REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

Ministère de l'Enseignement Supérieur et de Recherche Scientifique

Université Kasdi Merbah -Ouargla

Faculté des Nouvelles Technologies de l'Information et de la Communication

Département d'électronique et de télécommunication

Mémoire Master

Domaine : Sciences et technologies

Filière : Automatique

Spécialité : Automatique et systèmes

Présenté par

✍ **Mlle. DRIS Chima** ✍ **Mlle. BOUGHERARA Khedidja**

Thème

Proposition et Evaluation d'un système biométrique de reconnaissance à base d'empreintes des articulations des doigts.

Soutenu publiquement le 22/06/2023 devant le Jury composé de :

Nom et Prénom	Grade	fonction	Université
Mr. CHAA Mourad	MCB	Président de Jury	UKMO
Mr. BENSID Khaled	MCA	Examinateur	UKMO
Mr. TIDJANI Zakaria	MAA	Encadreur	UKMO

Année Universitaire : 2022 /2023

« Celui qui emprunte un chemin menant à l'apprentissage d'une science, Allah lui facilite l'accès au paradis. »

Notre prophète Mohammed ﷺ

Dédicaces

بسم الله الرحمن الرحيم

الحمد لله وكفى والصلاة على الحبيب المصطفى وأهله ومن وفى أما بعد.

الحمد لله الذي وفقني لتثمين هذه الخطوة في مسيرتي الدراسية هذه ثمرة الجهد والنجاح بفضله تعالى مهداة:

إلى من أدين بحياتي ونجاحي واحترامي له والدي العزيز **" بلقاسم"**.

إلى من جعل الله عزوجل الجنة تحت أقدامها والتي غمرتني بالحب والحنان والتي سعت جاهدة في اسعادي أمي الحبيبة **"جميلة "**.

إلى اخواتي وإخوتي الأعزاء الذين دعموني و شجعوني وساندوني طوال سنوات دراستي ولا يزالون.

إلى روح الفقيد **" جدي"** (رحمة الله عليه).

إلى جدتي وعماتي وأعمامي وخالاتي وأخوالي حفظهم الله ورعاهم ورزقهم الحياة السعيدة المليئة بالأفراح.

إلى زوج أختي على التشجيع والمساعدة التي قدمها لي دائما.

إلى أفراد عائلتي الكبيرة وكل من يحمل لقب دريس، طهراوي وباعلي.

إلى من أعطى وأجزل بعطائه، إلى من سقى وروى عقلنا علما وثقافة، إلى من ضحى بوقته وجهده الاستاذ **"التجاني ز."** زاد ك الله من علمه وفضله ونعمه أستاذي الفاضل.

إلى زملائي في دفعة **2023** وجميع معلمي الدراسة الذين تعلمت منهم الكثير.

إلى صديقتي الغالية والأعز الى قلبي شكرا على وجود ك في حياتي يا أعز وأغلى البشر **"خديجة بوغرارة "** دمت لي يا صديقتي.

Dédicaces

بسم الله الرحمن الرحيم

والصلاة والسلام على أشرف الأنبياء والمرسلين سيدنا محمد صلى الله عليه وسلم.

إلى الله بي المعين صاحب العظمة شكرا وحمدا بحجم السماء والأرض على نعمك العظيمة يالله.

إلى روح جدتي الطاهرة طيب الله ثراك ياغالية.

إلى الذي بين الرجال هو في الصف الأول الى الذي يكفيني فخرا أني أحمل اسمه أبي الغالي

" زهر "

إلى تلك الصامدة القوية الى كل حنان العالم أمي الغالية

" بن نجمة فاطمة الزهراء " شكرا ايتها الجنة

الى سندي واكتافي في هذه الحياة اخواتي وأخي وخاصة الى اختي عزيزتي الغالية **"نور الهدى"** وزوجها

والى نور وحبيبة العائلة الكتكوتة زينب حفظها الله.

إلى المميز الموسوعة الثرية الاستاذ **"التجاني ز."** حفظك الله وزادك علوا على علو استاذي الفاضل.

إلى توأم الروح وصديقة العمر وشريكة كل خطوة في إنجاز هذه المذكرة أختي التي لم تلدها أمي

"شيماء ويس"

إلى كل صديقاتي كل طلاب دفعة تخصص آلية وأنظمة **2023**.

Khedidja

Remerciements

Merci d'abord à **Dieu**, notre grand Seigneur, qui a éclairé nos chemins avec la lumière de la connaissance. **Dieu** merci.

Nous tenant à remercier sincèrement **Mr**. **TIDJANI Z.** et tous sont qui nous ont été tous le temps à l'écoute et très disponible tout au long de la réalisation de ce mémoire, Ils nous ont accompagnés à chaque étape avec d'excellents conseils et de précieuses informations. Merci du fond du cœur pour tous vos efforts et votre patience avec nous afin de compléter ce travail de fin d'études, ainsi pour l'inspiration, l'aide et le temps qu'ils ont bien voulu nous consacrer et sans quoi, ce n'aurait jamais vu le jour.

Nous tenions à remercier **Dr. CHAA Mourad** président de jury et également **Dr. BENSID K.** examinateur de notre travail d'avoir accepté de juger ce travail.

Nous tenons également à remercier nos professeurs pour la qualité de l'enseignement qu'ils nous ont prodigué au cours de ces cinq années que nous avons passées à l'université **Kasdi Merbah-Ouargla**, ainsi que les responsables et l'ensemble du personnel dudit Département.

Nous n'oublions pas nos parents pour leur contribution, leur soutien et leur patience.

Enfin, nous adressons nos plus sincères remerciements à tous nos proches et amis, qui nous ont toujours encouragés au cours de la réalisation de ce mémoire.

ملخص

تلعب القياسات البيو مترية التي تعتمد على اليد دورًا مهمًا في إرساء الأمان للبيئات في الوقت الفعلي والتي تتضمن تفاعلًا بشريًا وتعتبر ذات أداء أفضل من حيث السرعة والدقة. تم تطوير العديد من أنواع أنظمة القياسات البيو مترية الأحادية. ومع ذلك، فإن هذه الأنظمة قادرة فقط على توفير مستوى منخفض إلى متوسط من الأمان. وبالتالي، لتحقيق مستوى أمان أعلى، من الضروري الجمع بين اثنين أو أكثر من القياسات البيو مترية الأحادية (طرق متعددة). أصبح التعرف على الأفراد من خلال بصمات الأصابع من الجهة الظهرية مجالًا نشطًا جدًا للبحث في السنوات الأخيرة. تعد بصمة مفصل الإصبع (FKP) واحدة من الخصائص البيو مترية ذات التفرد الكافي للتعرف على الهوية الفردية. يقدم هذا العمل طريقة جديدة للتعرف والتحقق من الهوية بناءً على اندماج البصمات الثانوية والرئيسية لـ FKP. في هذا النظام، نستخدم خوارزميتين، وهما مرشح Gabor وميزات الصورة الإحصائية الثنائية (BSIF)، في خطوة استخراج المميزات. ولتحسين أداء المخطط المقترح، تم استخدام طريقة تحليل المكونات الرئيسية (PCA) + تحليل التمييز الخطي (LDA) الذي تم استعماله في خطوة تقليص الأبعاد. أخيرًا، أثناء خطوة المقارنة، تم استخدام مصنف أقرب جار (K-NN) بناءً على مسافة جيب تمام ماهالانوبيس (Mahcos). بالإضافة إلى ذلك، تم اقتراح نظام اندماج على مستوى النتائج يعتمد على المقاييس البيو مترية المتعددة. تم تطبيق مجموعة من القواعد لتحسين أداء التعرف على الأشخاص. وتم تقييم النظام في قاعدة البيانات العامة للبصمات المشتركة لمفاصل الأصابع الثانوية / الرئيسية.

الكلمات الرئيسية: القياسات البيو مترية متعددة الوسائط، مرشح Gabor، واصف BSIF، PCA + LDA، K-NN، Mahcos، أول مفصل ثانوي ومفصل إصبع رئيسي. الدمج على مستوى النتيجة.

Abstract

Hand-based biometrics play a crucial role in establishing security for real-time environments involving human interaction and are considered more efficient in terms of speed and accuracy. While several types of unimodal biometric systems have been developed, they can only provide a low to moderate level of security. To achieve higher security, combining two or more unimodal biometrics (multimodalities) is necessary. Recognition of individuals through fingerprints on the dorsal side has become a very active field of research in recent years. Finger Knuckle Print (FKP) is a biometric feature with sufficient uniqueness for individual recognition. This work presents a novel method for FKP recognition and verification based on fusing the minor and major first knuckle prints. The system utilizes two algorithms, namely the Gabor filter and binary statistical image features (BSIF), for feature extraction. To enhance the performance of the proposed scheme, principal component analysis (PCA) + linear discriminant analysis (LDA) is applied for dimensionality reduction. In the matching stage, the nearest neighbor classifier (K-NN) based on the Mahalanobis cosine distance (Mahcos) is employed. Furthermore, a score-level fusion system based on multimodal biometrics is proposed, and a set of rules is applied to improve recognition performance. The system is evaluated on the publically first minor / major Kunckel database.

Keywords : Multimodal biometrics, Gabor filter, BSIF descriptor, PCA+LDA, K-NN, Mahcos, first minor knuckle and major knuckle, score-level fusion.

Résumé

Les biométriques basées sur la main jouent un rôle important dans l'établissement de la sécurité pour les environnements en temps réel impliquant une interaction humaine et sont considérées comme plus performantes en termes de vitesse et de précision. De nombreux types de systèmes biométriques unimodaux ont été développés. Cependant, ces systèmes ne sont capables de fournir qu'un niveau de sécurité faible à moyen. Ainsi, pour obtenir une sécurité plus élevée, la combinaison de deux ou plusieurs biométriques unimodales (modalités multiples) est nécessaire. La reconnaissance des individus à travers les empreintes des doigtes sur la face dorsale est devenue un domaine de recherche très actif ces dernières années. Une des caractéristiques biométriques avec une unicité suffisante pour la reconnaissance de l'individualité est l'empreinte des articulations des doigts (FKP). Ce travail présente une nouvelle méthode de reconnaissance et de vérification de l'individualité basée sur la fusion des empreintes première mineures et majeures du FKP. Dans ce système, nous utilisons deux algorithmes, à savoir le filtre de Gabor et les caractéristiques d'images statistiques binarisées (BSIF), dans l'étape d'extraction des caractéristiques. Pour améliorer les performances du schéma proposé, la méthode de l'analyse en composantes principales (PCA) + analyse discriminante linéaire (LDA) a été utilisée dans l'étape de réduction de dimensionnalité. Enfin, lors de l'étape de comparaison, le classifieur du plus proche voisin (K-NN) basé sur la distance de Mahalanobis cosinus (Mahcos) a été utilisé .De plus, un système de fusion au niveau des scores basé sur une multi-biométrie a été proposé. Un ensemble des règles ont été appliquées pour améliorer les performances de reconnaissance. Le système a été évalué une la base de données publique des empreintes articulaires Première mineures/Majeures.

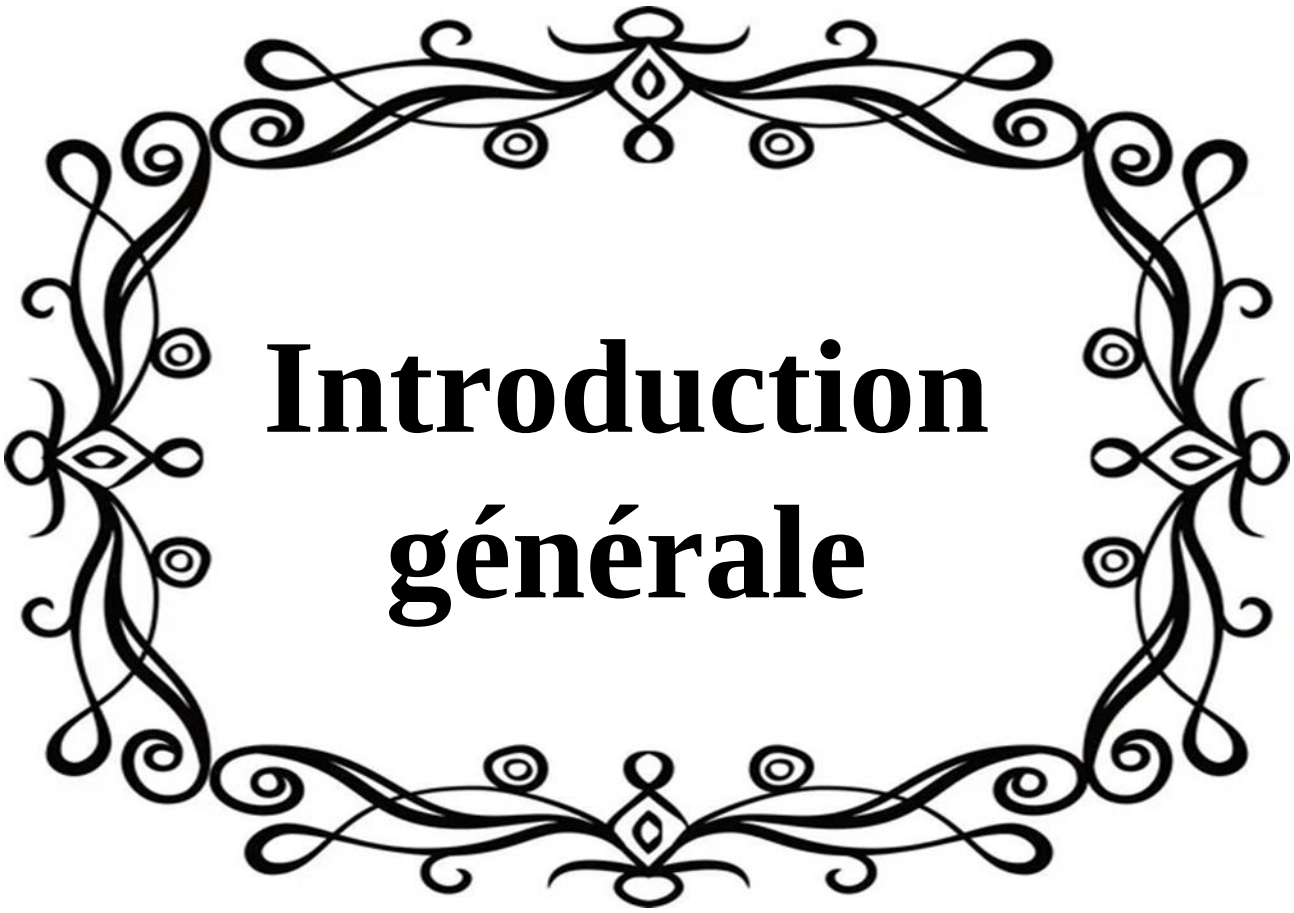
Mots-clés : Biométrie multimodale, Filtre de Gabor, Descripteur BSIF, PCA+LDA, K-NN, Mahcos, Première articulation mineure et articulation majeure du doigt. Fusion au niveau des scores.

Chapitre 2 : Des algorithmes et des Outils employés dans les systèmes biométriques

Chapitre 3 : Système biométrique proposé et Expérimentation

Liste des acronymes utilisés

ADN :	**A**cide **D**ésoxyribo **N**ucléique.
ASSR :	**A**daptive **S**ingle **S**cale **R**etinex.
BSIF :	**B**inarized **S**tatistical **I**mage **F**eatures (Caractéristiques d'images statistiques binarisées).
CMC :	**C**umulative **M**atch **C**urve (Courbe de correspondance Cumulative).
Deep CNN :	**Deep C**onvolutional **N**eural **N**etwork (Apprentissage approfondie des réseaux de neurones).
DIP :	**D**istal **I**nter **P**halangeal (Articulation inter-phalangienne distale).
EER :	**E**qual **E**rror **R**ate (Taux d'égale erreur).
FAR :	**F**alse **A**ccept **R**ate (Taux de fausses acceptations).
FKP :	**F**inger **K**nuckle **P**rint (Empreinte des articulations des doigts).
FRR :	**F**alse **R**eject **R**ate (Taux de faux rejets).
HOG :	**H**istogram of **O**riented **G**radient (Histogrammes d'orientation de Gradient).
IP :	**I**nter **P**halangea (Inter-phalangienne).
K-NN :	**K- N**earest **N**eighbors (K plus proches voisins).
LDA :	**L**inear **D**iscriminants **A**nalysis (Analyse discriminante linéaire).
LFD :	**L**ocal **F**eature **D**escriptor (Descripteur de caractéristique local).
MCP :	**M**eta **C**arpo **P**halangeal (Articulations métacarpo-phalangiennes).
PIP :	**P**roximal **I**nter **P**halangeal (Articulation inter-phalangienne proximale).
PCA :	**P**rincipal **C**omponents **A**nalysis (Analyse en composants principales).
ROC :	**R**eceiver **O**perating **C**haracteristic (Courbe Caractéristique de Fonctionnement du Récepteur).
ROI :	**R**egion **O**f **I**nterest (Région d'intérêt).
TPLBP :	**T**hree-**P**atch **L**ocal **B**inary **P**attern (Motif binaire local à trois patchs).



Introduction générale

Introduction générale

La sécurité des systèmes d'information est devenue un domaine de recherche d'une très grande importance. La conception d'un système d'identification fiable, efficace et robuste est une tâche prioritaire. L'identification de l'individu est essentielle pour assurer la sécurité des systèmes et des organisations.

Dans son environnement quotidien, un individu a besoin de s'identifier dans une multitude de contextes : accéder à un aéroport, entrer dans des endroits militaires, entrer à son lieu de travail, pour retirer de l'argent à un distributeur ou payer en magasin, pour demander un service social…Autant de codes et de mots de passe à mémoriser et à protéger. Afin de développer les moyens de reconnaissance, la recherche connaît depuis quelques années un renouveau spectaculaire et manifeste un intérêt majeur aux données **"biométriques",** c'est-à-dire aux caractéristiques propres à chaque personne : sa voix, ses empreintes digitales, les traits de son visage, la forme de sa main, sa signature et même son ADN. Cependant, plus récemment, l'augmentation de la fraude à l'identité a créé un besoin croissant de la technologie biométrique dans un certain nombre d'applications nécessitant un haut degré de sécurité : accès à des sites sensibles, surveillance d'aéroport...

L'identification humaine avec des systèmes biométriques multimodaux est un sujet de recherche passionnant et intéressant ces dernières années. La multimodalité est définie comme l'utilisation de plusieurs systèmes biométriques. Le principal objectif de la fusion de divers systèmes biométriques est de réduire les limites de la biométrie unimodale qui souffrent souvent de certains problèmes tels que la variation intra-classe, les données bruitées, les taux d'erreur inacceptables, etc. En effet, la combinaison de différents systèmes biométriques vise à améliorer les performances de reconnaissance en augmentant la quantité de données discriminantes de chaque personne, et à réduire le risque d'échec de l'enregistrement et la robustesse face aux fraudes.

En générale, la biométrie à base des traits de la main peut être divisée en deux grandes catégories : la partie palmaire et la partie dorsale. La première recouvre les zones proches de la paume. Les attributs biométriques largement utilisés extraits de cette partie de la main sont : L'empreinte digitale, palmaire, des veines du doigt, des veines de la paume, et des articulations du doigt palmaire. Par contre, la partie dorsale de la main occupe la zone située derrière la partie palmaire et la plupart des modalités biométriques utilisables de cette partie sont les suivantes : la géométrie de la main, les veines des mains et l'empreinte des articulations dorsale des doigts ou

FKP. En plus, les combinaisons des traits ci-dessus ont été aussi utilisées comme traits biométriques liés à une main. Cependant, les personnes laissent leurs traits biométriques liés à la partie palmaire tels que l'empreinte digitale inconsciemment partout où elles se touchent, ce qui augmente les possibilités d'attaques par des imposteurs sur ces systèmes de sécurité. En outre, cette zone est également plus exposée aux accidents, ce qui entraîne la perte de certaines de ces caractéristiques. Les modalités biométriques de la partie dorsale de la main gagnent donc en popularité. Par conséquent, les modalités biométriques de la partie dorsale de la main deviennent de plus en plus populaires. En raison de l'acquisition sans contact, ils ont moins de chance d'attaques d'imposteurs. Et comme il s'agit d'une zone inactive de la main, le risque de dégradation de l'information est réduit.

Dans ce travail, le FKP a été choisi comme sujet d'étude. Le FKP fait référence aux motifs de peau présents à la surface externe autour de l'articulation phalangienne du doigt et contient des caractéristiques structurelles distinctives, telles que des motifs de texture. En général, ces caractéristiques possèdent des aptitudes potentiellement discriminatoires et conviennent relativement bien à l'identification d'une personne par rapport aux autres.

Ce travail a pour objectif l'étude et la réalisation de système biométrique monomodale ou bien multimodale efficace et rapide, basé sur la fusion au niveau des scores. L'approche proposée utilise l'algorithme du filtre de Gabor et celui de la méthode de caractéristiques d'images statistiques binarisées (BSIF) dans l'étape d'extraction des caractéristiques. Ensuite, pour la réduction de la dimensionnalité, la technique analyse en composants principales + analyse discriminante linéaire (PCA+LDA) est utilisée. La méthode K plus proches voisins (K-NN) est utilisée pour la classification en se basant sur la distance de Mahalanobis cosinus (Mahcos). Enfin, plusieurs méthodes de fusions seront appliquées pour en choisir la plus efficace.

Ce mémoire se décompose en trois chapitres :

Le **premier chapitre** sera consacré à une introduction aux systèmes de reconnaissance biométrique, un aperçu sur la multimodalité, ses différentes architectures et ses différents niveaux de fusion possibles. Nous présenterons à la fin du chapitre, les techniques de mesure des performances des systèmes biométriques.

Le **deuxième chapitre** donnera un aperçu succinct des systèmes biométriques basés sur les traits FKP avec explication de ce choix. De même, nous présenterons un état de l'art des systèmes basés sur cette modalité. Par la suite, nous allons exposer les méthodes utilisées pour l'extraction des caractéristiques, la réduction de dimensionnalité, ainsi qu'une méthode pour la classification des

scores.

Dans le **troisième chapitre**, nous mettrons en avant le système proposé pour notre travail, tous en expliquant le processus d'extraction de la région d'intérêt. Nous décrirons également en détail la base de données utilisée ainsi que les mesures d'évaluation que nous allons employer. En outre, nous présenterons les résultats des tests effectués sur les systèmes unimodaux en utilisant les deux algorithmes d'extraction des caractéristiques : filtre de Gabor et BSIF de manière individuelle. Nous aborderons également les systèmes multimodaux qui reposent sur la fusion au niveau des scores obtenus. Nous terminerons ce chapitre par une étude comparative avec les travaux antérieurs.

A la fin, ce mémoire sera terminé par une conclusion générale avec présentation des perspectives de travail.

Chapitre 1 : Généralités sur les systèmes biométriques

1.1. Introduction

Au fil du temps, l'être humain a toujours essayé d'améliorer sa vie dans plusieurs domaines, notamment en matière de sécurité.

Avec le développement technologique rapide, la sécurité devient l'un des problèmes les plus préoccupants de notre société et pose un problème délicat aux citoyens, aux entreprises et au gouvernement dans la protection des informations sensibles et des données sensibles contre le vol. Pour toutes ses raisons, il était nécessaire de créer une nouvelle technique de contrôle. Ainsi, le système biométrique a connu naissance comme candidat pour constituer une solution efficace.

Dans ce chapitre, nous allons présenter quelques notions et définitions de base liées à la biométrie, nous donnerons les modalités biométriques utilisées, leurs phases et modes de fonctionnement, et nous présenterons une étude détaillée sur les systèmes biométriques multimodaux et leur différentes architectures. Nous allons examiner les différents niveaux de fusion, aussi, nous présenterons les outils utilisés pour mesurer les performances de ces systèmes biométriques.

1.2. C'est quoi la biométrie ?

Etymologiquement, le terme biométrie se compose du terme « bio » (du grec ancien βίος qui signifie « vie ») et du terme « métrie » (du grec ancien μέτρον, qui signifie « mesure ») [1]. Ainsi, dans son sens premier, biométrie signifie «mesure du vivant» et fait référence à l'étude scientifique et quantitative du monde vivant et des êtres vivants d'une manière plus simplifiée, la biométrie signifie la "mesure du corps humain".

La biométrie fait maintenant surtout référence à l'ensemble des techniques utilisées pour identifier un individu grâce à certaine de ses caractéristiques **biologiques**, **comportementales et morphologiques** [1].

Pour assurer leurs fiabilités, les modalités biométriques doivent être déterminées par quelques caractéristiques. Parmi les propriétés d'une modalité biométrique, on trouve [2] :

- **Universalité :** toute personne ayant accès à l'application doit posséder le trait.
- **Unicité :** le trait doit être suffisamment différent d'une personne à une autre.
- **Permanence :** le trait biométrique d'une personne doit être suffisamment invariant au cours d'une période de temps.
- **Mesurabilité :** il devrait être possible d'acquérir et de numériser les données biométriques à l'aide d'un dispositif approprié.

