République Algérienne Démocratique et Populaire
Ministère de l'enseignement Supérieur et de la Recherche Scientifique
Université de Mohamed El Bachir El Ibrahimi de Bordj Bou Arréridj
Faculté des Mathématiques et d'Informatique
Département d'informatique

MEMOIRE

Présenté en vue de l'obtention du diplôme

Master en informatique

Spécialité : Ajoutez votre spécialité ici

THEME

Système biométrique basé sur la fusion au niveaux des caractéristiques

Présenté par :
Naili Ammar Dhiya Eddine

Soutenu publiquement le : 20/06/2023
Devant le jury composé de:
Président : Bouziane Abderraouf
Examinateur : Belhadj Foudil
Encadreur : Attia Abdelouahab

2022/2023

Je dédie ce modeste travail à celle qui m'a donné la vie, le symbole de tendresse, qui s'est sacrifiée pour mon bonheur et ma réussite, à ma mère. A mon père, école de mon enfance, qui a été mon ombre durant toutes les années des études, et qui a veillé tout au long de ma vie à m'encourager, à me donner l'aide et à me protéger.

Que dieu les gardes et les protège ;

Je dédie toute la famille ;

A mes adorables sœurs ;

A mes amis ;

A tous ceux qui me sont chères ;

A tous ceux qui m'aiment ;

A tous ceux que j'aime.

Remerciements

Je tiens à remercier tout d'abord dieu qui a aidé à Réaliser ce modeste travail, et pour sa grâce toutes à la longue de notre vie professionnelle.

Je remercie chaleureusement mon encadreur et Professeur: M. Abdelouahab Attia pour son aide, sa disponibilité, son sérieux ainsi que ses encouragements et ses conseils.

Je tiens aussi à remercier : Tous les enseignants de département d'informatique qui ont contribué de près ou de loin à la réaffirmation de notre travail.

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

Merci à toutes et à tous.

Sommaire

Liste des figures

Liste des tableaux

Listes des Acronymes et Symboles

Acronymes	
FKP	Finger Knuckle Print
BSIF	Binarized Statistical Image Features
LDA	Linear Discriminant Analysis
PCA	Principal Component Analysis
ROC	Receiver Operating Characteristic
CMC	Cumulative Match Characteristic
HMM	Hidden Markov Model
DCT	Transformée en cosinus discrète
MAD	Les valeurs médianes et d'écart absolu médian
ACP	L'analyse en composantes principales
PhD	Pretty Helpful Development
ADN	Acide Désoxyribose Nucléique
BDD	Data Base ("Base des données")
CCD	Récepteurs à transferts de charge ("charge coupled device")
CMC	Cumulative Match Curve ("la courbe des scores cumulés ")
EER	Equal Error Rate ("Taux d'erreurs égales ")
FAR	False Acceptante Rate ("Taux de Fausses Acceptations")
FRR	False Rejection Rate ("Le taux de Faux Rejets ") HOG: histogramme oriented gradient (histogramme de gradients orientés)
Poly U	Base de données empreinte palmaire de l'université polytechnique de Hong Kong
Rang	Taux de reconnaissance

INTRODUCTION GENERALE

Au fil de la recherche scientifique dans le domaine des technologies de sécurité de l'information, l'identification des individus est devenue relativement facile et efficace par rapport aux méthodes traditionnelles telles que l'utilisation de noms d'utilisateur et de mots de passe. En effet, les systèmes biométriques ont largement envahi le domaine de la sécurité à l'échelle mondiale grâce à leur efficacité et leurs performances. Ces systèmes se basent sur deux catégories de caractéristiques : les caractéristiques physiques (iris, rétine, empreintes digitales, reconnaissance faciale, structure vasculaire, etc.) et les caractéristiques comportementales (traits vocaux, signature, dynamique de frappe, démarche, etc.) [1].

En général, l'authentification des personnes peut s'appuyer sur ce qu'elles sont, ce qu'elles possèdent, ce qu'elles savent et ce qu'elles font. Chaque individu naît avec des caractéristiques uniques, telles que son visage, qui permettent de le reconnaître. De plus, l'identification d'une personne peut également se faire en fonction de ce qu'elle possède, comme des cartes d'identité et des mots de passe. Lorsqu'une personne tente de se connecter à son compte bancaire ou à d'autres activités en ligne en utilisant un nom d'utilisateur et un mot de passe, cette méthode se base sur ce que la personne sait. Enfin, la reconnaissance d'une personne autorisée peut se baser sur sa façon de se comporter. Les biométries comportementales, telles que la voix, la démarche et la signature, sont les méthodes les plus connues dans le domaine de la sécurité. Ces techniques de reconnaissance ont attiré de nombreux chercheurs en raison de leur coût de mise en œuvre relativement faible par rapport aux caractéristiques physiologiques, de leur facilité d'utilisation et de leur complexité à imiter les habitudes de frappe d'autres individus [2].

Ainsi, le déploiement de telles méthodes d'authentification, en remplacement des mots de passe qui peuvent être facilement perdus ou oubliés, peut considérablement renforcer les fonctionnalités de sécurité pour l'identification en temps réel et contribuer à réduire les accès non autorisés à de nombreuses applications et services.

Par conséquent, la reconnaissance biométrique joue un rôle essentiel dans de nombreux domaines, tels que la sécurité, l'authentification et l'accès aux systèmes. Parmi les différentes modalités biométriques, l'empreinte du doigt (FKP) et l'empreinte palmaire sont deux méthodes largement utilisées pour l'identification des individus. Chacune de ces modalités présente ses propres avantages et limitations en matière de précision et de stabilité des caractéristiques [3].

Cependant, pour maximiser la précision de l'identification biométrique, il est possible d'exploiter les avantages de ces deux modalités en les fusionnant au niveau des caractéristiques. Cette approche de fusion permet de combiner les informations extraites des empreintes du doigts (FKP - Finger's Knuckle Print) et des empreintes palmaires, afin d'améliorer la précision et la robustesse du système de reconnaissance biométrique [4].

Dans le cadre de ce mémoire de nous proposons une architecture d'authentification basée sur la fusion des empreintes du doigts (FKP - Finger's Knuckle Print) et palmaires en utilisant le descripteur BSIF (Binarized Statistical Image Features) ainsi que les techniques de réduction de dimension LDA (Linear Discriminant Analysis) et PCA (Principal Component Analysis). L'objectif de notre travail est d'extraire un modèle en appliquant le descripteur BSIF aux empreintes du doigts (FKP) et palmaires, et d'utiliser les techniques LDA et PCA pour réduire la dimension des vecteurs extraits.

Nous avons conçu deux expériences principales dans notre étude. Dans la première expérience, nous avons mis en place un système unimodal qui utilise une seule modalité à la fois, en appliquant le descripteur BSIF au processus d'extraction des caractéristiques des empreintes du doigts (FKP) et palmaires. Dans la deuxième expérience, nous avons mis en œuvre une fusion multimodale pour obtenir de meilleurs résultats et un taux d'identification des erreurs plus faible, ce qui rend le système plus efficace pour une utilisation dans des applications nécessitant une sécurité élevée.

Pour évaluer les performances de notre système proposé, nous avons réalisé une comparaison entre les méthodes de fusion et de concaténation des images d'empreintes du doigts (FKP) et palmaires à différents niveaux et méthodes.

Le reste de ce mémoire est organisé comme suit : le chapitre 1 présent les concepts de base de la biométrie. Nous fournissons une description détaillée du processus de reconnaissance, y compris un bref aperçu du fonctionnement d'un système biométrique, pourquoi il est une alternative efficace aux systèmes d'identification classiques, pour discuter après comment les systèmes biométriques sont évalués en matière de performance.

Au chapitre 2, nous étudierons l'état de l'art de la fusion des caractéristiques entre l'empreinte palmaire et l'empreinte du doigt (FKP). Nous examinerons les caractéristiques propres à chaque modalité, les niveaux de fusion basés sur la fusion des caractéristiques, et l'importance de la normalisation des vecteurs dans ce processus

Dans le chapitre 3, nous détaillons notre système proposé, en expliquant les étapes de la fusion des caractéristiques au niveau des empreintes des doigts et palmaires en utilisant le descripteur BSIF.

Nous présentons également les résultats expérimentaux de notre système et discutons des performances de la fusion des caractéristiques que nous avons mentionnées, et l'interprétation des résultats.

Enfin, notre recherche vise à exploiter les avantages de la fusion des caractéristiques entre les empreintes du doigts (FKP) et palmaires pour améliorer la précision et la fiabilité de la reconnaissance biométrique. Les résultats de cette étude pourraient contribuer à fournir des fonctionnalités de sécurité supérieure et une identification en temps réel plus fiable, réduisant ainsi les risques d'accès.

Chapitre 01

GENERALITE DE SYSTEME BIOMETRIQUE

1.1. Introduction :

Généralement, on peut dire que la biométrie c'est la technique utilisée pour vérifier ou déterminer Sécurité, et surtout à la suite des attentats terroristiques du 11 septembre 2001et ceux de de Madrid en 2004 et de Londres en 2005. Dans ce chapitre en apprenons davantage sur cette technique grâce à l'exposition à certains éléments [5].

1.2. Historique et applications :

Le vocable le plus exact pour décrire le champ de la biométrie serait sans doute celui d'anthropométrie (du grec anthropo, « homme », et metron, « mesure »). Alphonse Bertillon (1853-1914), le fondateur de la police scientifique en 1880, avait recours à des données biométriques lorsqu'il traquait les récidivistes par le bertillonnage, en mesurant diverses parties du corps ou du visage qui ne changent pas à l'âge adulte. Quelques années plus tard, en 1892, le Britannique Francis Galton (1822-1911) allait révolutionner les méthodes policières en démontrant par la statistique le caractère unique des empreintes digitales [6]. Aujourd'hui, le progrès des sciences et des techniques permet d'autres modes d'identification des personnes. L'informatique supplante les fichiers manuels. Elle permet non seulement des traitements accélérés mais aussi des contrôles à distance. L'identification et l'authentification des personnes sont ainsi facilitées [7].

L'introduction de données biométriques a pour but de renforcer la sécurité des États à l'heure de la mondialisation. La menace terroriste revêt une particulière acuité : les attentats du 11 septembre 2001 aux États-Unis et du 11 mars 2004 en Espagne en sont l'illustration. La criminalité organisée et l'immigration illégale justifient également la prise de mesures particulières de protection.

La biométrie est de plus en plus utilisée dans les aéroports, les établissements pénitentiaires, pour l'accès à des locaux sécurisé, pour la garantie du vote électronique, la sécurité des paiements bancaires ou des transactions via Internet. Le marché associé à son développement est estimé à 900 millions de dollars pour 2006. Les enjeux économiques sont donc très importants et pèsent sur le choix des normes et des matériels en vue d'une interopérabilité [8].

L'amélioration de la sécurité qui résulte du recours à la biométrie ne doit pas pour autant porter atteinte aux libertés individuelles.

En médecine, la biométrie désigne l'étude statistique des dimensions et de la croissance des êtres vivants [biométrie fœtale, biométrie oculaire] (→ **biométrie** [MEDECINE]) [9].

1.3. Définition

La **biométrie** est la science qui porte sur l'analyse des caractéristiques physiques ou comportementales propres à chaque individu et permettant l'authentification de son identité.
Au sens littéral et de manière plus simplifiée, la biométrie signifie la "mesure du corps humain".
On distingue deux catégories de technologies biométriques : les mesures physiologiques, et les mesures comportementales.

Les **mesures physiologiques** peuvent être morphologiques ou biologiques.
Ce sont surtout les empreintes digitales, la forme de la main, du doigt, le réseau veineux, l'œil (Iris et rétine), ou encore la forme du visage, pour les analyses morphologiques [10].

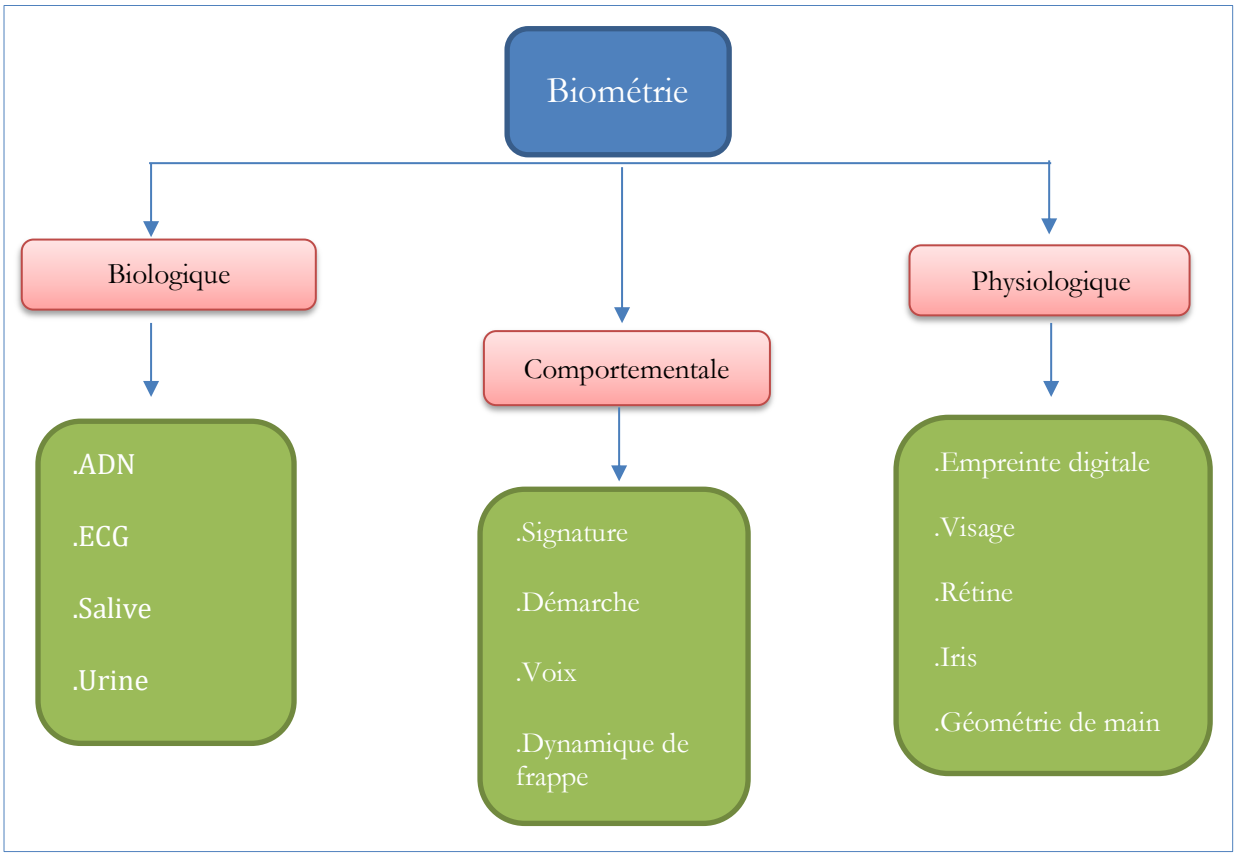

Figure 1-1 Principales modalités biométriques.

1.4. Exigence relative aux caractéristiques biométriques :

En théorie, la plupart des traits physiologiques ou comportementaux humains peuvent être utilisés en tant que modalités biométriques. Toutefois, pour tenir dans un système biométrique,

potentiellement précis, pratique et rentable, le trait/caractéristique utilisé doit également satisfaire à une série d'exigences proposées dans :

- L'universalité : toute personne doit posséder le trait biométrique,
- L'unicité : une probabilité quasi nulle que deux personnes soient les mêmes selon le trait caractéristique biométrique,
- La permanence : la stabilité du trait biométrique dans le temps,
- La mesurabilité : la quantification du trait biométrique d'une manière pratique,
- La performance : la précision et la vitesse de la reconnaissance à travers la caractéristique biométrique,
- L'acceptabilité : l'accord du public pour la mesure de la caractéristique,
- La non-circonvention : le degré de facilité ou difficulté avec laquelle le système peut être trompé en falsifiant la caractéristique biométrique [11].

Tableau 1-1 Comparaison de modalités biométriques.

Modalité	Acquisition	Unicité	Permanent	Acceptabilité	Performance
Visage	**Facile**	**Faible**	**Moyen**	**Fort**	**Faible**
Digitale	**Moyen**	**Forte**	**Forte**	**Moyen**	**Forte**
Rétine	**Difficile**	**Forte**	**Moyen**	**Faible**	**Forte**
Signature	**Facile**	**Faible**	**Faible**	**Forte**	**Faible**
Vocale	**Moyen**	**Faible**	**Faible**	**Forte**	**Faible**

1.5. Systèmes biométriques et modes de fonctionnements :

Un système biométrique est essentiellement un système qui acquiert des données biométriques d'un individu, extrait un ensemble de caractéristiques à partir de ces données, puis le compare à un ensemble de données stocké au préalable dans une base de données pour pouvoir enfin exécuter une action ou prendre une décision à partir du résultat de cette comparaison.

Par conséquent, un système biométrique est composé de quatre modules principaux :

1.5.1. Le module de capture :

Il est responsable de l'acquisition de la donnée biométrique.

Un lecteur, un scanner ou autres module de balayage approprié est requis pour l'acquisition des données biométriques brutes d'un individu.

1.5.2. Le module d'évaluation de qualité et d'extraction de caractéristiques :

La qualité des données biométriques obtenues lors de la capture doit être évaluée par ce module afin de déterminer sa convenance pour le processus de reconnaissance. Généralement, les données acquises doivent être soumises à des algorithmes de perfectionnement afin d'améliorer la qualité du signal. Ce module exige, parfois, la recapture des données avant de les traiter s'il s'avère que la qualité des données déjà capturées est inacceptable. Les données biométriques sont alors traitées d'une manière à extraire les traits fondamentaux et les caractéristiques qui permettront d'obtenir la signature biométrique de l'individu.

