants, bref on évolue et les mesures changent. Prenons le cas le plus simple, celui des empreintes digitales (mais la même chose s'applique à toute donnée

physique). Suivant les cas, nous présentons plus ou moins de transpiration, la température des doigts n'est pas régulière. Il suffit de se couper pour présenter une anomalie dans le dessin de ses empreintes. Dans la majorité des cas, les mesures du capteur et du logiciel associé retourneront un résultat différent de la mesure initiale de référence. Or, il faut pourtant bien réussir à se faire reconnaître. En pratique, cela sera réalisé dans la plupart des cas car le système est amené à autoriser une marge d'erreur entre la mesure et la référence. De manière générale, les faiblesses de ces systèmes ne se situent pas au niveau de la particularité physique sur laquelle ils reposent, mais bien sur la façon avec laquelle ils la mesurent, et la marge d'erreur qu'ils autorisent. Là encore, il convient de ne pas se laisser impressionner par une image illusoire de haute technologie - produit miracle. De plus, les experts techniques mettent au passif de cette technologie, d'une part, son cout, d'autre part, la question de sa révocation. En effet, confronté à une personne qui a subtilisé un mot de passe ou une signature manuscrite, le titulaire du mot de passe ou de la signature peut facilement les remplacer ou les révoquer. La chose semble plus complexe pour une empreinte digitale ou rétinienne. Si un tiers s'approprie une identité biométrique du type empreintes digitales ou identité visuelle, il peut au moyen de ces identités biométriques passer tout type d'actes au nom de la victime. Comment la victime pourrait-elle alors révoquer sa propre empreinte digitale ou identité visuelle ? Les experts en sécurité sont partagés sur la question, même si, en majorité, ils semblent considérer que cette révocation est possible. Tous reconnaissent cependant la difficulté à mettre au passif cette protection technique. Les données biométriques sont comparables à tout autre système de contrôle d'accès comme des mots de passe, ...etc.

Car du point de vue du système informatique, ce ne sont rien d'autres que des séries de bits comme toute donnée. Autrement dit, la difficulté réside dans la contrefaçon de la caractéristique physique et biologique que l'on mesure. Si la biométrie se généralise dans notre environnement, il est dangereux de penser qu'il s'agit de la réponse à tous les problèmes de sécurité. La biométrie, de par ses limites fonctionnelles, techniques et juridiques n'est en aucun cas synonyme de technologie miracle et de sécurité absolue.-

-Les limites fonctionnelles:

Les systèmes d'authentification biométrique représentent une grande partie des limites fonctionnelles. En effet, les systèmes biométriques laissent la place à un certain nombre de faux rejets et de fausses acceptations. Ils ne peuvent à eux seuls garantir à 100% que seules les personnes autorisées pourront passer le contrôle. Ils ne peuvent même pas garantir qu'une personne autorisée ne sera pas rejetée par le système. Il y aura toujours une marge d'erreur à prendre en compte, ce qui n'est pas forcément très rassurant.

- Les limites techniques :

Bien que cela représente un travail assez conséquent, les données biométriques peuvent être imitées, notamment celles qui laissent des traces sur le passage de l'individu telles que les empreintes digitales. Un individu mal intentionné peut récupérer les empreintes digitales sur un objet tenu par la victime, les imiter et tenter de passer le contrôle biométrique à l'aide de ces empreintes. De plus, les données biométriques sont dans la majeure partie des cas numérisées sur un support, de préférence individuel. Si ce support n'est pas protégé contre les intrusions et le piratage, tout le système biométrique tombe à l'eau.

1.5 Conclusion :

Dans ce chapitre, je présente quelques modalités biométriques avec leurs défis rencontrés dans les systèmes biométriques. Je évoque aussi les types et l'architecture d'un système biométrique avec leur application dans la vie réelle et enfin je discute l'évaluation d'un système biométrique. Dans le chapitre suivant, je présente un état de l'art sur les approches de la reconnaissance de palme.

Chapitre 2

2.1. Introduction :

Des recherches ont été menées durant ces années sur la reconnaissance de palmaire où plusieurs problèmes relatifs à ce domaine ont été recensés. Ce chapitre présente un état de l'art sur les recherches présentées dans la littérature. Notamment nous décrivons en particulier les captures d'acquisitions, et les systèmes existants.

2.2. La reconnaissance palmaire :

Palmaire désigne la surface interne de la paume de la main qui contient normalement quatre lignes principales, des plis secondaires et les crêtes. Les plis secondaires sont appelés rides. Les lignes principales et les plis secondaires sont formés à partir de 3e et 5e mois de grossesse [11] et les lignes superficielles apparaissent après notre naissance. Bien que les trois principales flexions soient génétiquement dépendantes, la plupart des autres plis ne sont pas identiques [12]. Même les jumeaux ont des images de palmaire différentes [12]. Ces données non génétiquement déterministes sont très utiles dans l'identification personnelle. Principalement, palmaire présente plusieurs avantages par rapport aux autres données biométriques, notamment:

- L'image de palmaire a une basse résolution (traitement plus rapide).
- Généralement elle ne nécessite pas un grand coût de calcul.
- Elle atteint une exactitude élevée.
- Peu de risques d'intrusion.

2.2.1. Les Caractéristiques de palmaire :

Les caractéristiques utilisées pour la reconnaissance de palmaire peuvent être divisées en cinq catégories selon le niveau de détails utilisés dans l'analyse des images palmaire [13]. Ces catégories sont:

2.2.1.1. Les caractéristiques géométriques

Ce sont les caractéristiques liées à la forme géométrique de la paume, telles que sa largeur, sa longueur et sa surface (Figure 2.1).

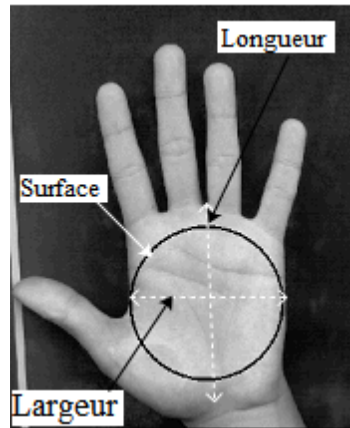


Figure 2.1 Caractéristiques géométriques de palmaire

Ces caractéristiques sont faciles à collecter, même avec des appareils à faible résolution. Dans certains cas, ces caractéristiques sont considérées comme des concepts de la géométrie de la main et ne sont pas considérées comme palmaire typiques.

2.2.1.2. Les lignes principales de palmaire :

Quatre principales lignes (ou Plis de flexion) apparaissent sur la paume de la main de chaque personne. Ces caractéristiques sont importantes pour la reconnaissance de l'image palmaire car elles présentent une grande capacité de collecte et de permanence qu'elles peuvent être capturées par des appareils à faible résolution. Quatre différentes lignes principales de palmaire peuvent être définies : la ligne de cœur, la ligne de tête, la ligne de vie, et la ligne de destin (Figure 2.2).

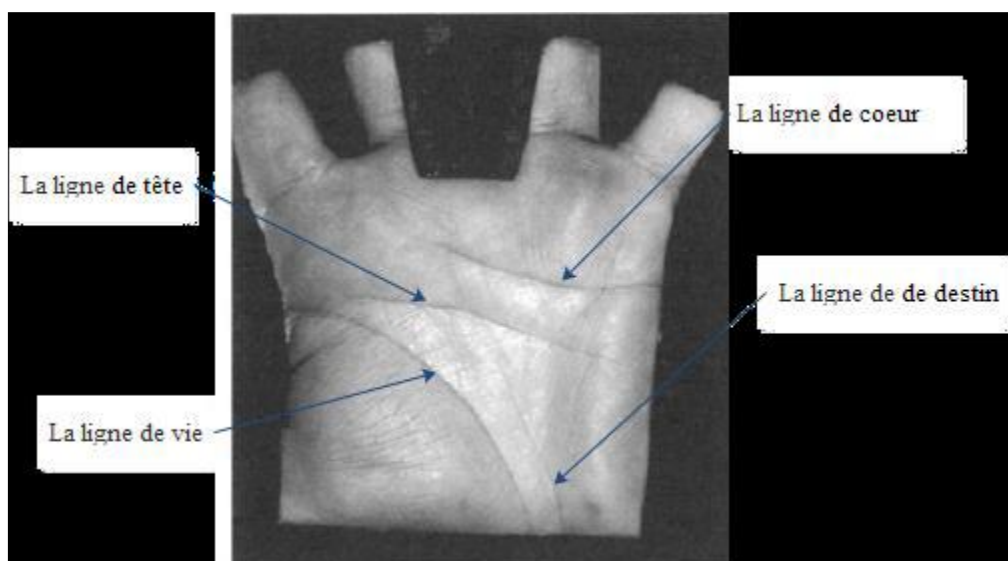


Figure 2.2 Les quatre principales lignes de l'image de palmaire [13]

2.2.1.3. Les caractéristiques de rides

Ces caractéristiques peuvent être considérées comme des lignes secondaires (ou des plis secondaires) et sont distinctives en raison de leur grande irrégularité. Ces caractéristiques présentent une bonne recevabilité mais sont moins permanentes que les lignes principales et peuvent être falsifiées (Figure 2.3).

