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

Mémoire de fin d'étude

Pour l'obtention du diplôme de MASTER Académique

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

LA RECONNAISSANCE AUTOMATIQUE PAR LES ARTICULATIONS DES DOIGTS

Présenté par :

Benharoun Noura Boumaza Chahinez

Sous la direction de :

Dr. Griouz Badreddine

Année Universitaire : 2024 - 2025


بسم الله الرحمن الرحيم

Remerciements

Nous tenons tout d'abord à remercier ALLAH, qui nous a donné la force et la patience d'accomplir ce modeste travail.

À l'issue de ce travail, il me tient à cœur d'exprimer notre profonde gratitude envers toutes les personnes qui ont contribué, de près ou de loin, à la réalisation de ce mémoire.

Tout d'abord, nous tenons à remercier Mr. GUERJOUZ BADEREDINE pour son encadrement précieux, ses conseils avisés et son soutien tout au long de cette recherche. Son expertise et sa bienveillance ont été une source d'inspiration constante.

Sans oublier de remercier Mr BOUROUBA pour l'aide et les informations précieuses qu'il nous a fournies.

Nous souhaitons également exprimer notre reconnaissance envers nos ENSEIGNANTS qui ont su nous apporter les connaissances essentielles à la réussite de notre parcours académique.

Nos remerciements les plus vifs s'adressent aussi LES MEMBRES DE JURY d'avoir accepté d'examiner et d'évaluer notre travail.

Un immense merci à nous CAMARADES et AMIS, pour leur soutien moral et leurs encouragements qui nous ont aidés à persévérer dans les moments de doute.

Enfin, une pensée spéciale nos MA Familles, dont l'amour, le soutien et les sacrifices nous ' ont permis d'atteindre cet objectif sans eux, rien N'aurait été possible.

À tous, merci infiniment.

CHAHINEZ *** Noura

الاهداء

اود أولاً أن نشكر الله، الذي منحنا القوة والصبر

لإنجاز هذا العمل المتواضع.

الى والدي الحبيبين اللذان رافقاني بروحهما وان فارقاني بجسدهما.

الى زوجي رفيق دربي وشريك حياتي

الى كل العائلة.

الى كل الأساتذة الذين ساعدونا في مذكرة التخرج.

الى كل الزملاء بمديرية التجارة.

نورة

الاهداء

بكل فخر وامتنان، أهدي هذا التخرج إلى من كان لهم الفضل بعد الله في دعمي ومساندتي.

إلى أمي العزيزة، منبع الحنان والعطاء، التي كانت دومًا سندي وملهمتي.
إلى أختي الغالية، التي لم تبخل عليّ بكلمات التشجيع والمساعدة.
إلى زوجي الحبيب، رفيق دربي، الذي تحمّل معي كل الظروف وكان دعمي الأول.
وإلى أبنائي الأحبّاء، مصدر قوتي وابتسامتي، الذين منحوني الدافع للاستمرار.

شكرًا لكم من القلب، فهذا الإنجاز هو ثمرة حبكم ودعمكم المستمر.

شاهيناز

ملخص

في الماضي كان العالم يستخدم تقنيات التوثيق مثل كلمة السر وبطاقة الهوية لتأمين الممتلكات مثل الأسلحة والمعلومات السرية خاصة في مجال الاستخبارات ولكنها غير كافية، لأن هناك من يستطيع تخمين أو سرقة كلمة السر أو بطاقة الهوية القابلة للتزوير. لذلك ابتكرت طريقة جديدة لإنهاء هذه المشكلة والحد منها، وتسمى هذه الطريقة" نظام القياسات الحيوية". أصبحت عملية التعرف على الأفراد ذات أهمية متزايدة في حياة الإنسان اليومية. يُستخدم التعرف البيو متري في العديد من التطبيقات مثل حماية الدخول إلى الحاسوب والهاتف المحمول والمؤسسة والبطاقات المصرفية وغيرها.

وقد تم تطوير العديد من التقنيات البيو مترية التي تعتمد جميعها على المُعرّفات البيولوجية والفسيولوجية والسلوكية مثل: قزحية العين، والصوت، وبصمات الأصابع، والوجه، وبصمة الوجه... إلخ. هذه الأنظمة أكثر موثوقية من الأنظمة التقليدية (المفتاح، كلمة المرور، إلخ) لصعوبة تزويرها.

النظام الذي تمت دراسته للتو هو نظام التعرف على الأشخاص من خلال صور الأسطح الخارجية لأصابعهم، وهو نظام يستخدم بصمة مفصل الإصبع (FKP).

تم اختيار هذه الطريقة لأنها تتمتع بالعديد من المزايا اللافتة في مجال القياسات الحيوية، بالإضافة إلى أنها تقنية بسيطة. وسهلة الاستخدام. هدف هذه الدراسة هو تطوير نظام بيو متري مثالي للتعرف على مفاصل الأصابع.

الكلمات المفتاحية:

نظام القياسات الحيوية. البيو متري. تحديد الهوية، بصمة مفصل الإصبع KNN - BSIF- – LPQ.- polyU FKP
IIT DELHI

Résumé

Dans le passé, le monde utilisait des techniques d'authentification telles que le mot de passe et la carte d'identité pour sécuriser des biens tels que des armes et des informations confidentielles, en particulier dans le domaine du renseignement mais n'est pas suffisant, car il y a ceux qui peuvent deviner ou voler le mot de passe ou falsifiable la carte d'identité. Donc nous sommes réfugiés d'établir une nouvelle méthode pour mettre fin et des limités à ce problème, cette méthode est dénommée "système de biométrique".

La reconnaissance des individus a connu plus d'importance dans la vie humaine quotidienne. La reconnaissance biométrique est utilisée dans de nombreuses applications telles que la protection de l'accès à un ordinateur, un téléphone portable, un établissement, et des cartes bancaires…etc.

De nombreuses technologies biométriques ont été développées, toutes basées sur les identificateurs biométriques biologiques et physiologiques et comportementales telles que : l'iris, la voix, les empreintes digitales, le visage, FKP... etc. Ces derniers sont plus fiables que les systèmes classiques (clé, mot de passe...) car ils sont difficilement falsifiables.

Le système qui vient d'être étudiés c'est celui de la reconnaissance des personnes par leurs images des surfaces extérieures des doigts, un système qui utilise l'empreinte des articulations des doigts (Finger Knuckle Print) "FKP".

Cette modalité a été choisie parce qu'elle a de nombreux avantages remarquables dans ce domaine de la biométrie, en plus c'est une technique, simple et facile à utiliser. L'objectif de cette étude est de développer un système biométrique idéal pour identifier les articulations des doigts.

Mots-clés :

Système biométrique, biométrie, identification, empreinte de l'articulation du doigt.

KNN - LPQ – BSIF - polyU FKP- IIT DELHI

Abstract

In the past, the world relied on authentication techniques such as passwords and ID cards to secure assets like weapons and confidential information, particularly in the field of intelligence. However, these methods are not sufficient, as there are individuals who can guess or steal passwords or forge ID cards. Therefore, we resorted to establishing a new method to address and limit this problem, known as the "biometric system."

The recognition of individuals has gained increasing importance in daily human life. Biometric recognition is used in many applications such as securing access to computers, mobile phones, buildings, bank cards, etc.

Many biometric technologies have been developed, all based on biological, physiological, and behavioral biometric identifiers such as the iris, voice, fingerprints, face, and FKP (Finger Knuckle Print), among others. These methods are more reliable than traditional systems (keys, passwords, etc.) because they are difficult to forge.

The system studied here is one that recognizes individuals by images of the outer surfaces of their fingers, using the fingerprint of finger joints (Finger Knuckle Print – FKP.

This modality was chosen because it offers many notable advantages in the field of biometrics. Moreover, it is a simple and easy-to-use technique. The objective of this study is to develop an ideal biometric system for identifying finger joints.

Keywords:

Biometric system, biometrics, identification, knuckle print. KNN - polyU FKP- LPQ. – BSIF- IITDELHI.

Table des matières

Chapitre I : Généralités Sur la Biométrie

Chapitre II : La biométrie de la main

Chapitre III : l'empreinte des articulations des doigts(FKP)

Chapitre IV : Résultats expérimentaux et discussions liste des figures.

Liste des figures

Chapitre I

Chapitre II

Chapitre III

Chapitre IV

Liste des tableaux

Liste des Abréviations

FKP : Finger Knuckle Print.

CLUSIF : Club de la Sécurité des systèmes d'Information Français.

FRR: False Rejet Rate.

FAR: False Accept Rate.

EER: Equal Error Rate.

GAR: Genuine Acceptance Rate**.**

ROC: Receiver Operating Characteristics.

CMC: Cumulative Match Characteristic.

DET: Detection Error Tradeoff.

ADN: Deoxyribonucleic Acid.

DSP : Digital Signal Processin.

USB : Bus Universel en Série.

ROI : Region of Interest.

PCA: Principal Component Analysis.

LDA: Linear Discriminant Analysis.

ICA: Independent Component Analysis.

OLDA: Analyse discriminante linéaire orthogonale.

LG: Log Gabor.

LPQ: Local Phase Quantization.

LPP: Locality Preserving Projections

LED: Light Emitting Diode.

CCD : Charge-Coupled Device.

STFT: transformée de Fourier à court terme.

BSIF: Binarized Statisitcal Image Features.

LBP : Local Binary Pattern.

UID : numéro d'identification d'utilisateur.

RVB : Rouge-Vert-Bleu.

KNN : k-Plus Proches Voisins.

SVM : Machine à vecteurs de support.

CNN : Convolutional Neural Network

LIF : left index finger

LMF : left middle finger

RIF: Right Index Fingers.

RMF: Right Middle Fingers.

TR : Taux de Reconnaissance.

SIFT : Scale-Invariant Feature Transform.

CLAHE: Contrast Limited Adaptive Histogram Equalization.

SURF: Speeded Up Robust Features.

2DWFT: Transformée Discrète de Fourier a Fenêtre a Deux Dimensions

INTRODUCTION GENERALE

Introduction générale :

Pour le moment on parle de plus en plus de l'insécurité dans divers secteurs ainsi que des moyens informatiques à mettre en œuvre pour contrer cette tendance. La vérification et l'identification des individus est l'un des moyens permettant d'assurer cette sécurité.