- **Performance :** la précision de la reconnaissance et les ressources nécessaires pour atteindre la précision que doit satisfaire les contraintes imposées par l'application.
- **Acceptabilité :** les individus qui vont utiliser cette application doivent être disposés à présenter leurs traits biométriques au système.
- **Contournement :** il s'agit de la facilité avec laquelle le caractère d'un individu peut être imité en utilisant des objets (par exemple : faux doigts dans le cas de traits physiques et le mimétisme, dans le cas de traits de comportement) [3].

1.3. Principaux modalités biométriques

Il existe plusieurs modalités biométriques utilisées dans divers secteurs, nous pouvons distinguer trois grandes catégories. **La Figure.1.1** présente les différents traits biométriques classées en trois catégories.

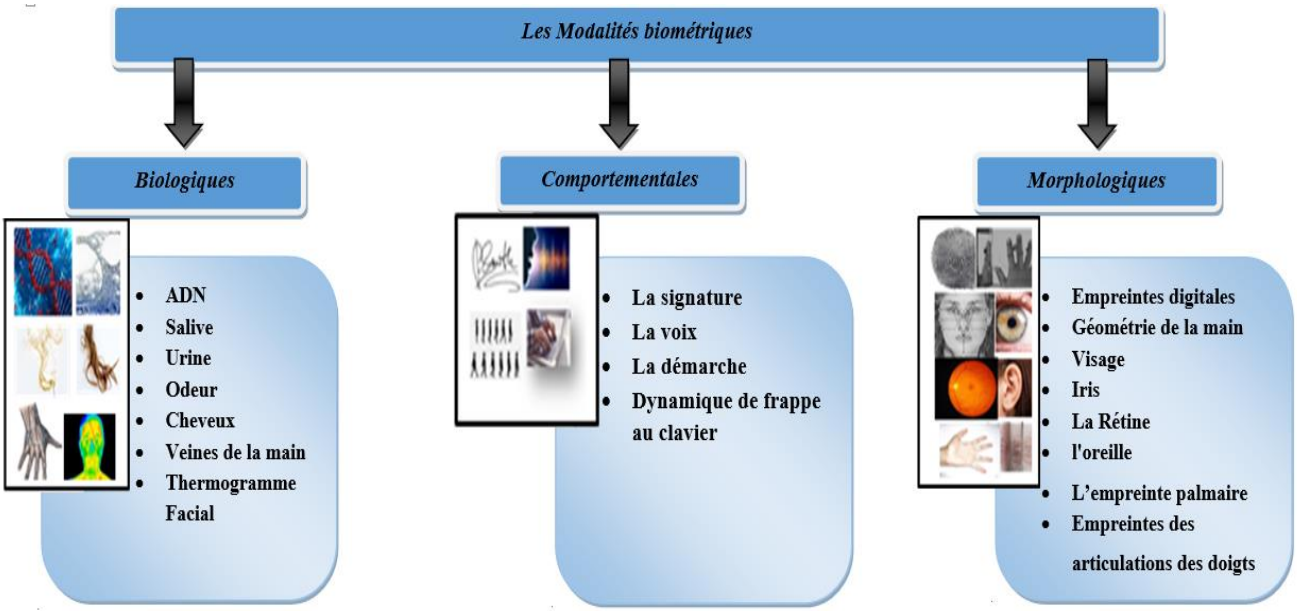


Figure. 1.1 : Exemple des traits biométriques classés en catégories.

Pour cela, nous définissons trois catégories de la modalité biométrique principale comme suit :

1.3.1. Modalités biologiques

Ces modalités basées sur les caractéristiques biologiques des individus (ADN, salive, urine, odeur…). Ce type de biométrie est très complexe à mettre en œuvre dans un système usuel de reconnaissance et n'est utilisé que dans un cas d'extrême nécessité (ex. : Enquête criminelle, test de paternité…etc.)[4].

a. ADN

L'ADN ou Acide Désoxyribo Nucléique (voir **Figure.1.2**), c'est une molécule qui porte l'information génétique propre à chaque individu. C'est une analyse caractérisée par la précision de

ses résultats, car son taux d'erreur est beaucoup plus faible que les autres analyses biologiques, ce qui, bien sûr, aidera à identifier l'identité par excellence et est beaucoup utilisé dans le domaine de la médecine légale.

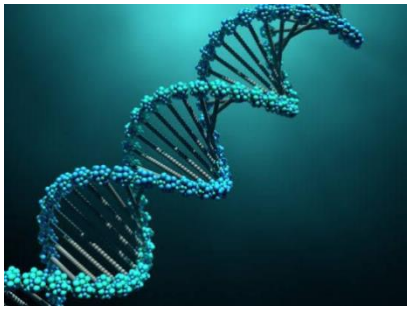


Figure.1.2 : l'ADN.

1.3.2. Modalités comportementales

Ces modalités se basent sur l'analyse de certains comportements d'une personne comme le tracé de sa signature, l'empreinte de sa voix, sa démarche et sa façon de taper sur un clavier [5].

a. Démarche

Il s'agit de reconnaître un individu par sa façon de marcher et de bouger (vitesse, accélération, mouvements du corps…), en analysant des séquences d'images. La démarche serait en effet étroitement associée à la musculature naturelle et donc très personnelle. Mais des vêtements amples, par exemple, peuvent compromettre une bonne identification [6]. **La Figure. 1.3** montre un exemple des squelettes de démarche.

Figure.1.3 : Exemple de squelettes de démarche.

b. Voix

La voix est une caractéristique extrêmement recherchée dans des systèmes liés à des applications à distance où la personne s'authentifie par téléphone par exemple. Elle est toutefois une caractéristique très délicate à utiliser car elle est extrêmement soumise aux conditions extérieures (maladie, stress de la personne, etc.). De ce fait, elle est une caractéristique à la fois physique et comportementale. Elle est parfois choisie en combinaison avec une autre caractéristique (voix et écriture par exemple) (voir **Figure.1.4**) [7].

Figure.1.4 : Signal de voix.

1.3.3. Modalités morphologiques (physiologiques)

Ces modalités sont uniques et permanentes. Leur principe est basé sur l'identification de traits physiques particuliers de la personne, par exemple la forme de l'oreille, la forme de la main, voir aussi la forme du visage, les empreintes digitales, l'iris, la rétine, etc.

a. Empreintes digitales

Une empreinte digitale est constituée d'un ensemble de lignes localement parallèles formant un motif unique pour chaque individu (voir **Figure.1.5**), on distingue les stries (ou crêtes, ce sont les lignes en contact avec une surface au toucher) et les sillons (ce sont les creux entre deux stries). Les stries contiennent en leur centre un ensemble de pores régulièrement espacés.

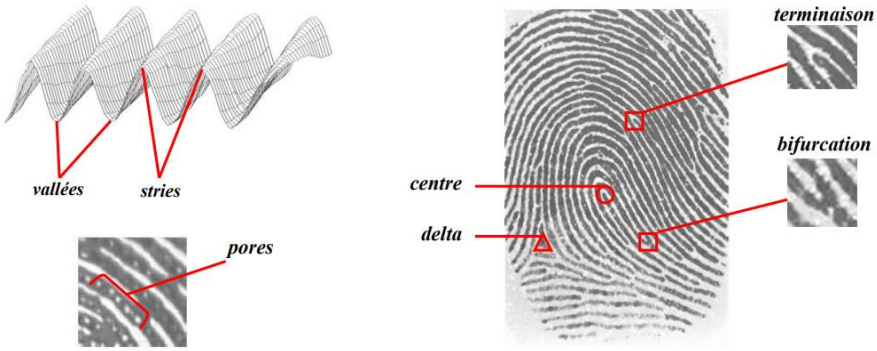


Figure.1.5 : Les caractéristiques de l'empreinte digitale.

Chaque empreinte possède un ensemble de points singuliers globaux (les centres et les deltas) et locaux (les minuties). Les centres correspondent à des lieux de convergences des stries tandis que les deltas correspondent à des lieux de divergence. Une étude a montré l'existence de seize types de minuties différentes mais en général les algorithmes ne s'intéressent qu'aux bifurcations et terminaisons qui permettent d'obtenir les autres types par combinaison [8].

b. Visage

Le visage est la biométrie la plus commune et la plus populaire. Elle reste la plus acceptable puisqu'elle correspond à ce que les humains utilisent dans l'interaction visuelle. Les caractéristiques jugées significatives pour la reconnaissance du visage sont : les yeux, la bouche et le tour du visage (voir **Figure.1.6**). Le problème de cette méthode vient des possibles perturbations pouvant transformer le visage (maquillage, faible luminosité, présence d'une barbe ou des lunettes, expression faciale inhabituelle, changement avec l'âge, etc.).

Cette technologie est employée dans des domaines très variés allant du contrôle d'accès physique comme la sécurisation des lieux ou logique comme la sécurisation d'une session informatique à la surveillance ou l'accès aux distributeurs automatiques de billets [9].

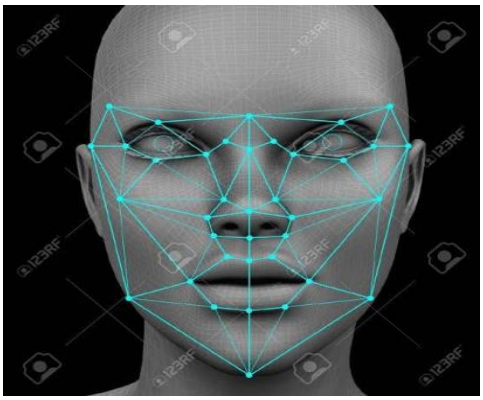


Figure.1.6 : La reconnaissance du Visage.

c. Empreintes des articulations des doigts

C'est une technologie biométrique basée sur la surface arrière du doigt, également connue sous le nom de dos de la main ou Finger Knuckle print (FKP) 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 [10].

La Figure. 1.7 illustre les articulations métacarpo-phalangiennes (MCP) connues sous le nom la deuxième articulation mineure (articulation de base), l'articulation inter-phalangienne proximale (PIP) connue sous le nom d'articulation majeure, l'articulation inter-phalangienne distale (DIP) connue sous le nom la première articulation mineure, et l'inter-phalangienne (IP) connue sous le nom d'articulation majeure du pouce). Les articulations des doigts ont des motifs spécifiques, qui comprennent des plis, des courbes, des lignes et des textures.

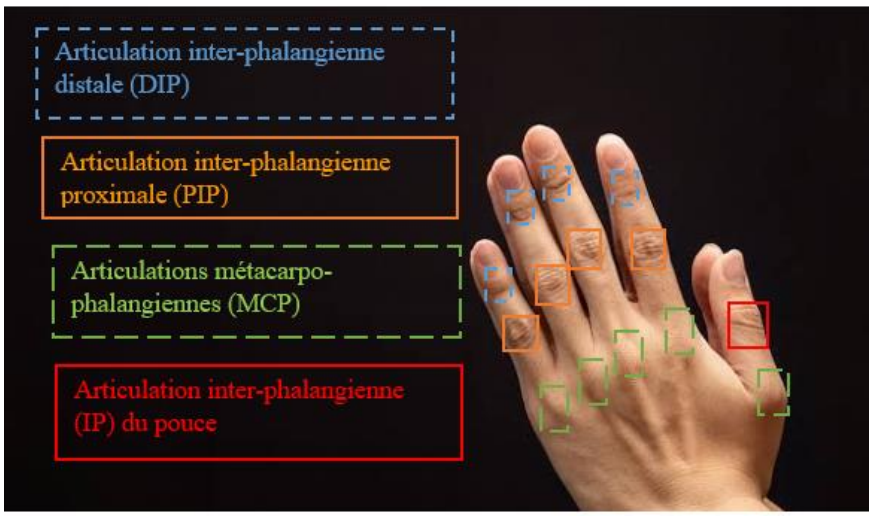


Figure. 1.7 : Illustration de la surface dorsale des articulations des doigts.

1.4. Phases et Modes de fonctionnement du système biométrique

Un système biométrique est un système de reconnaissance des formes qui procède en premier par l'acquisition des données biométriques de l'individu à reconnaître, puis extrait un ensemble de caractéristiques à partir de celles-ci, enfin il compare ces caractéristiques avec les modèles de la base de données [5].

Selon le contexte de l'application, un système biométrique peut fonctionner soit en mode **vérification** ou **identification**. Tout système biométrique comporte deux phases (processus) qui se chargent de réaliser les opérations **d'enrôlement** et de **reconnaissance** [9].

1.4.1. La phase d'enrôlement (d'apprentissage)

Cette phase consiste à créer un modèle biométrique d'un individu qui doit être une référence pour la phase de reconnaissance.

Pour ce faire, les caractéristiques biométriques de l'individu sont mesurées par un capteur biométrique, puis représentées sous forme numérique (signatures) et enfin stockées dans une base de données (voir **Figure.1.8**).

Pour assurer une certaine puissance du système aux variations temporelles de données, plusieurs échantillons d'acquisitions de la même donnée peuvent être réalisés.

Le traitement lié à l'enrôlement n'a pas de contrainte de temps, puisqu'il s'effectue «hors-ligne» [11].

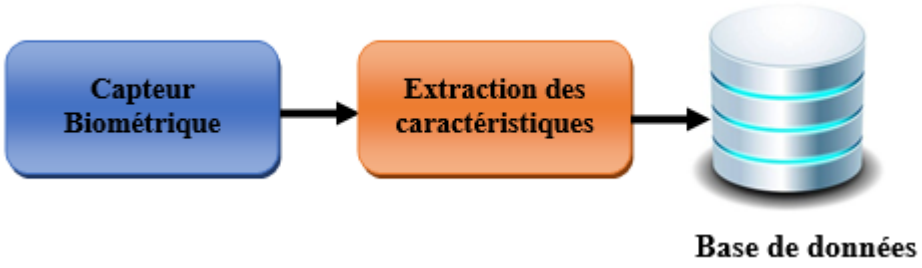


Figure.1.8 : La phase enrôlement d'un système biométrique.

1.4.2. La phase de reconnaissance (de test)

Opération se déroulant à chaque fois qu'une personne se présente devant le système, elle consiste en l'extraction d'un ensemble de caractéristiques comme pour l'étape d'apprentissage suivie d'une autre étape de comparaison et de prise de décision selon le mode opératoire du système [12]. La reconnaissance peut être **une vérification** ou **une identification**.

1.4.2.1. Le mode de vérification (d'authentification)

La vérification est une comparaison "1 à 1", dans lequel le système valide l'identité d'une personne en comparant les données biométriques saisies avec le modèle biométrique de cette personne stocké dans la base de données du système [11]. Dans un tel mode, le système doit répondre à une question de type : "Suis-je bien la personne que je prétends être ?". L'utilisateur propose une identité au système et le système doit vérifier que l'identité l'individu est bien celle proposée [13]. Le mode est illustré par **la Figure. 1.9.**

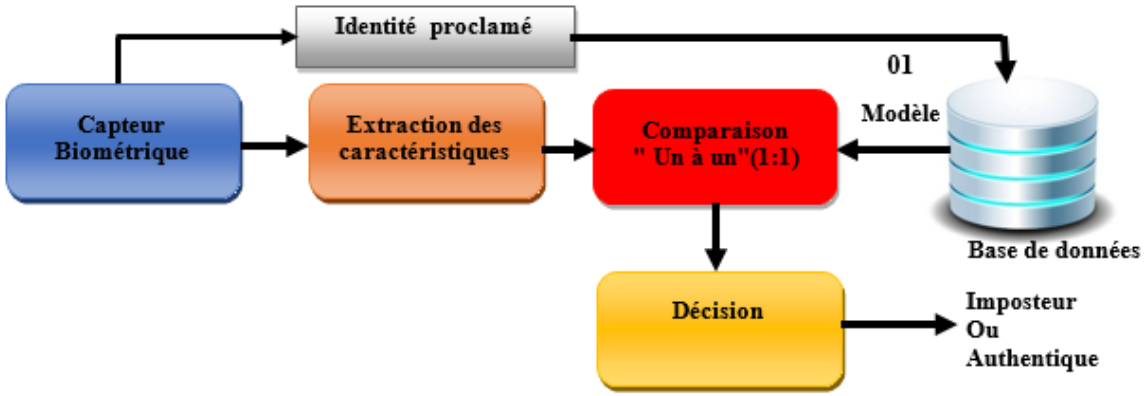


Figure.1.9 : Le mode vérification d'un système biométrique.

1.4.2.2. Le mode d'identification

L'identification permet d'établir l'identité d'une personne à partir d'une base de données. En d'autres termes, elle répond à des questions de type : « Qui suis-je ? ». Dans ce mode, le système compare le signal mesuré avec les différents modèles contenus dans la base de données, il s'agit d'une comparaison (1 à N) [11] [13]. Le mode est illustré par **la Figure.1.10.**

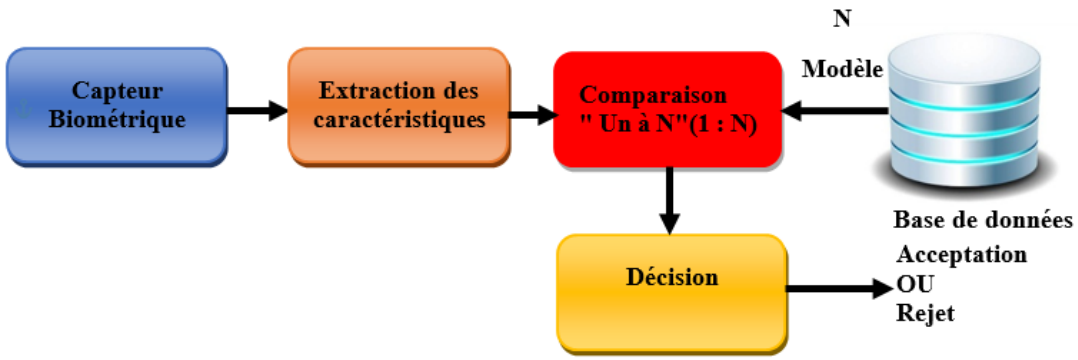


Figure.1.10 : Le mode identification d'un système biométrique.

Un tel système d'identification biométrique peut fonctionner selon deux modes d'identification : **en ensemble fermé** ou **en ensemble ouvert.**

a. Identification en ensemble fermé

C'est-à-dire que l'on est sûr que le personne appartient à la base de données des autorisés et le problème revient à déterminer laquelle des identités correspond au mieux à ce personne. Si l'échantillon possédé un certain degré de similitude avec les échantillons dans le système, la personne sera acceptée.

b. Identification en ensemble ouvert

Puisque l'on suppose qu'un individu qui n'a pas de modèle dans la base de données (imposteur) peut chercher à être reconnu. Si la plus grande similarité entre l'échantillon et tous les modèles est inférieure à un seuil de sécurité minimum fixé, la personne est rejetée, ce qui implique que l'utilisateur n'était pas une des personnes enrôlées par le système.

1.5. Structure d'un système biométrique

Un système biométrique est composé de cinq modules principaux :

a. Module de capteur biométrique

C'est un capteur chargé d'obtenir les données vitales des individus, qui peut se présenter sous la forme d'une caméra ou d'un lecteur d'empreintes digitales.

b. Module d'extraction des caractéristiques

C'est un capteur qui utilise les informations et les données générées par l'unité de capteur biométrique et les extraits pour finalement former une nouvelle représentation afin que chaque personne ait sa propre représentation.

c. Module de comparaison

Dans ce module, les valeurs des caractéristiques sont comparées à celles du modèle en générant un score de comparaison [14]. Le module de comparaison encapsule également un module de prise de décision, dans lequel l'identité revendiquée par un utilisateur est confirmée (vérification) ou l'identité d'un utilisateur est établie (identification) en fonction du score de comparaison [15].

d. Module de base de données

Il sert de dépôt des signatures biométriques obtenues lors de la phase d'enrôlement. Cette phase permet d'inscrire dans la base de données les informations biométrique et biographique (nom et prénom, n° d'identification, adresse…) des utilisateurs. Dans un sens figuré, ce module joue le rôle d'un annuaire des signatures biométriques [16].

e. Module de décision

Il vérifie l'identité affirmée par un utilisateur ou détermine l'identité d'une personne basée sur le degré de similitude entre les caractéristiques extraites et le(s) modèle(s) stocké(s) [6].

1.6. La biométrie multimodale

Face aux nombreuses limitations imposées par l'utilisation des systèmes biométriques unimodaux, la biométrie multimodale s'impose de manière indéniable comme une alternative d'avenir dans le domaine de la sécurité des personnes et leurs biens. Bien que le couplage des systèmes biométriques peut être effectué à différents niveaux, la fusion au niveau des scores est la plus courante puisqu'elle a été généralement prouvée plus efficace que le reste des niveaux de fusion.

La biométrie multimodale consiste à combiner plusieurs systèmes biométriques. Elle permet de réduire certaines limitations des systèmes biométriques, comme l'impossibilité d'acquérir les données de certaines personnes ou la fraude intentionnelle, tout en améliorant les performances de reconnaissance. Ces avantages apportés par la multi modalité aux systèmes biométriques "monomodaux" sont obtenus en fusionnant plusieurs systèmes biométriques [17].

1.6.1. Pourquoi la multimodalité ?

Bien que les techniques de reconnaissance biométrique promettent d'être très performantes, on ne peut garantir actuellement un excellent taux de reconnaissance avec des systèmes biométriques unimodaux, basés sur une unique signature biométrique. De plus, ces systèmes sont souvent affectés par les problèmes suivants [17] :

- Bruit introduit par le capteur.
- Non-universalité.
- Manque d'individualité.
- Manque de représentation invariante.
-Sensibilité aux attaques.

1.6.2. Les différents systèmes multimodaux

Le principe de la multimodalité au sens large est de combiner plusieurs sources d'information à partir de systèmes monomodaux. Selon les sources d'information combinées, cinq scénarios de multimodalité sont envisageables (voir **Figure. 1.11**) [18].

Dans les quatre premiers scénarios décrits ci-dessous, la fusion d'informations est réalisée à l'aide d'un seul trait, tandis que dans le cinquième scénario, plusieurs traits sont utilisés [15].

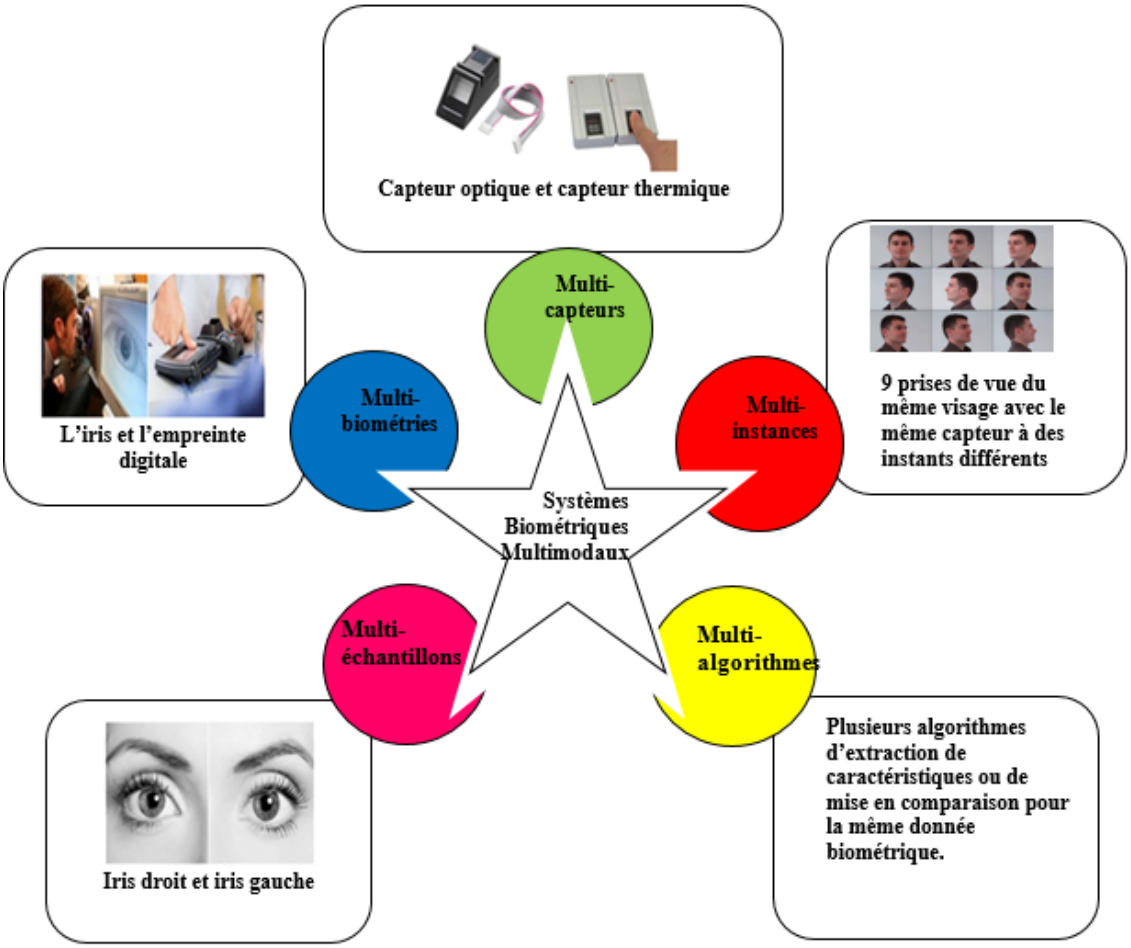


Figure. 1.11 : Les différents systèmes multimodaux.

a. Multi-capteurs

En cas de sélection de plusieurs capteurs dans un système biométrique afin d'obtenir des données. Par exemple un capteur optique et capteur thermique pour la reconnaissance d'empreintes digitales.

b. Multi-instances

En cas de choix de plusieurs positions ou directions pour prendre les informations pour la même caractéristique physique biométrique de la même personne. Par exemple l'acquisition de plusieurs images de visage avec des changements de pose, d'expression ou d'illumination.

c. Multi-algorithmes

Lorsque plusieurs algorithmes traitent la même image acquise, cette multiplicité des algorithmes peut intervenir dans le module d'extraction en considérant plusieurs ensembles de caractéristiques et/ou dans le module de comparaison en utilisant plusieurs algorithmes de comparaison [19].

d. Multi-échantillons

En cas de sélection de données différentes pour la même caractéristique biométrique, celle-ci doit être traitée avec le même algorithme [10]. C'est le cas par exemple de l'iris gauche et droit, ou deux empreintes digitales de doigts différents.

e. Multi-biométries

Dans le cas où plus d'une caractéristique biométrique (par exemple le visage et l'iris, l'iris et l'empreinte digitale etc.) est choisie, la force de ce choix réside dans l'augmentation de l'efficacité et de la sécurité des systèmes et leur protection contre la fraude.