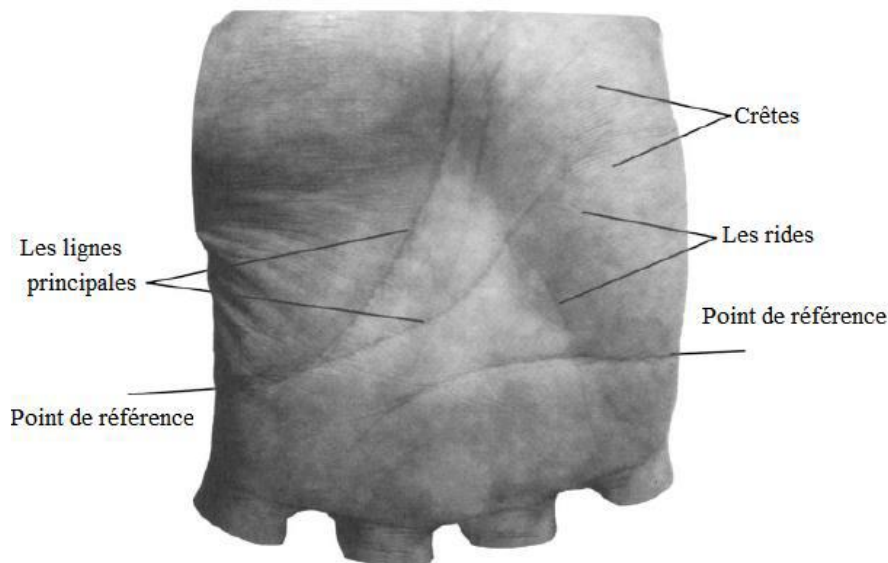


Figure 2.3 : Les rides, les crêtes et les points de référence sur l'image de palmaire [13]

2.2.1.4. Points de référence

Deux points d'extrémités appelés points de référence sont obtenus par les lignes principales (voir la Figure 2.3). Celles-ci se croisent des deux côtés d'une paume et fournissent un moyen stable d'enregistrer les empreintes de paume. La taille d'une paume peut être estimée en utilisant la distance Euclidienne entre ces points d'extrémité.

2.2.1.5. Les caractéristiques de minutie :

Les minuties de palmaire sont généralement similaires aux minuties de l'empreinte digitale. Elles sont utilisées pour la reconnaissance et correspondent aux points suivants : Delta, Fin de ligne, Lac, Bifurcation. Ils sont très distinctifs et permanents. Cependant, leur acquisition nécessite l'utilisation d'appareils à haute résolution (voir Figure 2.4)

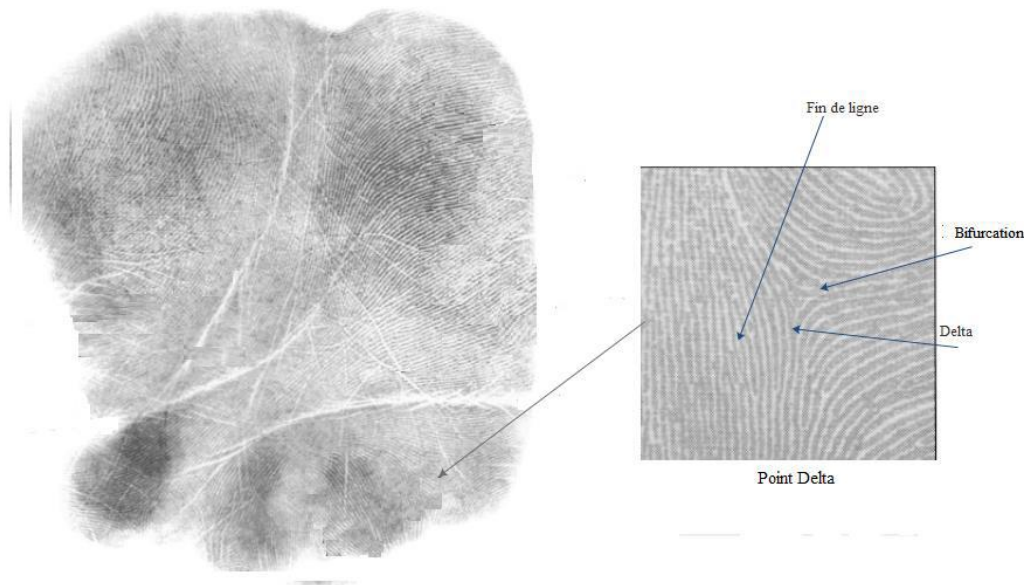


Figure 2.4. Minuties de palmaire

2.2.2. Reconnaissance de palmaire 3D :

2.2.2.1. Motivations de l'utilisation de palmaire 3D :

Palmaire 3D exploite l'information structurelle tridimensionnelle de la surface de la paume. Notamment la technique de l'imagerie à lumière structurée est utilisée pour acquérir les données tridimensionnelles de palmaire. Palmaire 3D contrairement au palmaire 2D ne peuvent pas être facilement falsifiées. De plus nombreuses informations de profondeur tridimensionnelles ne sont pas perdues dans le processus de traitement. En outre, de fortes variations d'illumination dans l'image de palmaire 2D posent des problèmes sur la reconnaissance palmaire 2D. Par conséquent, il y a un grand intérêt d'explorer de nouvelles techniques de reconnaissance de palmaire pour surmonter ces difficultés. Intuitivement, la reconnaissance de palmaire 3D est une bonne solution. De plus, la projection de la lumière laser sur la surface de la paume a une forte acceptabilité par les utilisateurs que celle sur le visage [14-16].

2.2.2.2. Acquisition des images de palmaire 3D :

Des capteurs infrarouges sont utilisés pour détecter la présence de la main sur le dispositif d'acquisition. Il y a une cheville dans le dispositif développé servant de point de contrôle pour fixer la main. Quand une main est détectée, le périphérique projette plusieurs modèles lumineux (lumière structurée) [17]. La lumière réfléchiée est captée par une caméra CCD, puis une série d'images ont été collectées. Après un

certain calcul, les informations de profondeur de surface 3D de l'objet sont obtenues. La Figure 2.5 montre le système d'acquisition de palmaire 3D développé par le centre de recherches biométriques de l'université polytechnique de Hong Kong.

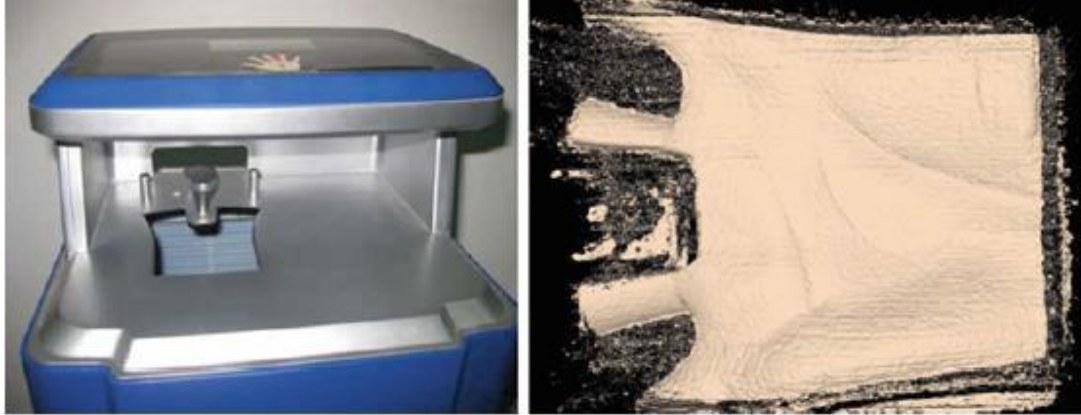


Figure 2.5. Dispositif d'acquisition d'images 3D basé sur la lumière et un exemple d'image de palmaire 3 D

2.2.2.3. Algorithmes de représentation des images de palmaire 3D :

Plusieurs algorithmes dans la littérature ont été proposés pour améliorer et présenter les informations de profondeur de palmaire 3D en image 2D. La courbure moyenne MCI «Mean Curvature Image» et la courbure gaussienne GCI «Gaussian Curvature Images» de chaque nuage de points dans la région d'intérêt (ROI) de palmaire 3D sont alors calculées [17]. Pour minimiser la complexité de calcul et accélérer le processus de traitement, la courbure moyenne MCI et la courbure gaussienne GCI sont convertis à des images de niveau de gris. Les informations de profondeur «Depth information» dans palmaire 3D reflète la distance relative entre le plan de référence et chaque point dans l'objet. Soit p un point de la surface S , Considérons que toutes les courbes C_i sur S passent par le point p . Chaque courbe C_i aura une courbure associée K_i à p . Parmi ces courbures, il y a deux courbures K_1 et K_2 connues comme les principales courbures du point p sur la surface [17]. La courbure moyenne H et la courbure gaussienne K de p sont définies comme suit :

$$H = \frac{1}{2}(K_1 + K_2) \quad (2.1)$$

$$K = K_1 * K_2 \quad (2.2)$$

Pour une image palmaire 3D capturée, la MCI et la GCI sont calculées par l'algorithme dans [18], pour sa simplicité et son efficacité comme suit :

$$H = \frac{(1 + f_x^2)f_{yy} + (1 + f_y^2)f_{xx} - 2f_x f_y f_{xy}}{2(1 + f_x^2 + f_y^2)^{3/2}} \quad (2.3)$$

$$K = \frac{f_{xx}f_{yy} - f_{xy}^2}{(1 + f_x^2 + f_y^2)^2} \quad (2.4)$$

Où f_x et f_y sont les dérivées partielles d'ordre 1 et f_{xx} , f_{yy} et f_{xy} sont les dérivées partielles d'ordre 2.

Les images de courbures H et K sont transformées en images des courbures \bar{H} et \bar{K} par les équations suivantes :

$$\bar{H}(i, j) = 0.5(H(i, j) - \mu)/(4\delta) + 0.5 \quad (2.5)$$

$$\bar{K}(i, j) = 0.5(K(i, j) - \mu)/(4\delta) + 0.5 \quad (2.6)$$

Où μ et δ sont la moyenne et l'écart-type de la courbure. Les valeurs des courbures seront normalisées dans l'intervalle $[0,1]$ pour l'obtention des images de niveau de gris de 8 bits comme suit:

$$G_H(i, j) = \begin{cases} 0, & \bar{H}(i, j) \leq 0 \\ \text{round}(255 \times \bar{H}(i, j)), & 0 < \bar{H}(i, j) < 1 \\ 255, & \bar{H}(i, j) \geq 1 \end{cases} \quad (2.7)$$

$$G_K(i, j) = \begin{cases} 0, & \bar{K}(i, j) \leq 0 \\ \text{round}(255 \times \bar{K}(i, j)), & 0 < \bar{K}(i, j) < 1 \\ 255, & \bar{K}(i, j) \geq 1 \end{cases} \quad (2.8)$$

$G_H(i, j)$ et $G_K(i, j)$ sont respectivement les images MCI et GCI. La Figure 2.6 illustre les images MCI et les images GCI de la même paume à différents moment.