1.5.3. Le module de correspondance (Matching) :

Compare l'ensemble des caractéristiques extraites avec le modèle enregistré dans la base de données du système et détermine le degré de similitude (ou de divergence) entre les deux [5].

1.5.4. Le module de décision :

Le résultat de cette comparaison va être utilisé pour prendre une décision sur le taux de correspondance de la signature biométrique pour la validation ou le rejet de l'identité de l'individu à reconnaitre [12].

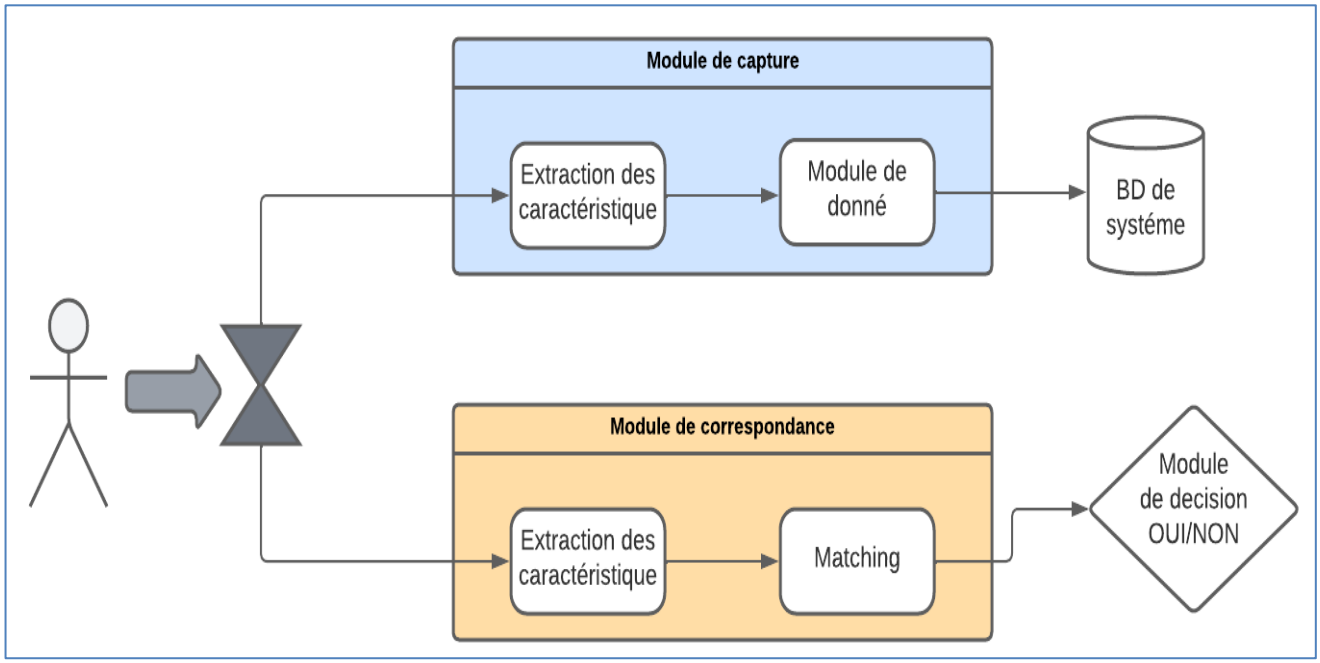

Figure 1-2 Architecture d'un système biométrique.

1.6. Les différentes modalités :

1.6.1. L'empreinte digitale :

Est une branche de la biométrie, une science qui permet d'identifier les personnes au moyen de leurs caractéristiques physiques ou biologiques [13].

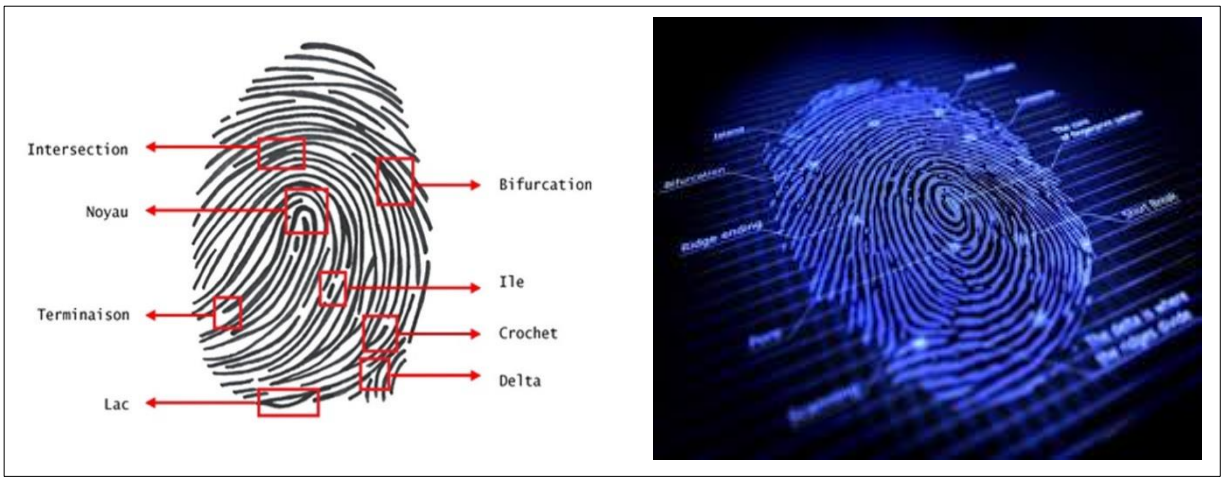

Figure 1-3 L'empreinte digitale.

1.6.2. Visage :

Il s'agit d'une méthode d'identification biométrique qui utilise les mesures corporelles dans ce cas, le visage et la tête, afin de vérifier l'identité d'une personne grâce à sa disposition et ses données biométriques faciales [14].

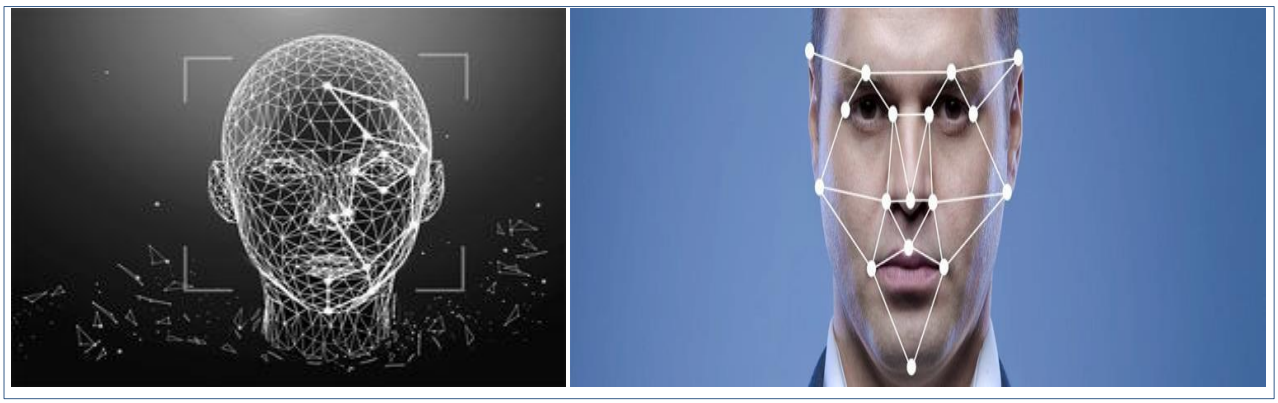

Figure 1-4 Le visage.

1.6.3. La rétine :

La rétine est la couche sensorielle de l'œil qui permet la vision, cette zone est parcourue par des vaisseaux sanguins dont leurs positions sont inchangeables durant toute la vie de la personne.

L'identification de la rétine n'est pas récente, elle remonte aux années 30. Cette technique est la plus

fiable toutefois elle est mal acceptée par les utilisateurs à cause des contraintes de l'acquisition [15].

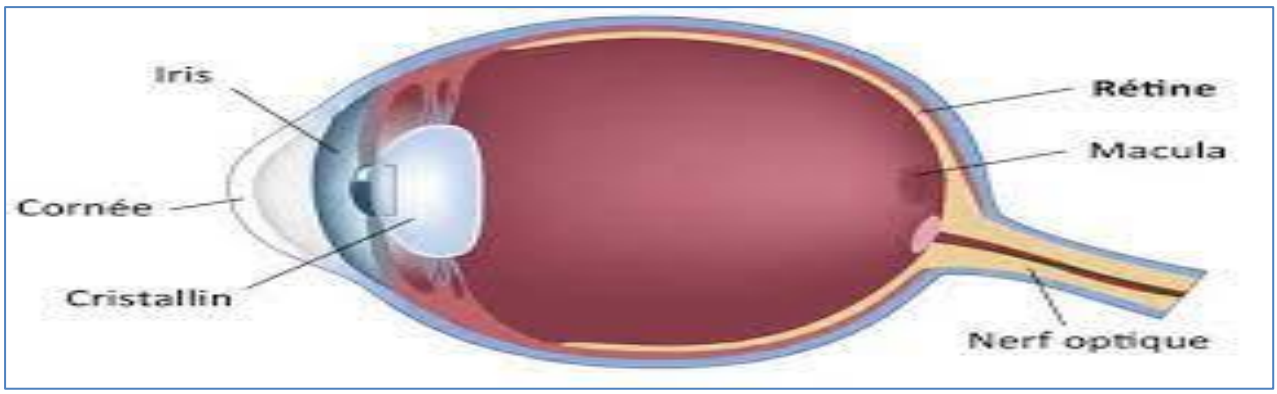

Figure 1-5 L'image de la rétine.

1.6.4. La géométrie de la main :

Est une donnée biométrique qui permet d'identifier les utilisateurs grâce au contour de leurs mains. Les lecteurs de géométrie de la main permettent de prélever plusieurs mesures qui sont comparées aux mesures stockées dans un fichier [16].

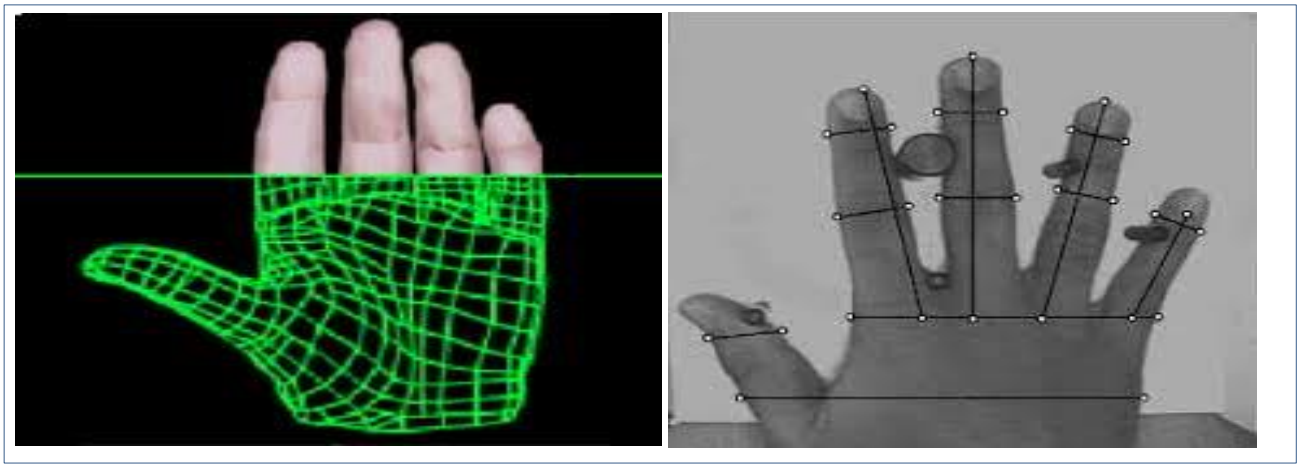

Figure 1-6 La géométrie de la main

1.6.5. La voix :

La biométrie vocale est un domaine scientifique et technologique de la reconnaissance vocale et visé à développer des applications permettant de vérifier l'identité d'une personne uniquement par sa voix [17].

Figure 1-7 La voix.

1.7. Les avantages et les inconvénients des techniques biométriques :

Tableau 1-2 Les avantages et les inconvénients des techniques biométriques.

Modalité	Avantages	Inconvénients
Empreintes digitales	**-La technique la plus éprouvée techniquement est la plus connue du grand public. -Petite taille du lecteur facilitant son intégration dans la majorité des applications (téléphones portables, PC). -Faible coût des lecteurs grâce aux nouveaux capteurs. -Traitement rapide**	**-Besoin de la coopération de l'utilisateur (pose correcte du doigt sur le lecteur). -Certains systèmes peuvent accepter un moulage de doigt ou un doigt coupé (la détection du doigt vivant permet d'éviter ce type d'usurpation).**
La rétine	**-L'empreinte rétinienne est peu exposée aux blessures (coupure, brûlure). -Les taux de faux rejet et de fausse acceptation sont faibles. -Très difficile, voire impossible, à imiter. -La rétine est différente chez les vrais jumeaux. -La rétine est stable durant la**	**-Système intrusif, il faut placer l'œil près du capteur. -Mauvaise acceptation du public (l'œil est un organe sensible). -Coût plus important que d'autres technologies. -Pas adapté pour un flux de passage important.**

	vie d'un individu	

La voix	**-Il est plus facile de protéger le lecteur que dans les autres techniques. Seule information utilisable via le téléphone. -Impossible d'imiter la voix. -Pas intrusif.**	**-Sensible à l'état physique et émotionnel de l'individu. -Fraude possible par enregistrement. -Sensible aux bruits ambiants. -Taux de faux rejet est fausse acceptation élevée.**
La géométrie de la main	**-Bonne acceptation des usagers. -Très simple à utiliser. -Le résultat est indépendant de l'humidité et de l'état de propreté des doigts. -Fichier "gabarit" de petite**	**-Trop encombrant pour un usage sur le bureau, dans une voiture ou un téléphone. -Risque de fausse acceptation pour des jumeaux ou des membres.**
Le visage	**-Très bien accepté par le public. -Ne demande aucune action de l'usager (peu intrusive), pas de contact physique. -Technique peu coûteuse.**	**-Technologie sensible à l'environnement (éclairage, position, expression du visage...). -Les vrais jumeaux ne sont pas différenciés. -Sensible aux changements**

L'iris	**-L'iris n'est pas modifiable même par Intervention chirurgicale. -Les iris sont uniques et différent même pour les vrais jumeaux. -Grande quantité d'informations contenues dans l'iris**	**-Acceptabilité très faible, contrainte d'éclairage.**

La signature	**-La signature écrite sur un document peut être conservée des certains documents**	**-Besoin d'une tablette graphique. -Sensible aux émotions de l'individu.**

1.8. Mesure de la performance d'un système biométrique :

Tout d'abord, afin de comprendre comment déterminer la performance d'un système biométrique, il nous faut définir clairement trois critères principaux :
le premier critère s'appelle le taux de faux rejet : la probabilité qu'un utilisateur connu soit rejeté par le système biométrique. Ce taux définit en partie le confort d'utilisation du système biométrique. Concerne la probabilité qu'un utilisateur connu soit rejeté (le pourcentage de faux de rejet d'un utilisateur légitime)**.** Sa formule est donnée comme suite :

$$\text{FRR} = \frac{nb\ de\ FR}{nb\ de\ clients}$$

Le deuxième critère est le taux de fausse acceptation ("False Accept Rate" ou FAR) : C'est la probabilité qu'un utilisateur inconnu soit identifié comme étant un utilisateur connu. Ce taux définit la sécurité du système biométrique. C'est la probabilité qu'un utilisateur non reconnu mais qui est accepté par le système (le pourcentage d'acceptation d'un imposteur). Le calcule de ce taux est comme suite :

$$\text{FAR} = \frac{nb\ de\ FA}{nb\ imposteurs}$$

Le troisième critère est connu sous le nom de taux d'égale 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 [18].

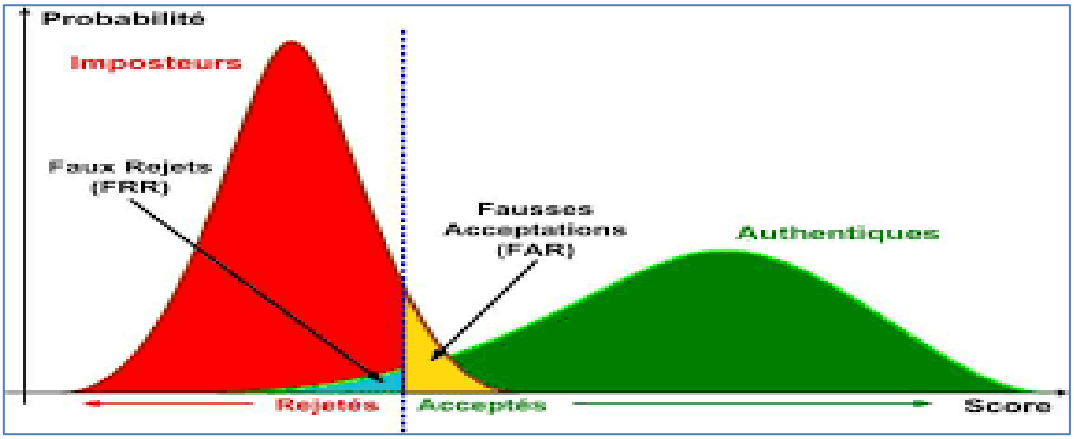

Figure 1-8 Illustration du FRR et du FAR.

Il existe deux manières de présenter les performances d'un système biométrique soit du type authentification ou identification :

– Pour le type authentification, la courbe la plus couramment utilisée est appelée La courbe ROC (Receiver Operating Characteristic) la courbe ROC (FIGURE. 1.7) Permets de représenter graphiquement la performance d'un système de vérification pour les différentes valeurs de θ. Le taux d'erreur égal (Equal Error Rate ou EER) correspond au point FAR =FRR, c'est-à-dire graphiquement à l'intersection de la courbe ROC avec la première bissectrice. Il est fréquemment utilisé pour donner un aperçu de la performance d'un système. Cependant, il est important de souligner que l'EER ne résume en aucun cas toutes les caractéristiques d'un système biométrique. Leseuil θ doit donc être ajustée en fonction de l'application ciblée : haute sécurité, basse sécurité ou compromis entre les deux [8].