L'être humain se sert quotidiennement de son système visuel pour identifier les personnes de façon automatique, bien que le processus mis en jeu soit complexe. L'homme a établi des méthodes de validation d'identité qui sont liés, soit à ce que possède un individu telle qu'un passeport ou une carte d'identité, soit à ce que sait cet individu, c'est le cas du mot de passe ou un code PIN, ces éléments peuvent être volés, falsifiés ou oublié. Pour contourner ces limitations, un système a été créé pour la reconnaissance des individus, appelé la biométrie.

La biométrie permet de vérifier que l'usager est bien la personne qu'il prétend être. Qui permet d'utiliser, non pas l'information qu'un individu possède ou connaît, mais une information intrinsèque à cette personne. De plusieurs technologies biométriques ont été évolué, toutes basées sur les identificateurs biométriques physiologiques et comportementales comme : l'iris, la voix, Empreinte des articulations de doigts (FKP), le visage et la signature…etc. Ces derniers sont plus fiables que les systèmes classiques (clé, mot de passe. .) dans la reconnaissance d'une personne car ils sont difficilement falsifiables.

C'est la raison pour laquelle les systèmes biométriques sont actuellement de plus en plus sollicités. En tant que membres importants de la famille de la biométrie liée à la main, l'authentification de personnes par l'empreinte des articulations de doigts. Les empreintes des articulations des doigts sont acquises par un simple appareil photo numérique et sont largement acceptées par les usagers. Indubitablement, FKP fait référence aux motifs de peau de la surface externe autour de l'articulation phalangienne de doigt et comporte des caractéristiques structurelles distinctives, telles que les motifs de texture. Généralement, ces caractéristiques possèdent des aptitudes potentiellement discriminatoires conviennent comparativement bien à l'identification d'un individu par rapport aux autres **[01].**

Le travail présenté dans cette mémoire se compose de quatre chapitres, plusieurs notions et concepts de la biométrie et réalisation des systèmes de reconnaissance vont être abordés les Quartes chapitres vont être comme suite :

Le premier chapitre présente les concepts de base sur la biométrique ainsi que ses caractéristique et ses principales modalités. Nous présentons aussi l'architecture et principale module d'un système biométrique, en suite on va parler sur les limitations des systèmes biométriques monomodaux, la multi modalité et les applications de la biométrie. Ce chapitre est finalisé par l'évaluation des performances des systèmes biométrique.

Le deuxième chapitre présente la biométrie de la main ainsi que les modalités biométriques liées à la main, les Avantages de la biométrie de la main, la géométrie de la main, système de reconnaissance des empreintes digitale, Système de reconnaissance des doigts entiers, Système

de reconnaissance des empreintes palmaires, Biométrie de la main entière , La dynamique du mouvement de la main , Le réseau veineux .

Le troisième chapitre sera dévoué à la présentation de la biométrie de l'empreinte de l'articulation de doigt (FKP), Etat de l'Art de l'empreinte des articulations des doigts, les méthodes de prétraitement et l'extraction des caractéristiques et la classification.

Le dernier chapitre est consacré pour les résultats expérimentaux. La première partie on parlera de la base de données, protocole de test ensuite l'extraction de la région d'intérêt que nous avons appliqué à l'empreinte des articulations de doigts (FKP), deuxième partie de ce chapitre discute les résultats expérimentaux obtenus par les méthodes LPQ et BSIF et enfin on a fait une comparaison entre ces deux méthodes utilisées. En termine par une conclusion générale qui résumera les résultats obtenus par les différentes approches.

CHAPITRE I

GÉNÉRALITÉS SUR LA BIOMÉTRIE

I.1 – Introduction :

La biométrie s'impose aujourd'hui comme une technique permettant de vérifier l'identité d'un individu en utilisant une ou plusieurs de ses caractéristiques personnelles. L'intérêt et d'augmenter le niveau de sécurité en utilisant comme identifiant une donnée qui contrairement aux mots de passe et codes pin, ne peut être perdue, volée ou falsifiée puisqu'elle est liée directement au corps ou au comportement de l'individu. On observe un regain d'intérêt pour ces Techniques depuis les années 2000, Période à partir de laquelle se mettent en place des politiques sécuritaires au niveau des pays du G 8 suite, entre autres aux attentats du 11 septembre 2001. On constate ainsi en ce moment le déploiement d'un certain nombre de système à très grande échelle tel que le passeport biométrique les cartes nationales d'identité. L'objet de ce chapitre est de présenter brièvement les systèmes biométriques et les différents défis posés aux chercheurs, face en particulier à un déploiement à large échelle.

I. 2 - Définition de la biométrie :

La biométrie est une mesure des caractéristiques biologiques pour l'identification ou l'authentification d'un individu à partir de certaines de ses caractéristiques comportementales (exemple de la dynamique de frappe au clavier), physiques ou physiologiques (exemple de l'ADN). Cette technique est utilisée de plus en plus aujourd'hui pour établir la reconnaissance des personnes dans un grand nombre d'applications diverses.

Le mot biométrie est une traduction du mot anglais « biométrics » qui correspond en français à l'anthropométrie. Il désigne dans un sens très large l'étude quantitative des êtres vivants, mais dans le contexte de la reconnaissance d'individus il est défini par :

* Selon le CLUSIF (Club de la Sécurité des systèmes d'Information Français), la biométrie est la science qui étudie à l'aide des mathématiques, les variations biologiques à l'intérieur d'un groupe déterminé.

* Selon la RAND (Public Safety and Justice), la biométrie est définie comme toute caractéristique physique ou trait personnel automatiquement mesurable, robuste et distinctif qui peut être employé pour identifier un individu ou pour vérifier son identité **[2].**

I.3 - Différentes modalités biométriques :

Il existe aujourd'hui une panoplie assez large de modalités biométriques qui sont utilisées dans divers systèmes biométriques. Au fur et à mesure, il en apparaît constamment de nouvelles. L'étendu des recherches dans les nouveaux procédés biométriques (oreille, démarche, odeur, etc.) est relativement convaincant.

Toutefois, les modalités les plus enclines et les plus éprouvées à grande échelle sur le terrain sont la reconnaissance des empreintes digitales, du visage, de l'iris et de la parole.

Il se trouve que ce sont les modalités biométriques qui, à ce jour, répondent le mieux aux critères d'unicité, de permanence et de régularité, leur capture par des instruments étant, par ailleurs, possible de manière ergonomique et économique. Des techniques propriétaires ont également vu le jour pour la géométrie vasculaire (veines de la paume et des doigts) et des mains.

Il est à noter qu'aucune modalité ne permet d'assurer à la fois une précision suffisante et un confort d'utilisation et cela dans toutes les situations d'usage. De plus, quelle que soit la modalité, il existe toujours des personnes réfractaires (mains usées de travailleurs manuels, visages voilés, voix enrouées).

Les modalités biométriques utilisées dans divers secteurs sont répertoriées en quatre catégories, à savoir, modalités biologiques, comportementales, morphologiques et cachées. Ces dernières sont en cours d'expansion **[3].**

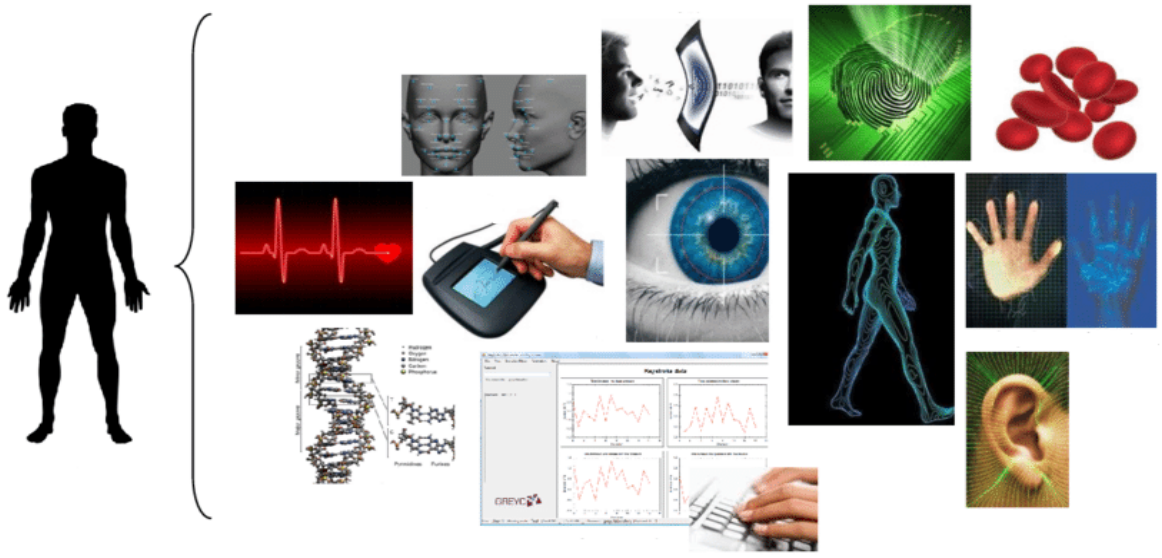

Figure I.1 : Différentes modalités biométriques.

I.4 - Types de Modalités Biométries :

La technologie biométrique est sophistiquée, plus intelligente, super sensible et mise en place pour aider à protéger les entreprises et les particuliers. Il existe divers traits présents chez l'homme, qui peuvent être utilisés comme modalités biométriques. Les modalités biométriques relèvent de trois types : morphologiques, comportementale et biologique **[4].**

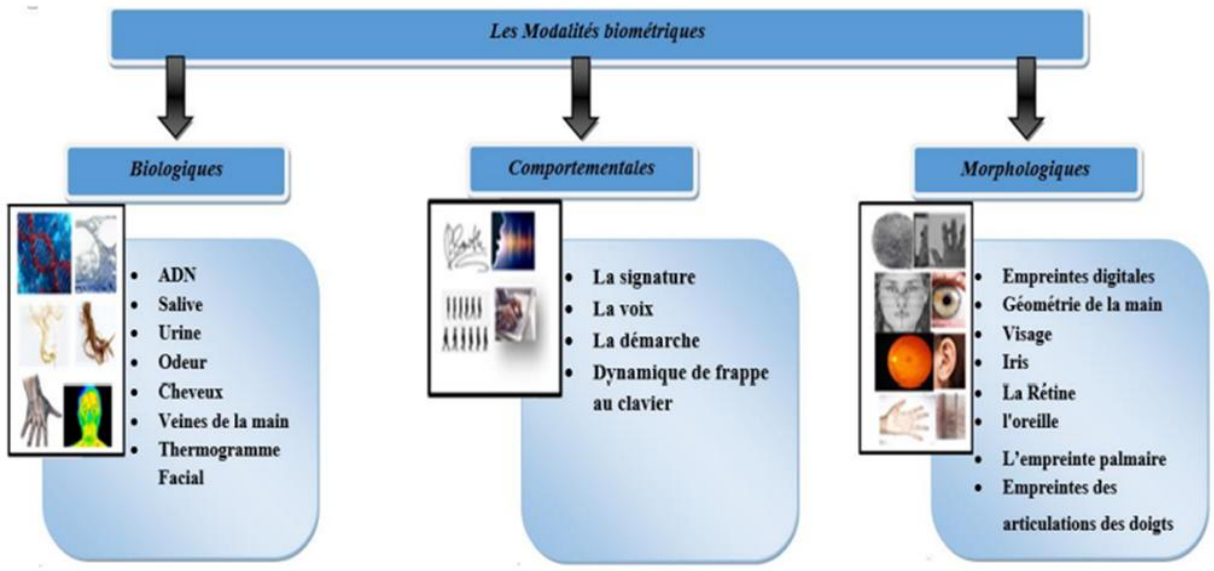

Figure I.2 : Structure des Types de Modalités Biométries.