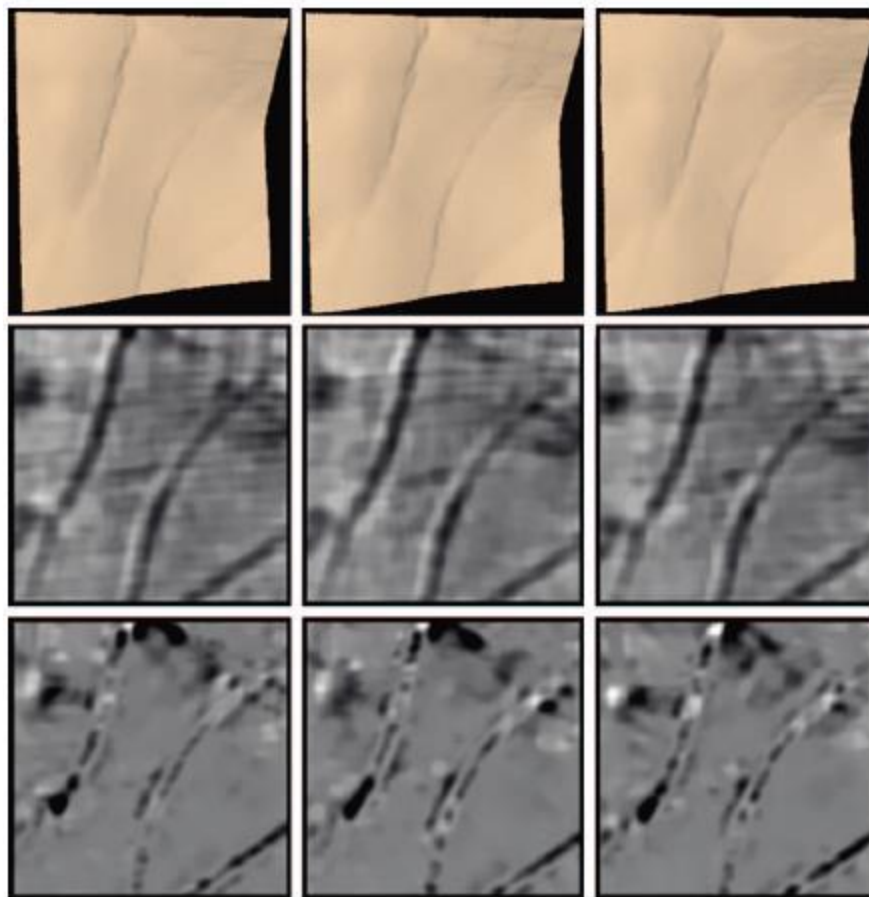


Figure 2.6 a) les ROI images de palmaire 3D. b) leurs images MCI. c) leurs images GCI

2.2.3. Algorithmes d'extraction de caractéristiques et classification des images palmaire (2D et 3D) :

Zhang et al dans [18], avaient extrait une image de courbure moyenne (MCI), une image de courbure gaussienne (GCI) et une image type de surface ST «surface type» à partir de la région d'intérêt (ROI) de 3D palmaire. Ensuite, la distance de Hamming a été utilisée pour l'étape de comparaison. Dans [30], Li et al avaient extrait trois niveaux de caractéristiques de 2D et 3D palmaire, y compris les caractéristiques de forme, caractéristiques de la ligne principale, et les caractéristiques de texture. La méthode ICP «IterativeClosest Point» a été utilisée pour effectuer un raffinement d'alignement de la texture selon les lignes principales et la forme de la paume si nécessaire. Le raffinement d'alignement réduit considérablement la prolongation et les variations de rotation des données de palmaire obtenues durant le processus d'acquisition. Dans [18], Li et al avaient proposé une autre approche, une fois que le MCI calculé à partir d'image ROI de palmaire 3D, les caractéristiques de ligne et

d'orientation de MCI ont été fusionnés au niveau du score ou au niveau d'extraction des caractéristiques. Le vecteur final obtenu est utilisé pour l'étape de comparaison. Dans [16], Zhang et al avaient présenté un nouveau système d'authentification personnel qui exploite simultanément les informations de palmaire 2D et 3D. Pour comparer deux palmaire 3D, les courbures de surface ST sont calculées, puis la corrélation locale normalisée (LC) est ensuite utilisée pour l'étape de comparaison. Dans [19], Yang et al avaient utilisé la représentation d'indice de forme pour décrire la géométrie de ROI de palmaire 3D. Puis, la méthode LBP «Local Binary Pattern» et les filtres de Gabor avaient été appliqué sur la représentation d'indice de forme pour l'extraction de vecteurs caractéristiques. Ensuite, ces deux vecteurs caractéristiques ont finalement été fusionnés au niveau des scores. Dans [20], Cui propose un système de reconnaissance multimodal efficace qui exploite les caractéristiques des palmaire 2D et 3D. Également, la fusion se fait au niveau des scores. Les vecteurs caractéristiques de 2D et 3D sont obtenus par analyse de composantes principales (PCA) suivies d'une représentation TPTSR «the two-phase test sampler présentation». Meraoumia et al [21], ont combiné les informations de palmaire 2D et 3D afin de construire un système biométrique multimodal efficace basé sur la fusion au niveau des scores. Par conséquent, la PCA et la transformée d'ondelettes discrètes (DWT) ont été appliquées sur l'image de palmaire (2D ou 3D) pour l'extraction de caractéristiques avec un modèle de Markov caché (HMM) pour la modélisation des vecteurs caractéristiques. Zhang et al [22] avaient introduit un système d'identification de 3D palmaire. Premièrement, l'image de ROI palmaire 3D a été divisée en blocs uniformes et l'histogramme de type surface (ST) de chaque bloc a été extrait. Ensuite, les histogrammes de tous les blocs sont concaténés pour former un seul vecteur caractéristique. Enfin, la représentation collaborative (CR) avec régularisation et l1-norme ou L2-norme ont été utilisée pour la classification.

2.3. Palmprints multi spectrales :

La reconnaissance de palmaire multi spectrale est une prometteuse technologie biométrique en raison de son caractéristique stable et unique. La richesse de l'information de texture en palmaire multi spectrale offre l'un des moyens les plus importants pour la reconnaissance personnelle. En effet, la texture de palmaire multi

spectrale a plusieurs avantages, telle que : l'image à basse résolution, le faible coût, les caractéristiques structurelles stables et l'acceptation des utilisateurs élevés [23].

La palmaire multi spectrale est largement utilisé dans la télédétection [24], l'imagerie médicale [25] et la machine de vision [26]. Plusieurs images peuvent être fournies dans une même scène mais avec des informations différentes (NIR, rouge, verte et bleue). Par conséquent, l'idée était d'utiliser l'information résultante dans ces images spectrales afin d'améliorer la performance du système de reconnaissance de palmaire multi spectrales.

2.3.1. Dispositif d'acquisition des images palmaire multi-spectrales :

La Figure 2.10 représente la structure interne d'un dispositif d'acquisition d'image palmaire multi-spectral. Ce dispositif se compose d'une caméra CCD à couplage de charge «charge-coupled device», d'un convertisseur A/D, d'une source lumineuse multi-spectrale, et d'un contrôleur de lumière. Une camera CCD est placé en bas de l'appareil. Le convertisseur A / D relie la CCD et l'ordinateur. Le contrôleur de lumière est utilisé pour le contrôle de la lumière multi spectrale [26-27]. Le système peut capturer des images palmaires dans une résolution de 352× 288. Un utilisateur est invité à mettre sa paume sur la plate-forme de l'appareil d'acquisition. Plusieurs piquets sont nécessaires pour fixer la main de l'utilisateur. La Figure 2.11 représente la structure externe d'un dispositif d'acquisition d'image palmaire multi spectrale. La Figure 2.12 représente la plate-forme d'entrée du système montrant ainsi comment la paume de la main est fixée

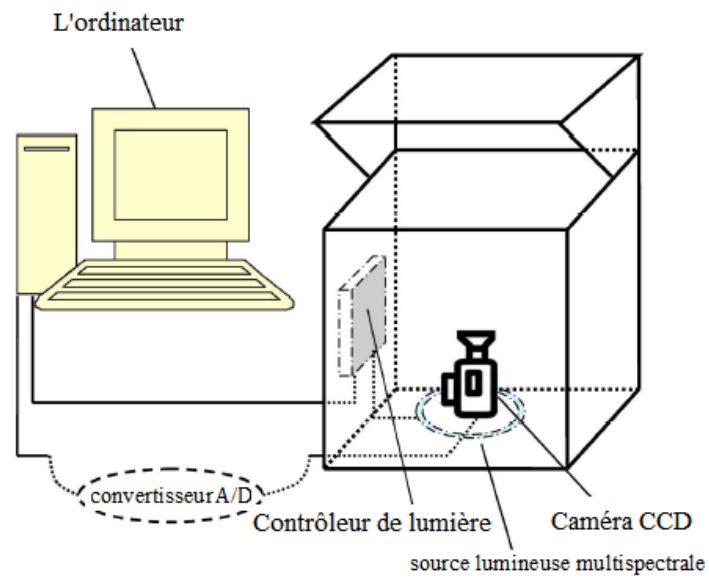


Figure 2.7 : Structure interne d'un dispositif d'acquisition d'image palmaire multi spectrale [28]



Figure 2.8 : Structure externe d'un dispositif d'acquisition d'image palmaire multi spectrale [28]

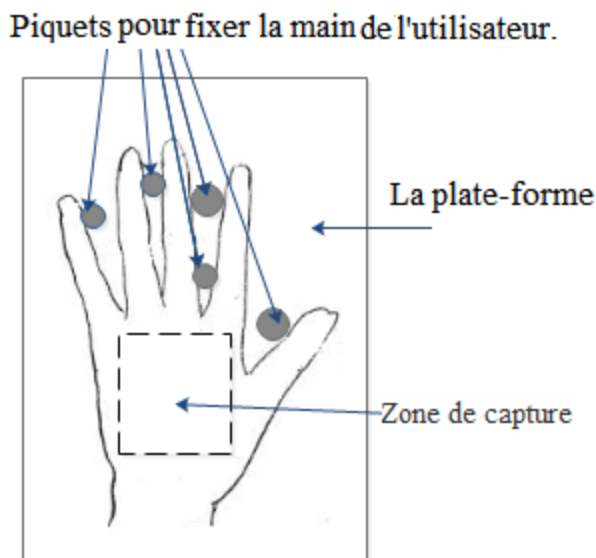


Figure 2.9 : Plate-forme de fixation de la main

Quatre images de la paume sont recueillies avec quatre longueurs d'onde de lumières spectrales : NIR (880 nm), rouge (660 nm), vert (525 nm) et bleu (470 nm) [28]. Ces longueurs d'onde ont été choisies parce que différentes lumières peuvent pénétrer dans différentes couches de la peau et pour améliorer différentes caractéristiques [29]. La commutation du temps entre les deux lumières consécutives est très courte, et les quatre images peuvent être capturées en très peu de temps (<1 s).