1.6.3. 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 simultanément, ce qui est appelé **architecture en parallèle**, ou successivement, ce qui est appelé **architecture en série** [20].

a. Architecture en parallèle

C'est la plus utilisée car elle permet d'utiliser toutes les informations disponibles. 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 (voire **Figure.1.12**) [6].

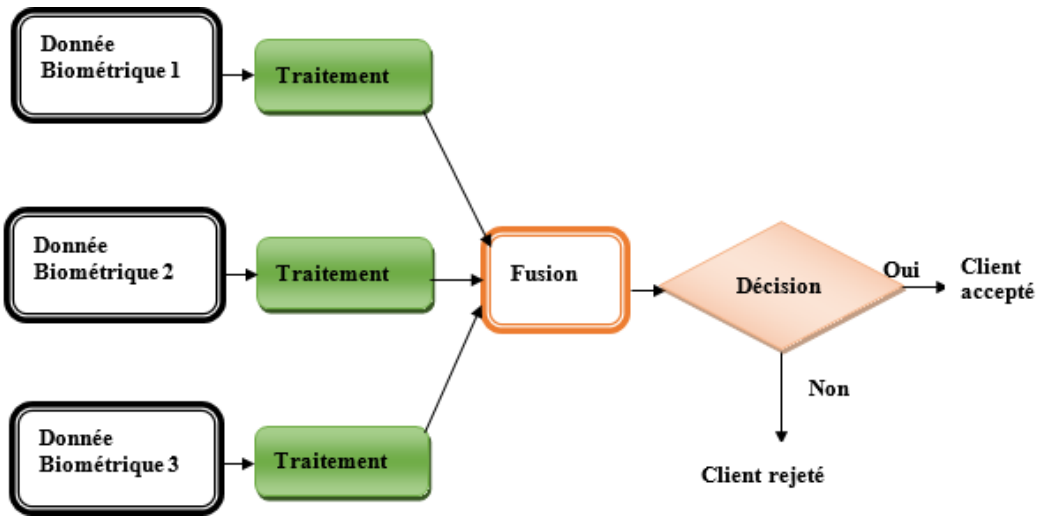


Figure. 1.12 : Architecture de fusion en parallèle.

b. Architecture en série

L'architecture en série peut être privilégiée dans certaines applications où la multimodalité est utilisée pour donner une alternative pour les personnes qui ne pouvant pas utiliser la modalité en question (voire **Figure.1.13**) [20].

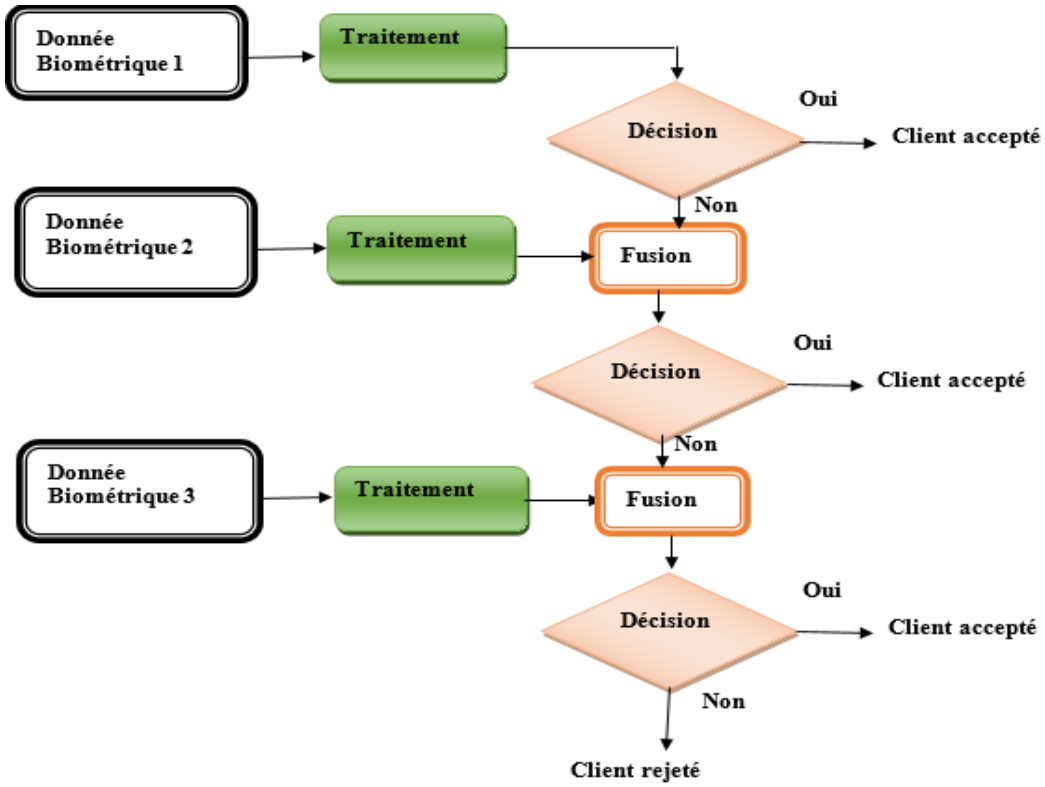


Figure. 1.13 : Architecture de fusion en série.

1.6.4. Les différents niveaux de fusion

Dans la littérature, différentes modalités peuvent être fusionnées afin d'améliorer la précision des systèmes biométriques. La fusion de plusieurs systèmes biométriques peut avoir lieu à quatre niveaux différents comme montre la **Figure.1.14.**

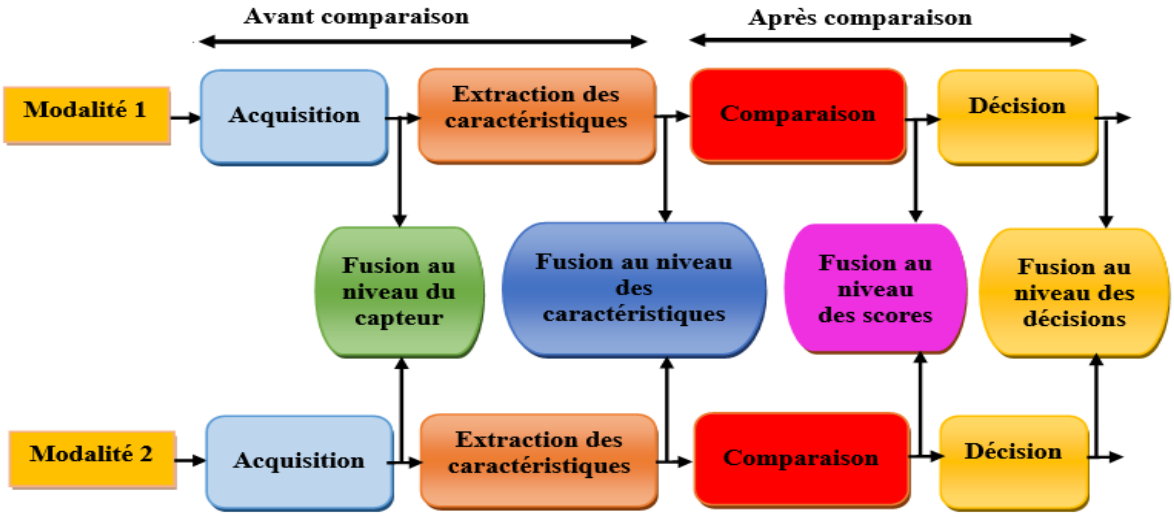


Figure.1.14 : Les différents niveaux de fusion dans un système biométrique multimodal.

Nous distinguons la fusion **au niveau du capteur**, **au niveau des caractéristiques** extraites, **au niveau des scores** correspondant et **au niveau des décisions**. Ces quatre niveaux peuvent être classés en deux sous-catégories, à savoir la fusion pré-classification (avant comparaison) et la fusion post- classification (après comparaison).

1.6.4.1. La fusion pré-classification (avant comparaison)

La fusion de pré-classification est la fusion des informations de plusieurs données biométriques **au niveau du capteur** (image brutes) ou **au niveau des caractéristiques** extraites par le module d'extraction de caractéristiques. La fusion au niveau de capteur est limitée car elle nécessite une homogénéité entre les données [6].

1.6.4.1. 1. La fusion au niveau du capteur (au niveau des donnés)

Les données brutes, obtenues à partir de la détection de la même caractéristique biométrique avec deux capteurs ou plus, sont combinées (voire **Figure.1.15**).La fusion au niveau de capteur est applicable uniquement si les sources multiples représentent des échantillons du même trait biométrique obtenus à l'aide d'un capteur unique ou de capteurs compatibles différents [21].

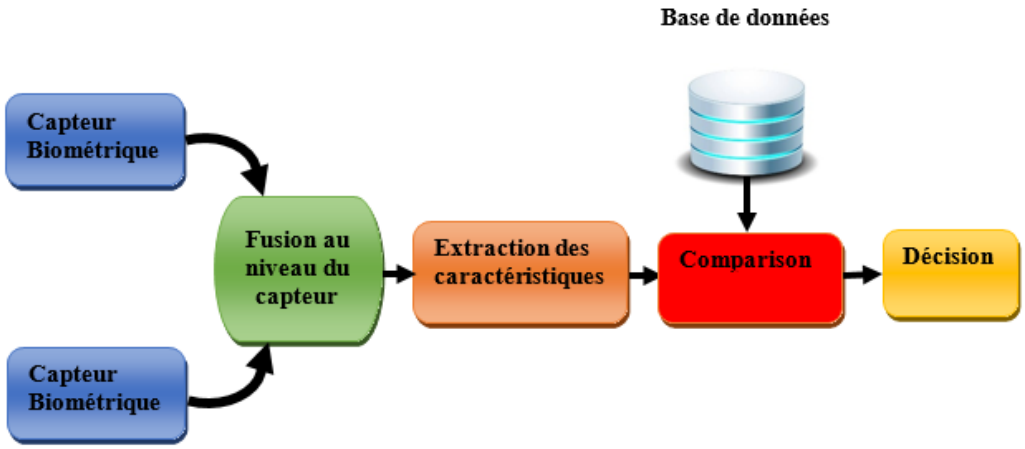


Figure.1.15 : La fusion au niveau du capteur (au niveau des donnés).

1.6.4.1. 2. La fusion au niveau des caractéristiques

C'est la combinaison des informations extraites après divers algorithmes de traitement et d'analyse des mesures pour extraire séparément les vecteurs de caractéristiques et 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 (voire **Figure.1.16**).

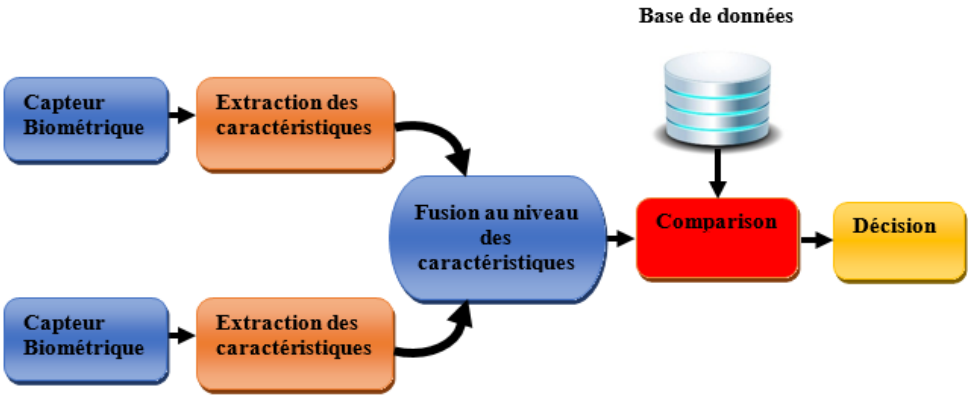


Figure.1.16 : La fusion au niveau des caractéristiques.

1.6.4.2. La fusion post-classification (après la comparaison)

Elle est très étudiée par les chercheurs. Cette fusion peut se faire **au niveau des scores** issus des modules de comparaison ou **au niveau des décisions**.

1.6.4.2.1. La fusion au niveau des scores

Ce niveau sera après la comparaison, et plus précisément, au cours duquel les informations seront fusionnées afin d'obtenir des informations complètes sur l'individu, c'est ce qui fait que ces phases sont les plus utilisées dans le traitement des données des systèmes biométriques (voire **Figure.1.17**).

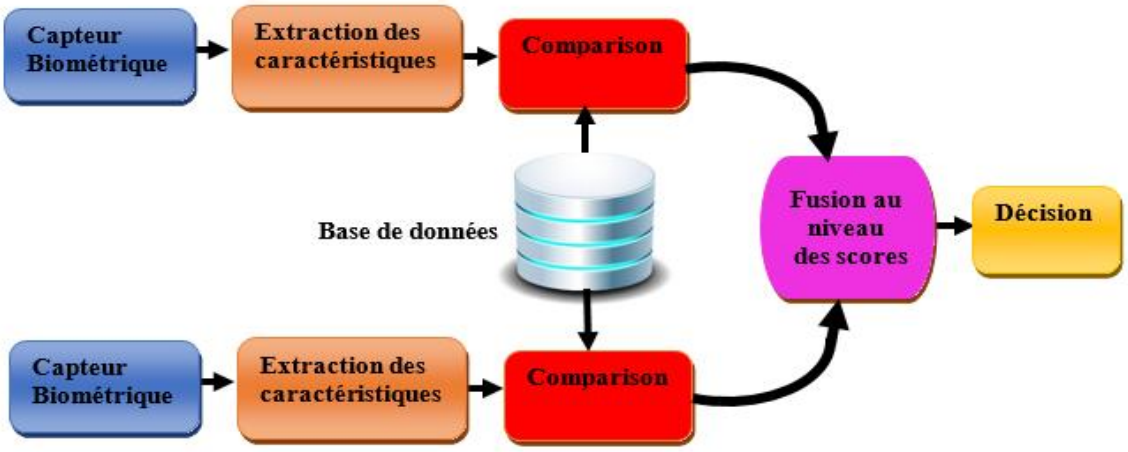


Figure.1.17 : La fusion au niveau des scores.

À cette étape, des techniques basées sur des règles sont utilisées. La fusion basée sur des règles comprend plusieurs méthodes. Soit S_i est le score du $i^{ème}$ modalité biométrique et N est le nombre de modalités biométriques. Les méthodes les plus utilisées pour le calcul du score après fusion (S) sont comme suit :

Tableau.1.1 : Méthodes de fusion usuelles.

Méthode	$\boldsymbol{S}$
La somme	$\sum_{i=1}^{N} S_i$
Le produit	$\prod_{i=1}^{N} S_i$
Le minimum	$\min(S_i)$
Le maximum	$\max(S_i)$
La moyenne	$\frac{1}{N}\sum_{i=1}^{N} S_i$
La médiane	$med(S_i)$
La somme pondérée	$\sum_{i=1}^{N} W_i S_i$ W_i: les poids de pondération dont la somme est égale à l'unité.

Aussi, nous trouvons :

Les t-normes (normes triangulaires) : sont le type le plus courant de fonctions binaires qui satisfont aux exigences de l'intersection des ensembles flous [22]. Une t-norme est une fonction T: $[0,1] \times [0,1] \rightarrow [0,1]$qui satisfait aux propriétés suivantes [23] :

1. $T(x,y) = T(y,x)$(T est commutative).
2. $T\big(x,T(y,z)\big) = T(T(x,y),z)$ (T est associative).
3. $T(x,1) = T(1,x) = 1$ (1 est un élément identité).
4. $y \leq z$ implique $T(x,y) \leq T(x,z)$ (T est croissante dans chaque variable).

Tableau.1.2 : Exemples de quelques t-normes.

T-norm	Formulation
Hamacher	$\frac{xy}{(x+y-xy)}$
Schweizer-Sklar $(p>0)$	$\left(max(x^p+y^p-1,0)\right)^{\left(\frac{1}{p}\right)}$
Yager $(p>0)$	$max\left(1-((1-x)^p+(1-y)^p)^{\left(\frac{1}{p}\right)},0\right)$
Schweizer-Sklar $(p<0)$	$(x^p+y^p-1)^{\left(\frac{1}{p}\right)}$
Einstein	$\left(\frac{xy}{(2-(x+y-xy))}\right)$
Frank $(p>0)$	$\frac{\log 10\left(1+\frac{(p^x-1)(p^y-1)}{p-1}\right)}{\log 10(p)}$

1.6.4.2.2. La fusion au niveau des décisions

Chaque modalité est d'abord identifiée de façon indépendante, puis la décision finale est prise en se basant sur la fusion des décisions des différents processus biométriques. Les résultats finaux de plusieurs classificateurs sont consolidés par des techniques comme celle de la majorité de votes. La fusion au niveau décision est considérée comme rigide en raison de la disponibilité des informations limitées (voire **Figure.1.18**).

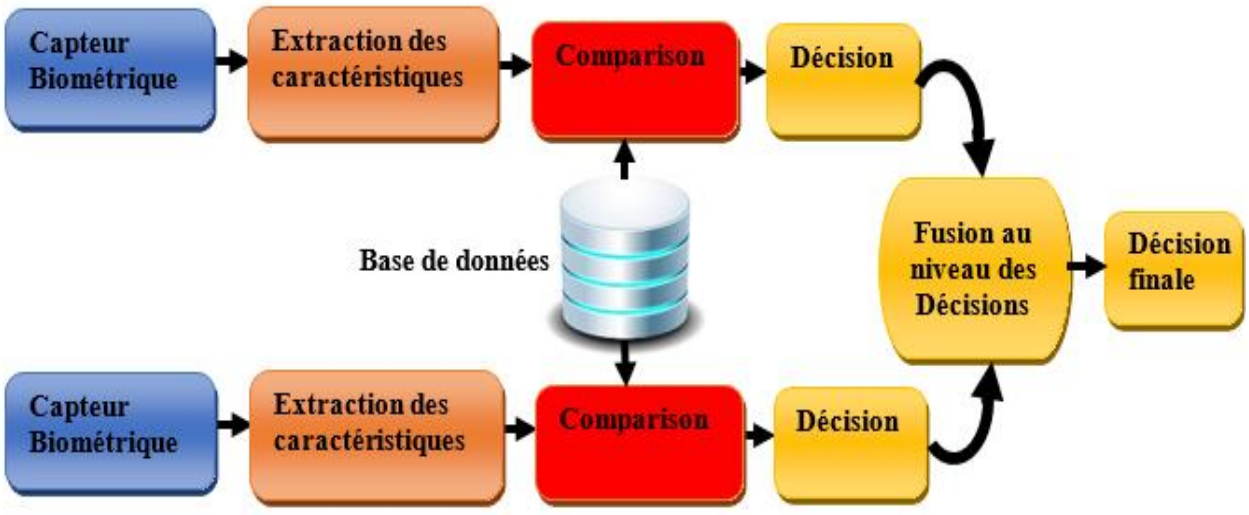


Figure.1.18 : La fusion au niveau des décisions.

1.7. Mesure de la performance d'un système biométrique

Les mesures de performance expriment les caractéristiques de fonctionnement du système de reconnaissance et permettent, ainsi de faire des comparaisons entre différents systèmes.

Il existe différents paramètres pour évaluer un système de reconnaissance : les **taux de faux rejets (False Reject Rate ou FRR)** et **taux de fausses acceptations (False Accept Rate ou FAR), taux d'égale erreur (Equal Error Rate ou EER)** [20].

1.7.1. Taux de faux rejets (False Reject Rate ou FRR)

Ce taux représente le pourcentage de personnes censées être reconnues, mais qui sont rejetées par le système. Il s'agit du rapport entre le nombre de fausses rejets (FR) et le nombre total de tests effectués sur des personnes légitimes.

$$FRR = \frac{Le\ nombre\ de\ clients\ rejetés}{Le\ nombre\ total\ d'accès\ clients} \quad (1.1)$$

1.7.2. Taux de fausses acceptations (False Accept Rate ou FAR)

Ce taux représente le pourcentage de personnes censées ne pas être reconnues, mais qui sont tout de même acceptées par le système.

Le **FAR**, est égal au nombre de fausses acceptations (FA) divisé par le nombre total d'accès imposteurs.

$$FAR = \frac{Le\ nombre\ d'imposteurs\ acceptés}{Le\ nombre\ total\ d'accès\ imposteurs} \quad (1.2)$$

1.7.3. Taux d'égale erreur (Equal Error Rate ou EER)

Ce taux est calculé à partir des deux premiers taux préalablement décrits et constitue un point de mesure de performance courant. Ce point correspond à l'endroit où FRR = FAR, c'est-à-dire le meilleur compromis entre les faux rejets et les fausses acceptations.

L'**EER** peut être calculé à l'aide de l'équation suivante :

$$EER = \frac{Le\ nombre\ de\ fausses\ acceptations + Le\ nombre\ de\ fausses\ rejets}{Le\ \ nombre\ total\ d'accès} \quad (1.3)$$

La **Figure.1.19** montre le FRR et le FAR à partir de distributions des scores authentiques et imposteurs, tandis que l'EER est représenté sur la **Figure. 1.20**.

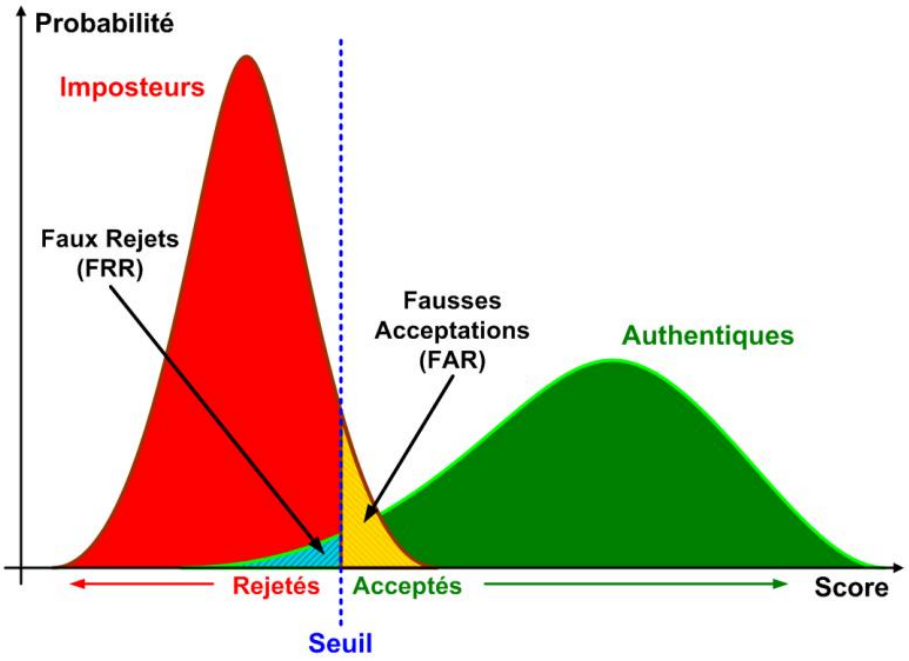


Figure.1.19 : Illustration du FRR et du FAR.

Selon la nature (authentification ou identification) du système biométrique, il existe deux façons d'en mesurer la performance :

- Lorsque le système opère en mode authentification, on utilise ce que l'on appelle **une courbe ROC** (pour Receiver Operating Characteristic en anglais). **La courbe ROC** (**Figure. 1.20**) trace le taux de faux rejets en fonction du taux de fausses acceptations. Plus cette courbe tend à épouser la forme du repère, plus le système est performant, c'est-à-dire possédant un taux de reconnaissance global élevé.