I.4.1 - Modalités Morphologiques :

La Forme du visage :

La reconnaissance de visages qui est classée parmi les techniques principales de la biométrie est facilement tolérée par les utilisateurs, peu intrusive et moins coûteuse la plus facile à utiliser car elle est non contraignante. En effet, elle n'exige pas beaucoup d'effort de la part de l'utilisateur lors de la saisie de mesures. Certains systèmes employant cette technique fonctionnent même sans que l'utilisateur en soit conscient **[05].**

Figure I.3: trait biométrique : visage

Les empreintes digitales :

Considéré la méthode d'identification de la personne la plus efficace et la plus populaire. Les empreintes digitales sont composées de lignes localement parallèles présentant des points singuliers (minuties) et constituent un motif unique, universel et permanent **[6].**

Minutie prétendaient être uniques à chaque doigt ; c'est la collection de points de minutie dans une empreinte digitale qui est principalement utilisée pour faire correspondre deux empreintes digitales.

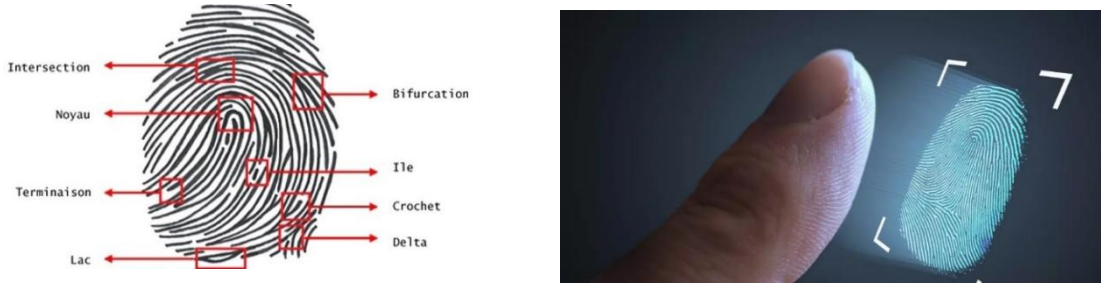

Figure I.4 : trait biométrique : L'empreinte digitale.

L'iris :

L'iris est la zone colorée visible entre le blanc de l'œil et la pupille. L'iris est un réseau de tubes fins dont l'enchevêtrement varie très peu durant la vie de l'individu contrairement à la couleur (des tubes) qui varie un peu avec le temps. Sa principale fonction est de moduler le diamètre de la pupille afin de contrôler la quantité de lumière qui parvient à la rétine. La reconnaissance par l'iris**.**

Est utilisée aussi dans le secteur financier pour les employés et les clients, dans les hôpitaux et dans les grands aéroports. Une personne voulant s'identifier place son œil à quelques centimètres du capteur et l'image de l'iris est prise par une caméra. Ensuite, les caractéristiques sont extraites de l'image de l'iris et comparées à celles enregistrées dans la base de données **[7].**

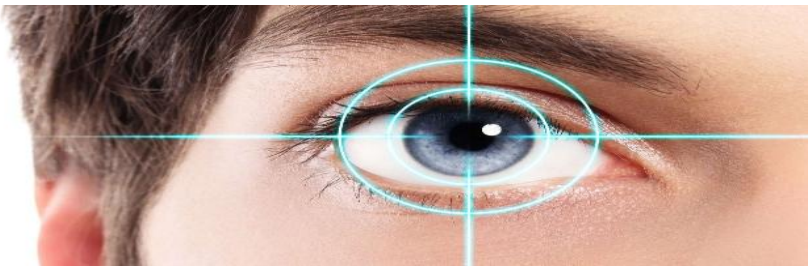

Figure I.5: trait biométrique : Iris.

La géométrie de la main :

Chaque individu à sa propre forme de la main. Les paumes des mains humaines contiennent un motif de crêtes et de vallées, tout comme les empreintes digitales**.**

La zone de la paume est beaucoup plus grande que la zone d'un doigt et par conséquent les empreintes de paume devraient être encore plus distinctives que les empreintes digitales.

On peut l'acquérir en utilisant un scanner spécialisé. La longueur des doigts, leur épaisseur et leur position relative sont des paramètres qui sont extraits de l'image et comparés à ceux existant dans une base de données. Néanmoins, cette biométrie est sujette à certaines modifications qui sont dues au vieillissement.

Les systèmes biométriques utilisant la forme de la main sont simples à mettre en œuvre, et sont très bien acceptée par les utilisateurs **[8].**

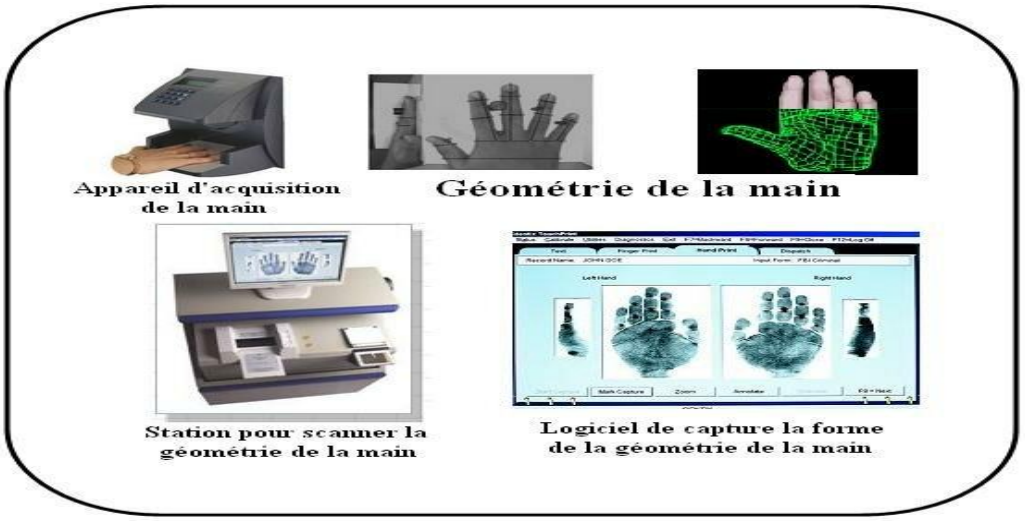

Figure I.6 : Image de la géométrie de la main.

- **Empreintes des articulations des doigts (FKP : Finger Knuckle print) :**

C'est la technologie biométrique basée sur la surface arrière de doigt, elle contient des caractéristiques distinctives, telles que les lignes principales, les lignes secondaires et les crêtés, 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 **[9].**

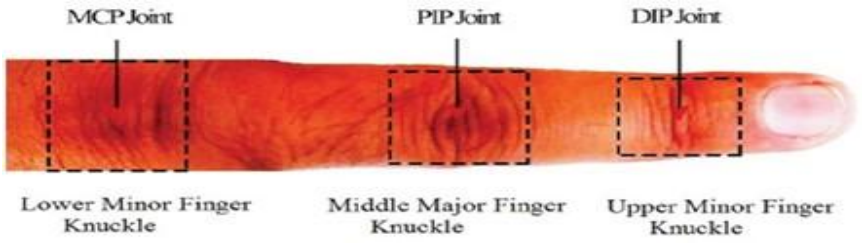

Figure I.7 : images des Empreintes des articulations des doigts.

Tableau I.1: Comparaison entre les modalités morphologiques [25].

	Avantages	Inconvénients
La géométrie de la main	• Acceptance par les individus. • Pas d'effet en cas d'humidité où D'impropriété des doigts.	• Perturbation possible par des Blessures. • Système encombrant
Les empreintes Digitales	• Facilité d'utilisation et traitement Rapide. • La plus éprouvée.	• Possibilité d'attaques. • Sensible en cas d'humidité où Malpropreté des doigts
Visage	• Bien accepté par les usagers. • Elle n'est pas très coûteuse	• Jumeaux identiques
Rétine	• Fiabilité. • Durabilité	• Mauvaise acceptation • Coûteuse.
Iris	• Contient grande quantité D'information. • Pas de confusion pour les vrais Jumeaux.	• Méthode invasive et non Conviviale. • Facilement photographié
ADN	• La plus distinctive	• Analyse trop lente à donner des Résultats. • Coût élevé
FKP	• Moins sensible à l'usure que les empreintes digitales • Capturable sans contact • Nouvel axe de recherche biométrique	• Moins précis que d'autres modalités • Peu connu et peu utilisé actuellement • Moins de bases de données disponibles

I. 4.2 - Modalités Comportementales :

Elle se base sur l'analyse de certains comportements d'une personne. Cette catégorie regroupe la reconnaissance vocale, la dynamique de frappe au clavier, la dynamique de la signature, l'analyse de la démarche, etc. Il existe, par ailleurs, une autre catégorie qui est l'étude des traces biologiques telles que : l'ADN, le sang, la salive, l'urine, l'Oder,… etc. **[10].**

La dynamique de Signature :

Chaque personne a un style d'écriture unique. On peut donc définir, à partir de la signature d'une personne, un modèle qui pourra être employé pour effectuer une identification. De plus, la signature est utilisée dans beaucoup de pays comme élément juridique ou administratif. Elle permet de justifier de la bonne foi d'une personne ou de la confondre devant des documents signés **[10].**

Figure I.8 : trait biométrique : Signature.