2.3.2. Algorithmes d'extraction des caractéristiques et classification des images de palmaire multi spectrales :

La palmaire multi spectrale est largement utilisée dans l'identification ou l'authentification personnelle pour une reconnaissance précise et robuste. Compte tenu d'une paire d'images multi-spectrales, l'objectif de l'authentification est de déterminer si elles proviennent ou non d'une même classe. La clé du succès du système biométrique est la fusion des informations. La fusion d'informations peut se faire à quatre niveaux différents: au niveau des capteurs, au niveau de l'extraction de caractéristiques, au niveau des scores et au niveau de la décision. Han et al [23] avaient proposé le premier système d'authentification de palmaire multi spectrale en ligne. Un dispositif de capture multi spectrale a été utilisé pour capter les images d'une même scène sous différentes lumières, y compris rouge, vert, bleu et infrarouge. La méthode de fusion à base d'ondelettes (trois niveaux de 'Haar') a été utilisée comme stratégie de fusion au niveau des données pour l'obtention d'une seule image

(image de fusion). Le Compétitif code algorithme [27] a été appliqué sur l'image de fusion pour l'extraction de caractéristiques et la comparaison. La fusion d'images multi spectrales à base d'ondelettes a donné un meilleur résultat que celui de l'utilisation des images multi spectrales de chaque canal seul. Zhang et al [28] avaient présenté un autre système de l'authentification de palmaire multi spectrale en ligne. Les images rouges, vertes, bleues et infrarouges sont captées en moins de 1 s, ce qui permet à ce système de répondre aux exigences d'une application en temps réel. Après l'extraction de caractéristiques de différentes bandes (rouge, verte, bleue et infrarouge, la fusion au niveau des scores de différentes Bandes a été utilisée pour intégrer les informations multi-spectrales. les résultats du système multimodal (la fusion au niveau des scores) sont meilleurs que ceux du système monomodal (chaque bande seule). Xu et al dans [29] proposèrent une autre approche pour la reconnaissance des palmaire multi-spectrales basée sur une matrice de Quaternion. Ensuite, l'analyse par composante principale (PCA) et la transformée en ondelettes discrètes (DWT) ont été respectivement appliquées sur la matrice pour extraire les caractéristiques du palmaire et l'étape de classification se fait par le calcul de la distance euclidienne. El-Tarhouni et al [30] avaient introduit un nouveau système pour l'identification des images palmaire multi spectrales. L'extraction de caractéristiques de chaque image de palmaire multi spectrale se fait par deux algorithmes : le LBP-HF «Local Binary Pattern Histogram Fourier Features» et le filtre de Gabor. Les vecteurs obtenus sont fusionnés pour trouver un long vecteur caractéristique. L'algorithme SR-KDA en «spectral regression kernel discriminant analysis» a été appliqué sur tous les vecteurs caractéristiques des images palmaires multi-spectrales pour la réduction de la dimensionnalité. Enfin, la méthode des k plus proches voisins KNN «k-nearestneighbor» avec la distance euclidienne est utilisée pour la décision finale. Hao et al [31] ont utilisé diverses techniques de fusion d'image au niveau des pixels et la représentation OLOF «Orthogonal Line Ordinal Feature» pour la reconnaissance de palmaire multi spectrale. La meilleure performance de reconnaissance a été obtenue lorsque la transformée en curvelettes a été utilisée pour la fusion des bandes. Dans [32] Khan et al, un système de vérification de palmaire multi spectrale basé sur l'algorithme du code de contour est proposé. Ici, les images de palmaire acquises dans six différentes bandes spectrales sont analysées de manière indépendante en utilisant cet algorithme avant d'effectuer la fusion au niveau des

scores. Bounneche et al [33] ont présenté une nouvelle approche de reconnaissance de palmaire multi spectrale. Un filtre de log-Gabor à multi-résolution (4 échelles et 6 orientations) a été utilisé pour l'extraction de caractéristiques où la carte caractéristique finale (feature map) est composée par des codes gagnants de la réponse de la banque de filtres les plus bas. Le processus de comparaison utilise une distance de Hamming de bit à bit et la divergence de Kullback-Leibler pour trouver l'intra et l'inter-similitude entre les cartes des caractéristiques de palmaire. Enfin, l'étape de la décision est réalisée à l'aide d'une fusion des scores générés à partir des différentes bandes spectrales. Cui.J [34] avait proposé un système de reconnaissance des images palmaire où la méthode IBLDA «Image-Based Linear Discriminant Analysis» a été utilisée pour l'extraction de caractéristiques. Deux bandes sont fusionnées au niveau des caractéristiques puis la fusion au niveau des scores est utilisée pour la reconnaissance des palmaire.

2.4. Conclusion :

Dans ce chapitre, nous avons analysé en détail les 2 modalités : palmaire et palmaire multi spectrale. Nous avons discuté les types de dispositifs d'acquisitions et le rôle de chaque élément dans ces dispositifs. Egalement, nous avons parlé des différentes caractéristiques du palmaire (Caractéristiques géométriques, les lignes principales de palmaire, les caractéristiques de rides...). Finalement, les motivations d'utilisation de palmaire 3D dans les systèmes biométriques ont été données. En plus, la plupart des contributions agissant sur ces modalités existent dans la littérature pour le prétraitement, l'extraction de caractéristiques et la classification et ont été exposées en détail.

Chapitre 3

3.1 Introduction :

Dans ce chapitre, On s'intéresse à la description de la méthode utilisée pour la représentation de la paume de la main dans un système de reconnaissance d'individu. Cette méthode est basée sur une représentation multi-échelle due à l'utilisation de l'ondelette de Gabor, puis une information texturale est extraite pour différentes échelles et orientations. La méthode SPH (Spatial Pyramid Histogram) permet de décomposer les images réponses sous forme pyramidales. Ensuite les histogrammes obtenus à chaque bloc seront normalisés dans l'intervalle $[0, 1]$ et concaténés ensemble pour former le vecteur caractéristiques global (GLSPH: Gabor LPQ SPH) de la paume de la main. Le classifieur K-NN est utilisé avec la distance intersection dans la phase de classification. De plus, deux représentations sont distinguées dans ce manuscrit dont : la première est appelée GLSPH (sans réduction de dimension), alors que la deuxième représentation est appelée Discriminant GLSPH (DGLSPH) obtenue par réduction de la dimension du vecteur caractéristique global par la méthode WLDA (Whitened Linear Discriminant Analysis (analyse linéaire discriminante blanchissement en français) afin de garder que les caractéristiques discriminantes.

Des expériences menées sur une base de données de la paume de la main PolyU 2D, montrent que la méthode décrite permet une amélioration significative des performances par rapport aux méthodes récemment proposées dans la littérature, en termes de précision.

3.2 Représentation palmaire par DGLSPH :

Dans cette partie, nous décrivons le système de représentation palmaire qui explore non seulement la propriété d'invariance au flou, mais également l'information spatiale entre différentes échelles et orientations.

La figure ci-dessous montre un schéma synoptique de la méthode utilisée dans ce manuscrit pour représenter l'empreinte palmaire dans un système de reconnaissance d'un individu basé sur la paume de la main, dont les détails sont décrits dans la section suivante. Le pipeline de cette méthode comprend cinq étapes: (i) Etape de prétraitement, (ii) Extraction des caractéristiques à l'aide de l'ondelette de Gabor, (iii) Descripteur de LPQ et (iv) Regroupement d'histogrammes obtenus à partir de la décomposition spatiale pyramidale (SPH) après normalisation. La représentation

globale de l'histogramme est ensuite utilisée par le classifieur K-NN pour la reconnaissance des empreintes palmaires.