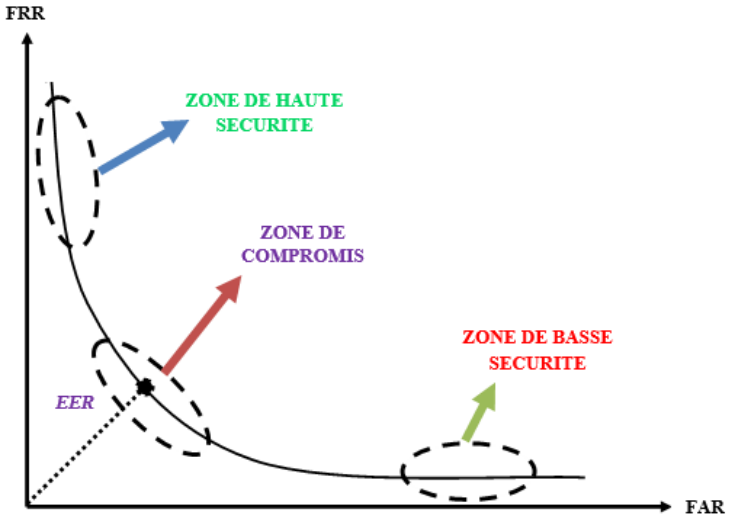


Figure. 1.20 : Courbe ROC.

En revanche, dans le cas d'un système utilisé en mode identification, on utilise ce que l'on appelle **une courbe CMC** (pour Cumulative Match Characteristic en anglais). **La courbe CMC** (**Figure. 1.21**) donne le pourcentage de personnes reconnues en fonction d'une variable que l'on appelle le rang. On dit qu'un système reconnaît au rang 1, lorsqu'il choisit la plus proche image comme résultat de la reconnaissance. On dit qu'un système reconnaît au rang 2, lorsqu'il choisit parmi deux images, celle qui correspond le mieux à l'image d'entrée, etc. On peut donc dire que plus le rang augmente, plus le taux de reconnaissance correspondant est lié à un niveau de sécurité faible.

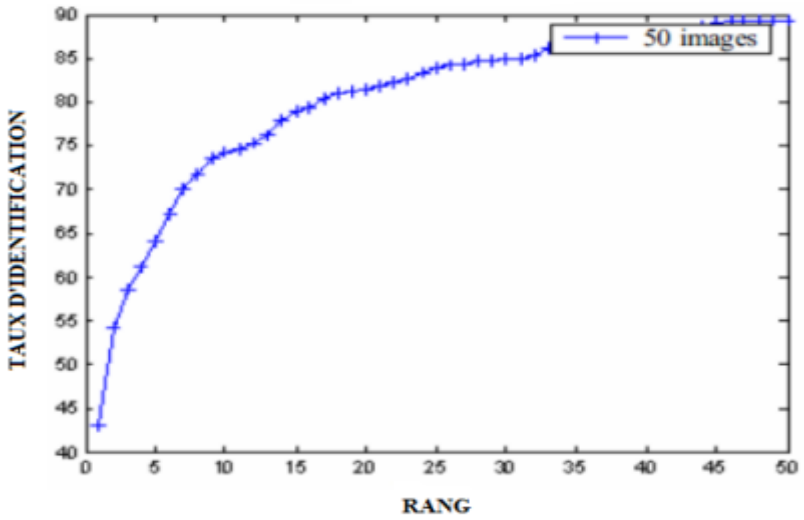
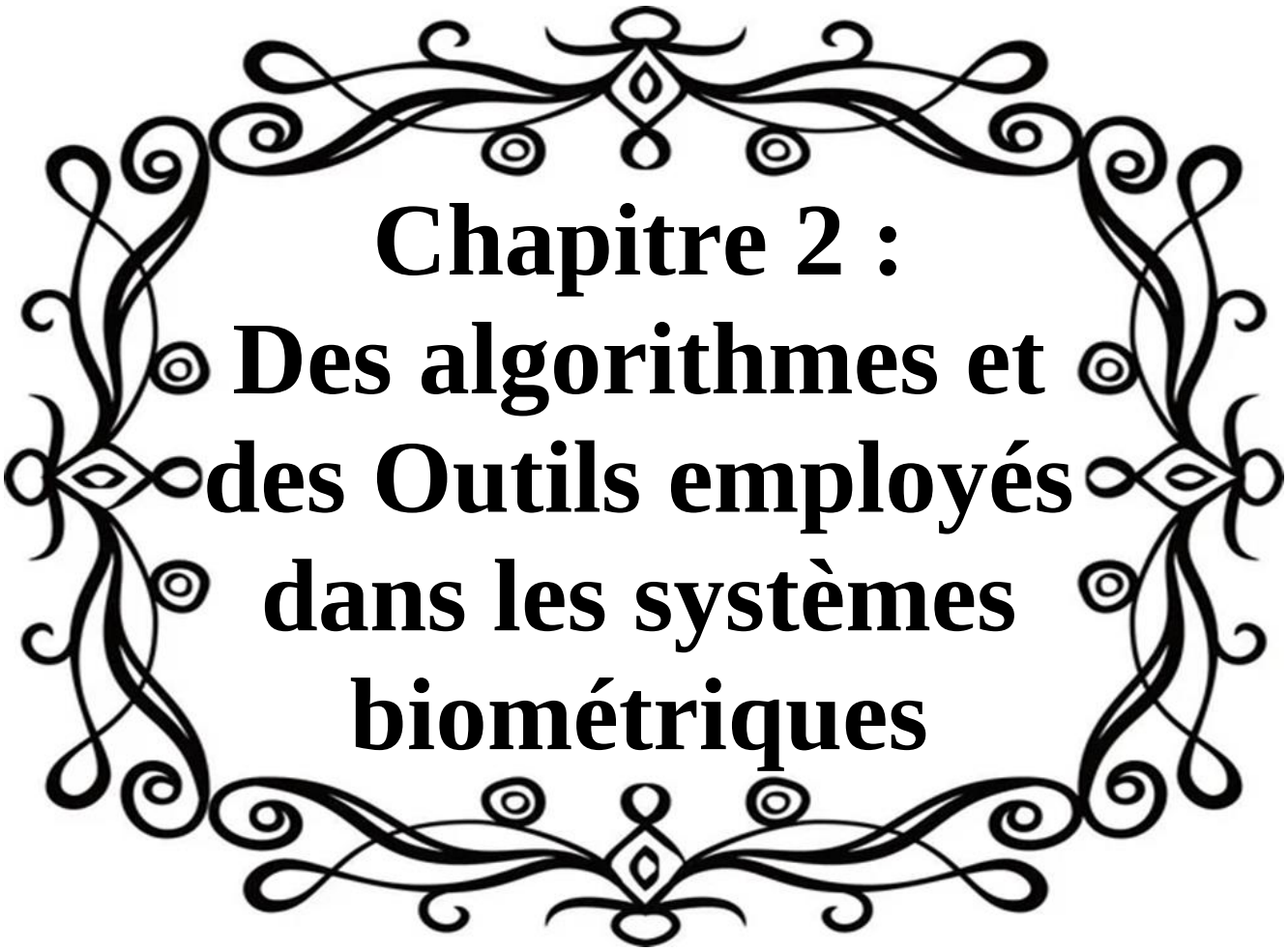


Figure.1.21 : Courbe CMC.

1.8. Conclusion

Dans ce chapitre, nous avons abordé les concepts généraux dans le domaine de la biométrie, qui est l'une des applications les plus populaires dans le monde de la technologie et qui augmente la sécurité et la confidentialité. Pour commencer, nous avons évoqué la définition et expliqué les principales modalités biométriques. Nous avons également discuté les phases et les modes de fonctionnement du système biométrique et de la structure du système biométrique et examiné les limitations de ces systèmes lorsqu'ils n'utilisent qu'une seule modalité biométrique.

Nous avons ensuite développé une façon de réduire les limitations des systèmes biométriques monomodaux en combinant plusieurs systèmes conduisant ainsi à la biométrie multimodale. Nous avons aussi présenté les différents types de multimodalités possibles, mais aussi les architectures et les niveaux de fusion. En dernier point de ce chapitre, nous avons expliqué la mesure de performance du système biométrique.



Chapitre 2 : Des algorithmes et des Outils employés dans les systèmes biométriques

2.1. Introduction

Les images de mains sont d'une importance capitale dans des domaines critiques tels que la sécurité et l'enquête criminelle. Elles peuvent parfois être la seule preuve disponible de l'identité d'un délinquant sur une scène de crime.

L'extraction de caractéristiques est d'abord effectuée à partir d'un ensemble initial de données mesurées et identifie les valeurs dérivées (caractéristiques) qui sont censées être utiles et non redondantes. Naturellement, l'extraction de caractéristiques et la réduction de dimensionnalité sont combinées. Lorsque les vecteurs sont trop volumineux pour être traités, redondants ou contiennent une redondance inutile, ils sont transformés ou réduits à une représentation précise des entités (le vecteur d'entités) et plus consistante. C'est précisément cette étape qui facilite le processus de classification, qui vise à découvrir la structure de base d'un ensemble de données en créant des groupes qui partagent des caractéristiques similaires.

Dans ce chapitre, nous nous sommes consacrés à expliquer le choix de la FKP en tant que biométrie de sécurité et l'état de l'art de l'FKP. Aussi nous allons donner des définitions de quelques algorithmes utilisés dans les systèmes biométriques, les algorithmes qu'on va discuter ce sont principalement les filtres de Gabor et le descripteur de caractéristiques d'images statistiques binarisées (BSIF) utilisés tous deux dans l'extraction des caractéristiques. Et pour réaliser la réduction de dimensionnalité des vecteurs de caractéristiques avec optimalité, nous parlerons des deux algorithmes : analyse en composantes principales (PCA) et analyse discriminante linéaire (LDA). En ce qui concerne la classification de scores, nous parlerons de la méthode des K plus proches voisins (K-NN).

2.2. Motivation du choix de la FKP

Les approches d'identification de personne, qui considèrent la main humaine comme un objet complexe composé de nombreux éléments, sont rares [24]. Il est donc important d'étudier l'unicité et la stabilité des informations qui peuvent être récupérées à partir des images dorsales des doigts. De plus, il existe diverses images forensiques enregistrées (voir **Figure .2.1**) dans lesquelles seules les caractéristiques dorsales des doigts sont disponibles pour établir l'identité d'un suspect. L'identification automatisée ou forensique des motifs de phalanges a suscité l'attention des chercheurs dans la littérature mais plusieurs questions concernant l'unicité et/ou la stabilité de ces motifs restent à élucider.

Figure .2.1 : (a)-(b)-(c)-(d) Exemple d'images des dorsaux des doigts de la main en action.

2.3. Pourquoi la biométrie par l'empreinte des articulations des doigts (FKP) ?

Le FKP est l'une des modalités biométriques physiologiques les plus récentes à être utilisées, car il a été observé récemment que les textures à l'arrière des doigts ont le potentiel d'être utilisées pour discriminer différents individus. Les motifs inhérents du FKP, constitués de lignes de pliage à la surface externe de la peau, sont très riches et uniques chez chaque individu, ce qui offre une manière nouvelle mais prometteuse d'identifier une personne [25].

De plus, les systèmes biométriques FKP ont le potentiel de réussir en raison de leur disponibilité, de l'acquisition d'images sans contact, de la facilité d'accès, des caractéristiques stables et de l'acceptabilité sociale. De plus, ils ne varient pas en fonction des émotions ou d'autres facteurs tels que la fatigue. Cependant, les motifs d'image FKP sont souvent affectés par des problèmes tels que des données de capteur bruyantes et des variations d'éclairage, de sorte que la reconnaissance d'une personne avec une forte confiance est une question critique. Ainsi, l'un des principaux défis pour améliorer les performances de reconnaissance FKP est de concevoir un schéma de reconnaissance fiable pour les motifs FKP [25].

2.4. Certains travaux sur l'empreinte des articulations des doigts (FKP)

Les systèmes biométriques basés sur les caractéristiques FKP ont suscité beaucoup d'attention de la part des chercheurs et ont connu une évolution importante, où différents systèmes ont été proposés et appliqués dans divers domaines d'application.

Kumar et Xu. [24] ont présenté la fusion des motifs des premières articulations mineures, des deuxièmes articulations mineures et des articulations majeures ainsi que de la surface dorsale de

la paume pour améliorer d'avantage les performances d'identification.

Attia et al. ([26] [27] [28]) ont étudié le descripteur de caractéristiques d'image statistique binaire (BSIF) dans l'extraction de caractéristiques pour le trait FKP. En particulier, un descripteur BSIF a été construit pour apprendre les caractéristiques. Ensuite, la technique PCA (Analyse en composants principales) + LDA (analyse discriminante linéaire) a été utilisée dans l'étape de réduction de dimensionnalité. Enfin, dans l'étape de correspondance, le classifieur de voisinage le plus proche basé sur la distance de Mahalanobis Cosine a été utilisé.

Chaa et al. [29] ont fusionné deux types d'histogrammes de gradients orientés (HOG) basés sur des caractéristiques extraites à partir d'images de réflectance et d'illumination FKP. Cependant, les auteurs ont utilisé l'algorithme de l'adaptive single scale retinex (ASSR) pour extraire les images d'illumination et de réflectance à partir de chaque image FKP. Ensuite, le descripteur HOG a été appliqué sur les deux images extraites. Ces vecteurs de caractéristiques ont été concaténés pour obtenir un grand vecteur de caractéristiques. Ensuite, une projection en sous-espace LDA a été réalisée.

Attia et al. [30] ont proposé une nouvelle méthode de reconnaissance d'empreintes des articulations des doigts (FKP) utilisant la technologie Log Gabor- Motif binaire local à trois patchs (TPLBP) (LGTPLBP). Un filtre Log Gabor 1D est utilisé pour extraire des images réelles et imaginaires de chaque région d'intérêt (ROI) des images FKP. Ensuite, le descripteur TPLBP est appliqué pour extraire des vecteurs de caractéristiques pour les images réelles et imaginaires, qui sont combinés pour former un grand vecteur de caractéristiques pour chaque image FKP. LDA est utilisée pour la réduction de dimensionnalité, et le cosinus de Mahalanobis est utilisé pour la correspondance.

K. Usha et M. Ezhilarasan. [31] ont étudié une nouvelle approche des informations personnelles dignes de confiance. Reconnaître la base de l'extraction et de l'intégration simultanée de la palpation et de la forme de l'articulation du doigt. La méthode proposée pour l'identification FKP comprend le prétraitement de l'image de l'articulation du doigt, l'extraction du retour sur investissement et l'extraction de l'angle informations d'ingénierie basées sur les fonctionnalités et informations d'attributs synthétiques basées sur la jointure Curvelet pour de meilleures performances. De plus, le système proposé gère les zones d'articulations déformées ou altérées et extrait de manière fiable des informations pour l'identification personnelle.

2.5. Des algorithmes utilisés dans les systèmes biométriques

2.5.1. Extraction de caractéristiques

L'extraction d'informations consiste à obtenir des caractéristiques qui doivent être discriminantes et non redondantes. L'extraction de caractéristiques est une étape essentielle, car son importance réside dans le choix des types de descripteurs de caractéristique. C'est pourquoi les descripteurs d'image locaux **Gabor** et **BSIF** ont été choisis comme étant très utilisés et populaires et en raison de leur bonnes performances.

2.5.1.1. Les filtres de Gabor

Les filtres Gabor sont généralement utilisés dans l'analyse de texture, la détection de contours, l'extraction de caractéristiques, etc. Les filtres Gabor sont des classes de filtres passe-bande spéciaux [32]. L'équation ci-dessous donne l'expression des filtres de Gabor.

$$G_{\theta,\sigma,\lambda,\varphi,\gamma}(x,y) = e^{-\left(\frac{x'^2+\gamma^2 y'^2}{2\sigma^2}\right)} e^{i\left(2\pi\frac{x'}{\lambda}+\varphi\right)} \quad (2.1)$$

Où $x' = xcos(\theta) + ysin(\theta)$

$y' = -xsin(\theta) + ycos(\theta)$

θ : Orientation de l'ondelette.

λ : Longueur d'onde ou fréquence de l'ondelette.

φ : Phase.

σ : Rayon de la Gaussienne (Echelle).

γ : Rapport d'aspect de la Gaussienne.

$e^{-\left(\frac{x'^2+\gamma^2 y'^2}{2\sigma^2}\right)}$ est la fonction de Gauss. Où, x et y sont la plage de valeurs pour la longueur et la largeur du masque de Gabor. Le filtre de Gabor est convolué ensuite avec l'image pour former les images filtrées de Gabor :

$$f(x,y) = I(x,y) \times G_{\theta,\sigma,\lambda,\varphi,\gamma}(x,y) \quad (2.2)$$

Ils autorisent une certaine « bande » de fréquences et rejettent les autres. Lorsqu'un filtre Gabor est appliqué à une image, il donne la réponse la plus élevée aux bords et aux points où les caractéristiques de texture changent. Un filtre répond à une caractéristique particulière, signifie que le filtre a une valeur distinctive à l'emplacement spatial de cette caractéristique. Lorsque nous appliquons des noyaux de convolution dans le domaine spatial, c'est-à-dire qu'il en va de même pour d'autres domaines, tels que les domaines fréquentiels. Les avantages importants du filtre de

Gabor sont l'invariance à l'éclairage, à la rotation, à la translation et à l'échelle [32].

Les filtres de Gabor sont capables de générer des informations à partir d'une image de texture à différentes échelles et sous différentes orientations [33]. Par exemple, pour l'extraction des caractéristiques de palmprint, des filtres de Gabor de différentes échelles et orientations sont utilisés afin de garantir que les informations maximales avec un minimum de redondance seront capturés [25]. La **Figure.2.2** montre un exemple d'une image de palmprint filtrées par plusieurs filtres de Gabor avec 08 orientations et 05 échelles. Les réponses en amplitudes sont calculées et représentées sur la même figure [33].

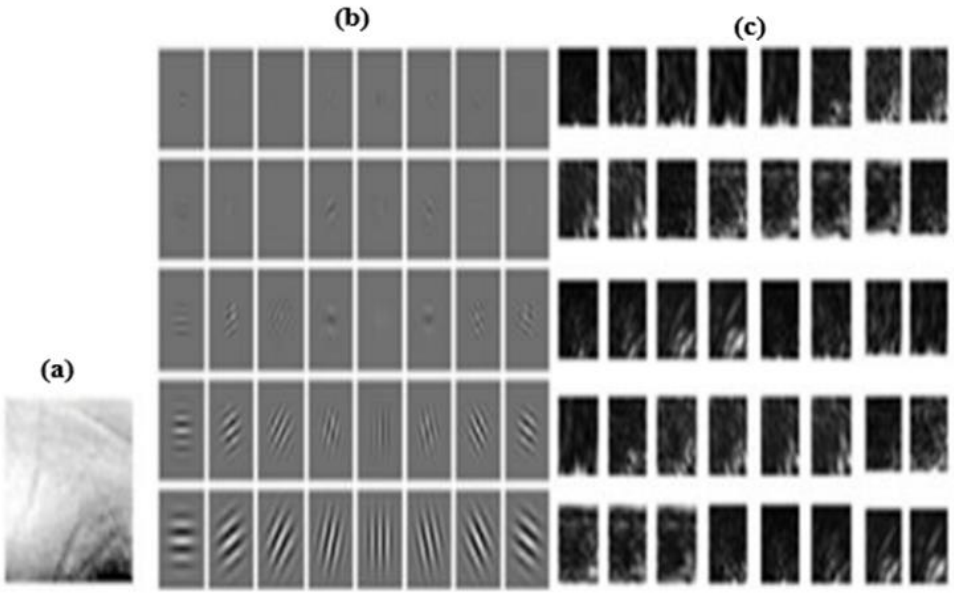


Figure.2.2 : (a) Exemple d'empreintes palmaires. **(b)** Filtres de Gabor (5 échelles et 8 orientations). **(c)** Les réponses des amplitudes de la convolution avec ces filtres.

2.5.1.2. Caractéristiques d'images statistiques binarisées (BSIF)

BSIF est un descripteur local relativement récent pour reconnaître des textures. Cette méthode d'extraction de caractéristiques a été proposée par (Kannala et Rahtu 2012) [34]. La méthode calcule un code binaire pour chaque pixel en projetant linéairement des patchs d'image locaux sur un sous-espace, dont les vecteurs de base sont appris à partir d'images naturelles via une analyse en composantes indépendantes, et en binarisant les coordonnées dans cette base via un seuillage. La longueur de la chaîne de code binaire est déterminée par le nombre de vecteurs de base. Les régions de l'image peuvent être représentées de manière pratique par des histogrammes des codes binaires des pixels.

Etant donné un patch d'image X de taille $l \times l$ pixels et un filtre linéaire W_i de même taille, la réponse s_i du filtre est représenté symboliquement par :

$$s_i = \sum_{u,v} W_i\,(u,v).X(u,v) \tag{2.3}$$

En fournissant un échantillon aléatoire de fragments d'image naturelle, nous déterminons le filtre W_i de sorte que les éléments s_i de s soient aussi indépendants que possible lorsqu'ils sont considérés comme des variables aléatoires. Le code binaire b, qui correspond au fragment d'image X, est obtenu en binarisant chaque élément s_i de s comme suit :

$$b_i = \begin{cases} 1 & if\ \ s_i > 0 \\ 0 & Sinon. \end{cases} \tag{2.4}$$

Dans cette méthode, on peut calculer une chaîne de code binaire b de n $-bits$ pour chaque pixel, où b_i est le $i^{ème}$ élément de b. Par la suite, la région de l'image peut être représentée par des histogrammes du code binaire des pixels.

BSIF caractérise efficacement les composants de texture de l'image. Il existe deux facteurs importants dans le descripteur BSIF : la taille du filtre l et n la longueur du filtre. L'image et l'image filtrée par BSIF correspondantes sont représentées sur **la Figure.2.3**. Cette dernière montre un exemple d'image de phalange majeure et mineure avec le traitement des filtres BSIF. **La Figure.2.3(a)** présente la ROI d'entrée de l'image majeure. **La Figure .2.3(b)** illustre le résultat du filtre BSIF avec une taille de 17x17 et une longueur de 11 bits et 12 bits, tandis que **La Figure.2.3(c)** présente la ROI d'entrée de l'image mineure. **La Figure.2.3(d)** représente les résultats de la convolution individuelle de la ROI de l'image mineure avec le filtre BSIF avec une taille de 17x17 et une longueur de 11 bits et 12 bits [26].

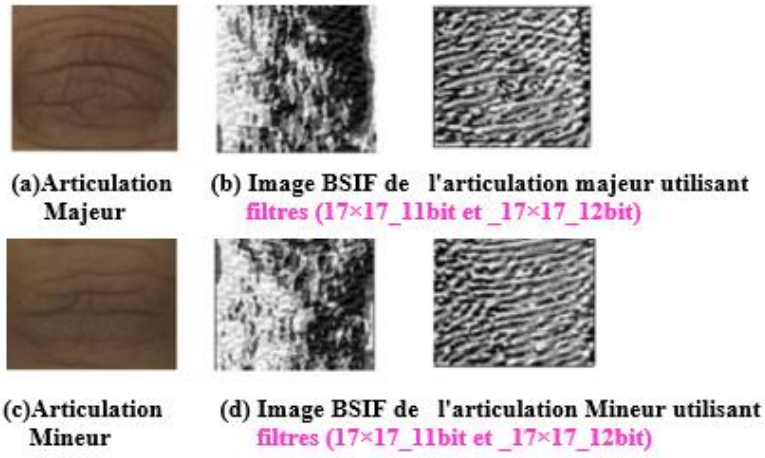


Figure.2.3 : Échantillons de l'image ROI majeure et mineure avec les sorties de niveau Filtre BSIF de taille 17×17 et de longueur 11 et 12 bits.

2.5.2. Réduction de dimensionnalité

Dans les applications de reconnaissance d'images, il y a un problème de collecte, de traitement et de stockage de grandes quantités de données. La réduction de dimensionnalité est devenue une nécessité pour déterminer les caractéristiques les plus discriminatives à utiliser lors de l'étape de classification. La réduction de données est utilisée pour résoudre ce problème. L'idée est de déterminer efficacement un sous-espace de faible dimension dans un espace d'image de grande dimension. Dans pratiquement tous les types de données imaginables, on peut utiliser un processus de réduction de dimensionnalité statistique pour déterminer quelles caractéristiques sont pertinentes pour le problème de classification [25]. Les deux techniques de réduction de dimensionnalité populaires sont l'Analyse en Composantes Principales (**PCA**) et l'Analyse Discriminante Linéaire (**LDA**).

2.5.2.1. Analyse en composants principales (PCA)

L'analyse en composantes principales (PCA) est une transformation linéaire qui permet d'obtenir la variance des données d'entrée. La PCA est une méthode puissante non supervisée pour transformer un certain nombre d'attributs possiblement corrélés en un certain nombre d'attributs non corrélés appelés composantes principales. Cette technique calcule les vecteurs propres de la matrice de covariance et approxime l'ensemble de données d'origine par une combinaison linéaire des vecteurs propres dominants.

L'idée d'utiliser l'approche de PCA est de réduire la taille d'un ensemble de données sans perdre beaucoup de fonctionnalités, où les vecteurs propres aident à trouver le sous-espace de fonctionnalités optimales dans la dimensionnalité inférieure nécessaire pour la reconnaissance d'une image de test [25].