La Voix (ou la parole) :

La Voix (ou la parole) Les systèmes de reconnaissance vocale ou vocale identifient une personne en fonction de ses paroles. La génération de la voix humaine implique une combinaison de caractéristiques comportementales et physiologiques. La composante physiologique de la voix dépend de la forme et de la taille des voies vocales, des lèvres, des cavités nasales et de la bouche.

La reconnaissance des haut-parleurs convient parfaitement aux applications comme la télé-banque, mais elle est assez sensible au bruit de fond et à l'usurpation de lecture. Encore une fois, la modalité vocale est principalement utilisée en mode de vérification **[04].**

Figure I.9 : trait biométrique : la Voix

La 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 **[04].**

Figure I.10 : Système biométrique basé sur la démarche.

Dynamique de Frappe sur un clavier :

La dynamique de la frappe est propre à chaque individu. Il s'agit en quelque sorte de la graphologie des temps modernes car nous écrivons plus souvent avec un clavier qu'avec un stylo. Les éléments analysés sont : vitesse de frappe, suite de lettre, temps de frappe, pauses...

L'objectif est de développer une solution biométrique à bas coût afin de renforcer la sécurité des mots de passe qui ne cessent de se multiplier dans la vie quotidienne. En associant la fourniture d'un mot de passe à la signature spécifique de la personne qui le tape sur un clavier, nous introduisons un deuxième facteur d'authentification peu onéreux et plus facilement accepté par les utilisateurs **[10].**

Figure I.11 : Système de reconnaissance de frappe sur un clavier

Tableau I.2 : Comparaison entre les modalités comportementales [25].

	Avantages	Inconvénients
La reconnaissance vocale	• Facilité.	• Sensible à l'état physique et Émotionnel de l'individu. • Vulnérabilité aux attaques.
La dynamique défrappe au clavier	• Acceptation forte par L'utilisateur	• Ne sont pas plus pratiques pour autant
La signature	• Acceptation forte par L'utilisateur	• couteuse. • Dépend de la fiabilité de la Signature
La démarche	• Peut-être repérée à grande Distance à l'aide d'une caméra À faible résolution • Observée ainsi de n'importe quel angle.	• Il est sensible aux change-ments D'habits, chaussures et surface

I.4.3 - Modalités Biologiques :

L'ADN :

L'analyse des empreintes génétiques est devenue en quelques années l'un des outils majeurs de la criminalistique, la science de l'identification des indices matériels. L'analyse de l'ADN est couramment utilisée en criminologie pour identifier une personne à partir d'un morceau de peau d'un couramment utilisée en criminologie pour identifier une personne à partir d'un morceau de peau d'un cheveu ou d'une goutte de sang **[11].**

La génétique a permis de démontrer que l'ADN (acide désoxyribonucléique) est la particularité la plus fiable pour identifier une personne.

Figure I.12 : trait biométrique : ADN

I.5 - Propriétés souhaitées dans une caractéristique biométrique :

Un certain nombre de caractéristiques biométriques peut être capturé dans la première phase du traitement. Toutefois, la capture automatique et la comparaison automatisée des données précédemment stockées nécessitent que les caractéristiques biométriques répondent aux caractéristiques suivantes :

- **Universalité :** la caractéristique biométrique doit exister, naturellement, chez toutes personnes (ex. empreinte).

- **Invariance :** les caractéristiques doivent être constantes sur une longue période de temps. Elles ne doivent être soumises à des différences significatives liées à l'âge.

- **Mesurabilité :** les propriétés biométriques doivent être mesurables. Les données doivent être facilement et passivement recueillies.

- **Singularité :** les caractéristiques biométriques doivent être uniques à chaque individu. Elles doivent être suffisantes pour distinguer une personne d'une autre.

- **Acceptation :** la saisie doit être possible d'une manière acceptable pour un grand Pourcentage de la population.

- **Fiabilité et inviolabilité :** l'attribut doit être impossible de masquer ou de manipuler. Le processus doit garantir un niveau élevé de fiabilité et de reproductibilité.

- **Confidentialité :** le processus ne doit pas violer la vie privée de la personne.

- **Inimitabilité :** pour une précision sans faille, l'attribut ne doit pas être reproductible par D'autres moyens **[12].**

I.5.1 – Comparaison :

À partir des critères cités auparavant une première comparaison des principales technologies biométriques est proposée sur le Tableau I.3.

Tableau I.3 : Comparaison de technologies biométrique [23].

Biométrie	Universalité	Unicité	Permanence	Mesurabilité	Performance	Acceptalité	Vulnérabilité
DNA	Haute	Haute	Haute	Faible	Haute	Faible	Faible
Oreille	Moyenne	Moyenne	Haute	Moyenne	Moyenne	Haute	Moyenne
Visage	Haute	Faible	Moyenne	Haute	Faible	Haute	Haute
Thermo. Visage	Haute	Haute	Faible	Haute	Moyenne	Haute	Faible
Empreinte	Moyenne	Haute	Haute	Moyenne	Haute	Moyenne	Moyenne
Démarche	Moyenne	Faible	Faible	Haute	Faible	Haute	Moyenne
Géométrie Main	Moyenne	Moyenne	Moyenne	Haute	Moyenne	Moyenne	Moyenne
Veines Main	Moyenne	Moyenne	Moyenne	Moyenne	Moyenne	Moyenne	Faible
Iris	Haute	Haute	Haute	Moyenne	Haute	Faible	Faible
Frappe Clavier	Faible	Faible	Faible	Moyenne	Faible	Moyenne	Moyenne
Odeur	Haute	Haute	Haute	Faible	Faible	Moyenne	Faible
Rétine	Haute	Haute	Moyenne	Faible	Haute	Faible	Faible
Signature	Faible	Faible	Faible	Haute	Faible	Haute	Haute
Voix	Moyenne	Faible	Faible	Moyenne	Faible	Haute	Haute

Ce n'est pas nécessaire que chaque modalité possède toutes ces propriétés. Elles peuvent les posséder avec des degrés différents. Parmi les techniques les plus matures, on distingue le visage, l'empreinte digitale, la géométrie de la main, l'iris et la rétine, qui présentent de bonnes caractéristiques. Mais aucune d'entre elles n'est parfaite **[23].**

Lors du choix de la biométrie, on ne parle pas de modalité parfaite ou idéale mais de son adaptation à des applications ciblées. Donc, le compromis entre la présence ou l'absence de certaines de ces propriétés se fait selon les besoins de chaque application.
Chaque technique possède des avantages et des inconvénients, acceptables ou inacceptables suivant les applications en termes de niveau de sécurité et/ou de facilité d'emploi, etc. Il faut motionner aussi que ces solutions biométriques ne sont pas systématiquement en concurrence **[23].**

I.6 - Les applications de la biométrie :

Les techniques biométriques sont appliquées dans plusieurs domaines et leur champ d'application couvre potentiellement tous les domaines de la sécurité où il est nécessaire de connaître l'identité des personnes. Les applications peuvent être divisées en trois groupes principaux **[10]** :

I.6.1 - Applications commerciales :

Telles que l'accès au réseau informatique, la sécurité de données électroniques, le commerce électronique, l'accès d'internet, la carte de crédit, le contrôle d'accès physique, le téléphone portable, la gestion des registres médicales, l'étude de distances, etc**.... [1].**

I.6.2 - Applications de gouvernement :

Telles que la carte nationale d'identifications, le permis de conduite, la sécurité sociale, le contrôle de passeport, etc....**[1].**

I.6.3 - Applications juridiques (légales) :

Telles que l'identification de cadavre, la recherche criminelle, l'identification de terroriste, les enfants disparus, etc. **[1].**

I.7 – Architecture D'un Système Biométrique :

Un système biométrique est un système qui possède en entrée l'acquisition des données biométriques à partir d'un appareil de mesure (cela peut être un appareil photo, un lecteur d'empreintes digitales, une caméra de sécurité…etc.). Il extrait l'ensemble des caractéristiques à partir des données acquises et les compare avec celles enregistrées dans la base de données.

Selon le contexte d'application, on distingue deux modes d'utilisation distincts d'un système biométrique : le mode d'identification et le mode de vérification **[23].**

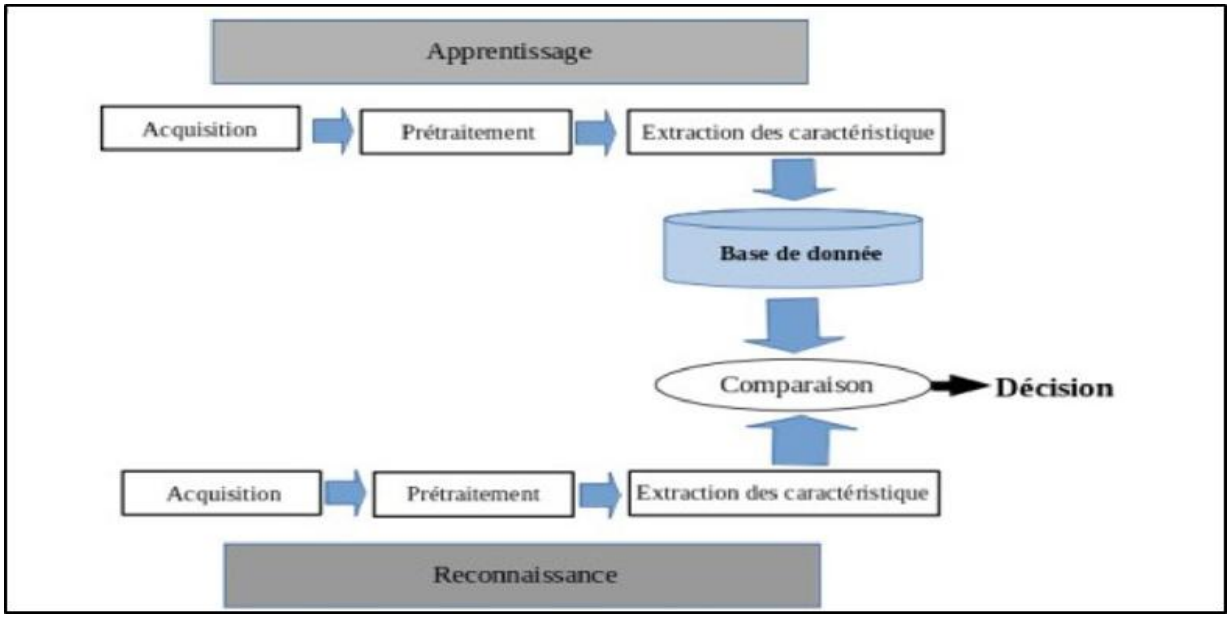

Figure I.13 : Architecture d'un système de reconnaissance biométrique.