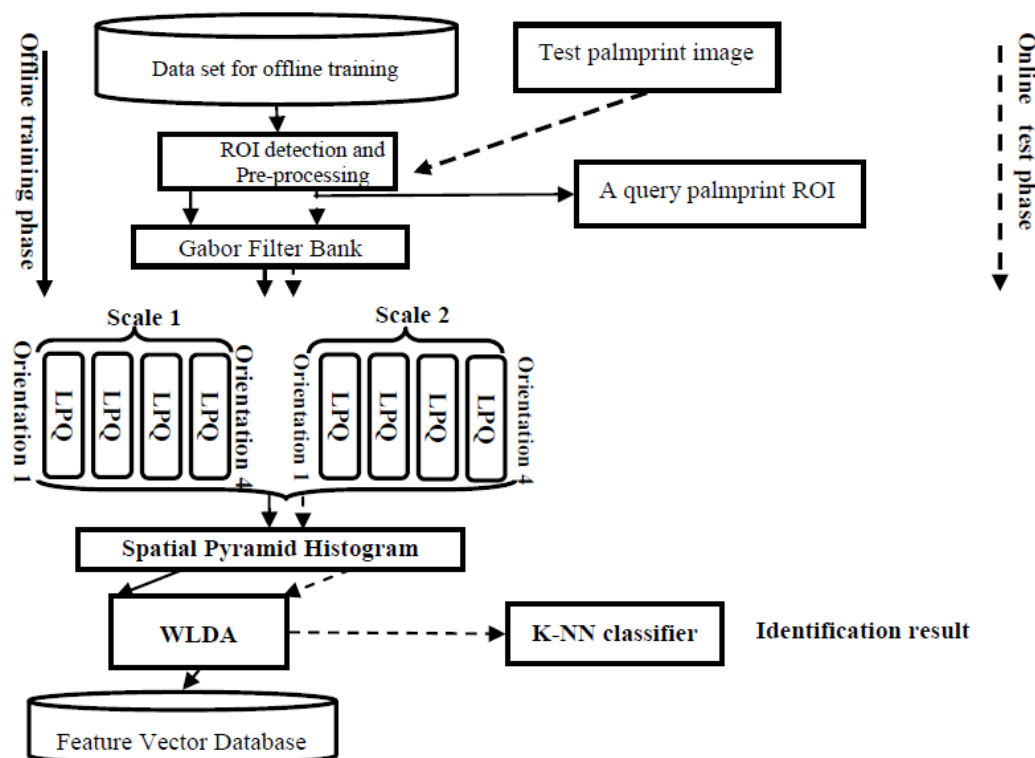


Figure 3.1: Schéma de principe de la méthode utilisée.

De plus, un aperçu de la méthode utilisée est présentée sur la Figure 3.1, Comme le montre la Figure 3.2, la région d'intérêt (ROI: Region Of Interest) de l'image palmaire est détectée par l'algorithme d'extraction de ROI [40], après la capture de l'image. Nous effectuons un prétraitement sur l'image ROI Palmaire (ROI-P), en appliquant un filtrage médian. Ensuite, les représentations multi-échelles et multi-orientations sont calculées, en convoluant le ROI-P avec la partie réelle de l'ondelette de Gabor, qui a la capacité de représenter simultanément une image dans le domaine spatial et fréquentiel. Ensuite, le descripteur de texture LPQ est appliqué à chaque réponse d'images ROI-P. Par conséquent, la propriété d'invariance au flou est explorée à différentes échelles et directions. Puis, le processus de la décomposition spatiale pyramidale (SPH) dans la direction verticale avec un niveau L est effectué. Tous les histogrammes obtenus à chaque niveau l ($l=0, \dots, L$) sont normalisés dans la plage $[0,1]$ et concaténés dans un grand histogramme. Afin de réduire davantage la haute dimensionnalité de l'histogramme global et de rendre ses caractéristiques plus discriminantes la technique de blanchiment LDA (WLDA) est appliquée.

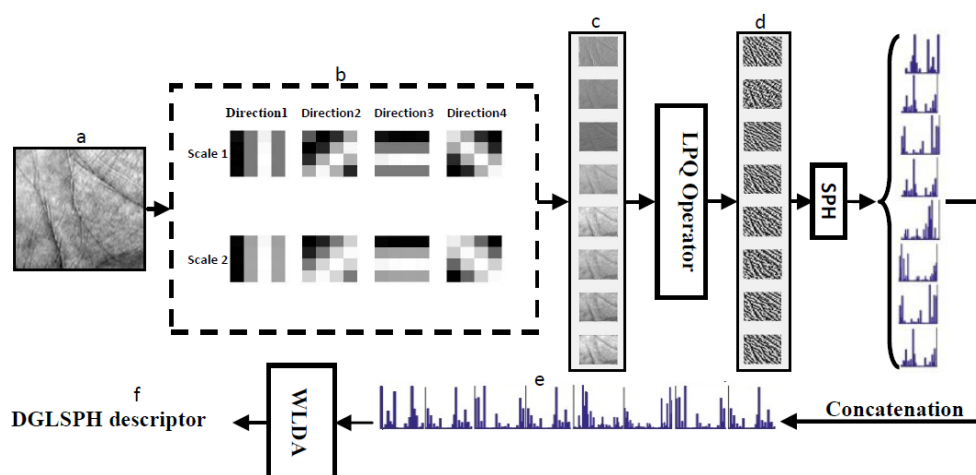


Figure 3.2 : Illustration de la représentation palmaire DGLSPH. (a) Image ROI, (b) Ondelette de Gabor, (c) Réponses de l'ondelette de Gabor, (d) Images LPQ, (e) Caractéristiques GLSPH, et (f) Caractéristiques DGLSPH.

Premièrement, l'algorithme décrit dans [40] extrait la surface de la peau entre le poignet et les doigts de l'empreinte palmaire est utilisé dans notre procédé d'extraction de ROI. L'image de la main acquise est binarisée, en utilisant un seuillage global pour extraire la paume de l'arrière-plan et suivie d'opérations morphologiques pour éliminer les petites informations d'arrière-plan non désirées. Le contour de l'image de la main est obtenu à l'aide de l'algorithme de traçage du contour [38] sur l'image de la main binarisée. Deux points de vallée situés entre les doigts sont détectés sur le contour de l'image de la main à l'aide d'un algorithme de détermination du maximum de courbure [41]. Une simple ligne perpendiculaire est ensuite étendue à partir de la ligne entre les deux doigts et une ROI est formé dans la zone de la paume. Après cela, une correction de l'éclairage non uniforme est appliquée. L'échantillon d'empreinte de paume et son région d'intérêt extraite sont illustrés à la Figure 3.3.

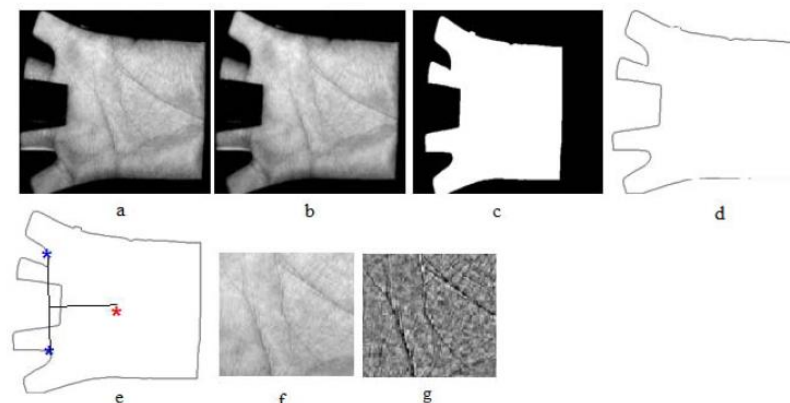


Figure 3.3 : Illustration de détection de la région d'intérêt (ROI) palmaire.

Deuxièmement, Le schéma d'extraction des caractéristiques est obtenu en construisant des informations structurelles et texturales pour différents niveaux de résolutions, en utilisant respectivement l'ondelette de Gabor et le descripteur LPQ. De plus, les caractéristiques locales sont obtenues à partir de la méthode SPH. La technique WLDA est utilisée pour: (i) Réduire la haute dimensionnalité de l'histogramme global, (ii) Renforcer la capacité de discrimination des caractéristiques.

L'ondelette de Gabor capture la structure locale correspondant à la fréquence spatiale, à la localité spatiale et à l'orientation sélective, qui sont révélées discriminantes et invariantes aux variations de l'éclairage et de l'expression dans la reconnaissance faciale [36]. Nous utilisons des filtres multi-échelles et multidirectionnels de Gabor pour coder les attributs de structure locaux intégrés aux images ROI-P. La représentation de Gabor d'une image d'empreinte palmaire est obtenue, en convoluant l'image ROI-P avec la famille de l'ondelette de Gabor telle que définie par:

$$G_{\mu,v}(z) = I(z) * \psi_{\mu,v}(z) \quad (3.1)$$

Où $G_{\mu,v}(z)$ désigne le résultat de convolution correspondant aux différents filtres de Gabor à l'orientation μ et à l'échelle v . $I(z)$ est le ROI de l'image palmaire. Dans le domaine spatial, le filtre de Gabor peut être défini comme une fonction du noyau gaussienne modulée par une onde plane sinusoïdale :

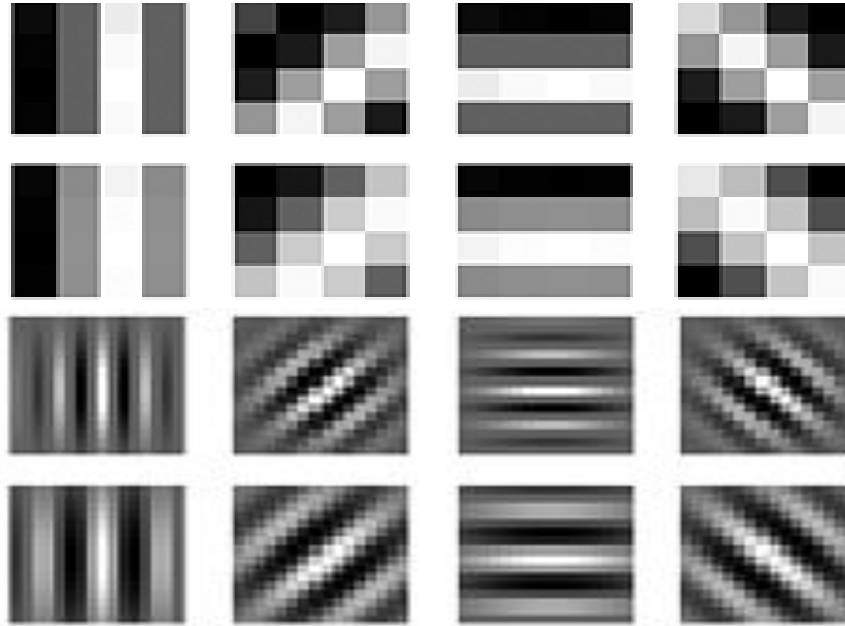


Figure 3.4 : Partie réelle de l'ondelette de Gabor avec deux échelles et quatre orientations. (a) Taille de la fenêtre est de 4x4, (b) Taille de la fenêtre est de 8x8.

$$\psi_{\mu,v}(z) = \frac{\|k_{\mu,v}^2\|}{\sigma^2} \text{Exp}\left(-\frac{\|k_{\mu,v}^2\|\|z^2\|}{2\sigma^2}\right) \left[\text{Exp}(ik_{\mu,v}z) - \text{Exp}\left(-\frac{\sigma^2}{2}\right)\right] \quad (3.2)$$

z est un vecteur de coordonnées $[x, y]^t$. $\|\cdot\|$ désigne l'opérateur de la norme euclidienne et le vecteur d'onde $k_{\mu,v}$ est défini comme suit:

$$k_{\mu,v} = k_v \text{Exp}(i\phi_\mu) \quad (3.3)$$

Où $k_v = k_{max}/f_v$, $k_{max} = \pi/2$, $f_v = f^v$, $f = \sqrt{2}$ et $\phi_\mu = (\pi \cdot \mu)/4$

k_{max} désigne la fréquence maximale et représente le facteur d'espacement entre les noyaux dans le domaine fréquentiel.