Le principe de PCA pourrait être décrit dans ces étapes [35]:

- Chaque image de la base de données est convertie en un vecteur à une dimension
- Calculer la moyenne de chaque vecteur en utilisant l'équation suivante :

$$X_m = \frac{1}{M}\sum_{i=1}^{M} X_i \tag{2.5}$$

- Soustraire la moyenne de tous les vecteurs pour produire un ensemble de vecteurs à moyenne nulle, il est donné par cette équation :

$$\varphi_i = X_i - X_m \tag{2.6}$$

- Calculer la matrice de covariance $C(N^2 \times N^2)$ en utilisant l'équation :

$$C = AA^T \tag{2.7}$$

Où $A = [\varphi_1, \varphi_2, \dots, \varphi_M](N^2 \times M\ matrice\ )$

- Calculer les valeurs propres de la matrice de covariance C. La matrice AA^T est très grande, considérez donc la matrice $C^T = A^T A\ (M \times M\ matrice\ )$ et calculez les valeurs propres u_i de C^T tels que :

$$C^T\ r_i = u_i\ r_i \tag{2.8}$$

Où r_i sont les vecteurs propres de C^T

- Sélectionner uniquement les K vecteurs propres correspondant aux valeurs propres les plus élevées pour former un vecteur des caractéristiques.

2.5.2.2. Analyse discriminante linéaire (LDA)

LDA est une technique basée sur l'apparence utilisée pour la réduction de dimensionnalité et a enregistré une grande performance en reconnaissance biométrique. Cette méthode fonctionne sur le même principe que la méthode PCA.

L'objectif de LDA est d'effectuer une réduction de dimensionnalité tout en préservant toutes les informations discriminatoires sur la classe et de trouver la direction dans laquelle les classes sont mieux séparées.

En d'autres termes, l'objectif de LDA est de maximiser la dispersion entre les classes S_B et de minimiser la matrice de dispersion intra-classe S_W dans le sous-espace projectif [21].

La matrice de dispersion intra-classe S_W et la matrice de dispersion inter-classes S_B sont définies comme suit [36]:

$$S_W = \sum_{j=1}^{C_s} \sum_{i=1}^{N_j} \left(\Gamma_i^j - \mu_j\right) \left(\Gamma_i^j - \mu_j\right)^T \tag{2.9}$$

Où Γ_i^j est le i échantillon de la class j, μ_j est la moyenne de la classe j, C_s est le nombre de classes, N_j est le nombre d'échantillons en classe j. Aussi,

$$S_B = \sum_{j=1}^{C_S} (\mu_j - \mu)(\mu_j - \mu)^T \tag{2.10}$$

μ : représente la moyenne de toutes les classes. Le sous-espace de LDA est couvert par un ensemble de vecteurs $W = [W1, W2, \ldots, Wd]$, satisfaisant :

$$W = \arg\max\left(\left|\frac{W^T S_B W}{W^T S_W W}\right|\right) \tag{2.11}$$

W peut être construit en calculant les vecteurs propres de la matrice $S_w^{-1}.S_B$ [21].

$$W = eig(S_w^{-1}.S_B) \tag{2.12}$$

Où $eig(S_w^{-1}.S_B)$: renvoie les valeurs propres (*eigen vectors*) de la matrice carrée $S_w^{-1}.S_B$.

La Figure.2.4, ci-dessous, souligne la différence entre les deux méthodes : PCA peut être décrit comme un algorithme « non supervisé », car il ignore les étiquettes de classe et cherche les directions (les composantes principales λ1, λ2) qui maximisent la variance dans un ensemble de données. Contrairement à PCA, LDA est « supervisé » et calcule les directions (« discriminants linéaires ») qui représenteront les axes maximisant la séparation entre les classes (la classe bleue et le classe verte projeté sur l'axe horizontal).

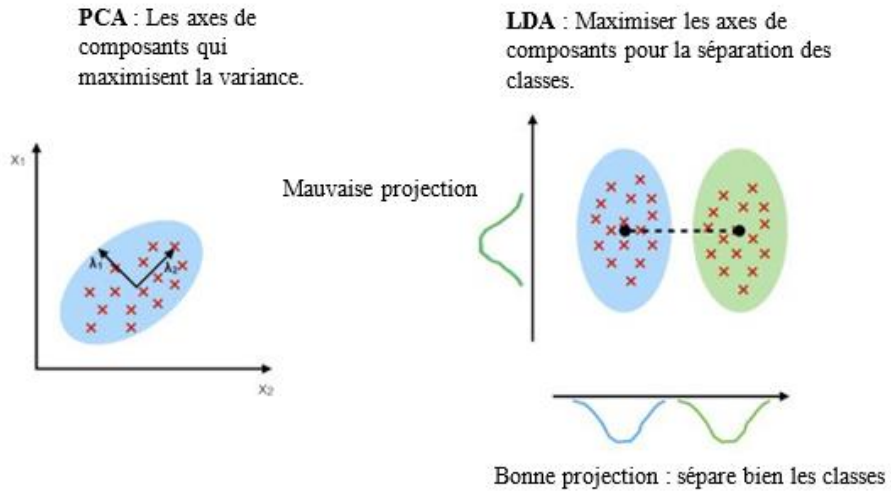


Figure.2.4 : La différence entre PCA et LDA.

2.5. 3. Classification de scores

Plusieurs classifieurs ont été utilisés pour classifier les scores de correspondance afin d'arriver à une décision. Dans l'approche par classification, un vecteur de caractéristiques est construit en utilisant les scores donnés en sortie par les systèmes individuels ; ce vecteur est ensuite attribué à une des deux classes : Client ou Imposteur. En général, le classifieur utilisé pour cette opération est capable d'apprendre la frontière de décision sans tenir compte de la manière dont le vecteur de caractéristiques a été généré. Ainsi, les scores en sortie de différentes systèmes peuvent être non-homogènes (mesure de distance ou de similarité, différents intervalles de valeurs prises, etc.…) et aucun traitement n'est requis avant de les envoyer dans le classifieur. Dans le domaine des systèmes biométriques multimodaux, plusieurs types de méthodes de classification ont été employés. Nous allons maintenant présenter la méthode des K plus proches voisins.

2.5.3.1. Méthode des K plus proches voisins (K-NN)

L'algorithme des K plus proches voisins ou *K-nearest neighbors* (k-NN) est un algorithme de Machine Learning qui appartient à la classe des algorithmes d'apprentissage supervisé dédié à la classification. L'idée principale de l'algorithme KNN vient de l'hypothèse que des choses similaires existent à proximité. En d'autres termes, des choses similaires sont proches les unes des autres [15].

K-NN est un algorithme non paramétrique, ce qui signifie qu'il ne fait aucune hypothèse sur les données sous-jacentes. Il est également appelé algorithme d'apprentissage paresseux car il n'apprend pas immédiatement à partir de l'ensemble d'apprentissage, mais il stocke l'ensemble de données et, au moment de la classification, il exécute une action sur l'ensemble de données.

Pour la classification K-NN, une entrée est classée par un vote majoritaire de ses voisins. C'est-à-dire que l'algorithme obtient l'appartenance à la classe de ses k voisins et génère la classe qui représente la majorité des k voisins [15]. Pour classer l'individu x dans un voisinage de $k = 1$ point, nous cherchons le voisin le plus proche de x. Le cercle noir entoure le point à classer et son voisin le plus proche. Comme le voisin le plus proche de x est un point noir, x sera donc affecté à la classe A. Dans le même problème, mais avec un voisinage de $k = 6$ points, nous cherchons les 6 points les plus proches de x afin de classer l'individu. Le grand cercle noir entoure l'individu à classer, x, ainsi que ses six voisins les plus proches. Parmi les 6 points les plus proches (voir **Figure.2.5**).

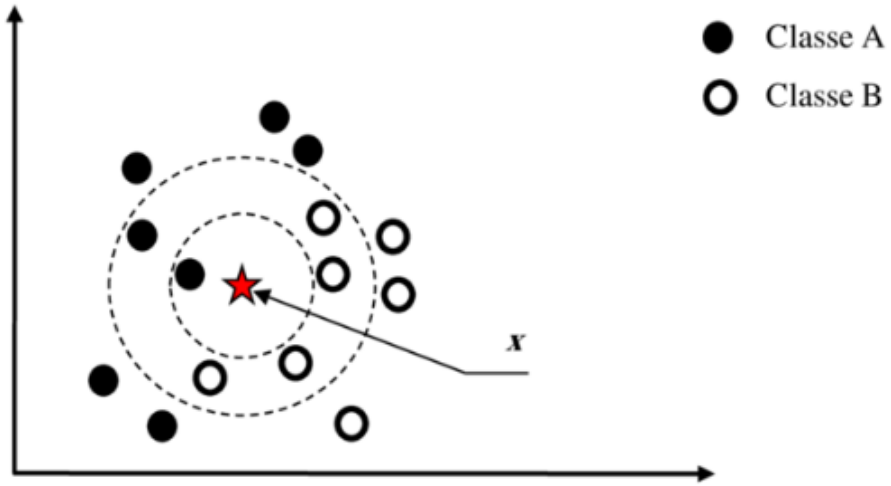


Figure.2.5 : Un exemple de classification K-NN.

Le principe de cet algorithme de classification est très simple. On lui fournit un ensemble de données d'apprentissage D, une fonction de distance d et un entier k. Pour tout nouveau point de test x, pour lequel il doit prendre une décision, l'algorithme recherche dans D les k points les plus proches de x au sens de la distance d, et attribue x à la classe qui est la plus fréquente parmi ces k voisins.

Cette algorithme est basée sur une fonction distance arbitraire d, les plus classiques sont :

- **Distance Euclidienne (Euc) :**

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

$$d(x,y) = \sqrt{\sum_{i=1}^{n}(x_i - y_i)^2} \tag{2.13}$$

- **Distance Manhattan (Cityblock (Ctb)) :**

La distance de Manhattan (aussi appelée distance « city-block » ou métrique absolue), qui calcule la somme des valeurs absolues des différences entre les coordonnées de deux points :

$$d(x,y) = \sum_{i=1}^{n}|x_i - y_i| \tag{2.14}$$

- **Distance de Minkowski (Mink) :**

Cette mesure de distance est la forme généralisée de la mesure de distance Euclidienne et de

celle de Manhattan avec une variable P, qui nous donne l'équation suivante :

$$d(x,y) = \left(\sum_{i=1}^{n} |x_i - y_i|^p\right)^{1/p} \quad (2.15)$$

- **Distance Chebychev (Cheb) :**

Pour $p = \infty$, on obtient la distance de Chebychev (aussi appelée distance « Queen-wise» ou encore métrique maximum), est la distance entre deux points donnés est la différence maximale entre leurs coordonnées sur une dimension, qui est donné par l'équation :

$$d(x,y) = \max_{i=1}^{n} |x_i - y_i| \quad (2.16)$$

- **Distance de Mahalanobis (Mah) :**

La distance de Mahalanobis est donnée par l'équation suivante :

$$d(x,y) = \sqrt{(x-y)^T . cov^{-1}(x-y)} \quad (2.17)$$

Où cov est la matrice de covariance. Si les éléments de x et de y sont indépendants, la matrice de Covariance sera l'identité et la distance de Mahalanobis serait égale à la distance Euclidienne. La boule associée à une distance de Mahalanobis est de forme elliptique, alors que la boule d'une distance Euclidienne est un cercle (en deux dimensions).

- **Distance de Mahalanobis cosinus (Mahcos)**

La distance de Mahalanobis cosinus est donnée par l'équation suivante :

$$d(x,y) = -\frac{x^T . cov(y)}{\sqrt{(x^T . cov(x))(y^T . cov\ (y))}} \quad (2.18)$$

Le Choix de la valeur de **K :**

- **Si K est trop petit :** Rend mieux compte de structure fine, nécessaire pour les petites bases d'apprentissage.
- **Si K est trop grand :** Moins sensible au bruit, une grande base d'apprentissage permet une plus grande plus grande valeur de k, le voisinage pourrait inclure des points d'autres classes.

2.6. Normalisation de scores

Les méthodes de normalisation des scores visent à transformer individuellement chacun des scores des sous-systèmes pour les rendre homogènes avant de les combiner. En effet, les scores de

chaque sous-système peuvent être de nature différente (scores de similarité, scores de distances ….). Certains systèmes produisent des scores de similarité, d'autres produisent des distances (plus la distance est faible, plus la référence et le test sont proches, plus l'utilisateur est un client).

De plus, chaque sous-système peut avoir différents intervalles de variations des scores, par exemple, pour un système, les scores varient entre 0 et 1 et pour un autre, les scores varient entre 0 et 1000.

On comprend bien la nécessité de l'étape de normalisation avant que les scores bruts de différents classificateurs puissent être combinés dans l'étape de fusion. La normalisation aborde le problème des scores incomparables représentant les résultats de différents classificateurs biométriques [21].

Nous présentons dans la suite, les trois méthodes de normalisation les plus connues en occurrence la méthode **Min-Max**, la méthode **Z-score** et la méthode **TanH** [2] :

- Normalisation par la méthode **Min-Max** : La méthode de normalisation la plus simple est la normalisation Min-Max. Cette méthode normalise les scores bruts tout en conservant leurs distributions à un facteur d'échelle près et transforme tous les scores dans l'intervalle [0,1] selon :

$$S_{no} = \frac{S - \min(S)}{\max(s) - \min(s)} \tag{2.20}$$

- Normalisation par la méthode **Z-Score** : La méthode de normalisation du score la plus couramment utilisée est la normalisation du score z .Cette méthode transforme les scores à une distribution avec une moyenne égale 0 et un écart type égale 1 selon :

$$S_{no} = \frac{S - \mu}{\sigma} \tag{2.21}$$

  Où μ est la moyenne arithmétique et σ l'écart-type des données.

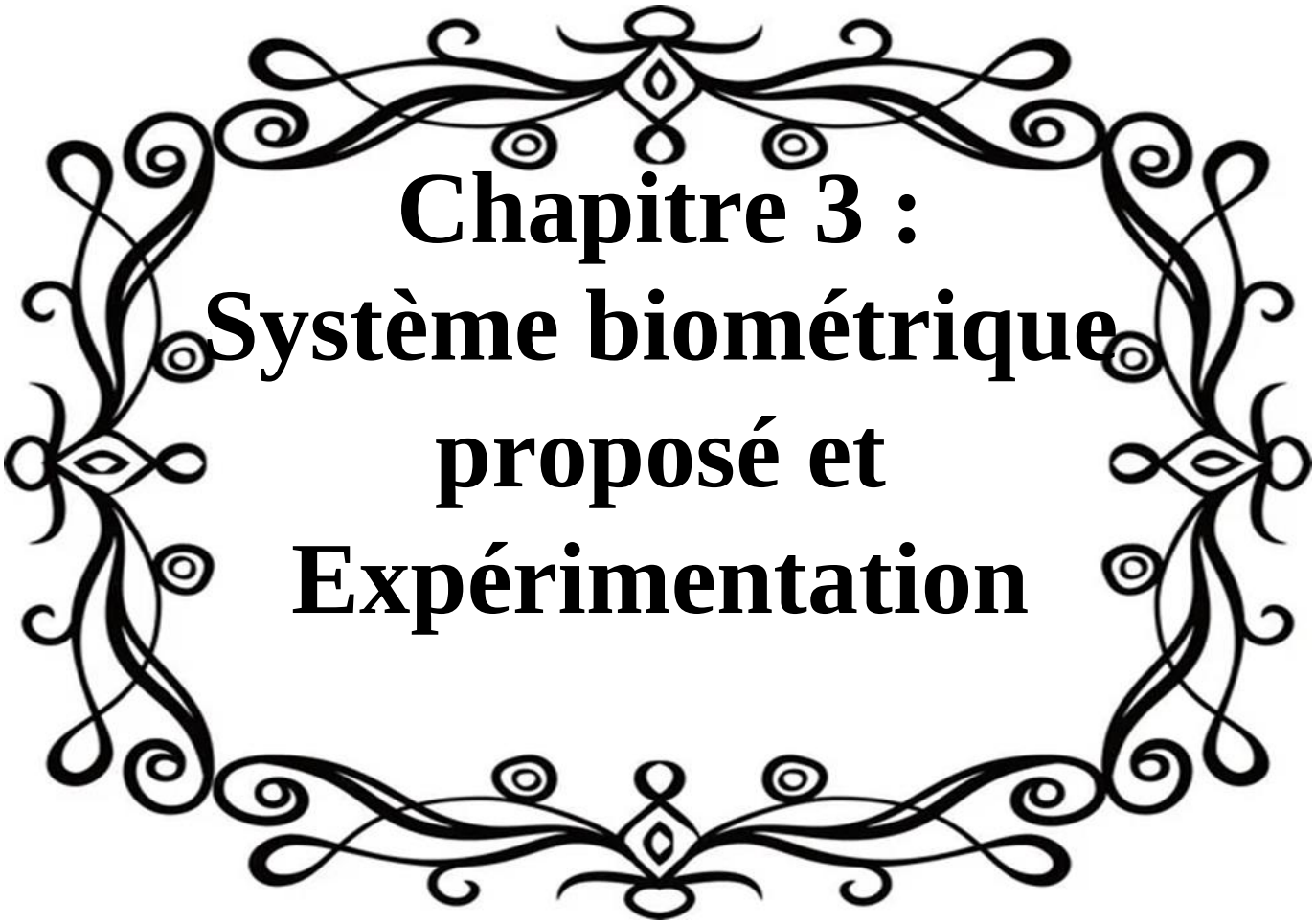
- Normalisation par la méthode **tangente hyperbolique "Tanh" :** Cette méthode est parmi les techniques statistiques les plus solides. Elle met chaque score normalisé dans l'intervalle [0, 1] selon :

$$S_{no} = 0.5\left[tanh\left(0.001\frac{S - \mu}{\sigma}\right) + 1\right] \tag{2.22}$$

  Où μ est la moyenne arithmétique et σ l'écart-type des données.

2.7. Conclusion

Dans ce chapitre, nous avons expliqué pourquoi la biométrie par FKP et un état de l'art dans ce domaine. Nous avons également défini certains des algorithmes couramment utilisés pour l'extraction des caractéristiques, la réduction de dimensionnalité et aussi une méthode pour la classification de scores. Enfin, nous avons discuté des principales méthodes de normalisation de scores.



Chapitre 3 : Système biométrique proposé et Expérimentation

3.1. Introduction

Ces dernières années, l'identification des empreintes des articulations des doigts (FKP) est devenue un sujet de recherche de plus en plus important dans les applications biométriques. Les FKP désignent les motifs de peau inhérents qui se forment au niveau des articulations à la surface du dos des doigts. Il a été constaté que les FKP sont extrêmement riches en texture et peuvent être utilisés pour la reconnaissance unique d'une personne. Cela nous a incités à les considérer comme un choix approprié pour notre étude expérimentale, qui sera exposée dans ce chapitre.

Dans ce chapitre, nous allons présenter le système biométrique d'identification proposé dans notre travail. Ainsi, nous allons parler de l'extraction de la région d'intérêt, ensuite, nous décrierons en détail la base de données que nous avons utilisée dans notre étude, ainsi que les mesures d'évaluation que nous allons utiliser pour évaluer les performances de notre système. Enfin, nous présenterons les résultats expérimentaux qui montreront à la fois les performances du système unimodal et du système multimodal où nous allons appliquer la fusion au niveau des scores. Nous allons ensuite élaborer une étude de comparaison pour terminer avec une conclusion.

3.2. Système proposé basé sur les motifs d'articulations dorsales des doigts

Un système biométrique comprend généralement deux phases principales : la phase d'apprentissage et la phase de test. La phase d'apprentissage permet de former le système en utilisant des données biométriques connues, tandis que la phase de test évalue les performances du système dans les modes d'identification et de vérification en utilisant de nouvelles données biométriques. Ces phases sont essentielles pour assurer la précision et la fiabilité du système biométrique.

Le système biométrique proposé, basé sur les motifs d'articulations des doigts (FKP), est illustré dans la **Figure.3.1**, qui montre le diagramme schématique du système de reconnaissance des personnes.

Dans ce système, nous allons appliquer le filtre de Gabor ensuite le descripteur BSIF pour l'extraction des caractéristiques représentatives pour en choisir le meilleur.

Ensuite, pour réduire la dimensionnalité des vecteurs de caractéristiques, nous utilisons la méthode PCA + LDA. Nous appliquons ensuite l'algorithme K-NN pour classer ces caractéristiques basées sur la distance de Mahalanobis cosinus (Mahcos).

Enfin, nous fusionnons les scores obtenus à partir des différentes modalités biométriques pour améliorer les performances de notre système en utilisant différentes règles de fusion.

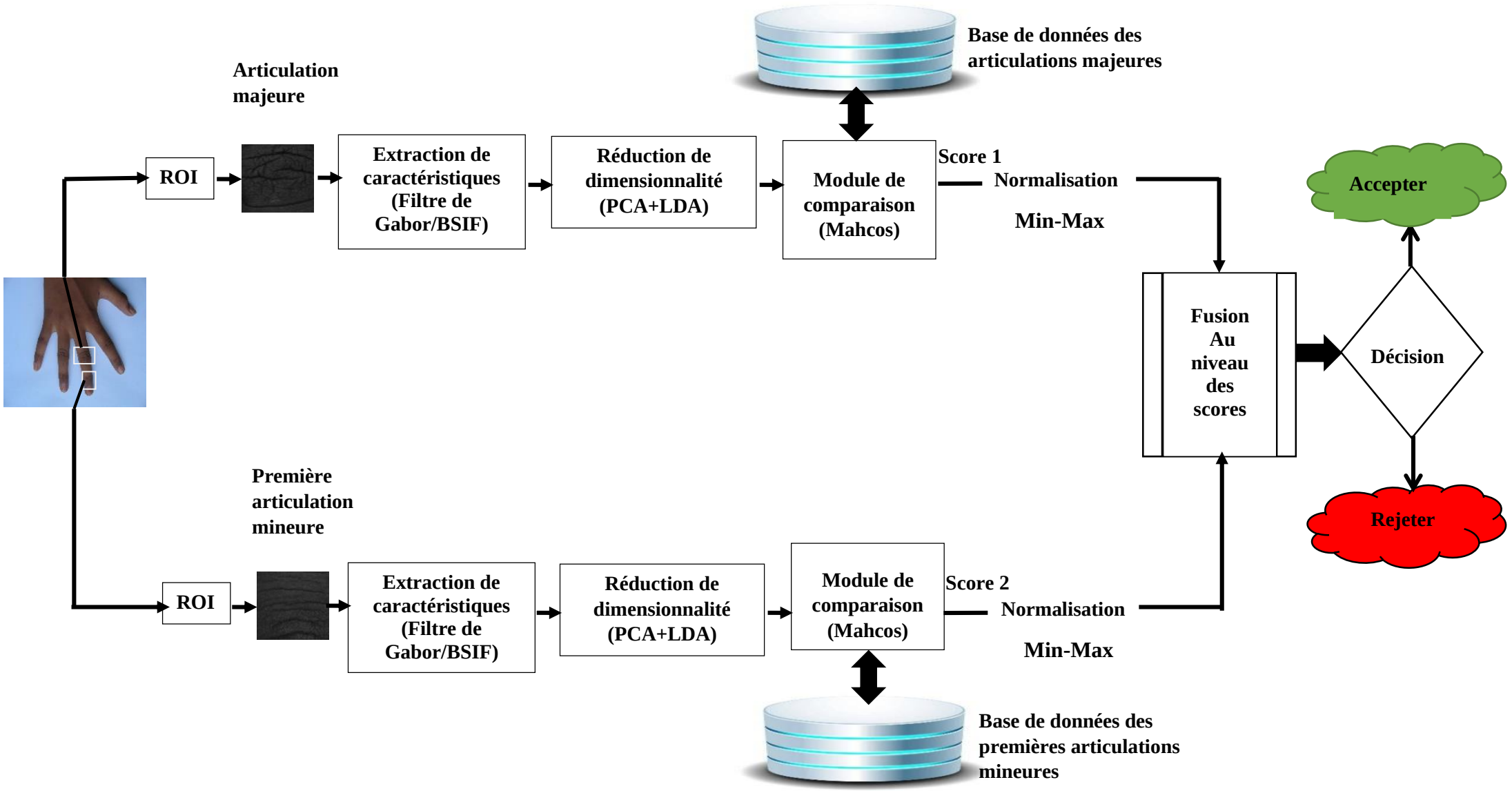


Figure.3.1 : Schéma en bloc du système biométrique proposé.

Les figures suivantes, **Figure.3.2 (a)** et **(b)** illustrent le système d'acquisition d'images utilisé pour capturer la surface du dos du doigt et l'image capturée, respectivement [37].

Figure.3.2 : (a) Système d'acquisition d'image FKP **(b)** Image de la surface du dos du doigt acquise**.**

3.3. Extraction de la région d'intérêt ROI de FKP

De nombreux types de recherche se sont concentrés sur les algorithmes de reconnaissance des articulations PIP pour évaluer les performances de la reconnaissance FKP. Les systèmes existants obtiennent une région d'intérêt (ROI) basée sur les caractéristiques de convexité locale du PIP [37].

La base de données utilisée fournit les échantillons des ROI. Ces modèles de ROI ont été extraits comme suit [38] :

Étape 1 : Binarisation de chaque image dorsale du doigt en utilisant la méthode de seuillage d'Otsu.