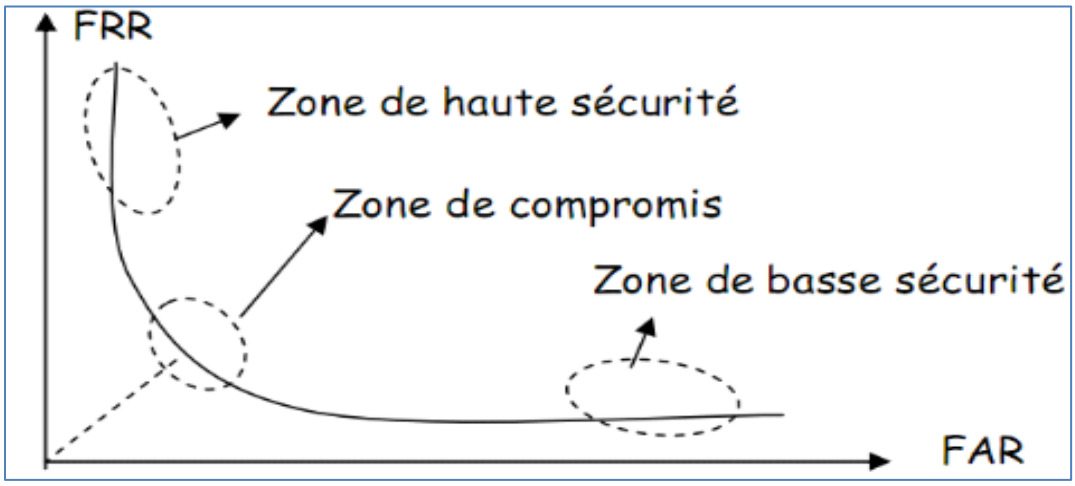

Figure 1-9 Courbe ROC

– Pour le type identification, la courbe la plus utilisée est appelée courbe CMC (Cumulative Match Characteristic) la courbe (FIGURE. 1.9) est une courbe qui représente la performance d'un système d'identification biométrique. Cette courbe mesure le pourcentage de personnes dont le modèle

biométrique est correctement identifié à un niveau donné de faux positifs. Elle est généralement utilisée pour comparer les performances de différents systèmes biométriques et mesurer leur précision. Elle est composée de points connectés qui représentent le taux de reconnaissance correcte en fonction du taux de faux positifs. Plus le taux de reconnaissance correcte est élevé et plus la courbe est proche de la ligne du haut, qui représente un taux de reconnaissance correcte de 100% [16].

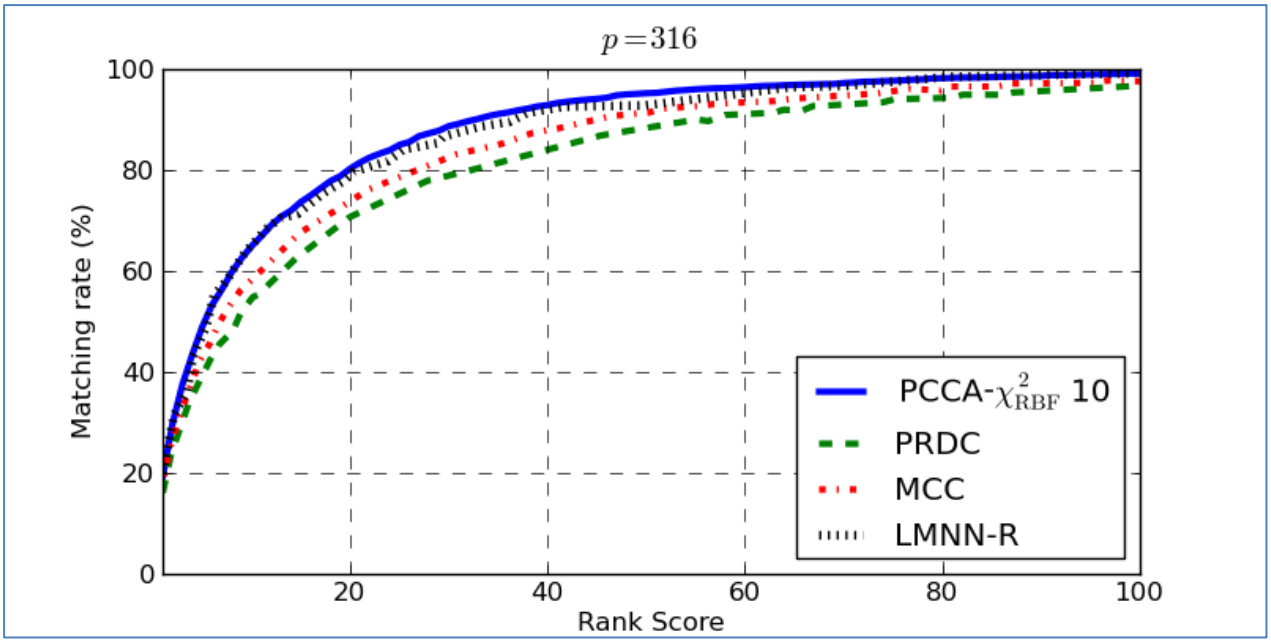

Figure 1-10 courbe CMC en fonction de r, pour PCCA et deux autre.

1.9. Comparaison des systèmes biométriques :

Une question qui se pose souvent dans ce domaine est la suivante : « Quelle est la meilleure technique biométrique ? »

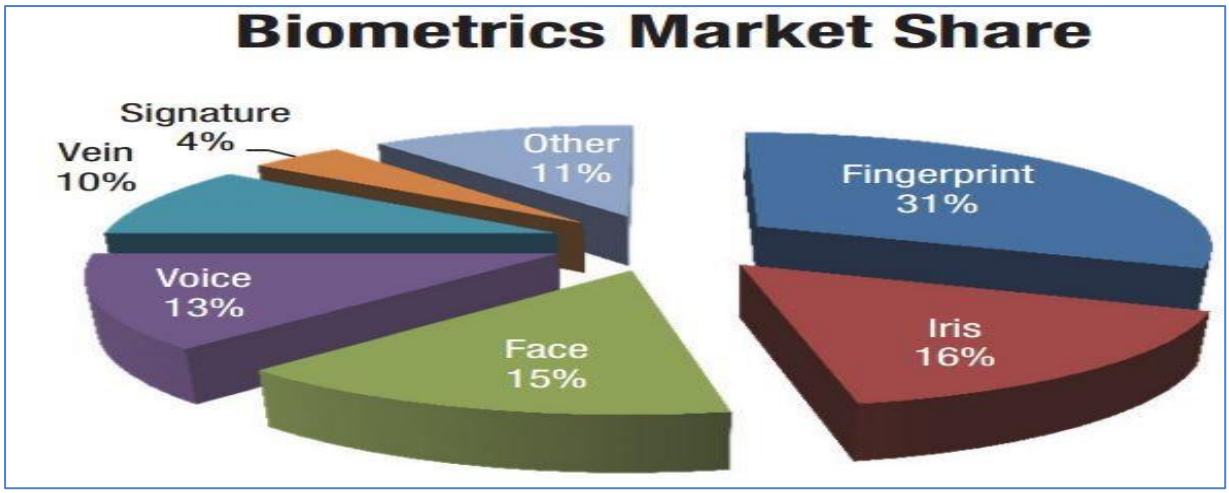

Figure 1-11 marché biométrique par type de système.

La comparaison des méthodes d'identification biométriques dans (tableau 1.3) en matière de fiabilité,

d'utilisation et de mesurabilité montre que chaque méthode a ses propres avantages et inconvénients. La reconnaissance faciale, par exemple, est une méthode très fiable et mesurable, mais elle peut être difficile à utiliser dans les environnements publics en raison des préoccupations liées à la vie privée. La reconnaissance vocale est une méthode facile à utiliser et mesurable, mais elle n'est pas aussi fiable que d'autres méthodes. La reconnaissance d'empreintes digitales est une méthode très fiable et facile à utiliser, mais elle peut ne pas être aussi mesurable que d'autres méthodes. La reconnaissance d'iris est très fiable et mesurable, mais elle peut être plus difficile à utiliser que d'autres méthodes.

La méthode d'identification par la rétine est considérée comme l'une des méthodes les plus fiables pour l'identification. Elle offre une mesurabilité exceptionnelle et une utilisation pratique et robuste. Cela en fait une excellente option pour les applications d'authentification et de vérification à haute sécurité. De plus, cette méthode présente un niveau de sécurité très élevé, ce qui en fait une solution très fiable et fiable pour l'identification.

La main géométrique est une méthode très fiable et facile à utiliser pour mesurer des objets. Il offre également une grande précision et une grande mesurabilité, ce qui en fait l'une des méthodes les plus précises et fiables disponibles. De plus, il est très facile à apprendre et à utiliser, ce qui en fait un choix populaire pour les professionnels et les étudiants. Enfin, le coût peu élevé et la facilité d'utilisation en font une méthode très avantageuse pour les utilisateurs

Enfin, la biométrie par signe vital est très fiable et mesurable, mais elle peut être difficile à utiliser et peut ne pas être aussi fiable que d'autres méthodes.

En conclusion, il est important de prendre en compte la fiabilité, l'utilisation et la mesurabilité de chaque méthode d'identification biométrique lors de la sélection d'une méthode appropriée pour un projet particulier [19].

Tableau 1-3 Comparaison entre quelques méthodes d'identification biométriques.

Méthode	Utilisation %	Nombre de points mesurables	Fiabilité
Empreintes digitales	**50**	**(80)**	**Assez bonne**
Reconnaissance faciale	**6**	**Selon la photo**	**Bonne**
Reconnaissance de la main	**10**	**(90)**	**Bonne**
Iris	**Peu utilisé**	**(244)**	**Proche de 99%**
Signature	**<5**	**Selon la signature**	**Variable**
Voix	**15**	**Dépends des bruits de fond**	**Peu fiable**
Rétine	**Rare**	**400**	**Excellente**

1.10. Conclusion :

Dans ce chapitre nous avons appris les généralités de la biométrie, et que les systèmes biométriques utilisent des différents traits biométriques pour améliorer la performance, Elle compare les données biométriques reçues par un ensemble de données stockées et puis pris la décision.

Alors en conclusion, on est d'accord que la biométrie a un rôle majeur dans l'amélioration des performances des systèmes d'identification.

Chapitre 02

L'ETAT DE L'ART DE LA FUSION AUX NIVEAUX DES CARACTERISTIQUES

2.1. Introduction

La biométrie est un domaine de recherche en constante évolution qui utilise les caractéristiques biologiques ou comportementales des individus pour les identifier ou les authentifier. La fusion biométrique consiste à combiner les informations provenant de plusieurs sources biométriques pour améliorer la précision et la fiabilité de la reconnaissance biométrique. Cette technique est utilisée pour augmenter la sécurité et l'efficacité des systèmes de reconnaissance biométriques. Les caractéristiques de fusion biométrique sont importantes pour déterminer la performance de ces systèmes [20].

Ce chapitre se concentre sur l'état de l'art de la fusion et des niveaux de fusion pour la reconnaissance d'empreinte palmaire et d'empreinte de l'articulation du doigt (FKP). Nous commencerons par une revue des travaux existant sur la fusion biométrique, en mettant l'accent sur les méthodes et les approches les plus couramment utilisées.

Nous discuterons ensuite des différents niveaux de fusion, qui représentent les étapes de la fusion des caractéristiques biométriques. Ces niveaux peuvent inclure la fusion au niveau des caractéristiques, des scores ou des décisions. Nous examinerons en détail les avantages et les inconvénients de chaque niveau de fusion, ainsi que les techniques mathématiques et statistiques utilisées pour combiner les informations biométriques [21].

L'objectif de ce chapitre est de fournir une vue d'ensemble complète de l'état de l'art de la fusion et des niveaux de fusion pour la reconnaissance d'empreinte palmaire et d'empreinte de l'articulation du doigt (FKP). Cette synthèse des connaissances existantes permettra de mieux comprendre les défis et les opportunités dans ce domaine, et de poser les bases pour les travaux de recherche futurs visant à améliorer la performance des systèmes biométriques utilisant ces modalités.

2.2. Etat de l'art de la fusion :

Ahmad et al. (AHMAD et al., 2014) ont proposé la fusion d'informations de la biométrie du visage et de l'empreinte palmaire au niveau de caractéristique. L'utilisation des méthodes PCA et LDA

réduit considérablement la dimension du vecteur de caractéristiques en supprimant les données de redondance et de bruit tout en augmentant la puissance discriminante dans l'espace des caractéristiques fusionnées. Dans cet article (BHARADI, PANDYA et NEMADE, 2014), un système biométrique multimodal basé sur l'iris et les empreintes digitales est proposé. L'extraction d'éléments de texture à l'aide d'ondelettes hybrides sont effectuée. Les caractéristiques des empreintes digitales et de l'iris sont extraites à l'aide de la décomposition à plusieurs niveaux de l'image échantillon capturée à l'aide d'une nouvelle famille d'ondelettes appelée hybride. Dans cet article, le classificateur KNN est utilisé pour la reconnaissance unimodale des empreintes digitales et la reconnaissance multi-instance de l'iris. Les vecteurs caractéristiques de l'iris et de l'empreinte digitale sont combinés à l'aide de la technique de fusion décisionnelle. L'analyse FAR-FRR est effectuée et les résultats suggèrent que les ondelettes hybrides ont une bonne capacité d'extraction des caractéristiques de texture et que le système proposé a obtenu une ration de classification correcte pouvant atteindre 77% [22].

Kim et al. (KIM, MIN SONG et RYOUNG PARK, 2018) ont présenté un système biométrie multimodale qui combine veine de doigt et forme de doigt utilisant un capteur de caméra infrarouge proche sur la base d'un réseau de neurones à convolution profond. Les distances correspondantes calculées en fonction des caractéristiques de la veine et de la forme des doigts obtenues à l'aide de modèles ResNet ont été fusionnées à l'aide de diverses méthodes de fusion, telles que la somme du poids, le produit pondéré et le perceptron. Soleymani et al. (SOLEYMANI et al., 2018) ont proposé une architecture CNN commune avec fusion au niveau de caractéristiques pour la reconnaissance multimodale utilisant de multiples modalités de visage, d'iris et d'empreintes digitales. Plutôt que de fusionner les réseaux au niveau de la couche softmax, les caractéristiques de compression optimale de toutes les modalités sont fusionnées aux couches entièrement connectées sans perte de précision des performances, mais avec une réduction significative du nombre de paramètres réseau [22].

2.2.1. Reconnaissance par empreinte palmaire :

Le système d'empreintes palmaires est une technique biométrique manuelle. L'empreinte palmaire a concerné la surface interne d'une main. Un palmier est recouvert du même type de peau que le bout des doigts et il est plus grand qu'un bout de doigt. Beaucoup les caractéristiques d'une empreinte palmaire peuvent être utilisées pour identifier de manière unique une personne, y comprises [22], Les empruntes palmaires contiennent plus informations que les empreintes digitales, elles sont donc plus distinctives. Capture d'empreintes palmaires les appareils sont beaucoup moins chers que les appareils à Iris. Les empreintes palmaires contiennent des caractéristiques distinctives supplémentaires telles que les rides et ridules principales, qui peuvent être extraites à partir d'images en basse résolution. En

combinant toutes les caractéristiques des palmiers [22].

2.2.1.1. Caractéristique des empreintes palmaires :

L'empreinte palmaire est une surface très large et interne dans la main, elle contient plusieurs traits de caractéristiques qui peuvent être exploités dans la reconnaissance des individus. Grace à cette large surface et la richesse des traits de caractéristiques, nous prévoyons que les empreintes palmaires sont très robustes aux bruits et uniques pour chaque individu. En comparaison aux autres caractéristiques physiques, l'identification par les empreintes palmaires a plusieurs avantages [23].

a. Caractéristique géométrique :

Comme toute image, l'empreinte palmaire présente des caractéristiques géométriques telles que : la longueur, la largeur, et la surface. Ses caractéristiques ne sont pas distinctives mais peuvent tout de même être utiles pour une première vérification.

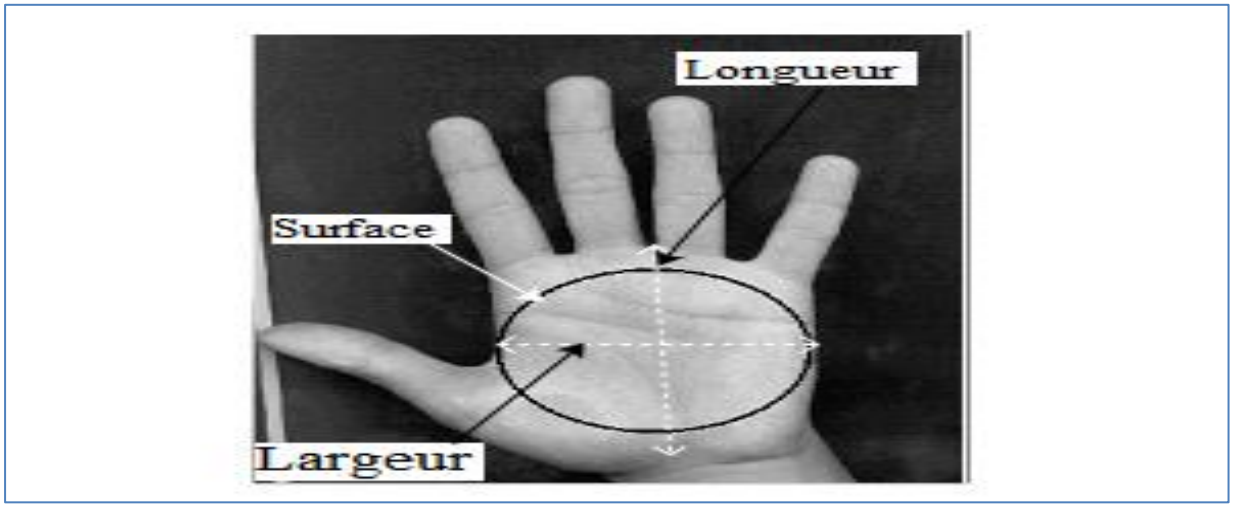

Figure 2-1 caractéristique géométrie de palmaire

b. Les lignes principales :

Les lignes principales sont les lignes courbes qui partent du poignet et se ramifient à travers la paume. Elles sont également appelées les "lignes de vie". Les lignes principales représentent les flux d'énergie dans la main et sont considérées comme les principales caractéristiques de l'empreinte palmaire.
Les lignes secondaires sont les lignes qui traversent la paume, perpendiculairement aux lignes principales. Elles sont également appelées les "lignes de tête", les "lignes de cœur" et les "lignes de destinée". Les lignes secondaires sont créées par la tension musculaire de la main et représentent la personnalité, la santé et le destin de la personne.