Tous les filtres peuvent être générés à partir d'une ondelette mère par dilatation et rotation. Dans ce travail, nous utilisons des filtres de Gabor à deux échelles $v \in \{0, 1\}$ et quatre orientations $\mu \in \{0, 1, 2, 3\}$ avec un paramètre $\sigma = 2\pi$ donnant par conséquent huit filtres. Leurs parties réelles sont présentées sur la Figure 3.4.

3.2.1 La méthode de la décomposition spatiale pyramidale (SPH) :

Nous utilisons la méthode SPH introduite par Lazebnik [42], basée sur l'histogramme de pyramide de Grauman [43]. Le processus de construction des histogrammes à partir de la méthode de décomposition pyramidale (SPH) avec un niveau L est réalisé

comme suit: on créant, dans la première étape, l'histogramme de niveau 0 (image entière).

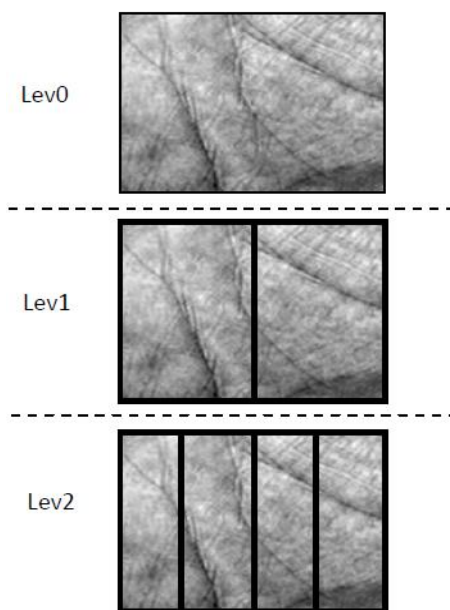


Figure 3.5 : Les stratégies de décomposition verticale en plusieurs sous-blocs.

Ensuite, l'image est divisée en deux régions de taille égale au niveau 1, en utilisant une décomposition verticale et l'histogramme est calculé à chaque région. Le processus est répété, en subdivisant récursivement chaque région et, en calculant les histogrammes dans chaque région jusqu'à atteindre le niveau souhaité L.

3.2.2 La méthode d'analyse discriminante linéaire blanchie (WLDA) :

Les méthodes d'analyse des données sont utilisées pour réduire la dimension d'espace initiale, tout en ne conservant que les propriétés les plus discriminantes des caractéristiques extraites. Plusieurs approches de projection linéaire ou non linéaire ont été utilisées dans la littérature pour la reconnaissance d'empreintes palmaires, afin de réduire la dimensionnalité des vecteurs caractéristiques, telles que: PCA [35], LDA [36]. Dans [44], la technique WLDA a démontré son efficacité par rapport aux PCA et LDA dans la reconnaissance faciale. L'idée de base de WLDA est d'appliquer une transformation de blanchiment des données avant de réaliser l'algorithme LDA.

3.2.3 Etape de classification :

Etant donné un nouveau échantillon Y de l'ensemble de test. Au début, nous calculons la représentation proposée (GLSPH) de cet échantillon. Ensuite, le vecteur des

caractéristiques obtenu est mis en correspondance avec tous les modèles stockés. Un classifieur de plus proche voisin est utilisé avec la similarité d'intersection, afin de calculer la distance entre deux histogrammes.

La similarité d'intersection entre deux histogrammes H^1 et H^2 de longueur N est définie comme suit :

$$d(H^1, H^2) = \sum_{l=1}^N \text{Min}(H^1(l), H^2(l)) \quad (3.4)$$

Dans le cas du vecteur caractéristique DGLSPH, la similarité en cosinus est utilisée. Cette similarité entre deux vecteurs x et y de longueur N est définie comme suit :

$$S(x, y) = \frac{x \cdot y}{\|x\| \|y\|} = \frac{\sum_{i=0}^{N-1} x_i y_i}{\sqrt{\sum_{i=0}^{N-1} (x_i)^2} \sqrt{\sum_{i=0}^{N-1} (y_i)^2}} \quad (3.5)$$

3.3 Etude Expérimentale :

Pour une évaluation approfondie de la méthode utilisée, nous avons effectué une série d'expérimentations, en utilisant le descripteur discriminant DGLSPH afin d'extraire des caractéristiques discriminantes à partir d'un ensemble d'images pour la modalité biométrique palmaire, en utilisant la base de données PolyU.

3.3.1 La base de données PolyU :

La base de données d'images palmaires PolyU [37] est créé à l'Université polytechnique de Hong Kong. Elle comprend 7752 images en niveaux de gris recueillies auprès des deux mains de 193 sujets (soit 386 paumes distinctes), dont 131 hommes et 62 femmes. Toutes les images palmaires de la base de données ont été capturées au cours de deux sessions distinctes par une caméra CCD avec une résolution de 75 dpi (Dots Per Inch). Dans chaque session, environ 10 images sont collectées (ou bien 20 images par sujet). L'intervalle moyen entre la première et la deuxième session était d'environ deux mois. Ainsi, il y avait 386 classes différentes d'images palmaires ou chaque classe contient 20 images palmaires. Au cours des expériences, N images de la première session sont prises pour l'apprentissage et toutes les images de la deuxième session sont conservées pour la phase de test.

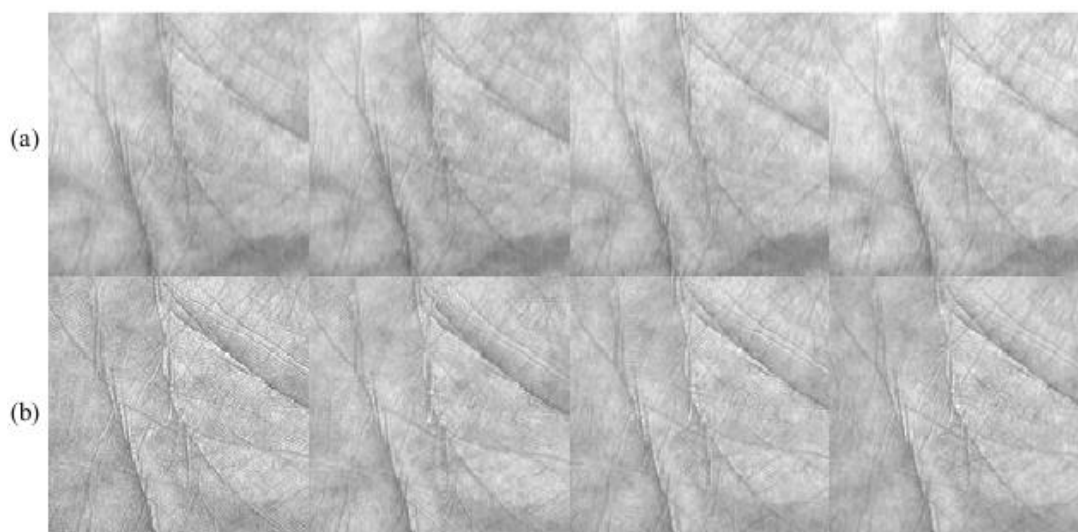


Figure 3.6 : Quelques ROIs extraits des images palmaires de la base de données PolyU (a) Première session, (b) Seconde session.

Pour mieux décrire la différence entre les images capturées à chaque session, la Figure 3.6 illustre certaines images palmaires capturées dans différentes sessions à partir d'une même paume. Les trois images de la première rangée (voir Figure 3.6 a) ont été capturées lors de la première session, tandis que les images de la deuxième rangée (Figure 3.6 b) ont été capturées lors de la deuxième session. On peut constater qu'il y a de profonds changements d'éclairage.

3.3.1.1 Expérimentation #1 :

Afin d'examiner l'effet des paramètres k et L sur les performances de reconnaissance palmaire, nous utilisons les trois premières images de la première session pour la phase d'apprentissage (1158 images) et toutes les images de la deuxième session (3863 images) sont utilisées dans la phase de test similaire à [39].

Les résultats obtenus dans Tableau 3.1 et Tableau 3.2 montrent l'influence du choix des paramètres k et L sur le système de reconnaissance pour les représentations DGLSPH et GLSPH, respectivement. Pour une fenêtre LPQ de taille k fixe, le taux de reconnaissance est augmenté proportionnellement à la décomposition du niveau L de la méthode SPH. Alors, qu'à un niveau de décomposition L fixe, le taux de reconnaissance est meilleur lorsque la fenêtre LPQ est suffisamment grande. Ceci est dû à la forte corrélation entre les pixels adjacents. Cependant, l'utilisation d'une

fenêtre LPQ de petite taille donne un faible taux de reconnaissance, même pour un niveau de décomposition L élevé.