Étape 2 : Les images résultantes sont débruitées en supprimant automatiquement les régions/pixels isolés, de sorte que le plus long objet représentant le doigt soit conservé.

Étape 3 : La forme du doigt binarisé est utilisée pour estimer l'emplacement de l'extrémité du doigt à partir de l'enveloppe convexe des images.

Étape 4 : L'emplacement de l'extrémité du doigt est utilisé pour supprimer l'image d'arrière-plan sur l'extrémité du doigt.

Étape 5 : L'orientation des doigts est estimée à partir de l'image binarisée en utilisant les méthodes des moments.

Étape 6 : Une segmentation grossière est utilisée pour segmenter une petite partie des images acquises du doigt.

Pour estimer le facteur d'échelle pour la normalisation des échelles, la largeur de l'image résultante est calculée et utilisée. Afin de localiser le centre de l'image de l'articulation du doigt, la détection des contours de l'image résultante est utilisée. Cela est réalisé en estimant d'abord l'emplacement du centroïde de l'image détectée des contours, puis en segmentant une région de

taille fixe qui représente la région de l'articulation du doigt.

Dans ce travail, deux parties importantes sont étudiées et appelées DIP (aussi appelée première articulation mineure) et PIP (aussi appelée articulation majeure) (voir **Figure.3.3**).

Figure.3.3 : (a) Image originale de FKP. **(b)** DIP (Premier mineur) **(c)** PIP (Majeur).

3.4. Expériences

Nous présentons ici la base de données utilisée dans l'évaluation expérimentale du système d'identification et d'authentification de personnes basé sur les motifs dorsaux des doigts, ainsi que les mesures d'évaluation des performances.

3.4.1. Base de données

Le schéma proposé a été testé sur la base de données publiquement disponible d'images dorsales de la main sans contact, fournie par l'Université Polytechnique de Hong Kong [39].Cette base de données a été constituée à partir de volontaires hommes et femmes. Elle a été en grande partie acquise sur le campus de l'IIT Delhi, sur le campus de l'Université Polytechnique de Hong Kong et dans certains villages en Inde entre 2006 et 2015. La base de données contient 2505 images dorsales de la main droite de 501 sujets différents illustrant trois motifs de phalanges pour chacun des quatre doigts de chaque sujet. Toutes les images sont au format jpg (*.JPG).

Cette base de données comporte également des images dorsales supplémentaires de la main provenant de 211 sujets différents. Ces images supplémentaires montrent uniquement les régions des premières articulations mineures et majeures et n'illustrent pas les régions des deuxièmes articulations mineures des doigts. La base de données combinée des images dorsales de la main de 712 sujets différents est rendue publiquement disponible.

De plus, des images segmentées et normalisées des première et deuxième articulations mineures ainsi que de l'articulation majeure des petits, annulaires, moyens et index, ainsi que des images dorsales redimensionnées, sont également incluses. Chaque type de doigt dispose de 5 images. Nous avons seulement utilisé des images des premières articulations mineures et des articulations majeures des doigts moyens et des index. La résolution de ces images est de 100x100 pixels pour première mineur et 80x100 pour majeure. La **Figure.3.4** représente un exemple de ces images. Il est à noter que les textures et les motifs sur les images de la base de données ne sont pas

assez distinctifs sans prétraitements.

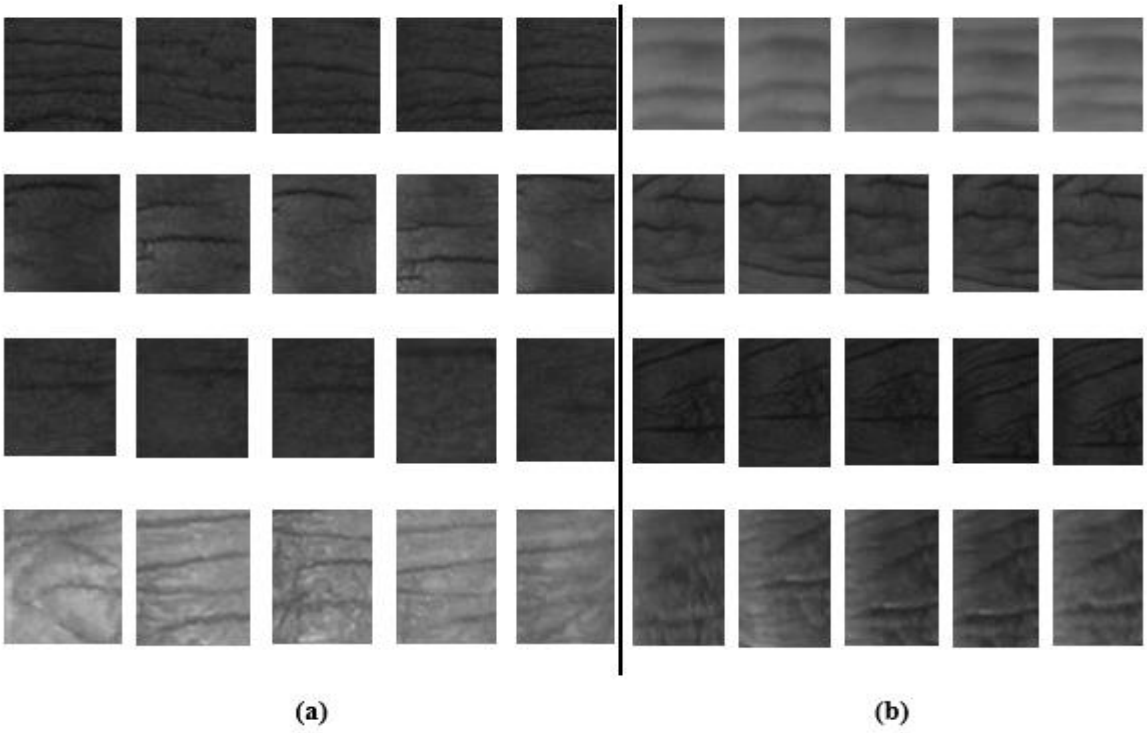


Figure.3.4 : Exemples d'images de ROI de différents doigts (moyen et index) de la base de données : (a) première mineure. (b) majeure.

3.4.2. Mesures d'évaluation des performances

En général, tout système de reconnaissance biométrique peut être évalué selon deux modes (vérification/identification). En mode d'identification, les résultats sont présentés sous forme de taux de reconnaissance appelé **Rang-1** (Rank-1) calculé selon la formule suivante :

$$Rang - 1 = \frac{N_i}{N}.100(\%) \tag{3.1}$$

Où N_i représente la quantité d'images effectivement assignées à la bonne identité, tandis que N représente le nombre total d'images tentant d'être identifiées. De plus, nous devons présenter les courbes de correspondance cumulatives **(CMC).**

En mode de vérification, le taux d'erreur égal (**EER**) est présenté, c'est-à-dire lorsque le **FAR** (taux de fausses acceptations) est égal au **FRR** (taux de fausses rejets). En plus de cela, les courbes caractéristiques de fonctionnement du récepteur (**ROC**) sont utilisées. D'autres mesures sont également largement utilisées en mode de vérification, telles que le $\boldsymbol{VR@1\%FAR}$ (c'est-à-dire le taux de vérification au point de fonctionnement de $\mathbf{1\%}\ \boldsymbol{FAR}$).

3.5. Résultats de l'expérience

Dans cette section, nous rendons compte de deux expériences différentes : Expérience I - où nous avons testé l'approche sur une seule modalité, et Expérience II - où nous avons testé l'approche sur un système multimodal.

3.5.1. Expérience I—Système unimodale

Le système unimodal où une seule modalité (Première mineure du moyen, première mineure de l'index, majeure du moyen et majeure de l'index) a été utilisée séparément à l'autre. Dans notre expérience, 4 images de chaque modalité ont été utilisées lors de la phase d'enrôlement. Ce choix vise à la validation du système biométrique choisis. Une seule image a été utilisée lors de la phase de test. Cette expérience consiste à l'utilisation de chaque type de modalité séparément avec les différents algorithmes (**filtre de Gabor**, **BSIF**) pour l'extraction de caractéristiques. En outre, pour chaque algorithme nous avons présenté les résultats trouvés par la variation des différents paramètres dans un tableau.

3.5.1.1. Résultats d'utilisation du filtre de Gabor

L'expérience avec le filtre de Gabor comprendra l'utilisation de quatre modalités, à savoir (la première mineure du moyen, la première mineure de l'index, la majeure du moyen et la majeure de l'index). Nous travaillerons sur les paramètres du filtre de Gabor dans l'ordre suivant **: l'orientation, l'échelle, puis le sous-échantillonnage.** Chaque fois, nous appliquerons ces paramètres aux quatre modalités étudiées. L'expérience sera divisée en trois étapes :

- **Variation de l'orientation :**

Le premier changement sera lié à l'orientation, sa valeur est comprise entre **5** et **12,** puis nous déterminons la meilleure valeur parmi tous les résultats. Cette valeur sera appliquée dans les étapes suivantes.

- **Variation de l'échelle :**

Deuxièmement, une fois que nous avons déterminé la meilleure valeur pour l'orientation, nous ajusterons les valeurs de l'échelle dans une plage allant de **6** à **12** afin de trouver la meilleure valeur pour cette variable.

- **Variation du sous-échantillonnage :**

Troisièmement, une fois que nous avons déterminé les deux meilleures valeurs pour les variables précédentes, à savoir l'échelle et l'orientation, nous allons modifier la troisième variable qui est le sous-échantillonnage pour quelle prennent une des valeurs **128, 64** et **32**. Nous sélectionnerons

ensuite la meilleure parmi ces trois valeurs. Nous donnons plus d'importance à l'identification.

Tableau.3.1 : Performance : **EER, Rank-1** et **VR@1%FAR** pour la modalité première mineure du moyen avec variation des paramètres du filtre Gabor.

Modalité : Première mineure du moyen			
Type de variation : l'orientation			
Orientation/échelle/sous-échantillonnage	Identification	Authentification	
	Rank-1 (%)	EER (%)	VR@ 1% FAR (%)
6/5/64	38.06	22.48	51.69
8/5/64	44.66	19.58	57.44
9/5/64	44.52	19.26	57.16
10/5/64	**44.66**	**18.98**	**58.15**
11/5/64	44.38	19.10	57.02
12/5/64	43.54	19.45	57.30
Type de variation : l'échelle			
Orientation/échelle/sous-échantillonnage	Identification	Authentification	
	Rank-1 (%)	EER (%)	VR@ 1% FAR (%)
10/5/64	44.66	18.98	58.15
10/7/64	54.78	16.74	66.15
10/8/64	57.44	15.44	68.96
10/9/64	60.39	14.26	72.05
10/10/64	**62.78**	**13.99**	**74.16**
10/11/64	62.64	14.02	74.72
10/12/64	62.64	14.30	74.72
Type de variation : sous-échantillonnage			
Orientation/échelle/sous-échantillonnage	Identification	Authentification	
	Rank-1 (%)	EER (%)	VR@ 1% FAR (%)
10/10/128	62.08	14.16	72.89
10/10/64	62.78	13.99	74.16
10/10/32	64.33	11.67	74.16
10/12/32	**65.17**	**13.79**	**74.72**

Les résultats des changements ont montré que le meilleur résultat de cette modalité était à (**10/12/32**).

Tableau.3. 2 : Performance : **EER, Rank-1** et **VR@1%FAR** pour la modalité première mineure de l'index avec variation des paramètres de filtre Gabor.

Modalité : Première mineure de l'index			
Type de variation : l'orientation			
Orientation/échelle/sous-échantillonnage	Identification	Authentification	
	Rank-1 (%)	EER (%)	VR@ 1% FAR (%)
6/5/64	46.63	17.69	61.80
7/5/64	51.54	18.12	64.89
8/5/64	55.34	17.56	66.85
9/5/64	55.76	17.39	67.28
10/5/64	**56.46**	**17.40**	**67.13**
11/5/64	56.32	17.69	67.56
12/5/64	55.20	18.02	67.42
Type de variation : l'échelle			
Orientation/échelle/sous-échantillonnage	Identification	Authentification	
	Rank-1 (%)	EER (%)	VR@ 1% FAR (%)
10/5/64	56.46	17.40	67.13
10/7/64	63.20	14.87	74.58
10/8/64	66.29	13.63	77.11
10/9/64	68.96	12.78	78.93
10/10/64	71.49	11.53	80.34
10/11/64	71.49	11.09	80.76
10/12/64	**71.77**	**11.31**	**88.76**
Type de variation : sous-échantillonnage			
Orientation/échelle/sous-échantillonnage	Identification	Authentification	
	Rank-1 (%)	EER (%)	VR@ 1% FAR (%)
10/12/128	69.80	12.06	80.20
10/12/64	71.77	11.31	80.76
10/12/32	**72.19**	**10.66**	**82.16**

Les résultats des changements ont montré que le meilleur résultat de cette modalité était à (**10/12/32**).

Tableau.3. 3 : Performance : **EER, Rank-1** et **VR@1%FAR** pour la modalité majeure du moyen avec variation des paramètres de filtre Gabor.

Modalité : Majeure du moyen			
Type de variation : l'orientation			
Orientation/échelle/sous-échantillonnage	Identification	Authentification	
	Rank-1 (%)	EER (%)	VR@ 1% FAR (%)
6/5/64	70.65	10.66	81.88
7/5/64	74.44	9.82	84.13
8/5/64	**78.09**	**8.44**	**85.25**
12/5/64	77.81	8.72	85.39
Type de variation : l'échelle			
Orientation/échelle/sous-échantillonnage	Identification	Authentification	
	Rank-1 (%)	EER (%)	VR@ 1% FAR (%)
8/5/64	78.09	8.44	85.25
8/**6**/64	81.60	7.45	87.92
8/**7**/64	82.87	7.16	89.47
8/**8**/64	84.83	6.47	90.45
8/**9**/64	85.39	5.90	91.29
8/**10**/64	85.96	5.76	91.29
8/**12**/64	**86.24**	**5.75**	**91.43**
Type de variation : sous-échantillonnage			
Orientation/échelle/sous-échantillonnage	Identification	Authentification	
	Rank-1 (%)	EER (%)	VR@ 1% FAR (%)
8/12/**128**	85.67	6.33	90.31
8/12/**64**	86.24	5.75	91.43
8/12/32	**86.80**	**5.59**	**92.28**

Les résultats des changements ont montré que le meilleur résultat de cette modalité était à (**8/12/32**).

Tableau.3. 4 : Performance : **EER, Rank-1** et **VR@1%FAR** pour la modalité majeure de l'index avec variation des paramètres de filtre Gabor.

Modalité : Majeure de l'index			
Type de variation : l'orientation			
Orientation/échelle/sous-échantillonnage	Identification	Authentification	
	Rank-1 (%)	EER (%)	VR@ 1% FAR (%)
6/5/64	61.24	14.64	72.33
7/5/64	64.33	12.95	75.28
8/5/64	68.82	12.55	77.39
9/5/64	**69.66**	**12.24**	**77.39**
10/5/64	68.40	12.23	76.97
11/5/64	68.12	12.07	77.11
12/5/64	67.84	11.97	76.83
Type de variation : l'échelle			
Orientation/échelle/sous-échantillonnage	Identification	Authentification	
	Rank-1 (%)	EER (%)	VR@ 1% FAR (%)
9/**5**/64	69.66	12.24	77.39
9/**7**/64	75.00	9.08	83.85
9/**8**/64	77.39	7.86	85.36
9/**9**/64	78.79	7.16	87.36
9/**10**/64	80.06	7.03	87.92
9/**11**/64	80.20	7.02	88.34
9/12/64	**80.48**	**6.87**	**88.34**
Type de variation : sous-échantillonnage			
Orientation/échelle/sous-échantillonnage	Identification	Authentification	
	Rank-1 (%)	EER (%)	VR@ 1% FAR (%)
9/12/128	78.37	8.01	86.66
9/12/64	**80.48**	**6.87**	**88.34**
9/12/32	80.20	7.30	88.20

Les résultats des changements ont montré que le meilleur résultat de cette modalité était à (**9/12/64**).

3.5.1.2. Résultats d'utilisation du descripteur BSIF

- **Variation de la taille et la longueur**

Chaque filtre BSIF avec une combinaison de paramètres différente est appliqué à chaque modalité individuelle (Première mineure du moyen, première mineure de l'index, majeure du moyen et majeure de l'index). Cela aidera à sélectionner les meilleurs paramètres BSIF. Cependant, les paramètres du filtre (taille du filtre (l) et longueur du filtre (n)). La taille du filtre de BSIF varie de (5x5 à 17x17), nous avons des filtres de 7 tailles différentes. La longueur des filtres du BSIF est fixée à 12 bits. Les résultats obtenus sont organisé dans les **Tableaux 3.5**, **3.6**, **3.7** et **3.8**

Tableau.3.5 : Performance : **EER**, **Rank-1** et **VR@1 % FAR** pour la première articulation mineure du moyen en utilisant différentes tailles de BSIF.

Première articulation mineure du moyen	Identification Rank-1 (%)	Authentification	
		EER (%)	VR@ 1 FAR (%)
17x17 et 12 bit	**82.02**	**4.49**	**90.87**
15x15 et 12 bit	76.12	6.59	88.06
13x13 et 12 bit	69.24	8.00	83.85
11x11 et 12 bit	54.78	11.94	74.58
9x9 et 12 bit	36.94	15.06	57.02
7x7 et 12 bit	19.52	21.47	36.66
5x5 et 12 bit	8.01	29.08	18.68

Tableau.3.6 : Performance : **EER**, **Rank-1** et **VR@1 % FAR** pour la première articulation mineure de l'index en utilisant différentes tailles de BSIF.

Première articulation mineure de l'index	Identification Rank-1 (%)	Authentification	
		EER (%)	VR@ 1 FAR (%)
17x17 et 12 bit	**74.44**	**7.17**	**86.10**
15x15 et 12 bit	68.12	8.98	82.72
13x13 et 12 bit	59.69	9.65	76.54
11x11 et 12 bit	47.47	12.78	68.40
9x9 et 12 bit	31.32	16.43	48.60
7x7 et 12 bit	15.31	25.73	31.18
5x5 et 12 bit	8.15	31.25	20.08

Tableau.3.7 : Performance : **EER**, **Rank-1** et **VR@1%FAR** pour l'articulation majeure du moyen en utilisant différentes tailles de BSIF.

Articulation majeure de l'index	Identification Rank-1 (%)	Authentification	
		EER (%)	VR@ 1% FAR (%)
17x17 et 12 bit	**92.13**	**3.09**	**96.35**
15x15 et 12 bit	89.61	3.25	94.66
13x13 et 12 bit	86.59	4.36	93.96
11x11 et 12 bit	78.65	6.17	89.04
9x9 et 12 bit	64.61	8.43	79.35
7x7 et 12 bit	38.20	15.84	56.60
5x5 et 12 bit	14.19	23.16	32.30

Tableau3.8 : Performance : **EER**, **Rank-1** et **VR@1%FAR** pour l'articulation majeure de l'index en utilisant différentes tailles de BSIF.

Articulation majeure du moyen	Identification Rank-1 (%)	Authentification	
		EER (%)	VR@ 1% FAR (%)
17x17 et 12 bit	**95.51**	**2.25**	**97.61**
15x15 et 12 bit	92.70	2.96	96.49
13x13 et 12 bit	90.59	2.96	95.65
11x11 et 12 bit	85.67	4.49	92.56
9x9 et 12 bit	72.89	6.32	86.52
7x7 et 12 bit	46.35	11.92	64.61
5x5 et 12 bit	14.04	21.53	34.13

D'après ces résultats**,** nous constatons que la taille de filtre **17x17** donne des meilleures performances pour tous les doigts. Cette valeur sera adoptée dans notre système biométrique.

Dans le but de déterminer le nombre de bits optimale des filtres, nous avons fait varier sa longueur (de 5 bits à 12 bits), ainsi nous avons des filtres de 08 longueurs différentes. Les **Tableaux 3.9**, **3.10**, **3.11** et **3.12** regroupent les résultats obtenus.

Tableau.3.9 : Performance : **EER**, **Rank-1** et **VR@1 % FAR** pour la première articulation mineure du moyen en utilisant différentes longueurs de BSIF.

Première articulation mineure du moyen	Identification Rank-1 (%)	Authentification	
		EER (%)	VR@ 1 FAR (%)
17x17 et 12 bit	**82.02**	**4.49**	**90.87**
17x17 et 11 bit	58.01	10.67	75.56
17x17 et 10 bit	68.12	7.44	84.27
17x17 et 9bit	31.04	35.67	22.47
17x17 et 8 bit	34.13	36.66	36.24
17x17 et 7 bit	3.37	45.77	7.87
17x17 et 6 bit	6.74	40.74	12.78
17x17 et 5 bit	2.11	45.48	7.72

Tableau.3.10 : Performance : **EER**, **Rank-1** et **VR@1 % FAR** pour la première articulation mineure de l'index en utilisant différentes longueurs de BSIF.

Première articulation mineure de l'index	Identification Rank-1 (%)	Authentification	
		EER (%)	VR@ 1 FAR (%)
17x17 et 12 bit	**74.44**	**7.17**	**86.10**
17x17 et 11 bit	43.68	14.61	62.50
17x17 et 10 bit	57.02	8.70	78.65
17x17 et 9bit	43.12	22.33	44.52
17x17 et 8 bit	11.94	43.27	13.34
17x17 et 7 bit	2.67	45.12	5.62
17x17 et 6 bit	9.41	35.54	17.42
17x17 et 5 bit	0.59	45.29	4.78

D'après les résultats du système unique utilisant BSIF appliquée aux modalités (Première mineure du moyen, première mineure de l'index, majeure du moyen et majeure de l'index), le meilleur performance est obtenu avec le filtre BSIF (**17×17**) ayant une longueur de **12** bits réalisé avec la modalité majeur. Ainsi, dans le cas du doigt moyen, le système a atteint **EER= 2,25 %, Rank-1= 95,51 %** et **VR@1%FAR= 97,61 %** en modes de vérification et d'identification respectivement.

Tableau.3.11 : Performance : **EER**, **Rank-1** et **VR@1%FAR** pour l'articulation majeure du moyen en utilisant différentes longueurs de BSIF.

Articulation majeure du moyen	Identification Rank-1 (%)	Authentification	
		EER (%)	VR@ 1 FAR (%)
17x17 et 12 bit	**95.51**	**2.25**	**97.61**
17x17 et 11 bit	84.83	4.50	92.84
17x17 et 10 bit	90.03	2.25	96.77
17x17 et 9bit	45.22	37.08	25.28
17x17 et 8 bit	23.60	41.31	18.82
17x17 et 7 bit	5.48	45.40	8.99
17x17 et 6 bit	5.62	44.10	8.57
17x17 et 5 bit	6.74	39.19	13.06

Tableau.3.12 : Performance : **EER**, **Rank-1** et **VR@1%FAR** pour l'articulation majeure de l'index en utilisant différentes longueurs de BSIF.

Articulation majeure de l'index	Identification Rank-1 (%)	Authentification	
		EER (%)	VR@ 1 FAR (%)
17x17 et 12 bit	**92.13**	**3.09**	**96.35**
17x17 et 11 bit	77.39	7.17	86.66
17x17 et 10 bit	83.71	4.75	91.85
17x17 et 9bit	40.03	38.11	8.29
17x17 et 8 bit	20.93	43.09	9.97
17x17 et 7 bit	3.79	44.51	6.32
17x17 et 6 bit	3.51	44.95	6.88
17x17 et 5 bit	1.40	45.32	6.46

- **Résultats de l'implémentation de BSIF :**

La **Figure.3.5** illustre l'image résultante après application de la méthode du BSIF avec un filtre de taille 17x17 ayant respectivement 11 bits et 12 bits.

Visuellement, nous constatons que les motifs des empreintes est amplifié ce qui donne une meilleure possibilité de distinctions.