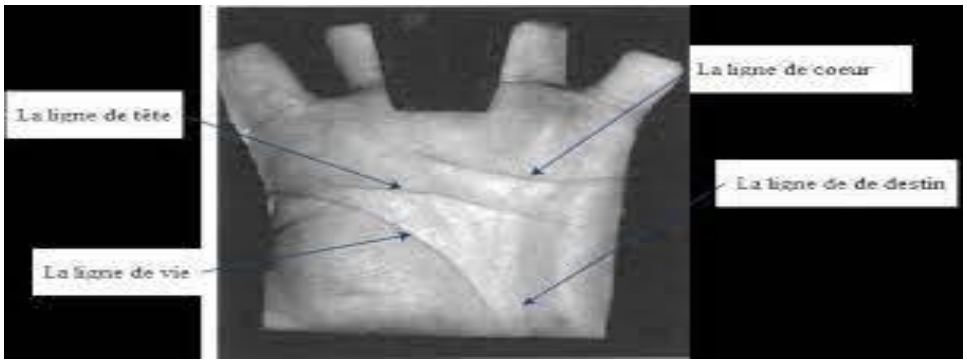

Figure 2-2 Les lignes principales et les lignes secondaires.

c. Les rides :

Les rides sont les marques qui se trouvent entre les lignes principales et les lignes secondaires. Les rides sont créées par l'utilisation régulière de la main et peuvent être utilisées pour identifier la personne en analysant leur position, leur profondeur et leur disposition.

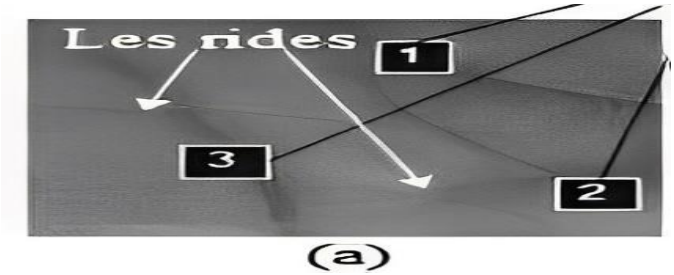

Figure 2-3 exemple des rides d'empreinte palmaire.

d. Les points de référence (Datum points) :

Les points représentant les deux extrémités de la paume de la main sont appelés Point de références. Ce sont les points à et b dans (la Figure 4) [24].

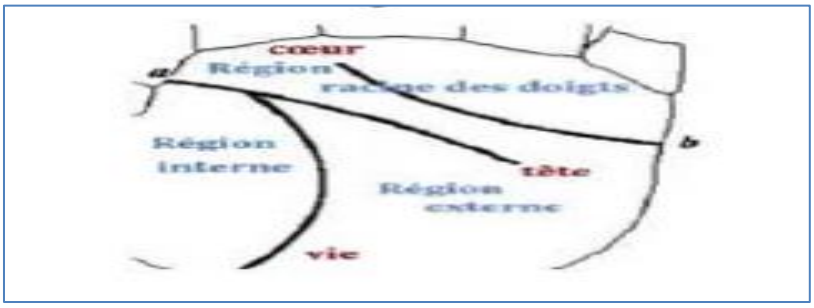

Figure 2-4 Points de référence de l'empreinte palmaire (a et b).

2.2.2. Système de reconnaissance FKP :

La FKP est une modalité récente qui se base sur l'extraction de la texture de la surface arrière du doigt. Ces inhérentes caractéristiques de la peau qui se trouvent autour de l'articulation phalangienne

sont bien distinctives entre les individus. C'est une technique biométrique basée sur la surface arrière du doigt, elle contient des caractéristiques distinctives telles que les lignes principales, les lignes secondaires et les crêtes, qui peuvent être extraites à partir des images à basse résolution.

La main contient plusieurs doigts, pour cela, il faut conserver les informations à chaque doigt pour une reconnaissance précise dans le domaine d'identification :

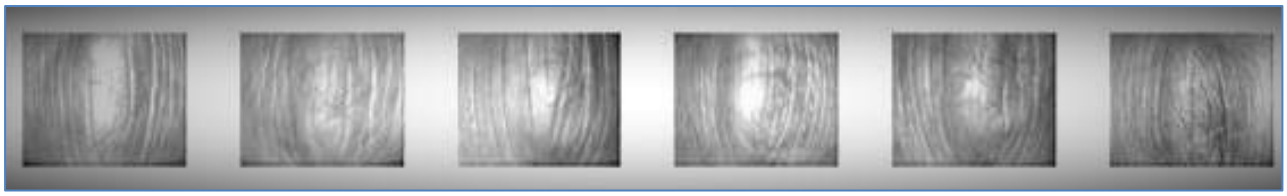

Figure 2-5 Exemple des images FKP de la base donné FKP data.

Cependant, la main contient plusieurs doigts, pour cela, plusieurs travaux montrent que l'empreinte de l'articulation du doigt (FKP) peut être utilisée dans le domaine d'identification des personnes pour une reconnaissance robuste et précise, si on utilise la combinaison ou la fusion de l'information prise de chaque doigt [15].

2.2.3. La fusion :

provenant de différentes sources ou modalités afin d'obtenir une image plus complète et plus précise la fusion est une technique de traitement de données qui consiste à combiner des informations, En fonction des sous-systèmes retenus dans le scénario, il est possible d'effectuer une fusion des données à différents niveaux de l'architecture du système de multi biométrie [25].

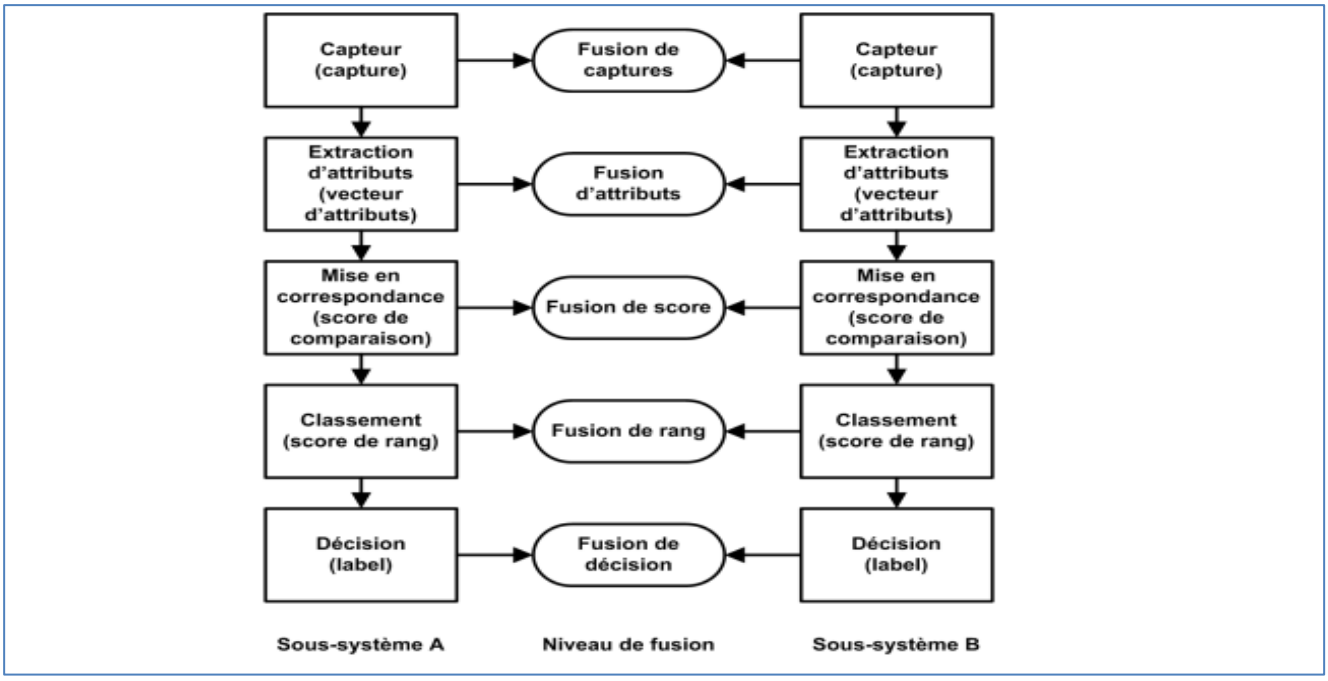

Figure 2-6 Liste des différents niveaux de fusion.

2.2.4. Etapes de l'opération de fusion :

Alignement : l'alignement ou conditionnement ou encore parfois, harmonisation, consiste à définir un espace commun, dans lequel les informations vont être projetées afin d'y être comparables. Cela veut dire que les observations ou les données sont ramenées dans un même référentiel.

Corrélation : cette étape concerne la détermination des relations entre les différentes données.

Association ou mise en correspondance : l'association est l'union des différentes représentations issues des informations multisources. Chaque mesure se trouve associée à l'entité correspondante (Le résultat de l'étape de corrélation est évidemment utilisé). Cette étape permet aussi de rejeter les données aberrantes suivant un critère sur la matrice de covariance par exemple.

Combinaison : seules les données obtenues après alignement et qui sont en accord avec l'étape d'association sont combinées pour obtenir une meilleure représentation de l'estimation correspondant à l'attribut avec lequel l'étape d'alignement a été réalisée [1].

Décision : c'est la dernière étape qui consiste à prendre une décision optimale sur un évènement donné en utilisant les règles dédiées, toujours selon la théorie appliquée [12].

2.2.5. Les niveaux de fusion :

Un système de fusion est généralement composé de sources d'information, de moyens d'acquisition d'information, de moyens de communication et de capacités à traiter l'information. Il peut être par conséquent très complexe. Il est fréquent et pratique, lors de l'étude ou de la présentation d'un système, de séparer les aspects topologiques et les aspects traitement d'informations, même s'il existe des interconnexions. La topologie a une influence importante sur le choix de l'architecture du système de fusion, sur les choix d'outils, des méthodes de traitement et de communication. On peut trouver dans la littérature plusieurs manières de classer les différentes étapes ou types de fusion. Cette différence provient principalement du niveau où l'opération de fusion est accomplie, de l'objectif de cette opération, du type de sources (ou capteurs) et de l'application considérée. 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 [26].

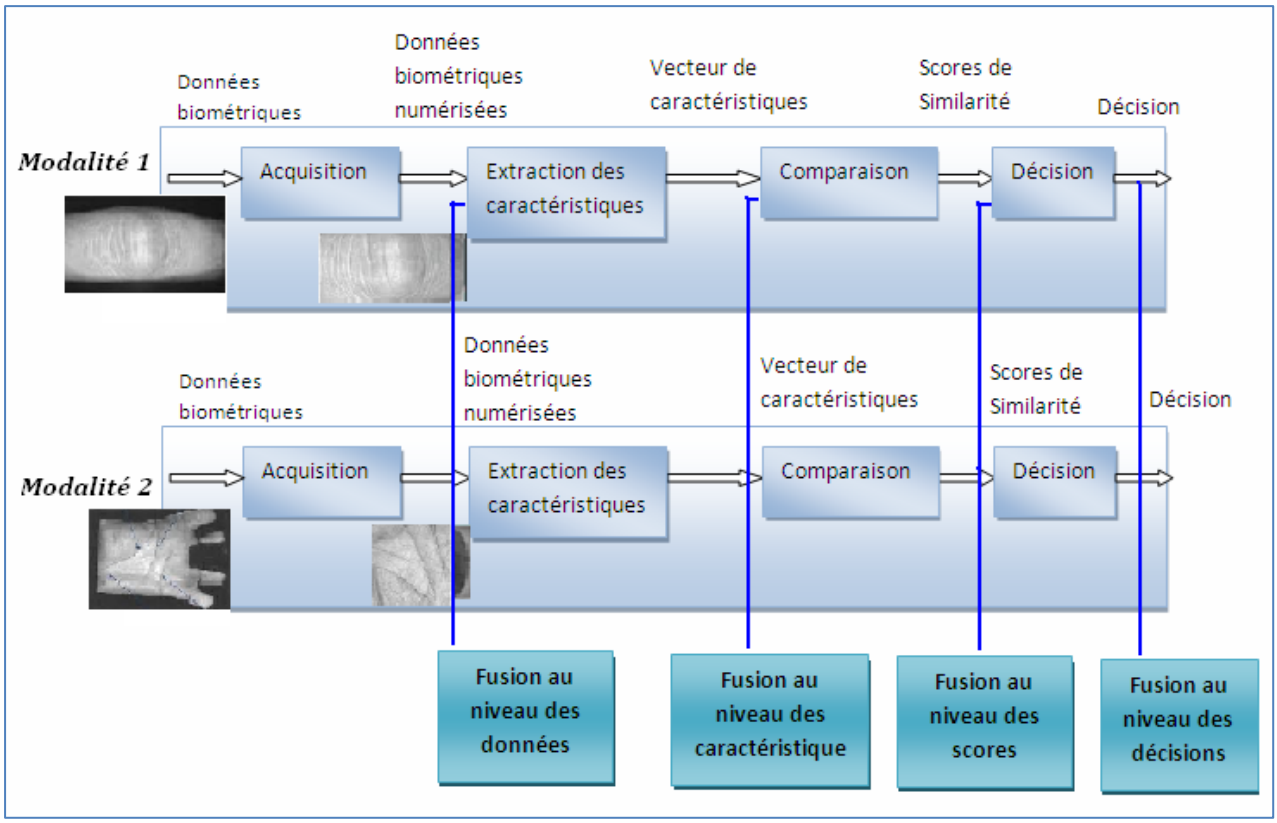

Figure 2-7 les déférent niveaux de fusion.

Ces niveaux de fusion que l'on peut répartir en deux grandes familles, la fusion avant la correspondance ("matching") et la fusion après la correspondance.

2.2.5.1. Avant le Matching:

a. Niveau Caractéristiques (Feature Level):

Niveau Caractéristique (Feature Level) La fusion aux niveaux caractéristiques consiste à combiner différents vecteurs de caractéristiques ("feature vectors") qui sont obtenus à partir d'une des sources suivantes : plusieurs capteurs du même trait biométrique, plusieurs instances du même trait biométrique, plusieurs unités du même trait biométrique ou encore plusieurs traits biométriques.

Quand les vecteurs de caractéristiques sont homogènes (par exemple, plusieurs images d'empreinte digitale du doigt d'un utilisateur), un unique vecteur de caractéristiques résultant peut-être calculé comme une somme pondérée des vecteurs de caractéristiques individuels [20].

b. Niveau Capteur (Sensor Level):

La fusion au niveau du capteur est le premier niveau de fusion. Le but de cette fusion est de générer une nouvelle capture, de meilleure qualité que les captures sources, pour être traité avant l'extraction des caractéristiques. Cette technique s'appelle la fusion d'images ou fusion de pixels dans la zone de

traitement d'images. Une telle fusion est relativement rare utilisée car il nécessite des données homogènes. La fusion au niveau du capteur est applicable uniquement si les sources multiples représentent des échantillons du même trait biométriques obtenus à l'aide d'un capteur unique ou des capteurs compatibles différents [22].

2.2.5.2. Aprés le Matching:

a. Niveau Décision (Decision Level):

Les sorties finales du multiple les classificateurs sont combinées. Un système de vote à la majorité peut être utilisé pour prendre la décision finale. La fusion au niveau de la décision inclut des niveaux d'information de sorte qu'ils sont moins préférés dans la conception systèmes biométriques multimodaux. Il s'agit de combiner les décisions des systèmes biométriques qui donnent chacune une réponse (accepté : 1 ou rejeté : 0, dans le cas de la vérification) selon l'entrée qui leur est présentée. Ce niveau de fusion peut s'opérer par des règles simples telles que l'ET, l'OU et le vote à la majorité, ainsi que par des règles plus complexes par vote pondéré ou par classification dans l'espace des décisions . La fusion au niveau des décisions a l'avantage d'être simple. Par contre, l'information dont elle fait usage est très limitée (0 ou 1) [27].

b. Niveau Score (Score Level) :

La grande majorité des systèmes audiovisuels de vérification du locuteur est basée sur la fusion des scores de deux systèmes de vérification du locuteur : l'un basé sur le signal acoustique seul, et l'autre basé sur le seul signal visuel. Nous n'entrerons pas dans les détails du premier. Des modèles de Markov cachés (HMM, pour Hidden Markov Model) dépendant du locuteur sont entraînés à l'aide de paramètres liés à la forme des lèvres dans, à l'aide de paramètres du type eigenlips (zone de la bouche transformée par analyse en composantes principales) dans et des coefficients DCT (transformée en cosinus discrèt) de la zone de la bouche dans. Dans les auteurs concluent cependant que l'utilisation de modèles de mélange de gaussiennes serait suffisante puisque les meilleures performances sont obtenues avec des HMM à un seul état. Tous ces travaux tirent la même conclusion selon laquelle la fusion des deux scores monomodaux (acoustiques et visuels) est un moyen simple et efficace d'améliorer les performances globales de la vérification d'identité, et tout particulièrement en milieu bruité [28].