K	3	5	7	9	11	13	15	17	19	21
Level 0	24.44	55.63	78.00	85.58	89.46	89.21	88.07	86.98	86.95	85.55
Level 1	55.92	83.41	92.39	95.34	96.35	96.12	95.91	95.75	95.63	95.37
Level 2	79.03	93.40	96.97	98.24	98.86	98.89	98.78	98.84	99.30	98.58
Level 3	89.90	96.71	97.90	98.89	99.53	99.59	99.74	99.61	99.84	99.40
Level 4	93.86	97.51	98.34	99.17	99.77	99.77	99.84	99.95	99.90	99.77

Tableau 3.1 : Taux d'identifications utilisant la représentation DGLSPH sur la base de données PolyU.

K	3	5	7	9	11	13	15	17	19	21
Level 0	30.29	44.47	58.09	65.44	70.13	71.16	69.79	70.18	69.32	67.93
Level 1	43.49	58.45	72.43	79.89	82.55	83.12	83.30	83.12	81.98	81.80
Level 2	53.27	70.10	83.38	88.43	90.97	90.99	91.56	91.74	91.85	91.38
Level 3	61.22	80.87	90.71	93.71	95.57	95.96	96.74	96.40	96.58	96.01
Level 4	66.37	87.63	94.25	96.76	97.80	98.14	98.71	98.52	98.32	98.21

Tableau 3.2 : Taux d'identifications utilisant la représentation GLSPH sur la base de données PolyU.

Nous pouvons voir dans Tableau 3.1 et Tableau 3.2, que le meilleur taux de reconnaissance est de 99,95% obtenu pour k=17 et L=4, utilisant la représentation DGLSPH et égal à 98,71% pour k=15 et L=4 avec la représentation GLSPH.

3.3.1.2 Expérimentation #2 :

Pour démontrer l'efficacité de la méthode proposée, une étude comparative a été faite avec certains travaux existants appliqués à la base de données PolyU. Les différents protocoles utilisés par ces méthodes sont résumés dans le Tableau 3.3.

Protocole	Apprentissage		Test	
	Session 1	Session 2	Session 1	Session 2
A	All images	All images	Not used	All images
B	First N images	All images	Not used	All images
C	First N images	All images	Remaining images	All images
D	First N images	Not used	Remaining images	Not used
E	Randomly selected N images	All images	Remaining images	All images
F	All images	Randomly selected N images	Not used	Randomly selected N images
G	K-Fold Cross Validation			
H	First N images	First M images	Not used	First M images

Tableau 3.3 : Différents protocoles d'identification des empreintes palmaires utilisés dans les bases de données PolyU et PolyU 2D/3D.

Méthodes	Nbr. classe	Protocole	N	IR(%)
Competitive code	386	C	3	97.88
Ordinal code	386	C	3	97.45
Fusion	386	C	3	96.06
BOCV	386	C	3	95.80
E-BOCV	386	C	3	96.41
RLOC	386	C	3	95.58
HOC	386	C	3	98.84
Méthode proposée	386	B	3	99.95

Tableau 3.4 : Etude comparative de la méthode proposée avec les méthodes de codage sur la base de données PolyU.

La Figure 3.7 montre que les taux d'erreur d'identification des méthodes de codage tels que le code concurrentiel, le code ordinal, le code de fusion, le BOCV, le E-BOCV et le HOC sont plus élevés que la méthode proposée. De plus, le Tableau 3.4 compare les taux d'identification.

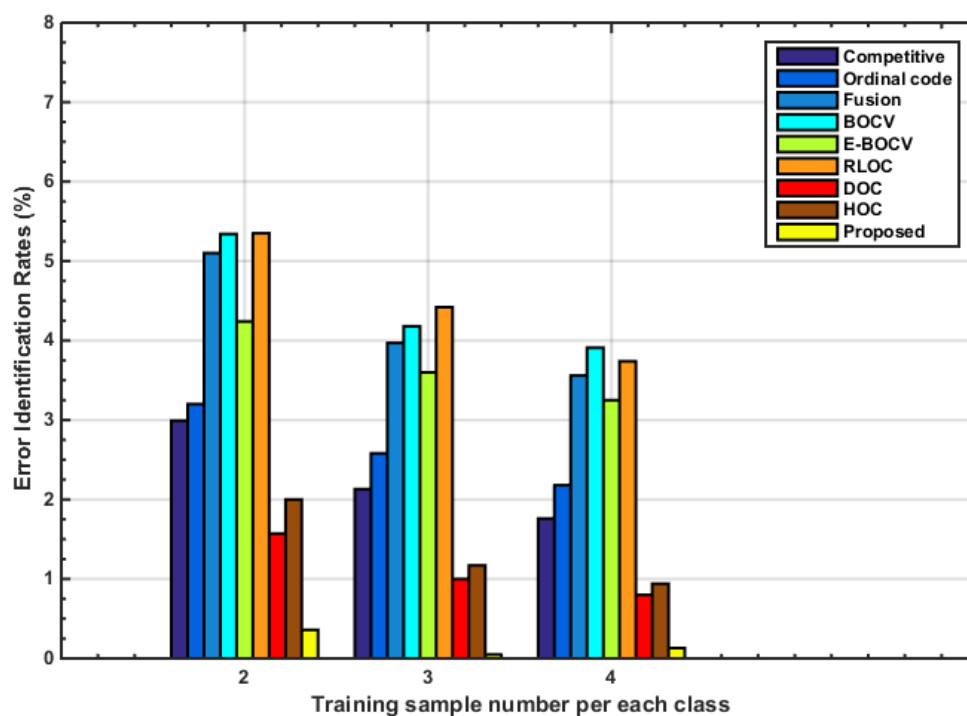


Figure 3.7 : Taux d'erreur d'identification palmaire sur la base de données PolyU.

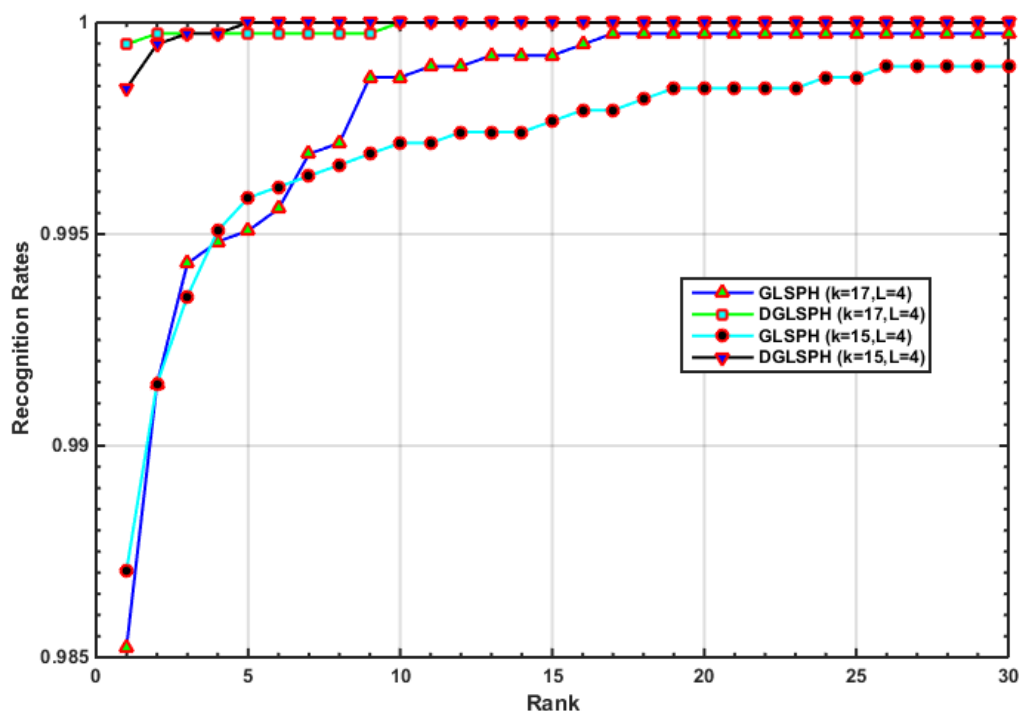


Figure 3.8 : Courbes CMC sur la base de données PolyU.

Le meilleur taux de reconnaissance $IR = 100\%$ est obtenu à partir des rangs 5 et 10 de la méthode proposée (DGLSPH), en utilisant le descripteur LPQ avec $k=15$ et $k=17$, respectivement.

3.4. Conclusion

Dans ce chapitre, nous avons illustré le principe de la méthode utilisée dans ce manuscrit afin de représenter l'empreinte palmaire dans système de reconnaissance biométrique. Elle consiste en une décomposition en ondelettes, utilisant l'ondelette de Gabor, le descripteur LPQ et la méthode SPH, visant à extraire des caractéristiques plus discriminantes. Des expériences approfondies montrent la performance de la méthode utilisée par rapport aux méthodes existantes dans la littérature. Cette représentation palmaire augmente efficacement la précision de l'identification des empreintes palmaires avec un coût de calcul remarquablement inférieur.

Conclusion générale

L'identification des individus par les empreintes palmaires (Palmprints), considérée comme un nouveau membre de la famille des modalités biométriques, est devenue un domaine de recherche très actif ces dernières années. Le travail effectué jusqu'à présent s'est basé sur les techniques de représentation d'images Palmprints pour une meilleure classification.

Les travaux présentés dans ce document s'inscrivent dans le contexte de l'identification automatique des personnes à partir de leurs descripteurs biométriques. Nous avons utilisé une nouvelle modalité biométrique, la dactyloscopie, pour créer les systèmes biométriques que nous proposons, tant monomodaux que multimodaux. Après avoir présenté les concepts généraux de la biométrie, nous avons présenté l'état de l'art des méthodes de fusion des modalités biométriques, en utilisant différentes techniques et niveaux de fusion. Nous avons également présenté quelques méthodes d'extraction des caractéristiques à base de texture. Nos tests utilisant les données dactyloscopiques FKP de l'Université Polytechnique de Hong Kong (PolyU) ont montré que notre méthode pouvait fournir d'excellents résultats en termes de taux d'erreur (EER), de taux de reconnaissance et de séparation globale entre les distributions des imposteurs et des clients.