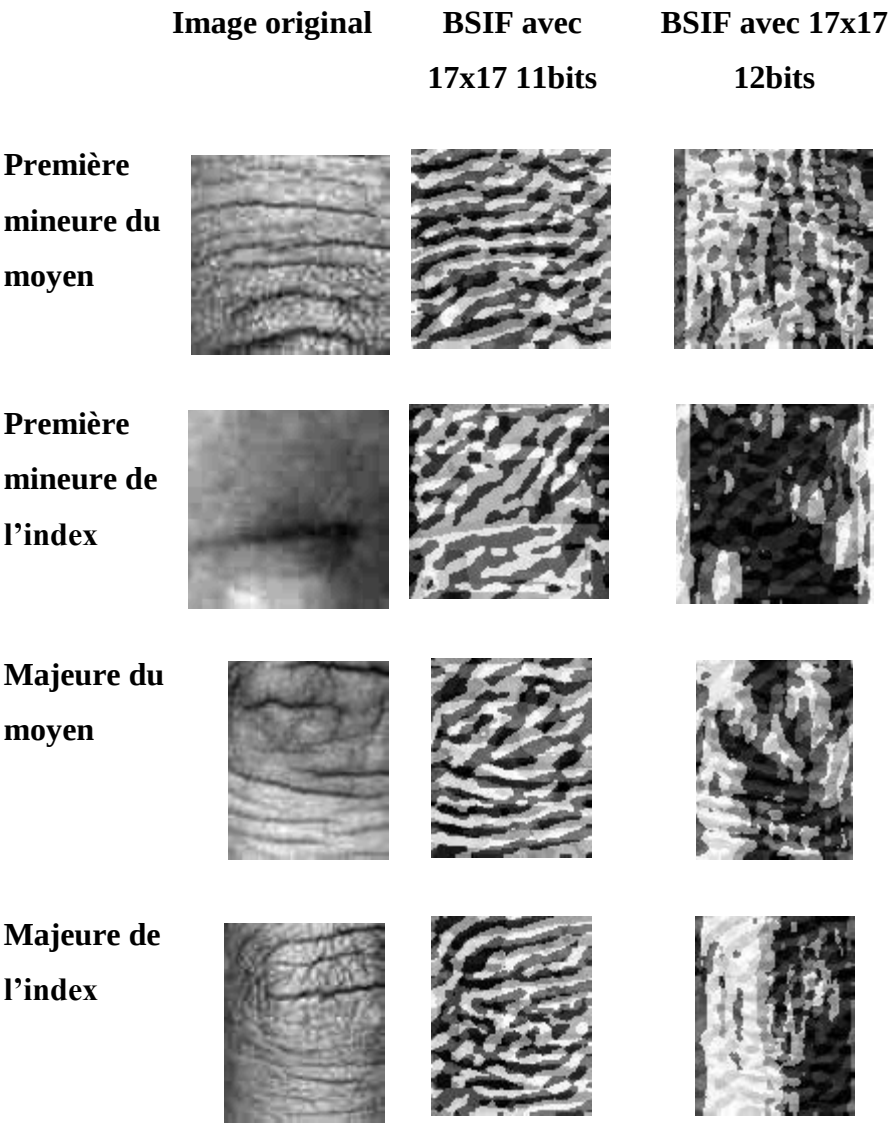


Figure.3.5 : Exemples des images de ROI première mineure et majeure et avec résultats après application du filtre BSIF.

3.5.2. Expérience II – système multimodal

L'objectif principal de cette expérience est d'étudier les performances du système sous la fusion d'informations, car les systèmes multimodaux qui combinent des informations provenant de différentes sources sont généralement capables d'améliorer la précision par rapport à celle des systèmes biométriques individuels.

Dans cette expérience, nous allons fusionner les informations de différentes modalités de chaque personne (Première mineure du moyen, première mineure de l'index, majeure du moyen et majeure de l'index). Néanmoins, cette fusion a été faite au niveau de scores pour chaque algorithme séparé (filtre de Gabor et BSIF).

Nous avons utilisé deux modalités ensemble, trois modalités ensemble et quatre modalités ensemble. Plus précisément, les informations sont combinées en utilisant plusieurs règles de T-norme (**Frank** et **Yager**). De plus, des fonctions classiques telles que la somme **(Sum)**, la somme pondérée **(Sum_w)**, le maximum **(Max)** et le minimum **(Min)** sont rapportées. Nous avons présenté les résultats trouvés par chaque règle dans un tableau.

3.5.2.1. Résultats d'application du filtre de Gabor

En complément des résultats du filtre de Gabor obtenu précédemment, et pour chaque groupe de multimodalité (2, 3 et 4 modalités), nous avons obtenu les résultats présentés dans les **Tableaux.3.13**, **3.14**, **3.15**, **3.16**, **3.17** et **3.19** pour chaque méthode de fusion, à savoir :

- Majeure du moyen(**MM)** *en anglais Major Middle.*
- Majeure de l'index (**MI)** *en anglais Major Index.*
- Première mineure du moyen (**FMM)** *en anglais First Minor Middle.*
- Première mineure de l'index (**FMI)** *en anglais First Minor Index.*

Tableau.3.13 : EER, **Rank-1** et **VR@1%FAR** obtenus par règle de fusion (**Sum**) avec le filtre de Gabor.

Règle : Sum			
Modalités	Identification Rank-1 (%)	Authentification	
		EER (%)	VR@ 1% FAR (%)
MM/MI	**93.54**	**3.20**	**96.49**
MM/FMM	91.29	4.24	94.80
MM/FMI	92.70	3.39	95.79
MI/FMM	91.29	4.24	94.80
MI/FMI	85.81	5.22	91.71
FMM/FMI	81.46	6.51	89.89
MM/MI/FMM	94.52	2.56	96.91
MM/MI/FMI	**95.08**	**2.97**	**96.93**
MM/FMM/FMI	93.26	3.10	96.21
MI/FMM/FMI	91.85	3.35	95.79
MM/MI/FMM/FMI	**95.08**	**2.38**	**96.91**

Tableau.3. 14 : EER, **Rank-1** et **VR@1%FAR** obtenus par règle de fusion (**Sum_w**) avec le filtre de Gabor.

Règle : Sum_w			
Modalités	Identification Rank-1 (%)	Authentification	
		EER (%)	VR@ 1% FAR (%)
MM/MI	**93.54**	**2.99**	**96.07**
MM/FMM	91.71	4.07	94.80
MM/FMI	92.56	3.22	95.93
MI/FMM	90.53	3.85	94.38
MI/FMI	86.24	5.21	91.57
FMM/FMI	81.46	6.51	89.89
MM/MI/FMM	94.52	2.82	96.63
MM/MI/FMI	**95.22**	**3.09**	**96.77**
MM/FMM/FMI	93.68	2.85	96.35
MI/FMM/FMI	91.43	3.64	95.51
MM/MI/FMM/FMI	**95.37**	**2.81**	**96.91**

Tableau.3. 15 : EER, **Rank-1** et **VR@1%FAR** obtenus par règle de fusion (**Min**) avec le filtre de Gabor.

Règle : Min			
Modalités	Identification Rank-1 (%)	Authentification	
		EER (%)	VR@ 1% FAR (%)
MM/MI	91.43	3.53	95.37
MM/FMM	85.67	5.10	92.98
MM/FMI	**91.99**	**3.52**	**95.08**
MI/FMM	88.76	3.48	94.38
MI/FMI	83.15	5.06	91.57
FMM/FMI	80.34	6.76	89.33
MM/MI/FMM	**92.56**	**2.85**	**96.35**
MM/MI/FMI	92.28	3.08	96.35
MM/FMM/FMI	88.76	3.22	95. 79
MI/FMM/FMI	89.75	2.90	95.37
MM/MI/FMM/FMI	**92.28**	**3.08**	**96.35**

Tableau.3. 16 : **EER**, **Rank-1** et **VR@1%FAR** obtenus par règle de fusion (**Max**) avec le filtre de Gabor.

Règle : Max			
Modalités	Identification Rank-1 (%)	Authentification	
		EER (%)	VR@ 1% FAR (%)
MM/MI	**86.80**	**5.77**	**91.71**
MM/FMM	84.97	6.43	90.73
MM/FMI	77.67	8.09	84.83
MI/FMM	78.23	9.06	85.39
MI/FMI	71.35	12.30	79.49
FMM/FMI	68.82	12.88	76.69
MM/MI/FMM	**85.81**	**6.40**	**90.31**
MM/MI/FMI	78.93	7.93	86.38
MM/FMM/FMI	78.23	8.21	85.81
MI/FMM/FMI	72.61	11.39	80.34
MM/MI/FMM/FMI	**79.49**	**8.08**	**86.52**

Tableau.3. 17 : EER, **Rank-1** et **VR@1%FAR** obtenus par règle de fusion (**Yage**r) avec le filtre de Gabor.

Règle : Yager avec p=1.75			
Modalités	Identification Rank-1 (%)	Authentification	
		EER (%)	VR@ 1% FAR (%)
MM/MI	**93.96**	**3.23**	**96.21**
MM/FMM	90.73	4.49	94.66
MM/FMI	92.56	3.23	95.79
MI/FMM	90.87	3.79	94.66
MI/FMI	86.10	4.91	91.71
FMM/FMI	82.30	6.32	90.31
MM/MI/FMM	**94.52**	**2.53**	**97.05**
MM/MI/FMI	95.37	2.92	96.77
MM/FMM/FMI	92.42	3.09	96.07
MI/FMM/FMI	93.42	3.09	95.93
MM/MI/FMM/FMI	**95.08**	**2.24**	**97.05**

Tableau.3. 18 : EER, **Rank-1** et **VR@1%FAR** obtenus par règle de fusion (**Frank)** avec le filtre de Gabor.

Règle : Frank avec p=1.75			
Modalités	Identification	Authentification	
	Rank-1 (%)	EER (%)	VR@ 1% FAR (%)
MM/MI	**95.22**	**2.85**	**96.91**
MM/FMM	94.52	2.81	96.91
MM/FMI	95.08	2.39	97.05
MI/FMM	94.10	2.95	96.49
MI/FMI	93.82	2.66	96.21
FMM/FMI	92.42	2.82	96.63
MM/MI/FMM	95.22	2.52	97.05
MM/MI/FMI	**95.37**	**2.67**	**96.91**
MM/FMM/FMI	94.66	2.39	97.05
MI/FMM/FMI	94.80	2.81	96.35
MM/MI/FMM/FMI	**95.22**	**2.39**	**97.05**

Il est clair que la fusion des scores des informations **MM / MI / FMM / FMI** en utilisant les règles de fusion Somme pondérée (**Sum_w**) , Somme (**Sum**) , **Frank** et **Yager** conduit à des performances supérieures en termes d'**EER**, **Rank-1** et **VR @ 1% FAR** pour les modes de vérification et d'identification. Par exemple, en utilisant **Yager** pour l'authentification (voir **Tableau 3.17**), nous obtenons un **EER** de **2.24%** et un **Rank-1** de **95.08 %** pour l'identification. D'autre part, la **Sum_w** (voir **Tableaux.3.14**) donne respectivement **2.81%** (**EER**) et **95.37%** (**Rank-1**) pour la vérification et l'identification. Les règles de **Sum, Sum_w, Yager** et **Frank** offrent de meilleurs résultats pour le système proposé par rapport à d'autres règles connues telles que, le **Min** et le **Max.**

3.5.2.2. Résultats trouvés avec le descripteur BSIF

Selon l'implémentation de l'algorithme BSIF pour chaque combinaison multimodale (2, 3 et 4 modalités), nous avons obtenus les résultats groupés dans les **Tableaux.3.19, 3.20 ,3.21, 3.22, 3.23** et **3.24** pour chaque règle de fusion.

Tableau.3.19 : **EER**, **Rank-1** et **VR@1%FAR** obtenus par règle de fusion (**Sum**) avec le descripteur BSIF.

Règle : Sum			
Modalités	Identification Rank-1 (%)	Authentification	
		EER (%)	VR@ 1% FAR (%)
MM/MI	**96.91**	**1.41**	**98.74**
MM/FMM	96.77	1.40	98.60
MM/FMI	96.35	1.70	97.89
MI/FMM	96.07	1.44	98.31
MI/FMI	95.08	2.24	97.47
FMM/FMI	90.87	3.09	96.35
MM/MI/FMM	**98.03**	**0.99**	**99.02**
MM/MI/FMI	97.89	1.27	98.74
MM/FMM/FMI	96.91	1.41	98.46
MI/FMM/FMI	97.05	1.52	98.46
MM/MI/FMM/FMI	**97.89**	**0.98**	**99.02**

Tableau.3.20 : **EER**, **Rank-1** et **VR@1%FAR** obtenus par règle de fusion (**Sum_w**) avec le descripteur BSIF.

Règle : Sum_w			
Modalités	Identification Rank-1 (%)	Authentification	
		EER (%)	VR@ 1% FAR (%)
MM/MI	97.19	1.40	98.60
MM/FMM	**97.47**	**1.41**	**98.60**
MM/FMI	96.91	1.60	98.17
MI/FMM	96.07	1.44	98.31
MI/FMI	95.51	2.25	97.47
FMM/FMI	90.87	3.09	96.35
MM/MI/FMM	**98.03**	**0.99**	**99.02**
MM/MI/FMI	97.75	1.25	98.74
MM/FMM/FMI	97.33	1.30	98.60
MI/FMM/FMI	97.19	1.41	98.60
MM/MI/FMM/FMI	**98.03**	**0.84**	**99.16**

Tableau.3.21 : **EER**, **Rank-1** et **VR@1%FAR** obtenus par règle de fusion (**Min**) avec le descripteur BSIF.

Règle : Min			
Modalités	Identification Rank-1 (%)	Authentification	
		EER (%)	VR@ 1% FAR (%)
MM/MI	94.10	1.82	97.89
MM/FMM	88.90	2.33	96.07
MM/FMI	87.78	2.99	96.35
MI/FMM	**95.37**	**1.68**	**98.03**
MI/FMI	91.71	2.17	97.33
FMM/FMI	87.64	3.24	94.10
MM/MI/FMM	**95.65**	**1.68**	**98.17**
MM/MI/FMI	93.26	1.80	97.75
MM/FMM/FMI	91.15	2.11	97.33
MI/FMM/FMI	94.80	1.54	98.03
MM/MI/FMM/FMI	**94. 94**	**1.39**	**98.31**

Tableau.3.22 : **EER**, **Rank-1** et **VR@1%FAR** obtenus par règle de fusion (**Max**) avec le descripteur BSIF.

Règle : Max			
Modalités	Identification Rank-1 (%)	Authentification	
		EER (%)	VR@ 1% FAR (%)
MM/MI	95.22	2.29	97. 47
MM/FMM	**95.65**	**2.24**	**97.61**
MM/FMI	94.80	2.69	97.05
MI/FMM	92.98	3.10	95.93
MI/FMI	89.61	4.28	94.24
FMM/FMI	85.11	4.57	92.56
MM/MI/FMM	**95.79**	**2.23**	**97.47**
MM/MI/FMI	94.94	2.49	96.91
MM/FMM/FMI	95.08	2.52	97.17
MI/FMM/FMI	92.28	3.97	95.37
MM/MI/FMM/FMI	**95.51**	**2.52**	**97.33**

Tableau.3.23 : **EER**, **Rank-1** et **VR@1%FAR** obtenus par règle de fusion (**Yager**) avec le descripteur BSIF.

Règle : Yager avec p=1.75			
Modalités	Identification Rank-1 (%)	Authentification	
		EER (%)	VR@ 1% FAR (%)
MM/MI	**97.05**	**1.26**	**98.74**
MM/FMM	95.93	1.40	98.46
MM/FMI	95.51	1.97	97.89
MI/FMM	96.07	1.54	98.46
MI/FMI	94.52	2.24	97.61
FMM/FMI	90.87	2.95	96.35
MM/MI/FMM	**97.75**	**0.84**	**99.16**
MM/MI/FMI	97.33	1.12	98.88
MM/FMM/FMI	96.35	1.39	98.03
MI/FMM/FMI	96.91	1.41	98.60
MM/MI/FMM/FMI	**98.03**	**0.98**	**99.02**

Tableau.3.24 : **EER**, **Rank-1** et **VR@1%FAR** obtenus par règle de fusion (**Frank**) avec le descripteur BSIF.

Règle : Frank avec p=1.75			
Modalités	Identification Rank-1 (%)	Authentification	
		EER (%)	VR@ 1% FAR (%)
MM/MI	**97.89**	**0.84**	**99.16**
MM/FMM	97.47	1.13	98.88
MM/FMI	97.33	1.12	98.88
MI/FMM	97.75	1.12	98.88
MI/FMI	97.19	1.27	98.60
FMM/FMI	96.07	1.55	98.31
MM/MI/FMM	97.89	0.84	99.16
MM/MI/FMI	**98.17**	**1.12**	**98.88**
MM/FMM/FMI	97.33	1.12	98.88
MI/FMM/FMI	97.61	1.24	98.88
MM/MI/FMM/FMI	**98.03**	**0.98**	**99.02**

Il est clair que la fusion au niveau des scores des informations **MM/MI/FMM/FMI** en utilisant les règles somme pondérée (**Sum_w**), **Yager**, **Frank et** la somme **(Sum)** offre de meilleurs résultats en termes d'**EER**, **Rank-1** et **VR@1%FAR** pour les deux modes : vérification et d'identification.

A titre indicatif, en utilisant la règle de **Sum_w** pour l'authentification (voir **Tableau.3.20**), on obtient **0,84% (EER**) et **98,03% (Rank-1)** pour l'identification. En revanche, **Yager** et **Frank** (voir **Tableau.3.23 et Tableau.3.24**), ont montré **0,98 % (EER)** et **98,03 % (Rank-1)** en modes de vérification et d'identification respectivement. Les règles **Sum_w**, **Yager, Frank et Sum** donnent de meilleurs résultats pour le système proposé par rapport à d'autres règles connues telles que la règle de **Min** et de **Max**.

3.6. Etude comparative entre le système monomodal et le système multimodal

Les résultats de comparaison entre les modalités individuelles et les modalités multimodales sont également illustrés en termes de courbes **CMC** et **ROC** qui peuvent être observées dans les **Figures.3.6, 3.7, 3.8, 3.9**, **3.10** et **3.1** pour chacun des filtres Gabor et BSIF.

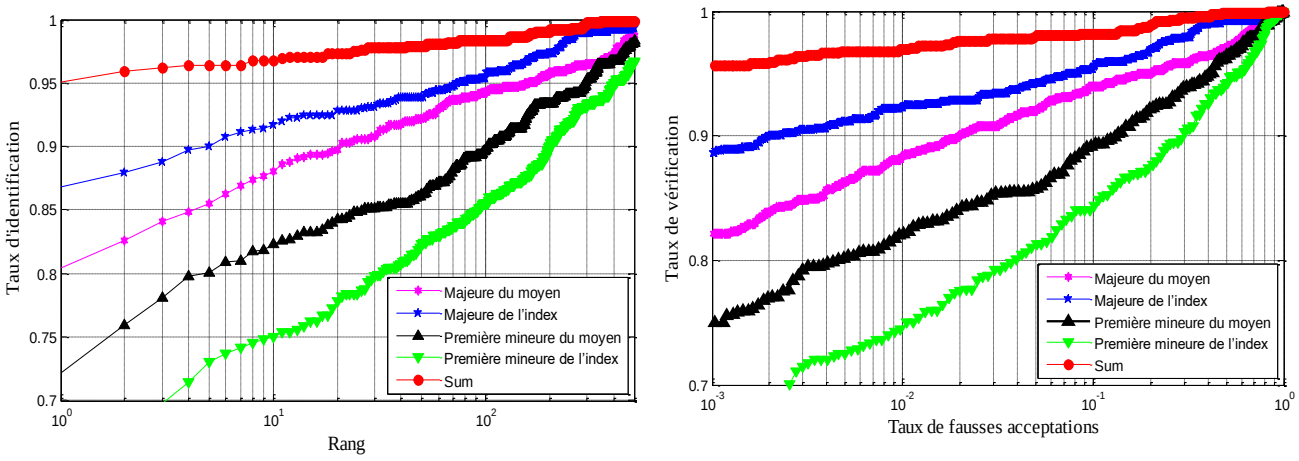


Figure.3.6 : Comparaison des systèmes unimodales et système multimodale (04 modalités/ fusion par la règle *Sum*/ descripteur filtre Gabor : **(a)** courbes CMC, **(b)** courbes ROC.

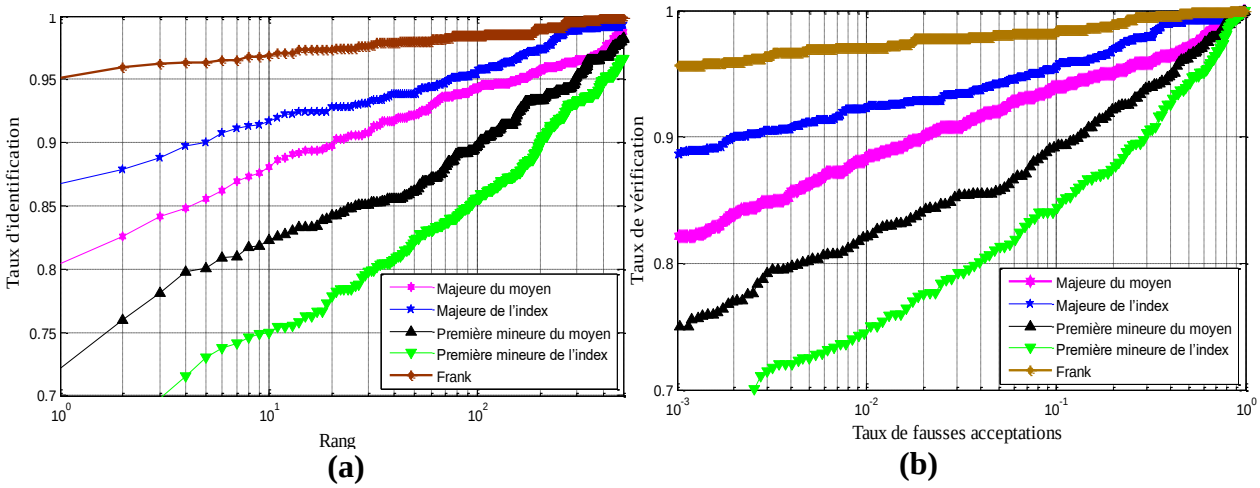
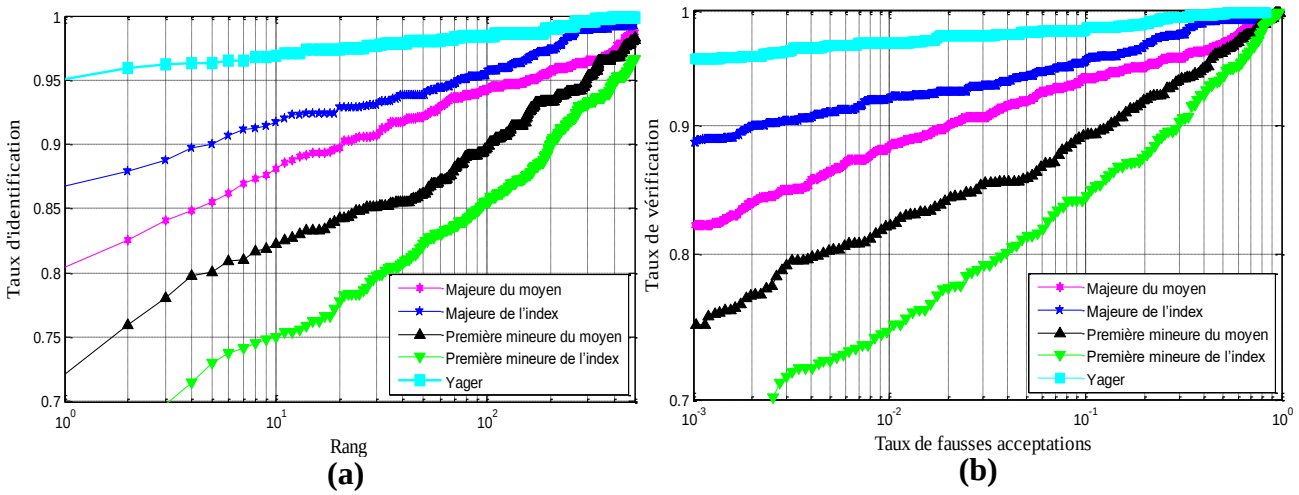
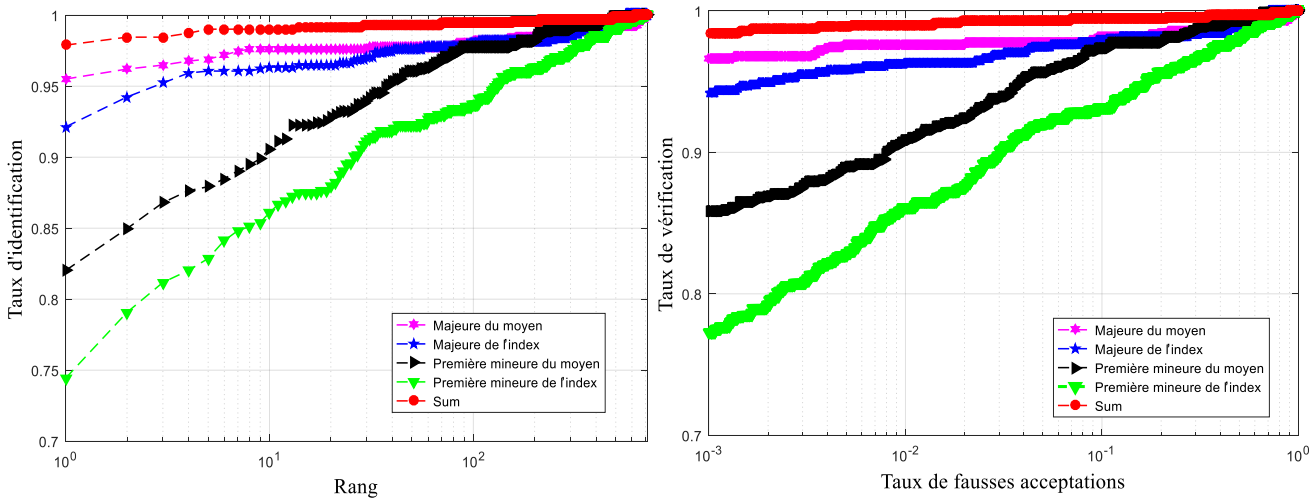


Figure.3. 7 : Comparaison des systèmes unimodales et système multimodale (04 modalités/ fusion par la règle Frank/ descripteur filtre Gabor : **(a)** courbes CMC, **(b)** courbes ROC.