2.2.6. La fusion au niveau de caractéristique :

La fusion au niveau caractéristique est très utile à la classification. Ce niveau de fusion concerne la combinaison d'informations extraites après diverses phases de traitement et d'analyse des mesures.

Différents vecteurs de caractéristiques, issues de plusieurs capteurs ou obtenus à l'aide de différents algorithmes d'extraction sont combinés [26], Les informations sont extraites à l'aide d'extracteurs de caractéristiques des capteurs, puis selon le type de modalité, il est ensuite stocké en vecteurs. Pour former une base pour l'étape suivante du processus, un vecteur de caractéristiques communs est créé en combinant tous les vecteurs de caractéristiques individuelles. Les ensembles de fonctionnalités sont obtenus par appliquer des algorithmes biométriques, pour obtenir un ensemble de fonctionnalités uniques à partir de nombreux ensembles, la réduction, la normalisation et la transformation sont appliquées. Pour mapper l'ensemble de fonctionnalités dans un l'emplacement du domaine et léchelle de l'ensemble de fonctionnalités sont modifiées, cela peut être fait en utilisant des techniques telles que Min-Max ou normalisation médiane. Pour réduire les dimensions d'un ensemble de fonctionnalités, des techniques de transformation comme Forward sélection séquentielle, PCA ou retour séquentiel la sélection est utilisée15. La fusion au niveau des caractéristiques fait une référence à la combinaison de divers vecteurs de caractéristiques qui peuvent être calculées soit par l'emploi de plusieurs algorithmes pour extraction de fonctionnalités ou utilisation de plusieurs capteurs sur mêmes données collectées par les capteurs16. Un seul vecteur de caractéristiques résultantes pourrait être calculé comme une moyenne des poids de tous les vecteurs de caractéristiques individuellement en cas de vecteurs de caractéristiques utilisées est homogène [29].

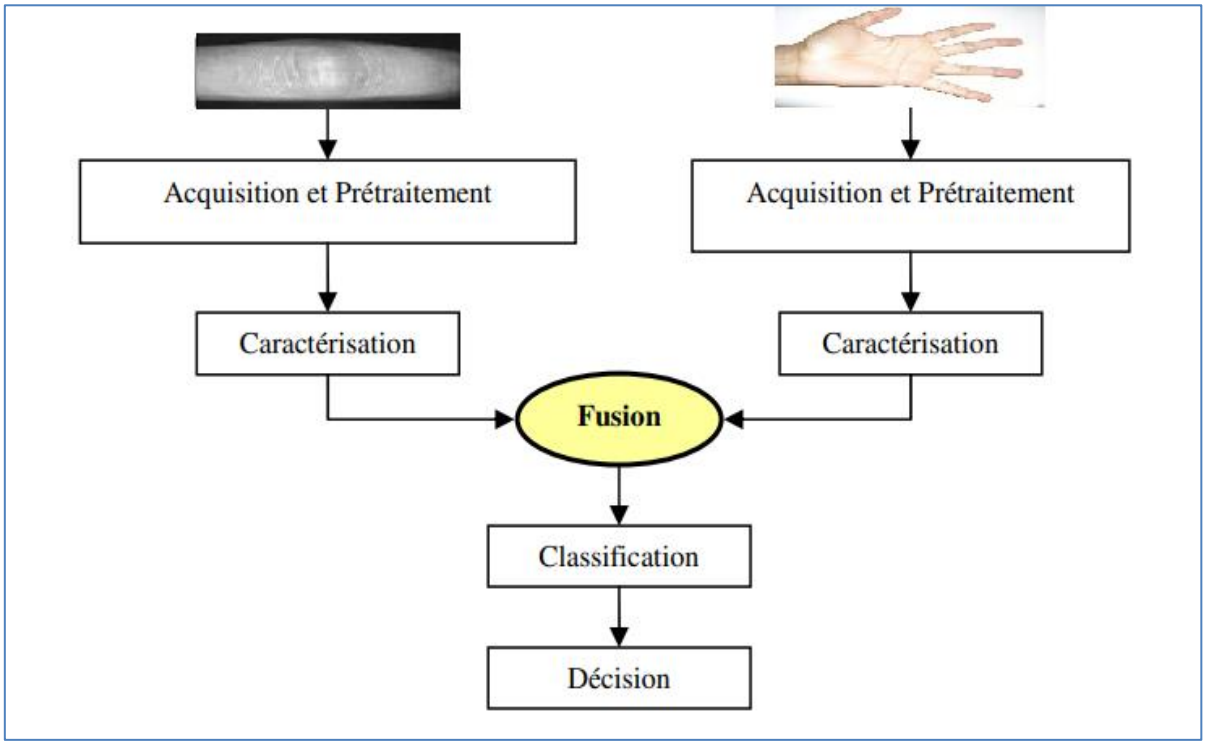

Figure 2-8 Étapes du système d'identification bimodale avec fusion au niveau des caractéristiques.

2.2.7. Normalisation du vecteur de caractéristiques:

a. Normalisation de la technique min-max calcule x :

Cette technique est efficace lorsque les valeurs minimales et maximales des valeurs des caractéristiques des composants sont connues à l'avance. Dans les cas où ces informations ne sont pas disponibles, une estimation de ces paramètres doit être obtenue à partir de l'échantillon disponible donnée d'entraînement. L'estimation peut être affectée par la présence de valeurs aberrantes dans les données d'apprentissage, ce qui rend normalisation min-max sensible aux valeurs aberrantes [30] Par exemple :

Les vecteurs de caractéristiques extraits indépendamment de FKP et de l'emprunt palmaire. L'image est de nature incompatible en raison de la variation de leur gamme et distribution. Une façon de surmonter ce problème est pour normaliser les vecteurs caractéristiques par schéma de normalisation (min-max, médiane). Ici, normalisation min-max schéma est appliquée, ce qui normalise les vecteurs de caractéristiques dans la plage [0,1]. Soit X={x1, x2, x3...xn} le vecteur caractéristique, le vecteur de caractéristique normalisé X peut être représenté en utilisant la normalisation min max [31].

$$X' = \frac{\mathrm{Xi} - \min(\mathrm{X})}{\max(\mathrm{X}) - \min(\mathrm{X})}$$

b. Normalisation de l'écart absolu médian (MAD) :

Les valeurs médianes et d'écart absolu médian (MAD) ne sont généralement pas influencées par la présence de valeurs aberrantes dans les données d'apprentissage. Par conséquent, le schéma de normalisation MAD est devrait être plus robuste aux valeurs aberrantes que le schéma min-max. L'efficacité de cette technique peut être relativement plus faible, car la médiane n'est pas un très bon estimateur des paramètres de localisation et d'échelle pour une distribution non gaussienne. Ici Xi= (xi1, xi2,⋯, xij,⋯, xin), $\acute{x}$ est la valeur de fonctionnalité normalisée obtenue après application de la normalisation. Cette technique peut alors être représentée par :

$$X' = \frac{\mathrm{X-MEDIAN}}{MAD} \quad \text{, MAD=constant (median 1 } -\text{mediank i)}$$

c. Normalisation Z-score :

La technique du score Z utilise les valeurs connues ou estimées de la moyenne et de l'écart type des données pour les normaliser. Cependant, étant donné que la moyenne et l'écart type sont sensibles aux valeurs aberrantes, il peut être prudent de supposer que cette technique manquera également de robustesse aux valeurs aberrantes, similaire au schéma de normalisation min-max. Ici xi= (xi1, xi2, ·

· · , xij , · · · , xin), x´i est la valeur de caractéristique normalisée obtenue après application de la normalisation min-max cette technique peut alors être représentée par [32] :

$$X' = \frac{\mathrm{X} - \mathrm{Moyenne(X)}}{Standars\ Deviation\ (\mathrm{X})}$$

2.2.8. Fusionner le vecteur de caractéristiques :

La fusion au niveau des caractéristiques est une simple concaténation de la fonctionnalité ensemble obtenue à partir de différentes sources d'information. Soit X = (x1, x2, ---------xm) et Y = (y1, y2, ---------, yn) dénotent comporté des vecteurs de visage ou d'empreintes digitales. La règle de concaténation est appliquée sur ces vecteurs caractéristiques représentés par le vecteur Z, qui aurait une meilleure capacité de reconnaissance des individuels. Le vecteur Z est ensuite entré dans le matcher qui calcule la proximité entre deux caractéristiques concaténées vectrices [33].

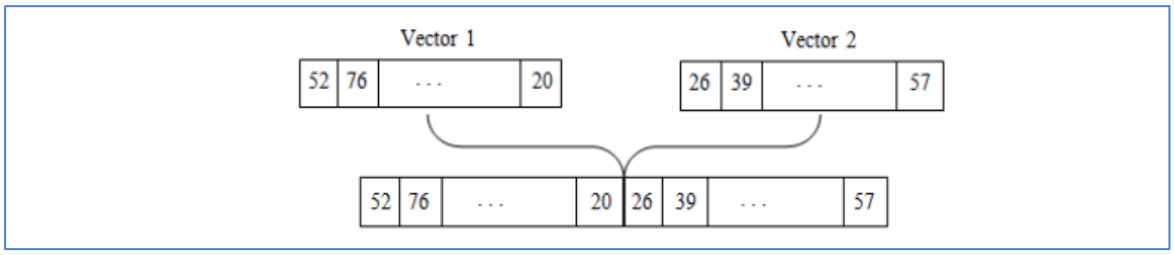

Figure 2-9 Concaténation de deux vecteur

2.3. Conclusion :

En conclusion, la fusion des caractéristiques et les normalisations jouent un rôle crucial dans l'amélioration des performances des modèles d'apprentissage automatique. L'état de l'art dans ce domaine est en constante évolution, avec de nouvelles techniques et approches émergentes. Il est important de rester informé des développements récents et d'adapter les techniques de fusion des caractéristiques et les normalisations en fonction des caractéristiques des données et des objectifs d'apprentissage.

Cependant, il est également important de considérer les contraintes de vitesse et de ressources lors de l'application de ces techniques, en adaptant les méthodes choisies en fonction des spécificités du problème et des contraintes du contexte d'utilisation.

Chapitre 03

CONCEPTION

3.1. Introduction :

Dans ce chapitre, nous proposons d'étudier et de développer des méthodes de fusion de caractéristiques entre l'empreinte palmaire et la FKP pour améliorer la reconnaissance biométrique. Nous examinerons les différentes étapes de la fusion, y compris l'extraction des caractéristiques, leur normalisation et leur sélection. Nous explorerons également diverses techniques mathématiques de fusion, telles que le min et le max, la somme pondérée, ou d'autres approches basées sur des distances ou des modèles probabilistes.

L'objectif principal de cette recherche est d'améliorer les performances de reconnaissance biométrique en exploitant la complémentarité des caractéristiques de l'empreinte palmaire et de la FKP. Nous évaluerons nos méthodes de fusion proposées en utilisant des ensembles de données standardisés et en comparant les résultats avec d'autres approches existantes.

3.2. L'extraction des caractéristiques :

L'extraction des caractéristiques est définie par un processus de conversion d'une image capturée, i.e. palmèrent, en une unique, distinctive et compacte forme de telle sorte qu'on puisse la comparer avec un enregistrement de référence [34].

Cette sous-section décrit le processus de région d'intérêt (ROI) pour les images d'empreintes palmaires. D'abord une caméra CCD a été utilisé pour capturer l'image de l'empreinte palmaire. Ensuite, le processus d'extraction du retour sur investissement commence pendant la première phase une opération de lissage gaussien été appliqué à l'image d'entrée puis suivi d'une binarisation pour l'image lissée en utilisant un seuil H une fois la binarisation effectuée, les frontières de là l'image binaire est extraite en appliquant un suivi de frontière algorithme alors les points P1 et P2 ont été déterminée pour localiser le motif ROI de l'image limite. En conséquence, le système ROI a été extrait, la région du Le ROI a été localisé par le rectangle Le retour sur investissement extrait et

illustré. Le représentent de l'image d'empreinte palmaire, tout en illustrant l'obtenu ROI en joignant les points de nuage correspondant aux pixels dans ROI [35].

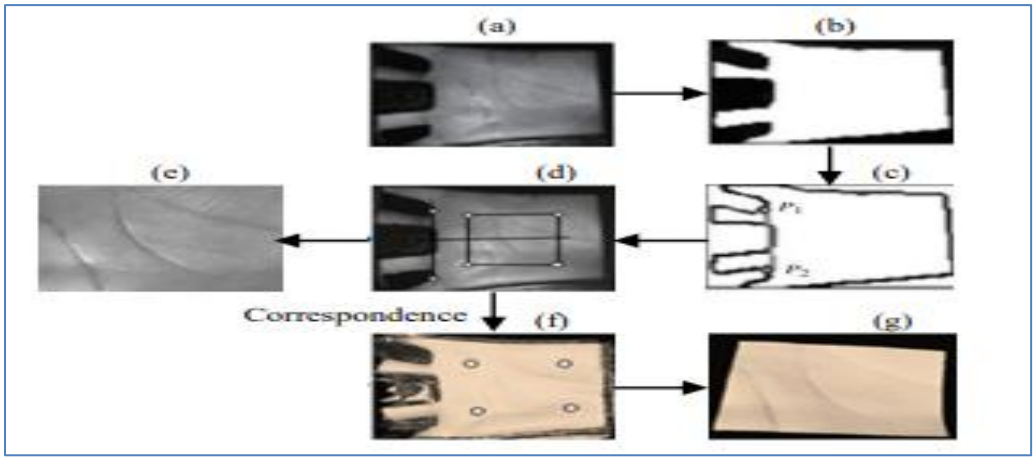

Figure 3-1 L'extraction des caractéristique d'empreinte palmaire

En plus que L'extraction des caractéristiques de la FKP il se déroule en quatre étapes :

1.déterminer l'axe X du système de coordonnées.

2.recadrer une sous-image Is. Les limites gauche et droite d'Is sont deux fixes valeurs évaluées empiriquement. Les limites supérieure et inférieure sont estimées en fonction à la limite des vrais doigts.

3.Détection des contours astucieuse.

4.déterminer l'axe Y du système de coordonnées [36].

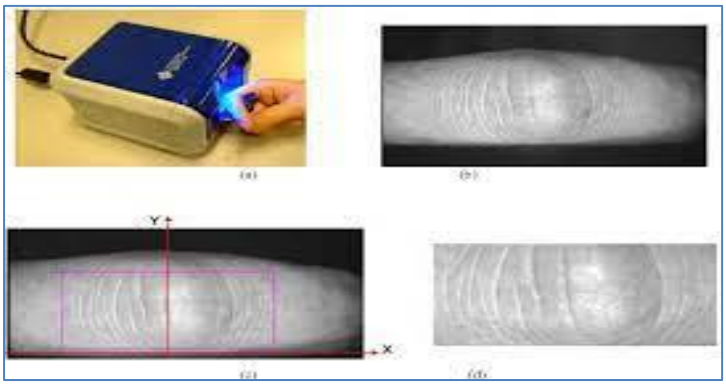

Figure 3-2 L'extraction des caractéristiques de FKP.

3.3. Descripteur Bsif :

Cette méthode calcule un code binaire pour chaque pixel en projetant linéairement des patchs d'image locales sur un sous-espace, dont les vecteurs de base sont appris à partir d'images naturelles via une analyse en composantes indépendante, et en binarisant les coordonnées dans cette base via seuillage.

La longueur de la chaîne de code binaire est déterminée par le nombre de vecteurs de base. Les blocs d'images sont représentés par des histogrammes de binaires codes. Cette méthode est différente des autres descripteurs qui produisent des binaires codes, tels que LBP et LPQ, dans le sens où l'approche proposée est basée sur des statistiques d'images naturelles et cela améliore sa capacité de modélisation. Nous avons extrait les caractéristiques BSIF à l'aide d'un filtre prédéfini de taille 17 ×17 apprit à partir d'images naturelles et d'une chaîne de 12 bits.

-la réponse du filtre est obtenue en calculant l'expression suivante [37]:

$$S = \sum Wi\ (u, v)X(u, v) = Wi\ T\ x,$$

3.4. : Analyse en composantes principales (ACP) :

L'analyse en composantes principales (ACP) est un outil standard dans l'analyse de données moderne - dans divers domaines allant des neurosciences à l'infographie - car il s'agit d'une méthode simple et non paramétrique. pour extraire des informations pertinentes à partir d'ensembles de données déroutantes [38].

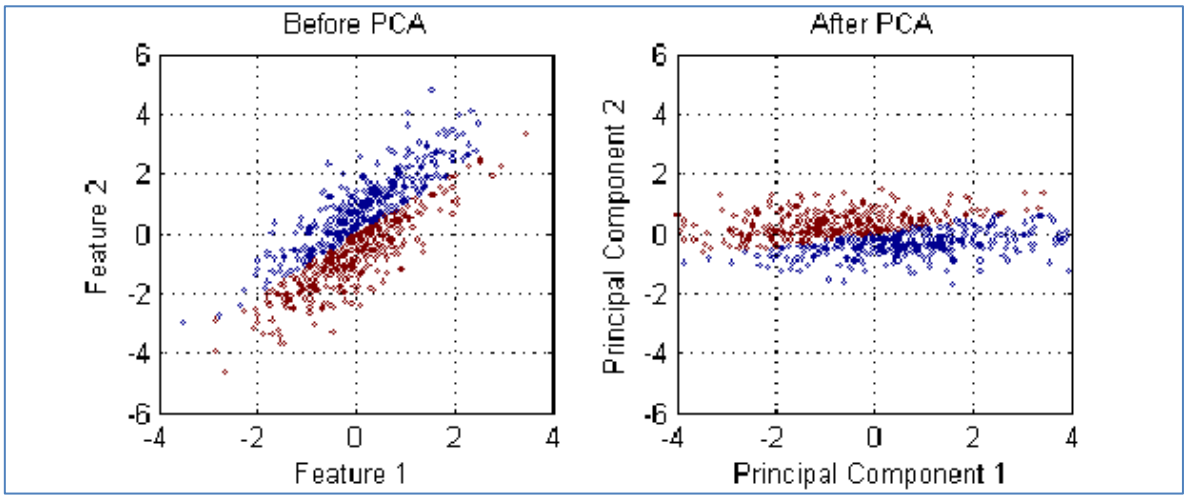

Figure 3-3 Exemple de PCA.