I.8 - Modes de fonctionnement d'un système biométrique :

Les systèmes biométriques peuvent fournir trois modes de fonctionnement à savoir : mode enrôlement, mode vérification (L'authentification) ou bien mode d'identification.

I.8.1 - Mode identification :

En mode identification, le système biométrique détermine l'identité d'un individu inconnu à partir d'une base de données d'identités, on parle de test 1 : N. Dans ce cas, le système peut alors soit attribuer à l'individu inconnu l'identité correspondant au profil le plus proche retrouvé dans la base (ou une liste des profils proches), soit rejeter l'individu. (Voir Figure I.14) **[27].**

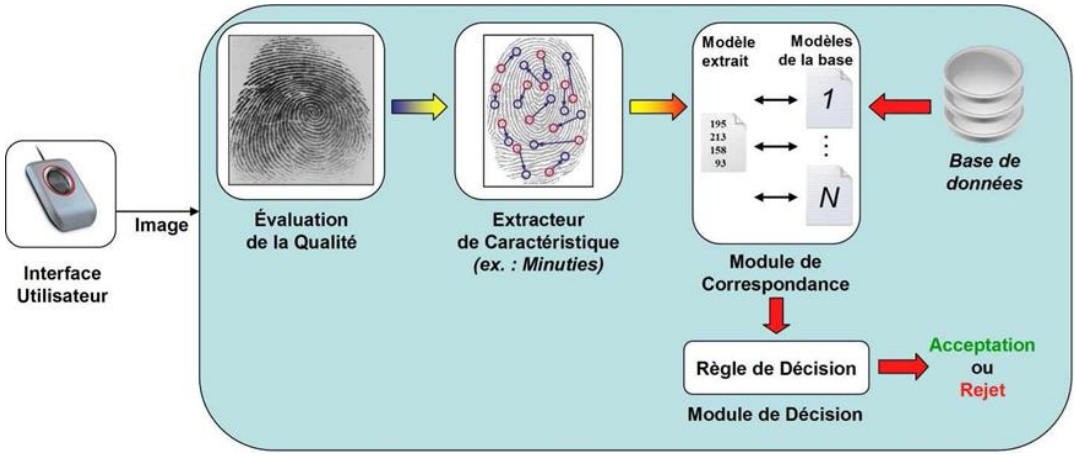

Figure I.14 : Identification d'une personne dans un système biométrique

I.8.2 - Le mode d'enrôlement :

L'enrôlement est la première phase de tout système biométrique. Il s'agit de l'étape pendant laquelle un utilisateur est enregistré dans le système pour la première fois. Elle est commune à la vérification et l'identification. Pendant L'enrôlement, la caractéristique biométrique est mesurée en utilisant un capteur biométrique afin d'extraire une représentation numérique.

Cette représentation est ensuite réduite, en utilisant un algorithme d'extraction bien défini, afin de réduire la quantité de données à stocker pour ainsi faciliter la vérification et l'identification **[27].** (Voir Figure I.15).

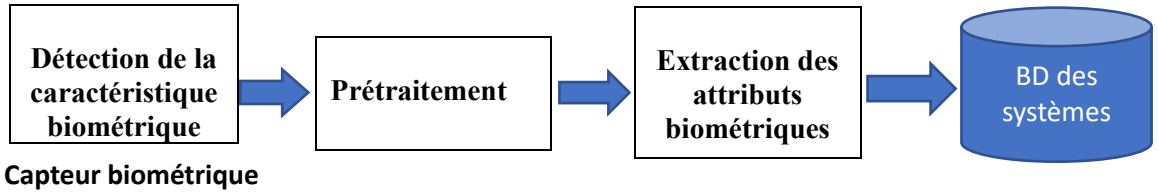

Figure I.15 : Enrôlement d'une personne dans un système biométrique.

I.8.3 – le mode de L'authentification (vérification) :

La vérification d'identité consiste à contrôler si l'individu utilisant le système est bien la personne qu'il prétend être. Le système compare l'information biométrique acquise avec le modèle biométrique correspondant stocké dans la base de données, en parle de teste 1 :1. Dans ce cas, le système renvoie uniquement une décision binaire (oui ou non) pouvant être pondérée.

Lorsqu'un système biométrique opère en mode authentification (Fig.I.16), l'utilisateur affirme son identité et le système vérifie si cette affirmation est valide ou non. **[27].**

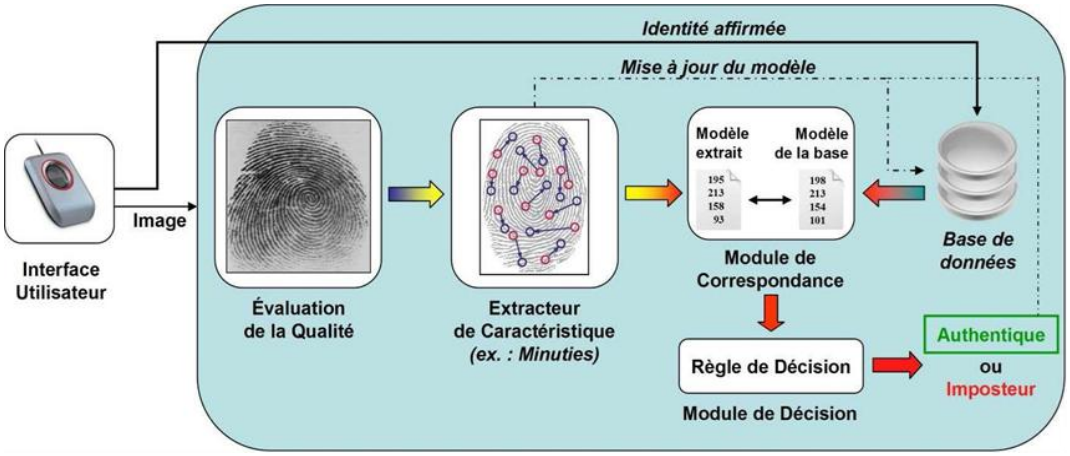

Figure I.16 : Authentification (vérification) d'une personne dans un système biométrique

I.9 - les Principaux modules qui composent un système biométrique :

Un système biométrique comporte deux phases essentielles : le module d'apprentissage et celui de reconnaissance et une phase facultative qui est le module d'adaptation.

I.9.1 - Module capteur biométrique :

Le module de capture qui consiste à acquérir les données biométriques afin. Une représentation numérique. Et ensuite utiliser pour le rendement la vérification ou l'identification. Capteur biométrique qui peut être de ce type sans ou avec contact **[27].**

I.9.2 - Module d'extraction des caractéristiques :

Les caractéristiques biométriques sont une solution alternative aux anciens moyens de vérification d'identité. L'avantage de ces derniers est qu'elles doivent être universelles, uniques, permanentes, enregistrables et mesurables.

L'intérêt principal de la biométrie est donc de reconnaître et d'identifier automatiquement les identités des individus, en utilisant les caractéristiques physiologiques ou comportementales.

L'extraction des caractéristiques clés de l'échantillon est sélectionnée ou améliorées. Typiquement, le processus d'extraction de caractéristiques repose sur un ensemble d'algorithmes ; le procédé varie en fonction du type d'identification biométrique utilisé **[6].**

I.9.3 - Module comparaison :

Ce module compare les caractéristiques biométriques d'une personne soumise à contrôle (volontairement ou à son insu) avec les « signatures » mémorisées. Ce module fonctionne soit en mode vérification (pour une identité proclamée) ou bien en mode identification (pour une identité recherchée) **[4].**

I.9.4 - Module base de données :

Dans lequel on stocke les modèles biométriques des utilisateurs enrôlés **[4].**

I.9.5 - Module de décision :

Le module de décision qui Détermine C'est l'indice de similarité retourner est suffisant pour déterminer l'identité d'un individu **[27].**

I.10 - Système Biométrique Uni modal :

Le système uni modal, c'est un système plus simple qui utilise une seule modalité biométrique, par exemple l'utilisation d'un seul doigt ou un seul algorithme pour identifier les personnes. Ce type des systèmes possède généralement un taux d'erreur très élevé. Ainsi, ce type des systèmes à plusieurs limitations qui peuvent être rend la sécurisation biométrique inapplicable pour des entreprises ou des personnes particulières **[9].**

I.10.1 - Limitations des systèmes unimodaux :

L'évaluation des performances d'un système biométrique est une phase importante dans le processus de sa conception et de sa mise en œuvre dans la mesure où elle permet de savoir si le système est suffisamment performant pour l'application visée. Cependant, les critères de performance d'un système biométrique ne sont pas les seuls à prendre en compte mais aussi les critères de coûts et d'acceptation par le public. Ainsi, selon les situations d'usage et les buts recherchés, chaque technologie biométrique (modalité) a ses points forts et ses inconvénients. Par conséquent, on ne peut garantir un excellent système de reconnaissance (un excellent taux de reconnaissance) avec l'utilisation d'une seule modalité biométrique.

Malgré les avantages des systèmes biométriques uni modaux par rapport aux systèmes traditionnels, leur utilisation souffre de plusieurs limitations qui peuvent dégrader considérablement leur intérêt. En effet, ces systèmes sont souvent affectés par les problèmes suivants **[15] :**

- **La non-universalité des biométries :**

Les systèmes unimodaux sont basés sur une seule modalité biométrique. Cependant, cette modalité doit être vérifiée à la condition d'universalité, ce que signifie que chaque personne devrait obligatoirement avoir cette modalité pour un système donné **[15].**

- **La variabilité lors de la capture :**

Ce type de variabilité n'est pas intrinsèquement lié à la modalité mais à l'acquisition de celle-ci. Il peut être introduit à plusieurs phénomènes **[15].**

- **La sensibilité aux attaques :**

Une autre limitation des systèmes biométriques est la sensibilité aux attaques (possibilité de fraude). Il est toutefois possible de reproduire certaines modalités biométriques **[15].**

- **La non-unicité des biométries :**

C'est la variabilité entre les modalités de plusieurs Individus. Cependant, les caractéristiques extraites à partir de données biométriques d'individus différents peuvent être relativement similaires **[9].**

I.11 - Système multimodal :

Les humaines se reconnaissent entre eux à partir de plusieurs modalités biométriques physiques ou comportementales. Chaque modalité en soi ne peut pas toujours être utilisée de manière fiable pour effectuer la reconnaissance **[16].**