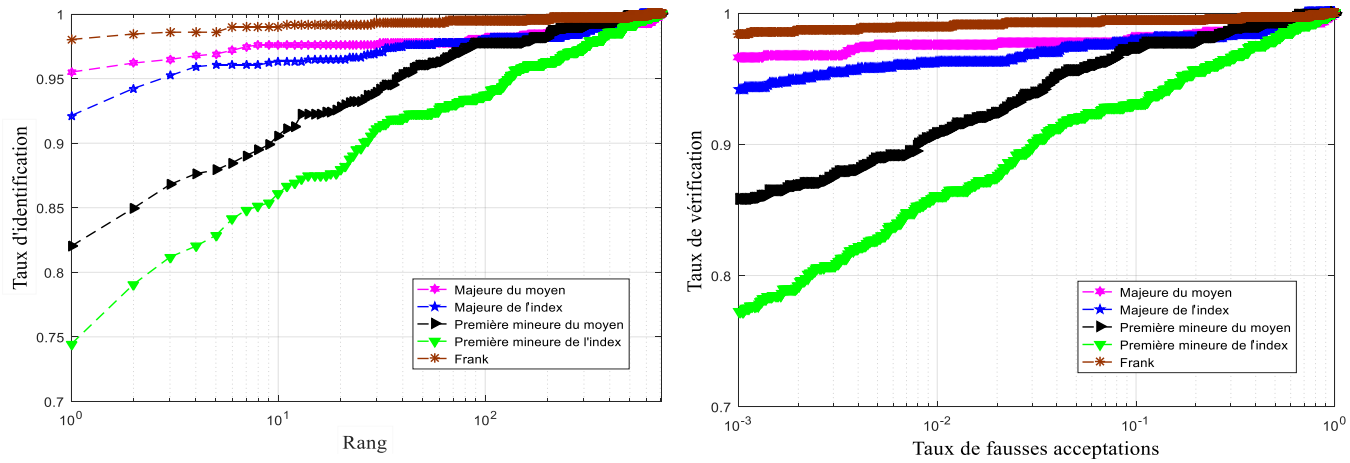
(a) **(b)**

Figure.3.8 : Comparaison des systèmes unimodales et système multimodale (04 modalités/ fusion par la règle Yager/ descripteur filtre Gabor : **(a)** courbes CMC, **(b)** courbes ROC.



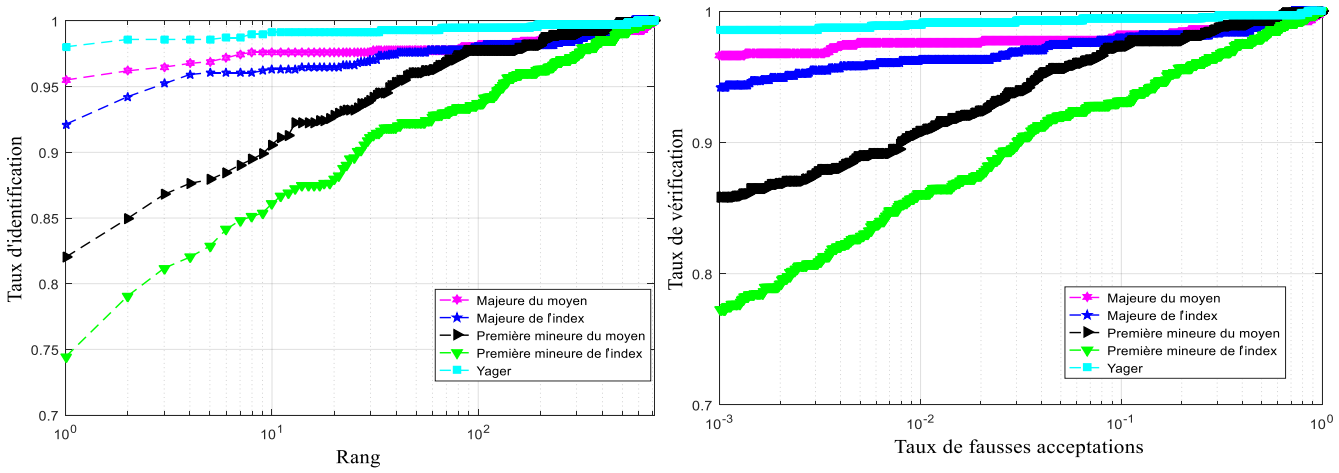
(a) **(b)**

Figure.3.9 : Comparaison des systèmes unimodales et système multimodale (04 modalités/ fusion par la règle *Sum/* descripteur filtre BSIF : **(a)** courbes CMC, **(b)** courbes ROC.



(a) **(b)**

Figure.3. 10 : Comparaison des systèmes unimodales et système multimodale (04 modalités/ fusion par la règle Frank/ descripteur filtre BSIF : **(a)** courbes CMC, **(b)** courbes ROC.



(a) **(b)**

Figure.3. 11 : Comparaison des systèmes unimodales et système multimodale (04 modalités/ fusion par la règle Yager/ descripteur filtre BSIF : **(a)** courbes CMC, **(b)** courbes ROC.

Tableau.3.25 : la comparaison entre les systèmes monomodaux et multimodaux.

Monomodal				
		Identification	Authentification	
		Rank-1 (%)	EER (%)	VR@ 1% FAR (%)
MM	Gabor	86.80	5.95	92.28
	BSIF	**95.51**	**2.25**	**97.61**
MI	Gabor	80.20	7.30	88.20
	BSIF	**92.13**	**3.09**	**96.35**
FMM	Gabor	65.17	13.79	74.72
	BSIF	**82.02**	**4.79**	**90.87**
FMI	Gabor	72.19	10.66	82.16
	BSIF	**74.44**	**7.17**	**86.10**
Multimodal				
La règle de fusion : Sum_w		Identification	Authentification	
		Rank-1 (%)	EER (%)	VR@ 1% FAR (%)
MM/MI/FMM/FMI	Gabor	95.52	2.82	96.63
	BSIF	**98.03**	**0.84**	**99.16**
La règle de fusion : Yager		Identification	Authentification	
		Rank-1 (%)	EER (%)	VR@ 1% FAR (%)
MM/MI/FMM/FMI	Gabor	95.08	2.24	97.05
	BSIF	**98.03**	**0.98**	**99.02**
La règle de fusion : Frank		Identification	Authentification	
		Rank-1 (%)	EER (%)	VR@ 1% FAR (%)
MM/MI/FMM/FMI	Gabor	95.22	2.39	97.05
	BSIF	**98.03**	**0.98**	**99.02**

D'après les résultats expérimentaux, il est constaté que l'algorithme **BSIF** offre un classement **Rank-1** (99.16%) supérieur et un **EER** (0.84%) plus faible par rapport au filtre de **Gabor,** que ce soit en utilisant un système monomodal ou un système multimodal.

En se référant aux résultats résumés dans le **Tableau.3.25**, on peut observer que l'utilisation d'un système multimodal à base du descripteur BSIF multmimodale à 04 modalité et à fusion par la méthode des somme pondérée offre un résultat satisfaisant (**Rank-1 = 99.16%** et un **EER=0.84%**) et plus performant que celui obtenu avec moins de modalité ou avec descripteur à base de filtre de Gabor.

3.7. Comparaison grossière avec des travaux sur la même base de données

Dans le but d'illustrer les performances du système proposé, nous avons recherché dans la littérature les systèmes biométriques utilisant la base de données primaire à 501 personnes ou étendue à 712. Parmi le peu de travaux nous citons :

1- L'étude mené par A. KUMAR et Z. XI dans [24], où il présente la méthode d'extraction des régions d'intérêt avec et une évaluation en utilisant un descripteur de caractéristique local (*Local Feature Descriptor « LFD »*). Dans l'expérimentation, les chercheurs ont utilisé un nombre de 10 images pour chacun des 501 personnes.

2- Le travail proposé par R. VYAS et co-auteurs dans la référence [39] dont les auteurs utilisent un descripteur à apprentissage approfondie des réseaux de neurones (Deep CNN). Le segment de la base de données utilisé est composé de 4650 images de la main droite prélevées de 501 personnes. Dans l'expérimentation, les chercheurs ont sélectionné un nombre de 09 images pour chacun des 501 personnes (mains gauche et droite) avec 5 images pour l'apprentissage, 02 images pour validation et 02 images pour le test.

Dans les **Tableaux 3.26** et **3.27**, nous avons regroupé l'ensemble des résultats obtenus par les différents systèmes proposés.

Tableau.3.26 : Résultats des méthodes appliquées à la même base de données (cas monomodal).

Monomodal				
Modalité	Méthode	Identification	Authentification	
		Rank-1 (%)	EER (%)	VR@ 1% FAR (%)
MM	**LFD** [24]	/	/	68.50
	Deep CNN [39]	88.90	4.10	92.03
	Gabor	86.80	5.95	92.28
	BSIF	**95.51**	**2.25**	**97.61**
MI	**LFD** [24]	/	/	72.60
	Deep CNN [39]	91.23	4.49	90.95
	Gabor	80.20	7.30	88.20
	BSIF	**92.13**	**3.09**	**96.35**
FMM	**LFD** [24]	/	/	50.50
	Deep CNN [39]	**84.57**	6.69	86.94
	Gabor	65.17	13.79	74.72
	BSIF	82.02	**4.79**	**90.87**
FMI	**LFD** [24]	/	/	56.74
	Deep CNN [39]	**74.81**	**6.41**	85.56
	Gabor	72.19	10.66	82.16
	BSIF	74.44	7.17	**86.10**

Tableau.3.27 : Résultats des méthodes appliquées à la même base de données (cas Multimodal).

		Multimodale	
Modalité	Méthode	Authentification	
		EER (%)	VR@ 1% FAR (%)
MM/FMM	**LFD** [24]	/	84.50
	Gabor	4.07	94.80
	BSIF	**1.41**	**98.60**
MI/FMI	**LFD** [24]	/	72.70
	Gabor	5.21	91.57
	BSIF	2.25	97.47

D'après le **Tableau .3.26**, nous constatons que notre système proposé réalise des meilleures performances par rapport aux deux autres systèmes. Avec le descripteur **BSIF** le taux d'identification **Rank-1 (95.51%)** dans le cas de la modalité majeur de la moyenne dépasse les taux des modalités individuelles de toutes les autres méthodes. Aussi, dans le cas d'authentification, le taux de reconnaissance atteint **97.61%** (cas du descripteur **BSIF**) nettement supérieur à celui de la méthode **Deep CNN (92.03%)** et celui de la méthode **LFD (72.60%).** De même l'**EER** enregistré **(2.25%)** est relativement le plus faible.

Quant à la multimodalité, nous constatons d'après le **Tableau .3.27** que dans le cas de combinaison des deux modalités, majeur et premier mineur, la système proposé permet d'atteindre un taux de reconnaissance égale à **98.60%** avec une erreur **EER=1.41%** ce qui est nettement supérieur à celui offert par le système à base de la méthode **LFD** dont le meilleur taux est égale à **84.50%** avec un taux d'erreur **EER=4.07%.**

3.8. Conclusion

Dans ce chapitre, nous avons présenté notre système de reconnaissance basé sur l'empreinte des articulations des doigts FKP. En particulier, nous avons constaté que le descripteur BSIF présente des performances nettement meilleures que l'algorithme Gabor que nous avons testé. Pour un système de vérification et/ou d'identification. Aussi, des meilleurs résultats sont obtenus avec la fusion des quatre modalités par la méthode

Les résultats expérimentaux présentés ont clairement démontré la que l'approche multimodale à base des de la méthode BSIF avec fusion au niveau de score par la méthode des somme pondéré et classification K-NN offre des performances supérieures par rapport au système

monomodal. Les résultats obtenus montrent d'une manière grossière que le système proposé à base du descripteur BSIF arrive à améliorer les taux de reconnaissance et le taux d'égale erreur par rapport à au deux autres méthodes présentées dans la comparaison.

Conclusion générale

Conclusion générale

Les biométriques jouent un rôle important dans le monde actuel. Les systèmes biométriques, et en particulier les systèmes biométriques multiples, ont un énorme potentiel de croissance. En utilisant les technologies biométriques, les procédures d'accès peuvent être simplifiées, accélérées et rendues plus sûres.

Durant ce travail de mémoire, d'abord nous avons commencé par en introduisant des notions de base sur les systèmes biométriques en général et les outils pour les évaluer. Ensuite nous avons présenté les différents aspects des systèmes biométriques multimodaux par leur architecture, leurs sources d'information et leurs niveaux de fusion.

La reconnaissance biométrique basée sur les empreintes des articulations des doigts FKP, est une approche biométrique plus récente qui a attiré une attention croissante en raison de ses avantages (considérée comme une caractéristique unique, riche en texture, stable, facile à obtenir, pouvant être utilisée dans différentes conditions environnementales et offrant des performances élevées).

L'objectif de ce mémoire est de proposer un système biométrique d'identifiation et/ou de vérification cohérent visant à améliorer les performances de l'identification biométrique à l'aide FKP en examinant plusieurs méthodes et ensemble d'opérations. Dans ce mémoire, le système de reconnaissance biométrique est planifié en se basant sur une fusion au niveau des scores des multiples traits du FKP tels que le DIP (premier mineur) et le PIP (majeur). Pour cela, nous avons fait la comparaison entre différentes méthodes d'extraction des caractéristiques, ce qui nous a permis d'en choisir celle qui est la mieux adaptée à notre problème, suivant les résultats obtenus, nous avons choisi la méthode qui consiste à l'utilisations de l'algorithme BSIF, qui a montré une amélioration des performances du système monomodal et du système multimodal. Ensuite, la technique PCA+LDA a été utilisée dans l'étape de réduction de dimension et d'optimisation. Le classificateur K-NN a été utilisé pour le processus de correspondance, en utilisant la distance de Mahalanobis cosinus (Mahcos). Ainsi, les deux systèmes, monomodal et multimodal, des premières articulations mineures et articulations majeures ont été étudiés et examinés.

Le système proposé avec la fusion au niveau des scores du premier mineure +majeure en utilisant des règles de T-norme, notamment Frank, Yager et la somme pondérée et la somme présente des performances Rank-1 de **98%** avec un EER de **0,99%.** Ainsi, le système proposé est efficace et capable d'authentifier la personne. De plus, les résultats expérimentaux rapportés

démontrent que le système proposé, basé sur les t-normes, la somme pondérée et la somme, surpasse les approches de base (règles Min et Max).

Enfin, les résultats obtenus sont extrêmement prometteurs, et démontrent l'efficacité du système multimodal par rapport à un système monomodal. Cela confirme que notre système est fiable et répond pleinement à l'objectif que nous nous étions fixé initialement. En effet, sa mise en œuvre permet une reconnaissance précise des individus avec un taux d'erreur très faible.

Nous proposons, en tant que perspective, de nous concentrer sur toutes les principales régions du dos de la main (premier mineur, deuxième mineur, majeur et centre dorsal) mentionnées dans la base de données susmentionnée, afin d'améliorer la sécurité et la robustesse du système multibiométrique contre les attaques d'usurpation. Cela peut être réalisé en utilisant différentes topologies d'apprentissage profond.

Bibliographie

Bibliographie

[1] **François LAMARE**, "OCT en phase pour la reconnaissance biométrique par empreintes digitales et sa sécurisation". Thèse de Doctorat, École doctorale : Informatique, Télécommunications et Électronique de Paris ,21 mars 2016.

[2] **Hafs Toufik**, " Reconnaissance Biométrique Multimodale basée sur la fusion en score de deux modalités biométriques : l'empreinte digitale et la signature manuscrite cursive en ligne". Thèse de Doctorat, département d'électronique, UNIVERSITE BADJI MOKHTAR – ANNABA ,2016.

[3] **Talib Hichem BETAOUAF**, " Identification biométrique des individus par analyse des caractéristiques de la rétine". Thèse de Doctorat, Département d'informatique, Université Aboubakr Belkaïd Tlemcen, Janvier 2018

[4] **Talib Hichem BETAOUAF**, "Caractérisation de la rétine pour la reconnaissance biométrique des personnes". Magister en Informatique, Département d'informatique, Université Aboubakr Belkaïd Tlemcen ,2011.

[5] **Mourad CHAA**, "système de reconnaissance de personne par des techniques biométriques". Thèse de Doctorat, département d'électronique, Université Ferhat Abbas – Sétif -1- UFAS (ALGERIE) ,28/11 /2017.

[6] **Ibtissam BENCHENNANE**, "Etude et mise au point d'un procédé biométrique multimodale pour la reconnaissance des individus ". Thèse de Doctorat, département d'électronique, Université Oran Mohamed Boudiaf, 2015/2016.

[7] Tour d'horizon des technologies biométriques Projet CCT – PFPDT – juin 2012.

[8] **Nicolas Galy**, " Etude d'un système complet de reconnaissance d'empreints digitales pour un capteur microsystème à balayage". Pour obtenir le grade de Docteur de l'inpg, d'l'Ecole Doctorale Electrotechnique, Automatique télécommunication, signal, le 14 Avril 2005.

[9] **AKROUF Samir**, "Une Approche Multimodale pour l'Identification du Locuteur". Thèse de Doctorat, Département d'informatique, UNIVERSITE FERHAT ABBAS-SETIF ,07/07/2011.

[10] **BENMAZA Oussama, ABDESSEMED Salim**, "Identification de personnes basée sur les articulations des doigts 3D ". Mémoire de Master, Département d'électronique et de télécommunication, Université Kasdi Merbah-Ouargla ,2021 /2022.

[11] **DOUAIDI Dahbia, GRINI Soumia**, "Identification et Reconnaissance Biométrique par L'utilisation des Empreintes Palmaires". Master Académique, Département Génie Électrique, Université Akli Mohand Oulhadj de Bouira 24/09/2017.

[12] **EL-Moundher HADJAIDJI, Khaled MAHDADI**, "Modélisation d'empreinte biométrique par un modèle flou de Sugeno optimisé". Mémoire de Master, Département d'Informatique et Technologie de l'information, Université Kasdi Merbah-Ouargla ,2016 /2017.

[13] **Florent Perronnin et Jean-Luc Dugelay,**"Introduction à la Biométrie Authentification des Individus par Traitement Audio-Vidéo". *Revue Traitement du Signal, volume 19, numéro 4,* 2002.

[14] **Arun Ross and Anil Jain**,"Information Fusion in Biometrics". *Appeared in Pattern Recognition Letters*, Vol. 24, Issue 13, pp. 2115-2125, September, 2003.

[15] **Maarouf KORICHI**. "Biometrics and Information Security for a Secure Person Identification". Thèse Doctorat, Department of Electronics and Telecommunications, Université Kasdi Merbah-Ouargla 22/06/2019.

[16] **LAHCINE Moubarek, MEZLI Khaled**, "L'utilisation des Techniques Evolutionnaires pour La Fusion Biométrique Multimodal ". Mémoire de Master en Informatique, Département de Mathématique et d'Informatique, Université Africaine d'Adrar, Décembre 2013.

[17] **LEMMOUCHI Mansoura**, "Reconnaissance Biométrique par Fusion Multimodale". Thèse de Doctorat, Département d'Électronique, Université Batna 2 – Mostefa Ben Boulaïd, 28/06/2020.

[18] **Nefissa Khiari Hili**. " Biométrie multimodale basée sur l'iris et le visage". Traitement du signal et de l'image [eess.SP]. Université Paris-Saclay ; Université de Tunis El Manar, 2016. Français. ffNNT : 2016SACLE014ff. fftel-01762973ff. https://hal.science/tel-01762973.

[19] **BASSIMANE Reyane, REZZOUG Balkis &SLAOUI Abderrahim,** " Identification des individus par l'empreinte de l'articulation de doigt (FKP). " Mémoire Master Académique, Département d'électronique et de télécommunication, Université Kasdi Merbah Ouargla, 2019/2020.

[20] **M. Ghalem Kamel ghanem**, "Authentification et identification de personnes par fusion d'information provenant des images de l'iris de l'œil droit et de l'œil gauche". Thèse de Doctorat, Département d'électronique, Université des Sciences et de la Technologie d'Oran Mohamed-Boudiaf USTOMB, 2017/2018.

[21] **Aldjia BOUCETTA**, " Approches évolutionnaires multi-biométriques pour l'identification des personnes". Thèse de Doctorat, Département d'informatique, Université Batna 2.

[22] **Abderrahmane Herbadji and Noubeil Guermat**,"Personal authentication based on wrist and palm vein images", *Int. J. Biometrics*, Vol. 11, No. 4, 2019.

[23] **Mohamed Cheniti1, Naceur-Eddine Boukezzoula1, Zahid Akhtar**,"Symmetric sum-based biometric score fusion", *IET Biom.*, 2018, Vol. 7 Iss. 5, pp. 391-395.

[24] **Ajay Kumar, Zhihuan Xu**, "Personal Identification using Minor Knuckle Patterns from Palm Dorsal Surface", *IEEE Transactions on Information Forensics and Security*, DOI 10.1109/TIFS.2016.2574309

[25] **Wafa El-Tarhouni**,"Finger Knuckle Print and Palmprint for efficient person recognition". Thèse de Doctorat, Department of Computer and Information Sciences, Northumbria University January 2017.

[26] **Abdelouahab Attia, Zahid Akhtar, Youssef Chahir**. "Feature-level fusion of major and minor dorsal finger knuckle patterns for person authentication". Signal, Image and Video Processing, 2021, ff10.1007/s11760-020-01806-0ff. ffhal-03002661ff. https://hal.science/hal-03002661.

[27] **Abdelouahab Attia, Zahid Akhtar, Nour Elhouda Chalabi, Sofiane Maza, Nour Elhouda Chalabi, et al**. "Deep rule-based classifier for finger knuckle pattern recognition system". Evolving Systems, 2021, 1, ff10.1007/s12530-020-09359-wff. ffhal-03002570ff. https://hal.science/hal-03002570.

[28] **Abdelouahab Attia, Mourad Chaa, Zahid Akhtar, Youssef Chahir**. "Finger kunckcle patterns based person recognition via bank of multi-scale binarized statistical texture features". Evolving Systems, 2020, 11 (4), pp.625-635. ffhal-01956894ff. https://hal.science/hal-01956894.

[29] **Mourad. Chaa, Nacer-Eddine. Boukezzoula and Abdallah. Meraoumia,** "Features- Level Fusion of Reflectance and Illumination Images in Finger-Knuckle-Print Identification System", *International Journal on Artificial Intelligence Tools,* Vol. 27, No. 3, pp. 1-10, 2018.

[30] **Abdelouahab Attia, Abdelouahab Moussaoui, Mourad Chaa, Youssef Chahir**. "Finger-Knuckle-Print Recognition System based on Features-Level Fusion of Real and Imaginary Images". Journal on Image and Vide Processing,2018,ff10.21917/ijivp.2018.0252ff. ffhal-01804052ff. https://hal.science/hal-01804052.

[31] **K. Usha, M. Ezhilarasan**,"Personal recognition using finger knuckle shape oriented features and texture analysis", *Journal of King Saud University – Computer and Information Sciences* (2016) 28, 416–431.

[32] **D. N. Satange, Akram Alsubari, R. J. Ramteke**,"Composite Feature Extraction based on Gabor and Zernike Moments for Face Recognition", *IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN : 2278-0661, p-ISSN : 2278-8727,* PP 17-23.

[33] **Griouz Badreddine**,"Reconnaissance automatique par signaux de la main". Thèse doctorat, Département d'Électronique et Télécommunications, Université 8 Mai 1945 Guelma ,2021.

[34] **Juho Kannala and Esa Rahtu**, "BSIF : Binarized Statistical Image Features, " University of Oulu, Finland, 2012.

[35] **Matthew Turk and Alex Pentland**, " Eigedces for Recognition ", *Journal of Cognitive Neuroscience*, volume 3, Number 1, p.71-86,1991.

[36] **Sung-Kwun Oh, Sung-Hoon Yoo, Witold Pedrycz**,"Design of face recognition algorithm using PCA -LDA combined for hybrid data pre-processing and polynomial-based RBF neural networks : Design and its application", *Expert Systems with Applications 40 (2013) 1451–1466.*

[37] **Waleed Dahea , H.S. Fadewar** . "Score Level Fusion of DIP (Minor) and PIP (Major) with GAs for Feature Selection of Finger Knuckle Print Recognition System".*Journal of the Maharaja Sayajirao University of Baroda ISSN : 0025-0422*, Volume-54, No.2 (XIV) 2020.

[38] **Nour Elhouda Chalabi, Abdelouahab Attia and Abderraouf Bouziane,** "multimodal finger dorsal knuckle major and minor print recognition system based on pcanet deep learning",*ictact journal on image and video processing* , volume: 10, issue:03, february 2020.

[39] **R. Vyas, H. Rahmani, R. Boswell-Challand, P. Angelov, S. Black and B. M. Williams,** "Robust End-to-End Hand Identification via Holistic Multi-Unit Knuckle Recognition," *2021 IEEE International Joint Conference on Biometrics (IJCB)*, Shenzhen, China, 2021, pp. 1-8, doi: 10.1109/IJCB52358.2021.9484356.