3.5. Analyse Discriminante Linéaire (ADL):

L'analyse discriminante linéaire (LDA) est une méthode bien connue pour la réduction de la dimensionnalité et la classification. ADL dans le cas de la classe binaire s'est avéré équivalant au cas linéaire régression avec l'étiquette de classe comme sortie. Cela implique que LDA pour les classifications de classes binaires peut être formulé comme un problème des moindres carrés. Avec la formulation des moindres carrés, LDA peut être appliquée à des classifications à grande échelle en utilisant des méthodes existant pour résoudre des problèmes de moindres carrés tels que ceux basés sur le gradient conjugué.

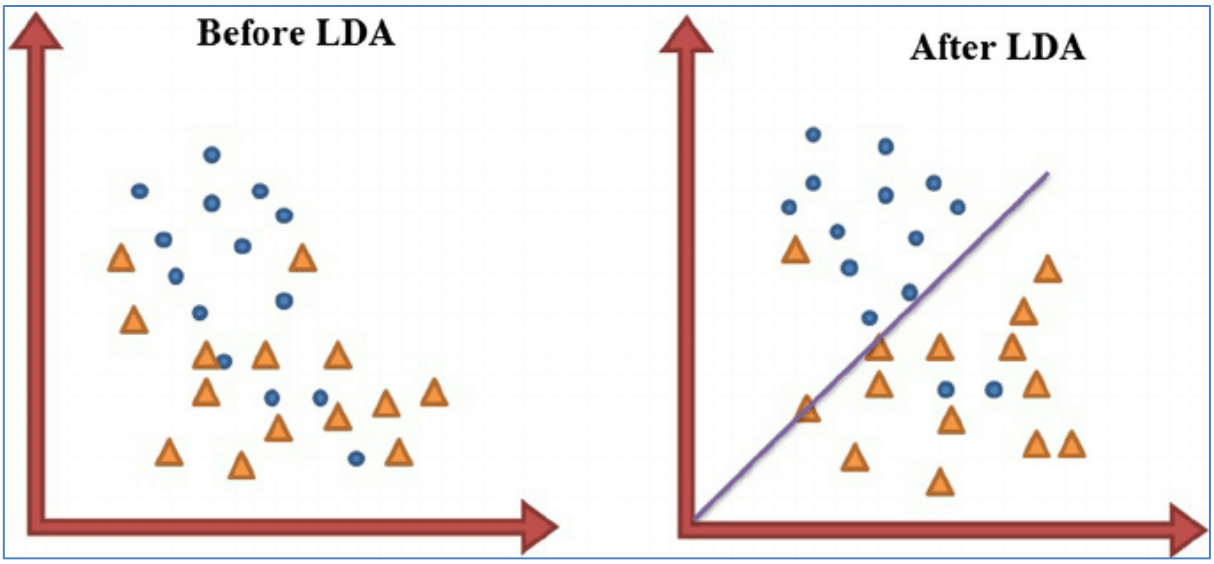

Figure 3-4 Exemple de LDA

3.6. Méthodes proposées :

3.6.1. L'architecture de fusion aux niveaux des caractéristiques

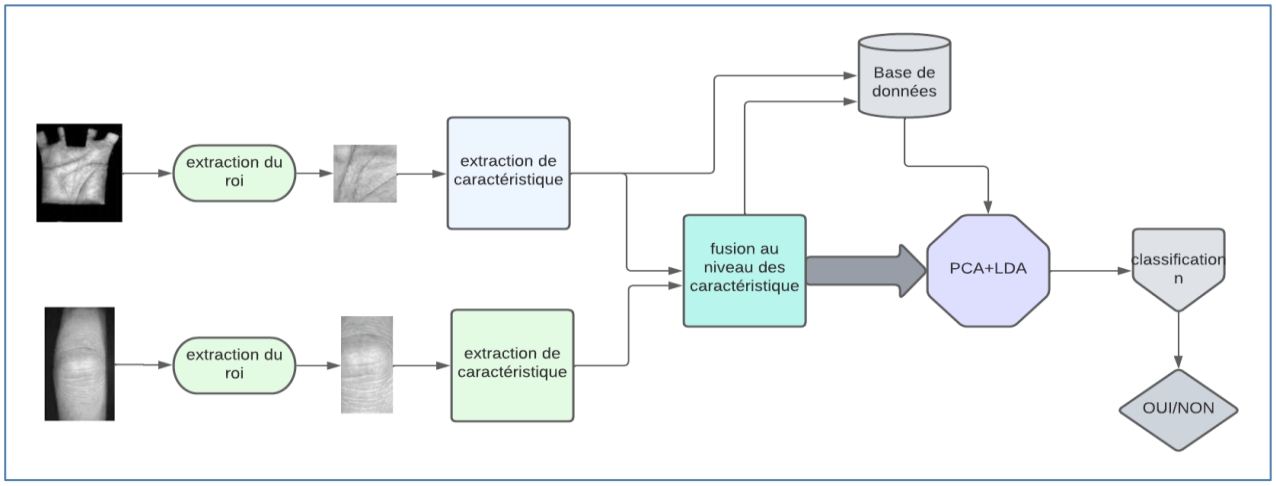

Figure 3-5 l'architecture de fusion au niveau des caractéristiques.

3.6.2. Base de données FKP :

Le système proposé a été testé sur l'ensemble de données FKP (fkpdata) accessible au public fourni par Université d'Oulu. Cette base de données contient 7920 images recueillies auprès de 165 personnes. Les images FKP ont été capturées de chaque individu Quatre types de doigts de chaque personne ont été collectées qui sont : index gauche (LIF), gauche milieu (LMF), index droit (RIF) et milieu droit (RMF). Chaque type de doigt a 12 images dans chaque session. Il y a nombre total de 1980 images pour chaque type de doigt.

3.6.3. Base de données de l'empreinte palmaire :

Le système proposé a été testé sur l'ensemble de données de l'empreinte palmaire (palm_multis_data) accessible au public fourni par Université d'Oulu. Cette base de données contient 24000 images recueillies auprès de 500 personnes. Les images d'empreinte palmaire ont été capturées de chaque individu. Quatre types de couleur de chaque personne ont été collectées qui sont : Blue, Green, NIR et RED. Chaque type a 12 images dans chaque session. Il y a nombre total de 6000 images pour chaque type de couleur.

3.6.4. L'extraction de caractéristique :

Dans cette étape, nous appliquons le descripteur BSIF, nous choisissons un filtre particulier ICAtextureFilters_17x17_12 bit duos à son identification élevée RANK-1 (%) et faible taux d'erreur égal (%). Cependant, le descripteur mentionné a été appliqué sur l'empreinte palmaire et FKP.

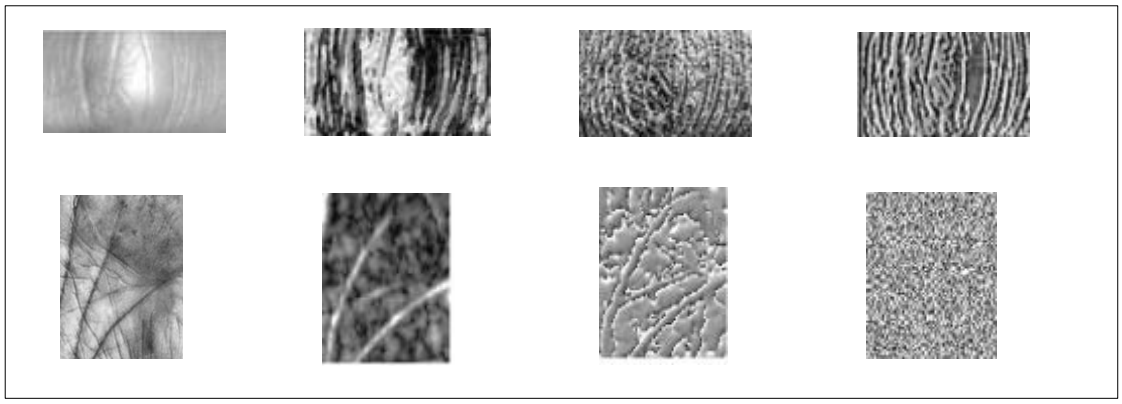

Figure 3-6 Échantillons de l'image ROI FKP et Palm Print avec niveau sorties filtre BSIF de taille 17×17 et de longueur 12 et 11 et 10 bits.

3.6.5. Fusion d'extraction de caractéristique :

L'étape suivante est une fusion entre tous les vecteurs extraits de l'étape précédente, qui comprend l'empreinte palmaire et l'FKP.

3.6.6. Réduction dimensionnelle :

Dans cette étape, nous utilisons les principaux PCA et LDA comme réduction de dimensionnalités techniques, leur travail consiste à effectuer sur de grands vecteurs de grandes dimensions avant stade correspondant.

3.6.7. Protocole d'évaluation :

L'identification FKP et l'empreinte palmaire consiste en un processus d'appariement, dans notre étude nous avons pris les quatre premières images (n = 1..4) pour le modèle d'apprentissage et le reste pour le modèle de test (n = 4..12).

3.6.8. Enrôlement :

Dans la procédure à venir, les données sont stockées pour une étape de correspondance ultérieure.

3.6.9. Classification :

Le classificateur NN (plus proche voisin) est appliqué à partir de l'outil PhD pour la classification phase, la fonction prend cinq paramètres (modèle entraîné, identifiants entraînés, données pour le test, les résultats des identifiants, le "type de correspondance"). Classé en calculant la distance au plus proche cas d'apprentissage, le signe de ce point détermine alors le classement de l'échantillon.

3.6.10. Décision :

Enfin, une décision doit être prise afin d'accepter ou de rejeter une personne, quelle qu'en soit la raison. Dépendent des résultats de la phase d'appariement.

3.7. Les outils de développements :

3.7.1. MATLAB 2016 :

Matlab est un langage de programmation utilisé principalement par les ingénieurs et les analystes de données pour calculs numériques. Il existe une variété de boîtes à outils disponibles lors du premier achat Matlab pour améliorer encore les fonctions de base déjà disponibles à l'achat. Matlab est disponible sur les environnements Unix, Macintosh et Windows, mais est également disponible pour les étudiantes utilisations sur les ordinateurs personnels [39].

3.7.2. PhD Tools :

La boîte à outils de reconnaissance faciale PhD (Pretty Helpful Development functions for) est une collection de fonctions et de scripts Matlab destinée à aider les chercheurs travaillant dans le domaine de la reconnaissance faciale. La boîte à outils a été produite en tant que sous-produit de mes travaux de recherche et est disponible gratuitement en téléchargement.

La boîte à outils PhD propose des implémentations de plusieurs techniques populaires de

reconnaissance faciale, telles que l'analyse en composantes principales, l'analyse discriminante linéaire, l'analyse en composantes principales par noyau ou l'analyse de Fisher par noyau. En plus de ces techniques, elle contient des fonctions pour la construction de filtres de Gabor, l'extraction de caractéristiques de Gabor, le calcul de la congruence de phase et d'autres fonctions. Une partie importante de la boîte à outils concerne également les outils d'évaluation qui permettent de construire les courbes de performance les plus courantes (par exemple, ROC, DET, CMC, EPC) utilisées pour évaluer les systèmes de reconnaissance faciale [40].

3.8. Résultats obtenus :

Le tableau ci-dessous montre le taux d'identification et de vérification de la modalité d'empreinte palmaire au niveau des caractéristiques en utilisant le descripteur BSIF.

Tableau 3-1 résultats des modalités d'empreinte palmaire.

FILTER		**NIR**		**GREEN**		**BLUE**		**RED**	
K	**n**	Rank -1(%)	ERR (%)	Rank -1(%)	ERR (%)	Rank – 1(%)	ERR (%)	Rank – 1 (%)	ERR (%)
17X17	**12**	95.66	3.64	94.75	6.64	98.08	6.76	96.67	3.13
17X17	**11**	93.84	2.72	94.24	5.96	96.87	6.78	96.87	3.03
17X17	**10**	92.32	2.86	92.73	5.87	95.05	6.36	96.77	2.86
17X17	**9**	91.01	3.83	89.19	5.72	91.52	5.04	94.55	3.05
17X17	**8**	87.68	4.9	81.92	6.86	86.26	6.48	92.02	3.43
15X15	**12**	94.14	3.41	94.44	6.62	97.37	6.57	97.58	3.66
15X15	**11**	93.84	3.33	93.64	5.36	96.57	4.92	97.58	2.09
15X15	**10**	90.71	3.33	92.02	6.06	94.55	5.56	96.67	2.80
15X15	**9**	89.90	4.03	87.58	6.11	92.83	5.34	95.76	3.02
15X15	**8**	86.57	5.35	82.32	6.55	86.67	6.06	90.81	3.93
13X13	**12**	93.23	4.85	94.75	7.10	97.17	6.55	96.97	4.20
13X13	**11**	90.40	4.30	93.43	5.89	96.97	5.44	97.58	3.42
13X13	**10**	92.22	3.53	93.13	4.74	95.56	4.01	97.74	2.61
13X13	**9**	86.36	4.64	86.16	6.02	90.71	5.16	95.56	3.51
13X13	**8**	83.13	5.90	80.00	7.27	85.56	6.18	89.19	4.55
11X11	**12**	89.80	6.26	94.44	6.67	96.67	5.77	96.67	4.63
11X11	**11**	88.69	5.14	92.32	5.63	96.26	4.37	95.86	3.64
11X11	**10**	86.26	4.59	90.20	5.55	94.85	4.38	94.75	3.40
11X11	**9**	81.62	5.32	84.14	6.56	90.91	5.12	92.22	4.11
11X11	**8**	77.27	6.29	77.37	7.05	85.15	5.68	86.46	5.24

La méthode proposée utilise la base de données (NIR, Green, Blue, RED). Ensuite, nous pouvons observer que le filtre 17x17 12 bits de la base bleue est plus performant que les autres. Le système atteint une précision de rang-1 de 98,08 % et à un taux d'erreur d'égalité (EER) de 6,76 %.