Cependant, la consolidation d'information présentée par les déférentes modalités peut par amètre une reconnaissance précise de l'identité. Cette stratégie peut être utilisée pour réduire quelques problèmes et limitations, liées aux systèmes multimodaux. En effet, la combinaison

de plusieurs modalités a pour but d'améliorer les performances se reconnaissance. En augmentant la quantité d'informations discriminantes de chaque personne, on souhaite augmenter le pouvoir de reconnaissance du système (vérification ou l'identification) **[17].**

I.11 .1 - Fusion des données :

La fusion des données est une technique utilisée en traitement d'informations issues des sources multiples Elle consiste à combiner des données issues de plusieurs sources afin d'obtenir une décision meilleure que celle obtenue à partir de chacune des sources prise isolément. La fusion de données a été initialement développée surtout dans un contexte militaire pour des objectifs tels que la localisation des cibles ennemies et la fusion d'images radar **[18].**

Les systèmes employés ont recours à des techniques diverses issues de domaines variés tel le traitement du signal, l'intelligence artificielle, la reconnaissance des formes, la classification, etc... De façon générale, la fusion de données est une opération d'intégration de plusieurs données en vue d'en extraire une nouvelle information plus représentative de l'ensemble des données. Actuellement, la fusion des données prend une place de plus en plus importante dans de nombreux domaines. Elle permet d'aider efficacement les scientifiques à extraire des informations de plus en plus pertinentes et précises. La fusion de données a d'abord visé d'améliorer la qualité des réponses aux problèmes posés par les militaires mais aujourd'hui elle touche énormément de domaines telles que la télédétection, la prévision météorologique, la biométrie multimodale, l'application médicale et la robotique **[18].**

I.11.2 - Sources des informations :

Le problème général de la fusion est la synthèse d'un ensemble d'informations obtenues à partir de la mise en commun d'informations provenant des sources différentes. Cependant, il existe, de nombreux scénarios possibles pour les sources d'information qui peuvent être considérées dans un système biométrique multimodal **[20].**

I.12 - Les Différentes sources des systèmes biométriques multimodaux :

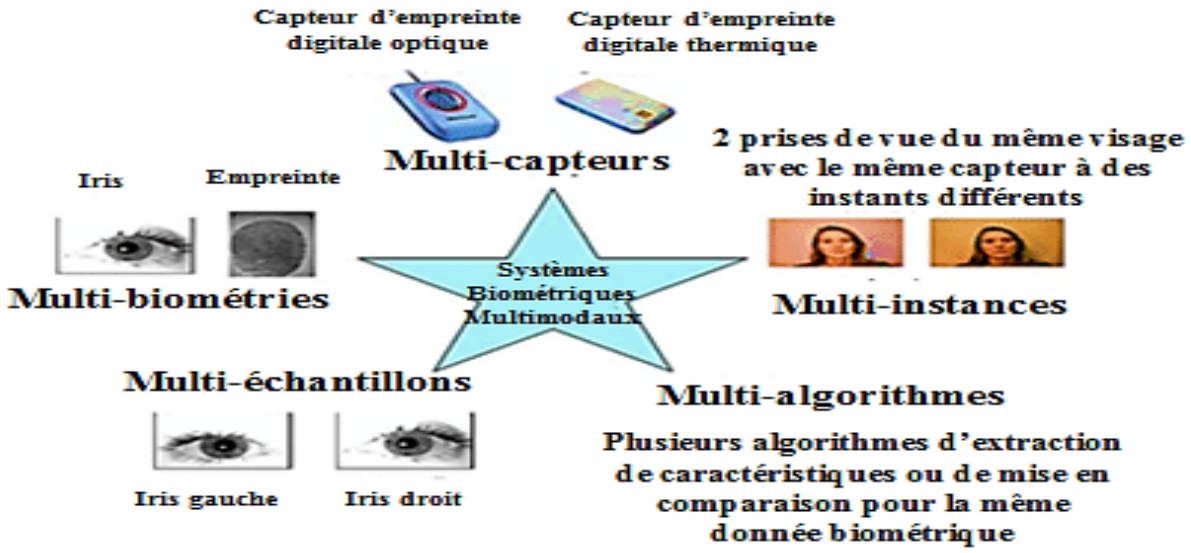

Figure I.17 : Les Différentes systèmes biométriques multimodaux.

I.12.1 - Systèmes multi-algorithmes :

Dans les systèmes multi- algorithmes, la même donnée biométrique est vérifiée à l'aide de plusieurs algorithmes de reconnaissance (par exemple, reconnaissance d'empreinte digitale à partir de la comparaison de minuties et de texture). Le coût d'une telle solution est peu élevé en raison de l'utilisation d'un seul capteur. Elle est peu contraignante pour l'utilisateur en raison de l'absence d'interactions supplémentaires. L'utilisation de plusieurs algorithmes peut cependant entraîner une augmentation du coût de calcul **[27].**

I.12.2 - Systèmes multi-capteurs :

Dans un système multi-capteurs, le même caractère biométrique est capturé à l'aide de plusieurs capteurs différents, afin d'acquérir le plus d'informations différentes possibles (Par exemple, utilisation d'un lecteur d'empreinte digitale capacitif et d'un lecteur d'empreinte digitale résistif).

Le cout du système est plus élevé en raison de l'utilisation de plusieurs capteurs. L'expérience utilisateur peut être dégradée si ces capteurs doivent être utilisés séquentiellement **[27].**

I.12.3 - Systèmes multi-instances :

Les systèmes multi- instance nécessitent de capturer plusieurs instances du même

Caractère biométrique (par exemple, capture des iris droit et gauche, ou capture du pouce et de l'index de la main droite). Le même capteur peut être utilisé par capturer toutes les données biométriques, dans ce cas le cout de la solution n'est pas plus élevé, mais l'utilisateur doit effectuer la capture de toutes les instances, ce qui peut être contraignant.

Il est également possible d'utiliser un nouveau capteur capable d'acquérir toutes les données simultanément. Dans ce dernier cas, le cout du système peut être plus élevé, mais en contrepartie, l'expérience utilisateur n'est pas plus contraignante quel que soit le nombre d'instances **[27].**

I.12.4 - Systèmes Multi-biométries :

Les systèmes multi-biométrie utilisent l'information de plusieurs caractères biométriques différents pour authentifier les individus (par exemple, reconnaissance faciale associée à la reconnaissance de la parole). Le cout d'un tel système nécessairement plus important en raison de la nécessité de disposer d'un capteur spécifique par caractère **[27].**

I.12.5 - Systèmes multi-échantillons :

Un système multi-échantillons (ou multi- impressions) nécessite de faire plusieurs acquisitions d'une même donnée biométrique. Il s'agit donc d'une variante d'un système multi-instance. L'intérêt d'un tel système est d'augmenter la robustesse au bruit en augmentant le nombre de captures de la donnée.

En contrepartie d'expérience utilisateur est fortement dégradée, sauf s'il s'agit de système exploitant la vidéo. Une vérification peut être effectuée sur chacune des captures ou une super capture peut-être générée à l'aide des différentes captures **[27].**

I.13 - Composants de Base d'un Système Biométrique :

Le système biométrique se compose de quatre (04) éléments importants, à savoir :

I.13.1 - Interface d'entrée (capteurs) :

Fait au niveau du capteur, qui est la partie responsable de la conversion des données biologiques humaines sous forme numérique. Par exemple : la photo en cas de systèmes de reconnaissance visage **[4].**

I.13.2 - Base de données Stocke :

La base de données stocke l'échantillon enregistré après son appel pour effectuer une correspondance et en même temps s'authentifier. Pour l'identification, nous pouvons y trouver n'importe quel marqueur d'accès aléatoire (RAM) ou serveur de données. Pour vérification, nous notons que l'élément de stockage est amovible tel qu'un contact ou une carte utilisée **[4].**

I.13.3 - Unité de traitement :

La partie responsable du traitement est le microprocesseur, ordinateur qui traite les données capturées par les capteurs ou un processeur de signal numérique (DSP). Pour traiter un échantillon biométrique, il doit contenir :

- ✓ Un échantillon d'amélioration d'image.

- ✓ Un échantillon de normalisation d'image.
- ✓ Extraction de caractéristiques.
- ✓ Comparaison de l'échantillon biométrique avec tous les échantillons stockés dans la base de données **[4].**

I.13.4 - Interface de sortie :

L'interface de sortie, Il s'agit de la dernière étape où nous sommes informés de la décision d'approuver ou non **[4].**

I.14 - Evaluation des systèmes biométriques :

De nos jours, l'évaluation des systèmes biométriques est un enjeu majeur en biométrie Grâce à son utilisation dans plusieurs applications quotidiennes, notamment, l'accès aux Sociétés privées, aéroports, sites sécurisés, etc.
L'évaluation des systèmes biométriques est généralement réalisée selon trois aspects dont L'objectif est de diminuer les limitations de ces systèmes. (La figure I.18**)** illustre les aspects d'évaluation des systèmes biométriques, en l'occurrence, la performance, l'usage et la sécurité **[3].**

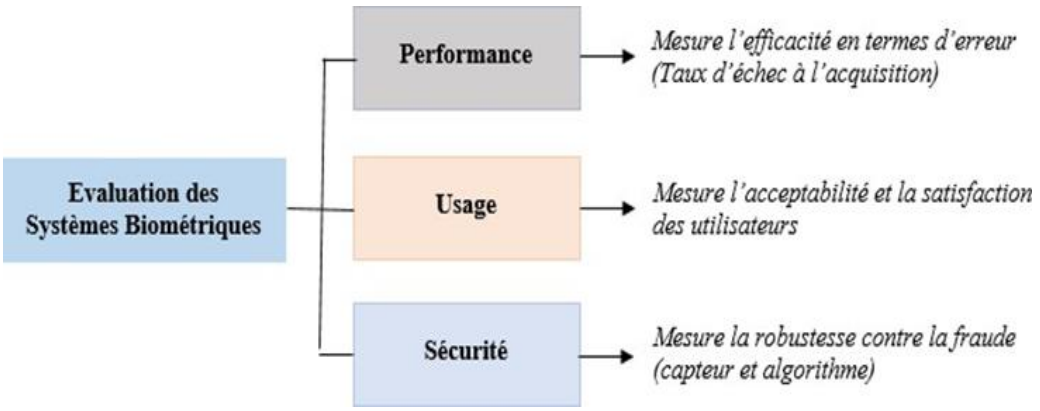

Figure I.18 : Aspects d'évaluation des systèmes biométriques

I.15 - Mesure de performance des systèmes biométriques :