A la fin de nos travaux, nous prévoyons d'utiliser d'autres méthodes (PCA, GABOR...etc.) dans nos travaux futurs pour extraire les caractéristiques des modalités biométriques. Ainsi, nous chercherons à utiliser d'autres niveaux de fusion (niveau d'image, niveau caractéristique et niveau de décision).

Bibliographie

- [1]: S. Prabhakar, S. Pankanti, and A. K. Jain. Biometric recognition: Security and privacy concerns. *IEEE Security & Privacy*, 1:33–42, 2003. [Cite p. 8]
- [2]: J. Daugman. Recognizing Persons by Their Iris Patterns. In A. K. Jain, R. Bolle, and S. Pankanti, editors, *Biometrics: Personal Identification in a Networked Society*, pp. 103- 121, Kluwer Academic Publishers, 1999.
- [3]: N. Rudin, K. Inman, G. Stolovitzky, and I. Rigoutsos. *Biometrics: Personal Identification in Networked Society*, chapter DNA Based Identification, pages 287–309. Kluwer Academic Publishers, 2002. [cit´e p. 8]
- [4]: International Biometric Group. [Http: //www.biometricgroup.com/](http://www.biometricgroup.com/), 2010. [Cite p. 1, 15, 154]
- [5]: L. O’Gorman. Comparing passwords, tokens, and biometrics for user authentication. In *Proceedings of the IEEE*, volume 91, pages 2021–2040, 2003. [Cite p. 11]
- [6] : Fedias Meriem., "Combinaisons de donn´ees d’espaces couleurs et de m´ethodes de v´erification d’identit´e pour l’authentification de visages", Universit´e Mohamed Khi der – Biskra.
- [7] : DANG Hoang Vu., "Biom´etrie pour l’identification", Rapport final, Institut de la Francophonie pour l’Informatique, Hanoï, Vietnam, 07 – 2005.
- [8] : Nicolas MORIZET., "Reconnaissance Biom´etrique par Fusion Multimodale du Visage et de l’Iris", Th`ese pr´esent´ee pour obtenir le grade de Docteur, Ecole Nationale Sup´erieure des T´el´ecom munications, Paris, 18 Mars 2009.
- [9] : revues.univ-biskra.dz/index.php/cds/article/view/455/422
- [10] : Moulay Brahim Oussama, Arbaoui Mohamed Ibrahim., "Authentification des personnes par les articulations des doigts", UNIVERSITE KASDI MERBAH OUARGLA, 2015.
- [11] Cannon, M., Byrne, M., Cotter, D., Sham, P., Larkin, C., & O’Callaghan, E. (1994). Further evidence for anomalies in the hand-prints of patients with schizophrenia: a study of secondary creases. *Schizophrenia Research*, 13(2), 179-184.

Bibliographie

- [12] Kong, A. W. K., Zhang, D., & Lu, G. (2006). A study of identical twins' palmprints for personal verification. *Pattern Recognition*, 39(11), 2149-2156.
- [13] Zhang, D., Zuo, W., & Yue, F. (2012). A comparative study of palmprint recognition algorithms. *ACM Computing Surveys (CSUR)*, 44(1), 2.
- [14] Genovese, A., Piuri, V., & Scotti, F. (2014). *Touchless palmprint recognition systems (Vol. 60)*. Switzerland: Springer.
- [15] Zhang, D., & Lu, G. (2013). *3D biometrics: systems and applications*. Springer Science & Business Media.
- [16] Zhang, D., Kanhangad, V., Luo, N., & Kumar, A. (2010). Robust palmprint verification using 2D and 3D features. *Pattern Recognition*, 43(1), 358-368.
- [17] Zhang, D., Lu, G., Li, W., Zhang, L., & Luo, N. (2008, September). Three dimensional palmprint recognition using structured light imaging. In *Biometrics: Theory, Applications and Systems, 2008. BTAS 2008. 2nd IEEE International Conference on* (pp. 1-6). IEEE.
- [18] Zhang, D., Lu, G., Li, W., Zhang, L., & Luo, N. (2009). Palmprint recognition using 3-D information. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, 39(5), 505-519.
- [19] Yang, B., Wang, X., Yao, J., Yang, X., & Zhu, W. (2013). Efficient local representations for three-dimensional palmprint recognition. *Journal of Electronic Imaging*, 22(4), 043040-043040.
- [20] Cui, J. (2014). 2D and 3D palmprint fusion and recognition using PCA plus TPTSR method. *Neural Computing and Applications*, 24(3-4), 497-502.
- [21] Meraoumia, A., Chitroub, S., & Bouridane, A. (2013). 2D and 3D palmprint information, PCA and HMM for an improved person recognition performance. *Integrated Computer- Aided Engineering*, 20(3), 303-319.
- [22] Zhang, L., Shen, Y., Li, H., & Lu, J. (2015). 3D palmprint identification using blockwise features and collaborative representation. *IEEE transactions on pattern analysis and machine intelligence*, 37(8), 1730-1736.

Bibliographie

- [23] Han, D., Guo, Z., & Zhang, D. (2008, October). Multispectral palmprint recognition using wavelet-based image fusion. In *Signal Processing, 2008. ICSP 2008. 9th International Conference on* (pp. 2074-2077). IEEE.
- [24] Chang, C. I. (Ed.). (2007). *Hyperspectral data exploitation: theory and applications*. John Wiley & Sons.
- [25] Wang, C. M., Chen, C. C. C., Chung, Y. N., Yang, S. C., Chung, P. C., Yang, C. W., & Chang, C. I. (2003). Detection of spectral signatures in multispectral MR images for classification. *IEEE Transactions on Medical Imaging*, 22(1), 50-61.
- [26] Pietikinen, M. K. (2001). *Texture analysis in machine vision*. Series in machine perception artificial intelligence.
- [27] Kong, A. K., & Zhang, D. (2004, August). Competitive coding scheme for palmprint verification. In *Pattern Recognition, 2004. ICPR 2004. Proceedings of the 17th International Conference on* (Vol. 1, pp. 520-523). IEEE.
- [28] Zhang, D., Guo, Z., Lu, G., Zhang, L., & Zuo, W. (2010). An online system of multispectral palmprint verification. *IEEE transactions on instrumentation and measurement*, 59(2), 480-490.
- [29] Xu, X., Guo, Z., Song, C., & Li, Y. (2012). Multispectral palmprint recognition using a quaternion matrix. *Sensors*, 12(4), 4633-4647.
- [30] El-Tarhouni, W., Boubchir, L., Al-Maadeed, N., Elbendak, M., & Bouridane, A. (2016, October). Multispectral palmprint recognition based on local binary pattern histogram fourier features and gabor filter. In *Visual Information Processing (EUVIP), 2016 6th European Workshop on* (pp. 1-6). IEEE.
- [31] Hao, Y., Sun, Z., Tan, T., & Ren, C. (2008, October). Multispectral palm image fusion for accurate contact-free palmprint recognition. In *Image Processing, 2008. ICIP 2008. 15th IEEE International Conference on* (pp. 281-284). IEEE.
- [32] Khan, Z., Mian, A., & Hu, Y. (2011, November). Contour code: Robust and efficient multispectral palmprint encoding for human recognition. In *Computer Vision (ICCV), 2011 IEEE International Conference on* (pp. 1935-1942). IEEE.

Bibliographie

- [33] Bounneche, M. D., Boubchir, L., Bouridane, A., Nekhoul, B., & Ali-Chérif, A. (2016). Multi-spectral palmprint recognition based on oriented multiscale log-Gabor filters. *Neurocomputing*, 205, 274-286.
- [34] Cui, J. R. (2012). Multispectralpalmprint recognition using image-basedlinear discriminant analysis. *International Journal of Biometrics*, 4(2), 106-115.
- [35]. S. Ribaric and I. Fratric, "A biometric identification system based on eigenpalm and eigenfinger features," *IEEE Trans. Pattern. Anal. Mach. Intell.*, 27(11), pp. 1698-1709 (2005).
- [36]. X. Wu, D. Zhang and K. Wang, "Fisherpalms based palmprint recognition," *Pattern Recogn. Lett.*, 24(15), pp. 2829-2838 (2003).
- [37]. J. Yang, D. Zhang, J. Yang and B. Niu, "Globally maximizing, locally minimizing: unsupervised discriminant projection with applications to face and palm biometrics," *IEEE Trans. Pattern Anal. Mach. Intell.*, 29(4), pp. 650-664 (2007).
- [38]. Y. Yan, Y. J. Zhang, "Discriminant projection embedding for face and palmprint recognition," *Neurocomputing*, 71(16), pp. 3534-3543 (2008).
- [39]. Y. Luo, L. Zhao, B. Zhang, W. Jia, F. Xue, J. Lu, Y. Zhu and B. Xu, "Local line directional pattern for Palmprint Recognition," *Pattern Recognit.*, 50 (2), pp. 26-44 (2016).
- [40]. G. Li, J. Kim, "Palmprint Recognition with Local Micro-structure Tetra Pattern," *Pattern recognition journal* (2016).
- [41]. J. Cui, "2D and 3D palmprint fusion and recognition using PCA plus TPTSR method," *Neural Comput. &Applic.* 24, pp. 497-502 (2014).
- [42]. S. Lazebnik, C. Schmid and J. Ponce, "Beyond bags of features: Spatial pyramid matching for recognizing natural scene categories," in *Proceedings of the 2006 IEEE Computer Society Conference on Computer Vision and Pattern Recognition -Volume 2*. IEEE Computer Society, pp. 2169-2178 (2006).
- [43]. K. Grauman and T. Darrel, "The pyramid match kernel: Discriminative classification with sets of image features," in *Proceedings of the tenth IEEE*

Bibliographie

International Conference on Computer Vision –volume 2. IEEE Computer Society, pp. 1458-1465 (2005).

[44]. V.D.M. Nhat, S.Y. Lee and H.Y. Youn, "Whitened LDA for face recognition", CIVR'07, Amsterdam, the Netherlands, 2007.