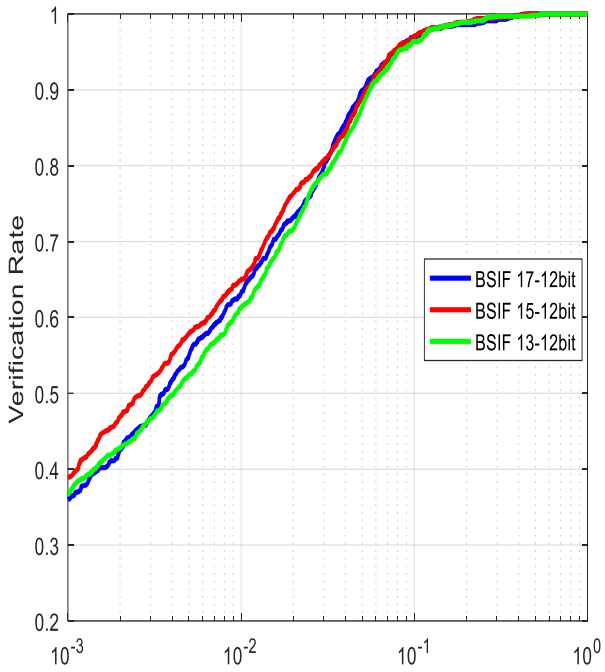

Figure 3-10 (a) roc blue

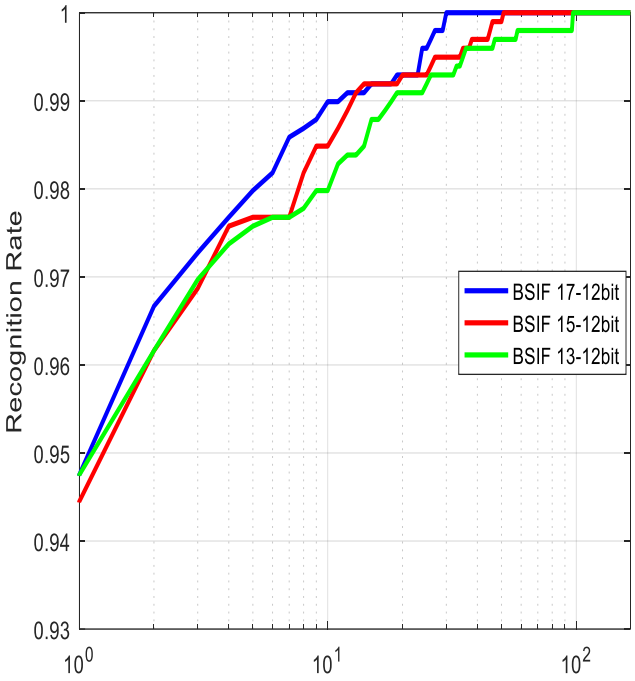

Figure 3-9 (b) cmc blue

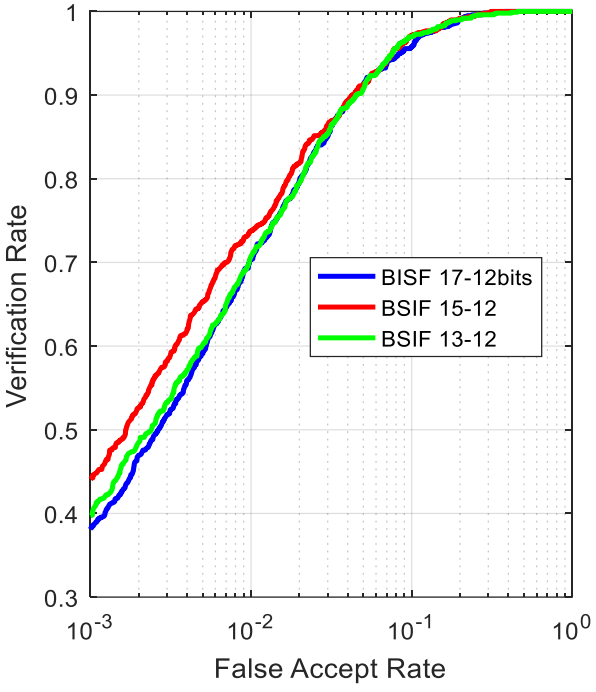

Figure 3-8 (a) roc green

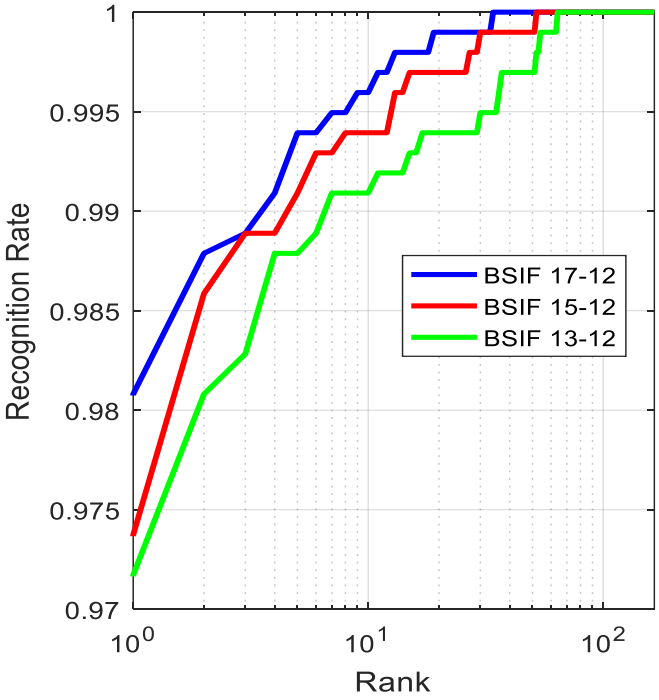

Figure 3-7 (b) cmc green

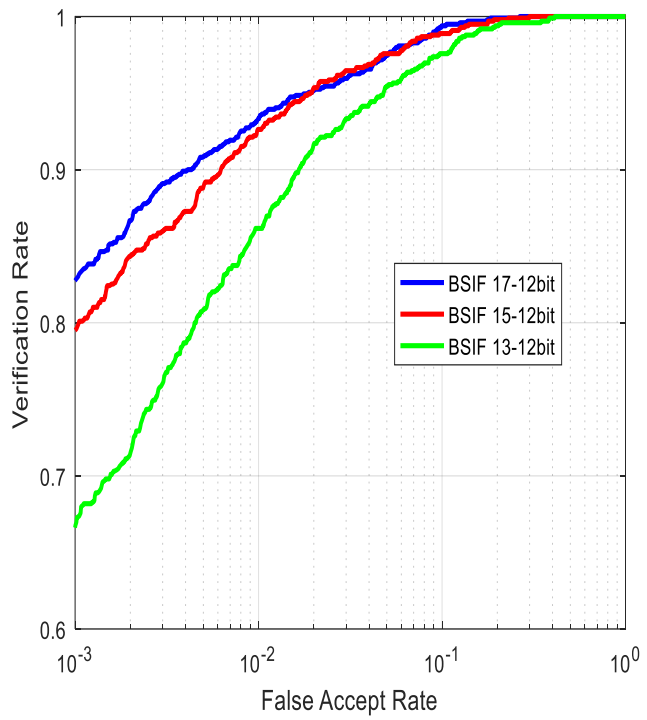

Figure 3-12 (a) roc nir

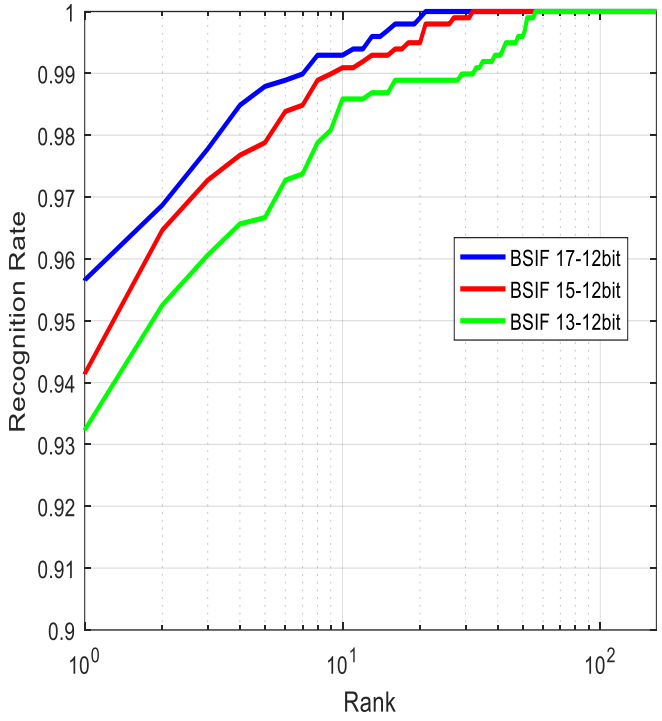

Figure 3-11 (b) cmc nir

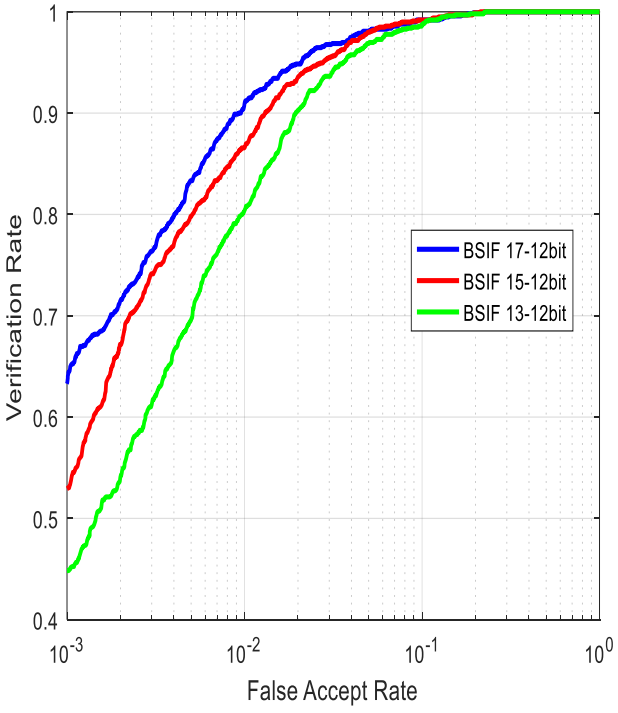

Figure 3-14 (a) roc red

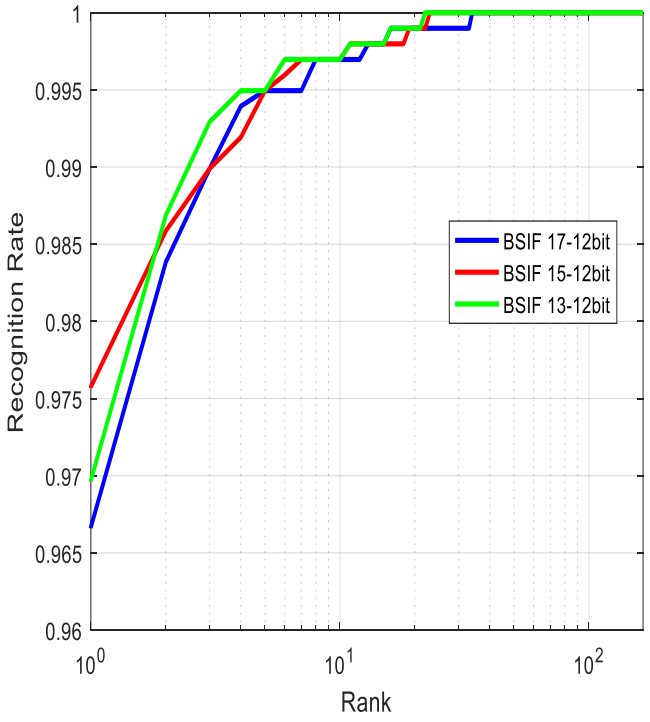

Figure 3-13 (b) cmc red

Le tableau ci-dessous montre le taux d'identification et de vérification de la modalité FKP au niveau des caractéristiques en utilisant le descripteur BSIF.

Tableau 3-2 résultats des modalités d'empreinte de doigt (FKP).

Parameters		LMF		LIF		RIF		RMF	
k	*n*	Rank-1 (%)	EER (%)	Rank-1 (%)	EER (%)	Rank-1 (%)	EER (%)	Rank-1 (%)	EER (%)
17×17	12	98.08	0.30	97.88	0.30	96.57	0.51	98.08	0.20
17×17	11	95.56	0.89	95.66	0.91	95.05	0.91	95.96	0.51
17×17	10	87.98	2.02	87.68	2.22	87.27	3.03	89.60	2.21
17×17	9	83.54	2.93	83.94	3.23	81.11	4.76	84.04	3.64
17×17	8	79.49	4.27	81.41	4.04	77.27	5.13	77.88	5.13
15×15	12	98.28	0.22	98.38	0.30	97.58	0.61	98.89	0.10
15×15	11	96.36	0.81	96.97	0.59	95.35	0.79	96.57	0.38
15×15	10	89.80	2.02	89.29	2.02	88.79	2.22	89.70	1.54
15×15	9	84.65	3.12	81.72	3.13	81.62	4.14	85.15	2.53
15×15	8	80.81	3.74	81.82	4.15	82.12	3.52	80.81	3.64
13×13	12	98.08	0.20	98.48	0.30	97.27	0.40	98.59	0.20
13×13	11	96.46	0.41	97.07	0.51	96.16	0.61	97.37	0.51
13×13	10	91.62	1.21	90.61	1.62	87.88	2.41	90.40	2.12
13×13	9	84.95	2.44	86.16	2.52	84.14	3.84	85.45	2.83
13×13	8	82.63	3.85	83.94	3.13	82.93	3.54	84.14	3.44
11×11	12	98.79	0.20	98.89	0.20	97.68	0.40	98.89	0.10
11×11	11	96.46	0.30	97.37	0.40	96.06	0.81	97.17	0.30
11×11	10	90.51	1.92	91.52	1.72	87.68	2.42	92.53	1.62
11×11	9	85.96	2.63	86.97	2.83	83.74	3.94	86.06	2.92
11×11	8	85.35	2.93	85.45	2.91	83.84	3.33	88.79	2.31

La méthode proposée utilise les bases de données RIF, LIF, RMF et LMF. De plus, il est observé que le filtre 15x15 12 bits de la base RMF est plus performant que les autres.

Le système atteint une précision de rang-1 de 98,89 % et présente un taux d'erreur d'égalité (EER) de 0,10 %.

3.9. Résultats de fusion :

Le tableau ci-dessous représente les résultats de la fusion au niveau des caractéristiques de l'empreinte palmaire et de l'empreinte de doigt (fkp) à l'aide de descripteur BSIF en utilisant les méthodes (MAX, MIN, SOMME).

Tableau 3-3 les résultats de la fusion au niveau des caractéristique de l'empreinte palamair et de l'empreinte de doigt (fkp).

EER/ROR(%) Auth/Ident	Fusion de l'empreinte palamair avec l'FKP							
	Nir-RMF		Nir-LMF		Nir-LIF		Nir-RIF	
	EER(%)	ROR(%)	EER(%)	ROR(%)	EER(%)	ROR(%)	EER(%)	ROR(%)
SOMME	1.31	97.68	1.20	98.89	1.50	97.98	1.44	98.89
MAX	1.11	97.88	1.01	98.79	1.11	98.69	1.53	98.99
MIN	5.96	91.41	6.90	91.72	6.89	90.10	6.78	91.62
EER/ROR(%) Auth/Ident	Fusion de l'empreinte palamair avec l'FKP							
	Blue-RMF		Blue-LMF		Blue-LIF		Blue-RIF	
	EER(%)	ROR(%)	EER(%)	ROR(%)	EER(%)	ROR(%)	EER(%)	ROR(%)
SOMME	1.52	99.49	1.92	98.89	1.51	98.69	1.33	98.38
MAX	1.42	98.69	1.51	99.19	1.54	98.69	1.52	98.08
MIN	3.10	96.57	2.52	95.35	3.43	96.36	2.54	95.76
EER/ROR(%) Auth/Ident	Fusion de l'empreinte palamair avec l'FKP							
	Red-RMF		Red-LMF		Red-LIF		Red-RIF	
	EER(%)	ROR(%)	EER(%)	ROR(%)	EER(%)	ROR(%)	EER(%)	ROR(%)
SOMME	0.83	99.09	0.71	98.89	1.01	99.19	0.89	99.09
MAX	0.81	98.99	0.73	98.99	0.81	99.39	0.91	99.09
MIN	3.41	95.05	4.04	94.95	5.38	93.13	3.13	95.96
EER/ROR(%) Auth/Ident	Fusion de l'empreinte palamair avec l'FKP							
	Green-RMF		Green-LMF		Green-LIF		Green-RIF	
	EER(%)	ROR(%)	EER(%)	ROR(%)	EER(%)	ROR(%)	EER(%)	ROR(%)
SOMME	1.82	97.58	2.02	97.47	1.93	97.78	1.82	97.27
MAX	1.92	97.07	2.02	97.37	2.33	97.88	1.92	96.97
MIN	3.03	96.06	3.26	95.45	3.89	94.65	3.33	96.26

D'après ce que nous avons conclu des deux tableaux précédents, nous avons sélectionné le filtre 17x17 12 bits qui présenté les meilleures performances.

Nous avons ensuite appliqué les méthodes Min, Max et Somme pour fusionner les résultats.

Les résultats obtenus montrent que les meilleurs résultats dans la méthode Min de la fusion est dans la base Blue Rmf, avec un taux de reconnaissance de 96,57 % et une erreur de 3,10%.et pour la base Red-Lif, la méthode Max a également donné de bons résultats dans, avec un taux de reconnaissance de 99,39 % et une erreur de 0,81 %.

Enfin, la méthode Somme a donné des meilleurs résultats dans la base (Blue-RMF), avec un taux de reconnaissance de 99,49 % et une erreur de 1,52 %.

En conclusion, nous pouvons affirmer que la méthode de fusion Somme a obtenu d'excellents résultats.

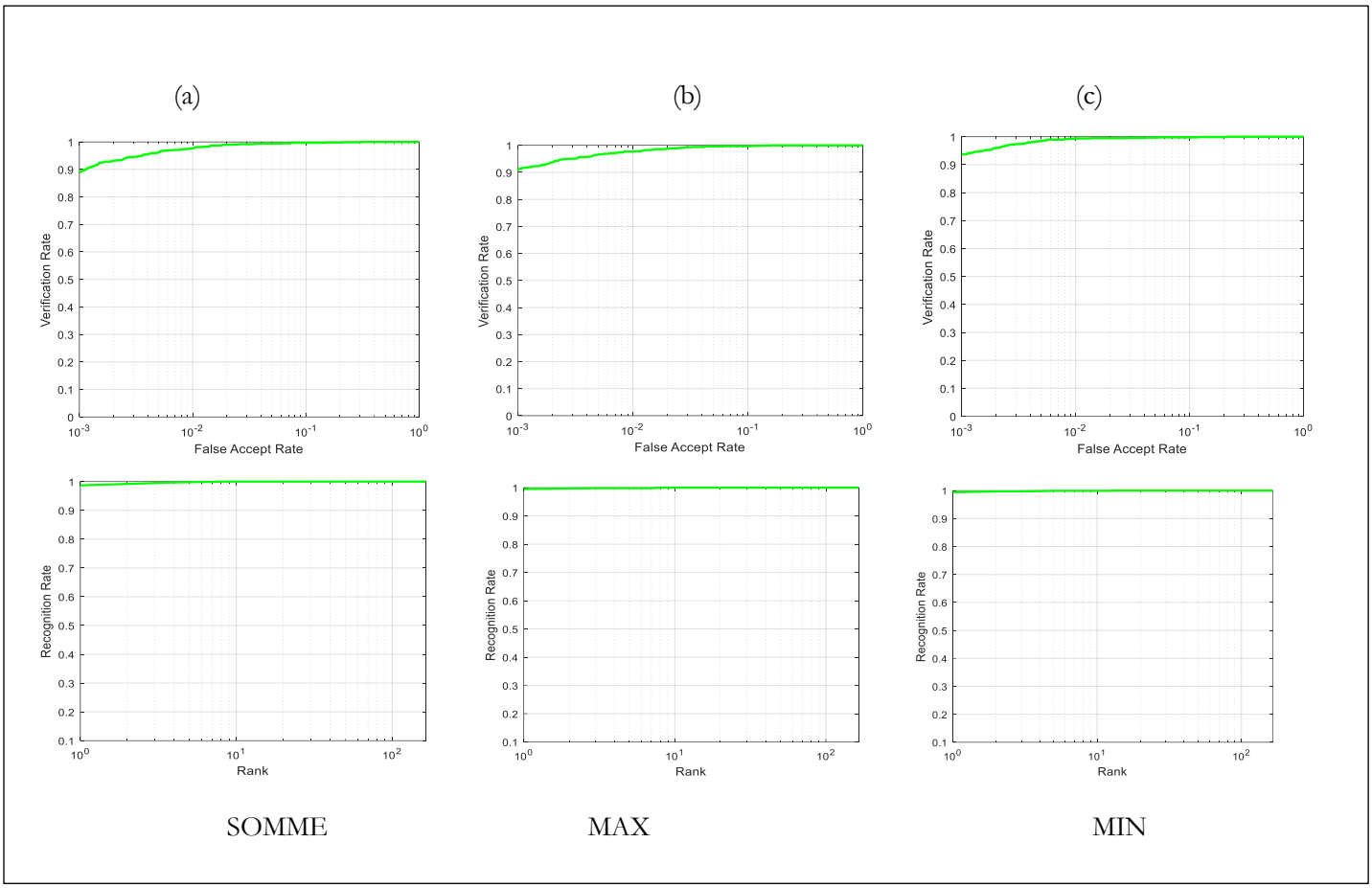

Figure 3-15 Courbes CMC & ROC obtenues à partir de la fusion descripteur-BSIF avec différentes règles.