La performance mesure l'efficacité et la fiabilité d'un système biométrique dans un contexte d'utilisation donnée. Dans cette section, nous présentons les différentes mesures utilisées pour quantifier la performance d'un système biométrique **[27].**

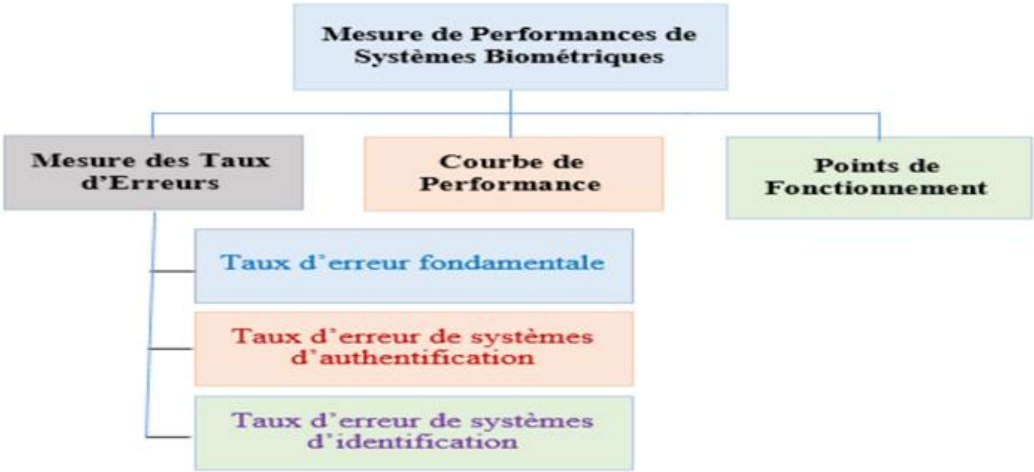

Figure I.19 : Mesure de performance des systèmes biométriques.

I.15.1 - Taux de faux rejets (False Rejet Rate où) FRR :

Ce taux détermine la probabilité qu'un système ne reconnaisse pas une personne qui aurait normalement dû être reconnue. C'est un rapport entre le nombre de personnes légitimes dont l'accès a été refusé et le nombre total de personnes légitimes qui se sont manifestées **[24].**

$$\text{FRR} = \frac{\text{nombre des clients rejetés}}{\text{nombre total d'accès clients}} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \text{(I.1).}$$

I.15.2 - Taux de fausse acceptation (False Accept Rate ou FAR) :

Ce taux détermine la probabilité qu'un système reconnaisse une personne qui normalement n'aurait pas dû être reconnue. C'est un rapport entre le nombre de personnes qui ont été acceptées lorsqu'elles n'auraient pas dû l'être et le nombre total de personnes non autorisées qui ont tenté d'être acceptées **[24].**

$$\text{FAR} = \frac{\text{nombre des imposteurs acceptés}}{\text{nombre total d'accès imposteurs}} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \text{(I.2).}$$

I.15.3 - Taux d'égale erreur (Equal Error Rate ou EER) :

Ce taux est calculé à partir des deux premiers critères et constitue un point de mesure des performances actuelles. Ce point correspond à l'endroit où FRR = FAR, c'est le meilleur compromis entre les faux rejets et les fausses acceptations **[24].**

$$\text{EER} = \text{nombre de fausses acceptations} + \frac{\text{nombre de faux rejets}}{\text{nombre total d'accès}} \quad \ldots\ldots\ldots\ldots\ldots\ldots \text{(I.3).}$$

La (**figure I.20**) représente la distribution des taux de vraisemblance des utilisateurs légitimes et des imposteurs. Les deux taux d'erreurs « FAR » et « FRR » sont liés et dépendent d'un seuil de décision qui doit être ajusté en fonction de la caractéristique ciblée du système biométrique haute ou basse sécurité :

- ✓ Plus le seuil est bas, plus le taux de fausses acceptions est élevé. Dans ce cas, le système biométrique acceptera des imposteurs.

- ✓ Plus le seuil est élevé, plus le taux de fausses acceptions est bas. Dans ce cas, le système biométrique est robuste aux imposteurs mais rejette de vrais utilisateurs **[3].**

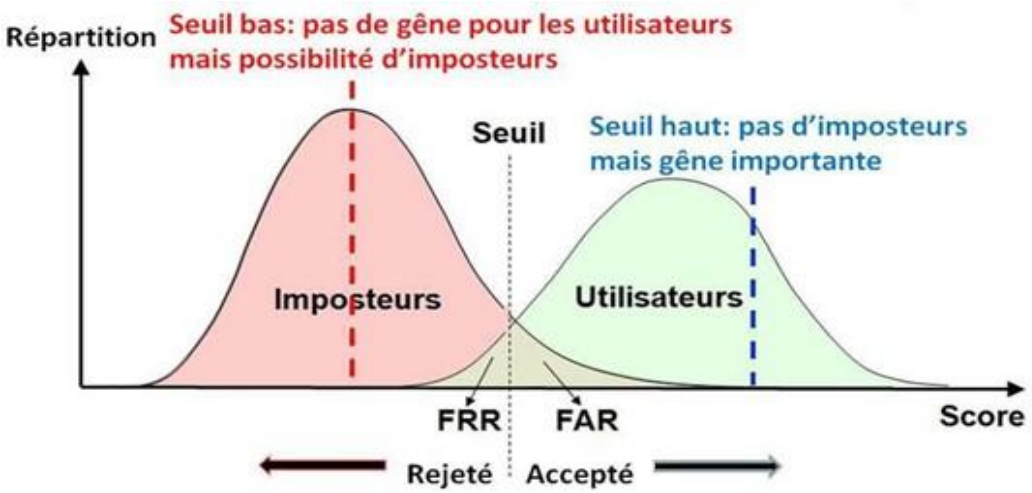

Figure I.20 : Taux de vraisemblance des utilisateurs légitimes et des imposteurs d'un système d'authentification biométrique.

I.15.4 - Taux d'acceptation réel (Genuine Acceptance Rate ou GAR) :

Le taux d'acceptation réel (GAR) est une mesure de la précision globale du système biométrique il est Calculé par la formule **[24] :**

$$GAR(\%) = 100 - FRR \quad \text{(I.4)}.$$

I.15.5 – Les Courbes de performances :

- **ROC (Receiver Operating Characteristics):**

Les performances d'un système biométrique peuvent être présentées graphiquement à l'aide de la courbe ROC (Receiver Operating Characteristic).

Cette courbe représente les valeurs de FRR en Fonction de FAR. Ceci est obtenu en calculant le couple (FAR, FRR) pour toutes les valeurs des seuils De test. Celui-ci diffère de la plus petite valeur obtenue à une valeur supérieure. Cette courbe peut etre décomposée en trois zones : zone de haute sécurité, zone de compromis et zone de basse Sécurité **[24].**

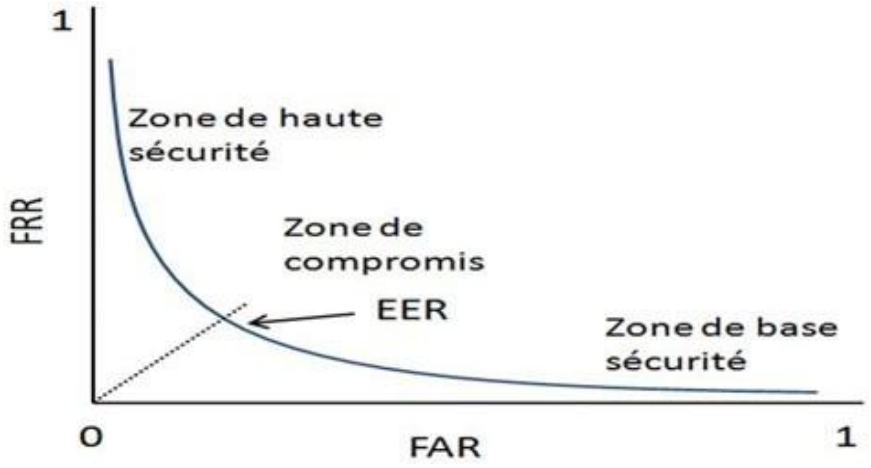

Figure 1.21 : Courbe ROC : Variation du taux de Faux Rejets (FRR) en fonction du Taux de Fausses Acceptations (FAR) lorsque le seuil de décision varie.

Courbe de scores cumulés (Cumulative Match Characteristic ou CMC) :

Cette courbe (voir figure I.22) donne le pourcentage de personnes reconnues selon une variable Appelée rang **[24].**

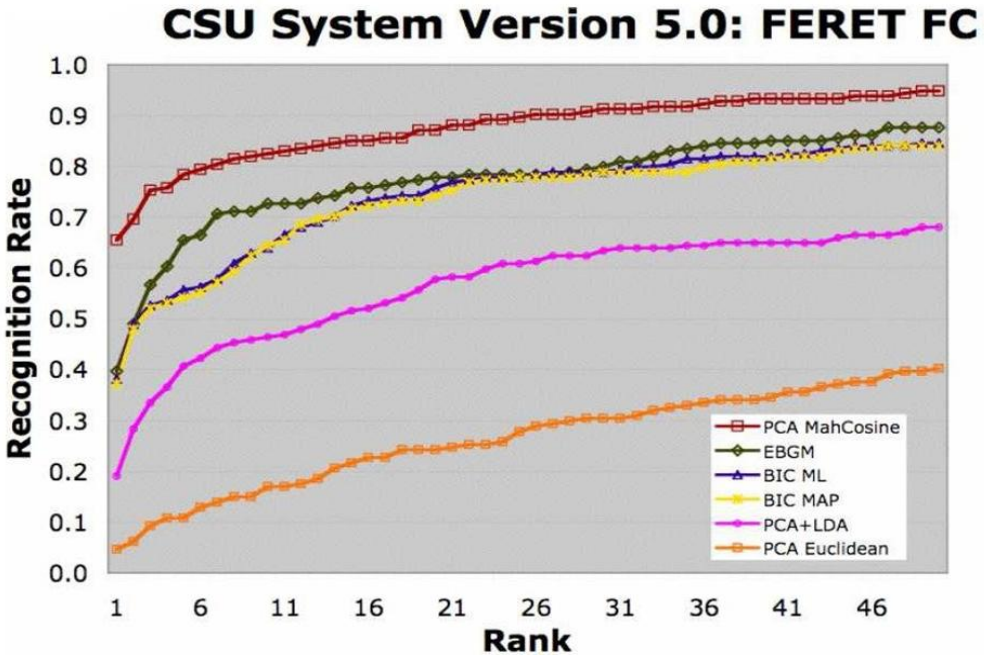

Figure I.22 : Courbe CMC.