(a): Courbes CMC & ROC obtenues à partir de la fusion descripteur-BSIF avec la règle somme
(b): Courbes CMC & ROC obtenues à partir de la fusion descripteur-BSIF avec la règle max
(c): Courbes CMC & ROC obtenues à partir de la fusion descripteur-BSIF avec la règle min

La figure ci-dessus présente les courbes CMC et ROC des meilleurs résultats de la fusion au niveau des caractéristiques en utilisant le descripteur BSIF avec les règles de fusion Somme, Max et Min (a), (b), (c) respectivement. Nous pouvons observer que les courbes CMC sont très similaires, avec un taux de reconnaissance élevé et un taux de vérification presque égal à 1. En ce qui concerne les courbes ROC, il y a une légère différence dans les valeurs. Les règles Somme et Max affichent des taux de vérification très proches, tandis que la règle min ne présente un taux de vérification légèrement plus bas que les autres règles.

3.10. Discussion :

Enfin, les résultats obtenus à partir des méthodes proposées étaient satisfaisants. Par conséquent, lors de la fusion des caractéristiques de correspondance en utilisant le descripteur BSIF, l'application de la règle min a donné des résultats légèrement inférieurs par rapport à la fusion utilisant les règles de somme et de max, qui se sont avérées être les plus performantes. De plus, la fusion basée uniquement sur les caractéristiques, en utilisant le descripteur BSIF, s'est révélée très précise et a offert de meilleures performances.

3.11. Conclusion :

En conclusion, la fusion au niveau des caractéristiques entre l'empreinte palmaire et l'empreinte de doigt (FKP) se présente comme une approche prometteuse pour améliorer les performances des systèmes biométriques. Cette approche permet de tirer parti des avantages uniques de chaque modalité, offrant ainsi des résultats plus précis et fiables.

Les résultats obtenus lors de cette étude fournissent des preuves solides de l'efficacité de la fusion au niveau des caractéristiques entre l'empreinte palmaire et l'empreinte de doigt (fkp). Cette approche ouvre de nouvelles perspectives pour le développement de systèmes biométriques plus performants, contribuant ainsi à renforcer la sécurité et l'exactitude des applications biométriques dans divers domaines tels que la sécurité, l'identification personnelle et l'accès aux systèmes.

CONCLUSIONS GENERALES ET PERSPECTIVES

La biométrie est un domaine scientifique qui étudie les caractéristiques biologiques et les mesures spécifiquement dans le but d'identifier les individus. La fusion au niveau des caractéristiques s'est révélée être une approche prometteuse pour améliorer les performances de l'identification biométrique. Nos travaux ont contribué à une meilleure compréhension de la fusion au niveau des caractéristiques et ont ouvert de nouvelles perspectives pour la conception de systèmes biométriques plus précis et fiables.

Les résultats obtenus ont montré que l'utilisation du descripteur BSIF dans la fusion des caractéristiques permet d'obtenir une meilleure discrimination entre les individus, en exploitant les informations uniques et spécifiques contenues dans leurs caractéristiques biologiques. Cela a conduit à une amélioration significative des performances d'identification biométrique, notamment en matière de précision et de robustesse face aux variations environnementales.

Cependant, il est important de noter que cette conclusion générale doit être adaptée en tenant compte des résultats et des contributions spécifiques de notre mémoire sur la fusion au niveau des caractéristiques. Nous devons prendre en considération les limites de notre étude, telles que la taille de l'échantillon, la nature des données utilisées et les méthodes de fusion mises en œuvre. Ces facteurs peuvent influencer la généralisation des résultats et doivent être pris en compte lors de l'application de cette conclusion à d'autres contextes ou domaines.

Références Bibliographiques

[1] « These-Hafs-Toufik.pdf ». Consulté le: 2 juin 2023. [En ligne]. Disponible sur: https://biblio.univ-annaba.dz/wp-content/uploads/2016/11/These-Hafs-Toufik.pdf

[2] Ra. Halimi et A. Seddiki, « Système Biométrique pour la Reconnaissance des Articulations des Doigts et la Méthode de Quantification de phase Local », Thesis, 2020. Consulté le: 2 juin 2023. [En ligne]. Disponible sur: http://dspace.univ-ouargla.dz/jspui/handle/123456789/29001

[3] A. Bentahar, « Sécurité de l'internet des objets en utilisant la biométrie », Thesis, 2022. Consulté le: 3 juin 2023. [En ligne]. Disponible sur: http://dspace.univ-tebessa.dz:8080/jspui/handle/123456789/http//localhost:8080/jspui/handle/123456789/4421

[4] B. A. ADJAINE. Elmechri et M. K. B. M. Z. Tidjani, « Authentification et Identification biométrique des personnes par les empreintes palmaires », nov. 2019, Consulté le: 3 juin 2023. [En ligne]. Disponible sur: http://dspace.univ-ouargla.dz/jspui/handle/123456789/21880

[5] A. Mattelart, « Identifier et surveiller : Les technologies de sécurité », *Identifier Surveill.*, p. 1‑196, 2007.

[6] E. Cherrier, « Authentification biométrique: comment (ré)concilier sécurité, utilisabilité et respect de la vie privée? ».

[7] F. Dagognet, *Mémoire pour l'avenir: vers une méthodologie de l'informatique*. Vrin, 2007.

[8] L. Laniel et P. Piazza, « Une carte nationale d'identité biométrique pour les Britanniques : l'antiterrorisme au cœur des discours de justification », *Cult. Confl.* nº 64, Art. nº 64, déc. 2006, doi: 10.4000/conflits.2174.

[9] J. M. Tanner, « CURRENT ADVANCES IN THE STUDY OF PHYSIQUE: PHOTOGRAMMETRIC ANTHROPOMETRY AND AN ANDROGYNY SCALE », *The Lancet*, vol. 257, nº 6654, p. 574‑579, mars 1951, doi: 10.1016/S0140-6736(51)92260-X.

[10] C. Loudot, E. Zanin, C. Fogliarini, M. Boulze, L. Souchon, et D. Denis, « Étude de la biométrie oculaire chez l'enfant hypermétrope : apport du biomètre Lenstar LS 900 (Haag-Streit®) », *J. Fr. Ophtalmol.*, vol. 34, nº 6, p. 369‑375, juin 2011, doi: 10.1016/j.jfo.2010.12.008.

[11] A. Plateaux, P. Lacharme, C. Rosenberger, et A. Josang, « Biométrie à usage unique pour la monétique », présenté à Conférence sur la Sécurité des Architectures Réseaux et des Systèmes d'Information (SAR SSI), 2014. Consulté le: 25 mai 2023. [En ligne]. Disponible sur: https://hal.science/hal-00990776

[12] B. Ammour et T. (Rapporteur) Bouden, « Contribution au développement de systèmes biométriques à base du visage et de l'iris », Thesis, 2018. Consulté le: 3 juin 2023. [En ligne]. Disponible sur: http://dspace.univ-jijel.dz:8080/xmlui/handle/123456789/3967

[13] Z. Benhemimed, A. Bourouis, et W. Birouk, « Reconnaissance de l'empreinte palmaire pour des applications civiles et criminalistiques », Thesis, université jijel, 2018. Consulté le: 3 juin 2023. [En ligne]. Disponible sur: http://dspace.univ-jijel.dz:8080/xmlui/handle/123456789/1892

[14] N. K. Hili, « Biométrie multimodale basée sur l'iris et le visage ».

[15] S. Aliouche, H. E. Chetibi, et W. (encadreur) Birouk, « Reconnaissance biométrique des personnes par la caractérisation de la rétine », Thesis, Université jijel, 2021. Consulté le: 3 juin 2023. [En ligne]. Disponible sur: http://dspace.univ-jijel.dz:8080/xmlui/handle/123456789/10938

[16] A. Chaari, « Nouvelle approche d'identification dans les bases de données biométriques basée sur une classification non supervisée », phdthesis, Université d'Evry-Val d'Essonne, 2009. Consulté le: 3 juin 2023. [En ligne]. Disponible sur: https://theses.hal.science/tel-00549395

[17] « Combler les lacunes entre la recherche et la pratique dans le cas de la biométrie vocale: améliorations de l'entrainement et apprentissage par similarité pour une vérification plus robuste - ProQuest ». https://www.proquest.com/openview/f26106efa7584ae22fad2ccf864a843a/1?pq-origsite=gscholar&cbl=18750&diss=y (consulté le 3 juin 2023).

[18] S. Idriguen et W. Bahloul, « Réalisation d'un Système de Reconnaissance Biométrique Multimodal », Thesis, Université Akli Mouhand Oulhadj-Bouira, 2018. Consulté le: 3 juin 2023. [En ligne]. Disponible sur: http://dspace.univ-bouira.dz:8080/jspui/handle/123456789/6958

[19] R. O. Belguechi, « Sécurité des systèmes biométriques : révocabilité et protection de la vie privée », phdthesis, Ecole nationale Supérieure en Informatique Alger, 2015. Consulté le: 3 juin 2023. [En ligne]. Disponible sur: https://theses.hal.science/tel-01230691

[20] N. Morizet, « Reconnaissance Biométrique par Fusion Multimodale du Visage et de l'Iris », phdthesis, Télécom ParisTech, 2009. Consulté le: 3 juin 2023. [En ligne]. Disponible sur: https://pastel.archives-ouvertes.fr/pastel-00005811

[21] N. Zouied, « L'empreinte palmaire multispectrale », Working Paper, oct. 2020. Consulté le: 3 juin 2023. [En ligne]. Disponible sur: http://dspace.univ-guelma.dz/jspui/handle/123456789/10255

[22] A. Boucetta, « Approches évolutionnaires multi-biométriques pour l'identification des personnes. ».

[23] « ZOUIED_NESREDDINE_Electronique._Instrumentation.pdf ». Consulté le: 3 juin 2023. [En ligne]. Disponible sur: https://dspace.univ-guelma.dz/jspui/bitstream/123456789/10255/1/ZOUIED_NESREDDINE_Electronique._Instrumentation.pdf

[24] M. Kertous, A. Rezai, et I. (Encadreur) Bouraoui, « Classification des empreintes palmaires multi-spectrales par les réseaux de neurones convolutionnels. », Thesis, Université de Jijel, 2021. Consulté le: 3 juin 2023. [En ligne]. Disponible sur: http://dspace.univ-jijel.dz:8080/xmlui/handle/123456789/10683

[25] « mémoire complet.pdf ». Consulté le: 3 juin 2023. [En ligne]. Disponible sur: http://dspace.univ-bouira.dz:8080/jspui/bitstream/123456789/2849/1/m%C3%A9moire%20complet.pdf

[26] « These-Hafs-Toufik.pdf ». Consulté le: 3 juin 2023. [En ligne]. Disponible sur: https://biblio.univ-annaba.dz/wp-content/uploads/2016/11/These-Hafs-Toufik.pdf

[27] N. Charfi, « Biometric recognition based on hand schape and palmprint modalities », phdthesis, Ecole nationale supérieure Mines-Télécom Atlantique, 2017. Consulté le: 3 juin 2023. [En ligne]. Disponible sur: https://theses.hal.science/tel-01781354

[28] R. Landais, H. Bredin, L. Zouari, et G. Chollet, « Vérification audiovisuelle de l'identité », *Trait. Anal. Inf. Méthodes Appl.*, mai 2007.

[29] N. Charfi, « Reconnaissance biométrique basée sur les modalités de la forme de la main et de l'empreinte palmaire », These de doctorat, Ecole nationale supérieure Mines-Télécom Atlantique Bretagne Pays de la Loire, 2017. Consulté le: 3 juin 2023. [En ligne]. Disponible sur: https://www.theses.fr/2017IMTA0003

[30] « 600_Data-Normalization-using-Median-&-Median-Absolute-Deviation-(MMAD)-based-Z-Score-for-Robust-Predictions-vs-Min–Max-Normalization.pdf ». Consulté le: 3 juin 2023. [En ligne]. Disponible sur: https://journalspress.com/LJRS_Volume19/600_Data-Normalization-using-Median-&-Median-Absolute-Deviation-(MMAD)-based-Z-Score-for-Robust-Predictions-vs-Min%E2%80%93Max-Normalization.pdf

[31] « ijaerv13n5_89.pdf ». Consulté le: 3 juin 2023. [En ligne]. Disponible sur: https://www.ripublication.com/ijaer18/ijaerv13n5_89.pdf

[32] object Object, « Feature-level fusion in multimodal biometrics », Consulté le: 3 juin 2023. [En ligne]. Disponible sur: https://core.ac.uk/reader/230456340

[33] M. F. Nadheen et S. Poornima, « Feature Level Fusion in Multimodal Biometric Authentication System », *Int. J. Comput. Appl.*, vol. 69, nº 18, p. 36‑40, mai 2013.

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

[35] N. E. Chalabi, A. Attia, et A. Bouziane, « BLOCK WISE 3D PALMPRINT RECOGNITION BASED ON TAN AND TRIGGS WITH BSIF DESCRIPTOR », *ICTACT J. SOFT Comput.*, vol. 11, nº 02, 2021.

[36] « Théses-Algérie: Doctorat, Magister, Master... » https://www.theses-algerie.com (consulté le 3 juin 2023).

[37] N. Boulfiza et C. Flici, « Syst eme de reconnaissance des personnes par l'empreinte d'articulation des doigts avec des algorithmes de normalisation d'eclairage », Thesis, université akli mohand oulhadj-bouira, 2021. Consulté le: 3 juin 2023. [En ligne]. Disponible sur: http://dspace.univ-bouira.dz:8080/jspui/handle/123456789/12196

[38] J. Shlens, « A Tutorial on Principal Component Analysis ». arXiv, 3 avril 2014. Consulté le: 3 juin 2023. [En ligne]. Disponible sur: http://arxiv.org/abs/1404.1100

[39] C. Ozgur, T. Colliau, G. Rogers, Z. Hughes, et E. Bennie, « MatLab vs. Python vs. R », *J. Data Sci. JDS*, vol. 15, p. 355‑372, juill. 2017.

[40] « The PhD face recognition toolbox » 4 juin 2023. https://www.mathworks.com/matlabcentral/fileexchange/35106-the-phd-face-recognition-toolbox (consulté le 3 juin 2023).

ملخص:

أصبحت تقنيات القياسات الحيوية أساسًا لمجموعة واسعة من الأدوات عالية الأمان لتحديد هوية الأفراد والتحقق منهم.

في مذكرتنا استكشفنا طرقًا بيومترية مختلفة مثل بصمات الكف وبصمات الأصابع (FKP) لتحديد المستخدمين والتحقق منهم. لتحسين الأداء ، استخدمنا واصف ميزات الصورة الإحصائية الثنائية (BSIF) وقمنا بإجراء دمج على مستوى الميزات باستخدام أساليب مختلفة.

يتكون اندماج التسلسل من الجمع بين الميزات المستخرجة من بصمات الكف وبصمات مفاصل الأصابع (FKP) لإنشاء تمثيل مشترك. تتيح هذه الطريقة إمكانية الاستفادة من المعلومات التكميلية التي توفرها هاتان الطريقتان البيومتريتان.

الإضافة إلى ذلك ، استخدمنا عوامل التشغيل min و max و sum لدمج قيم الميزات المستخرجة. يفضّل الدمج بواسطة عامل التشغيل min القيم الدنيا ، بينما يفضّل الدمج بواسطة عامل التشغيل الأقصى القيم القصوى. يضيف Sum fusion قيم المعالم.

تتيح هذه الأساليب إمكانية استغلال المعلومات المختلفة الموجودة في الميزات المستخرجة ودمجها بشكل مناسب لتحسين الأداء في مهام تحليل الصور المختلفة.

Résumé :

Les techniques biométriques sont devenues la base d'une vaste gamme d'outils hautement sécurisés pour l'identification et la vérification du personnel.

Dans notre mémoire, nous avons exploré différentes méthodes biométriques telles que les empreintes palmaires et les empreintes des articulations des doigts (FKP) pour identifier et vérifier les utilisateurs. Pour améliorer les performances, nous avons utilisé le descripteur BSIF (Binarized Statistical Image Features) et réalisé la fusion au niveau des caractéristiques en utilisant différentes approches.

La fusion par séquence consiste à combiner les caractéristiques extraites des empreintes palmaires et des empreintes des articulations des doigts (FKP) pour créer une représentation combinée. Cette méthode permet de tirer parti des informations complémentaires fournies par ces deux modalités biométriques.

Par ailleurs, nous avons utilisé les opérateurs min, max et somme pour fusionner les valeurs des caractéristiques extraites. La fusion par l'opérateur min privilégie les valeurs minimales, tandis que la fusion par l'opérateur max privilégie les valeurs maximales. La fusion par somme additionne les valeurs des caractéristiques.

Ces méthodes permettent d'exploiter différentes informations contenues dans les caractéristiques extraites et de les combiner de manière appropriée pour améliorer les performances dans diverses tâches d'analyse d'images.

Abstract:

Biometric techniques have become the foundation of a wide range of highly secure tools for personnel identification and verification.

In our thesis, we explored different biometric methods such as palm prints and finger joint prints (FKP) to identify and verify users. To enhance performance, we utilized the BSIF (Binarized Statistical Image Features) descriptor and performed feature-level fusion using various approaches.

Sequence fusion involves combining the extracted features from palm prints and finger joint prints (FKP) to create a combined representation. This method leverages the complementary information provided by these two biometric modalities.

Additionally, we employed the operator's min, max, and sum to merge the values of the extracted features. Min fusion prioritizes minimum values, while max fusion prioritizes maximum values. Sum fusion adds up the feature values.

These methods allow for the utilization of different information present in the extracted features and their appropriate combination to enhance performance in various image analysis tasks.