Dans le cas d'un système utilisé en mode identification, on utilise la courbe CMC (**C**umulative **M**atch **C**haracteristic). Cette courbe représente le pourcentage de personnes Reconnues en fonction du rang. Le rang est une variable propriétaire au système de reconnaissance. On dit qu'un Système reconnaît au rang 1 lorsqu'il choisit la plus proche image comme résultat de Reconnaissance. On dit qu'un système reconnaît au rang n, lorsqu'il choisit, parmi n images, Celle qui correspond le mieux à l'image d'entrée. Il est clair que le système devient

plus Performant lorsque le rang diminue **[23].**

- **Courbe *DET* (*Detection Error Tradeoff*)**

Cette courbe illustre la relation entre le FRR et le FAR. Elle est obtenue en faisant varier le seuil de décision et en calculant à chaque fois les deux valeurs FRR et FAR. (La figure **1.23)** illustre un exemple de la courbe DET **[3].**

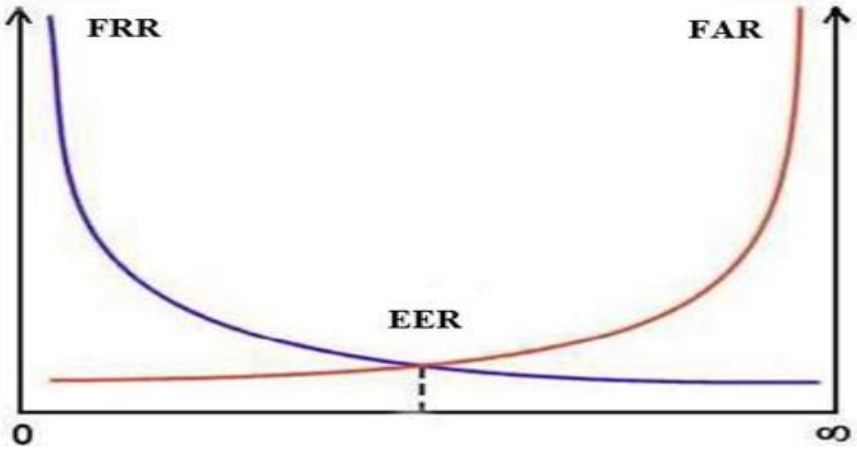

Figure 1.23 : Courbe DET : Variation du taux de Faux Rejets (FRR) en fonction du taux de Fausses Acceptations (FAR) en échelle Logarithmique lorsque le seuil de décision vari

I.16 – Conclusion :

Dans ce premier chapitre qui concerne la biométrie et après la définition de ce terme, nous avons présenté quelques modalités qui sont les plus utilisées actuellement.

On a vu aussi l'architecture d'un système biométrique et sur quels critères on se base pour évaluer les performances de ce dernier. En fin, ce chapitre se termine par les applications et les contraintes des systèmes biométriques. Des modalités telles que l'empreinte digitale, la reconnaissance faciale, l'iris, la voix, ou encore des approches émergentes comme la reconnaissance des articulations des doigts (FKP), permettent de répondre à divers besoins en matière d'accès sécurisé, de contrôle d'identité et de lutte contre la fraude.

En somme, la biométrie représente un champ en constante évolution, à la croisée des technologies et des enjeux éthiques, dont le potentiel continue de transformer les méthodes d'authentification à l'échelle mondiale.

CHAPITRE II

LA BIOMÉTRIE DE LA MAIN

II.1- Introduction :

La main est une région particulièrement riche en informations pouvant être utilisées pour l'authentification ou pour l'identification des individus. Parmi les divers solutions disponibles, l'empreinte digitale est certainement une des modalités les plus utilisées, notamment grâce à son invariance dans le temps. Son utilisation a bien entendu évolue au fil du temps, soutenue par l'émergence de système de capture de plus en plus performants.

Hormis l'empreinte digitale, d'autres caractéristiques plus ou moins robustes mais aussi plus au moins acceptables pour l'utilisateur peuvent être considérées. Nous pouvons citer par Exemple : la morphologie de la main, les réseaux veineux des doigts, de la paume ou même de l'avant-bras. L'empreinte et les lignes Palmaires. Évidemment. L'utilisation de telle ou telle modalité dépend des domaines d'application. Évidemment. Utilisation. De tel hôtel. Modalité dépend des domaines d'application in fine. Par exemple, si l'on désire mettre en place une gestion et un contrôle d'accès Physique, on privilégiera de préférence l'utilisation de la biométrie basée sur la morphologie de la main qui est parfaitement adaptée à cette tâche. Techniquement il s'agit d'effectuer des mesures telles que la longueur, la largeur des doigts, Ainsi que d'autres mesures relatives aux articulations et à la paume. Au final un vecteur résultant concaténant l'ensemble des caractéristiques peut être utilisé dans le cadre de la reconnaissance des individus**.**Ce type de biométrie nécessite l'utilisation d'un système l'utilisateur pose sa main sur un gabarit sur lequel les emplacements du pouce, de l'index et du majeur sont physiquement matérialisés par des chevilles **[27].**

Afin d'obtenir une capture riche en informations, une analyse sous des angles différents est effectuée. En général, deux clichées suffisent pour un rendu tridimensionnel. La biométrie par l'étude des caractéristiques de la morphologie de la main présente quelques avantages. Tout d'abord il faut souligner une très grande simplicité de mise en œuvre mais également d'utilisation. De plus, très peu intrusive cette technologie est bien acceptée par les utilisateurs. La robustesse a diverses blessures (c'est-à-dire coupures, Brûlures), mais aussi à la propriété ou l'humidité (transpiration) n'affectent nullement son utilisation. Les éventuelles barrières psychologiques pouvant existées lors des relevés des empreintes digitales n'ont plus lieu d'être.

Cependant cette technologie présente plusieurs inconvénients. Nous pouvons en distinguer au moins deux grandes catégories. La première et propre à la stabilité de la main dans le temps, il existe une évolution évidente, chez les sujets jeunes, des caractéristiques intrinsèques de la main avec le temps.

Il peut également arriver que des déformations importantes empêchent une bonne robustesse lors de son utilisation. Qu'elles soient liées à des pathologies ou bien tout naturellement au vieillissement de la personne. L'arthrite, par exemple, peut induire des déformations significatives des doigts tant dans l'heure géométrie intrinsèque que Dans leur agencement en termes de segment (déformation des articulations). Nous devons également noter que certains problèmes sont directement liés à des « parasite», tels des bagues ou autres bijoux. Un second

pôle d'inconvénient peut être également identifie. Il s'agit de la taille du dispositif (scan aire + unité de traitement) qui rond malheureusement inaccessible cette technologie a d'éventuel systèmes portatifs comme il peut en exister par. Ailleurs pour d'autres modalités (Lecteur d'empreinte digitale contenu dans une clé USB, Par exemple) **[27].**

Dans le domaine de la biométrie de la main, la tendance actuelle des systèmes de capture s'orie ente vers la biométrie, dites sans contact touchless ou Contatles l'avantage majeur de cette techno logis est que la main / doigt ne touche pas le système. Ainsi l'acquisition peut se faire à quelques centimètres seulement du capteur. De plus, les techniques d'acquisition vont au de la du domaine du visible. Autrement dit on s'intéresse de plus en plus à une capture en proche infrarouge.

Le principe consiste principalement affaire apparaître les veines de la main ou du doigt et par conséquent a les caractériser tout en assurant une certaine robustesse. En identifiant et étudiant les différentes modalités accessibles au niveau de la main (Caractérisation des empreintes digitales, des lignes de la main ou bien encore des veines), il est intéressant de souligner que la structure de ces région présente, d'une certaine façon, des caractéristiques semblables. Par conséquent, des approches de traitement du signal fondées sur l'extraction des points d'extrémité et des points de bifuracation (Minuties) peuvent être efficacement utilisées. **[27].**

II.2 - Les modalités biométriques liées à la main :

Les traits biométriques basés sur la main peuvent être divisés en deux grandes catégories **:** Les unes appartenant à la partie palmée et les autres à la partie dorsale de la main.

- **La partie palmée** : est la partie intérieure et saisissante de la main. Les attributs biométriques largement utilisés extraits de cette partie sont :

✓ Empreinte digitale (finger print).

✓ Empreinte palmaire (palmprint).

✓ Les réseaux veineux (palm vein, finger vein).

✓ Les motifs d'articulation de doigt sur la face de la paume de la main (finger inner knuckle print IKP).

➢ **La partie dorsale de la main** : occupe la zone située derrière la partie palmée) :

Les traits biométriques appartenant à la partie dorsale de la main n'ont pas été explorés autant que leurs contreparties palmées. Les traits utilisés dans cette partie sont :

✓ La morphologie de la main (hand geometry or shape).

✓ Géométrie de doigts (finger geometry).

✓ Les réseaux veineux (dorsal hand vein).

✓ Les motifs d'articulation du doigt sur la partie dorsale de la main (Finger dorsal knuckle print FKP) **[1].**

PARTIE PALMAIRE PARTIE DORSALE

Figure II .1 : La main (face dorsale et face palmaire).

II-3 Les avantages de la biométrie de la main :

II.3.1- Avantage 1 : Pas de prise d'empreinte digitale :

Cette technologie n'effectue aucune lecture d'empreintes digitale. La mesure des épaisseurs des doigts s'effectue à l'aide de miroirs et d'une caméra haute définition infrarouge ; on parle alors démesures biométriques en trois dimensions, La biométrie de la main est largement acceptée par les utilisateurs car elle ne mémorise pas les empreintes digitales **[28].**

II.3.2 - Avantage 2 : La biométrie de la main, biométrie sans trace :

La biométrie de la forme de la main est dite "biométrie qui ne laisse pas de traces". En effet, les mesures effectuées par cette technologie sont des relevés en trois dimensions de la main (comme l'épaisseur des doigts).

A aucun moment l'utilisateur ne laisse de traces de l'épaisseur de ses doigts, il ne laisse donc pas de traces de son passage. Sa liberté est ainsi préservée. Pas de traces : facilement accepté **[28]**.

II.3.3 - Avantage 3 : Biométrie de la main, biométrie largement diffusée :

La biométrie de la main, par sa souplesse, est largement utilisée dans les domaines aussi divers que la gestion du temps, gestion des cantines scolaires, pointeuse biométrique, badgeuse biométrique, sécurité avec la gestion des accès, gestion de la distribution des clés **[28].**

II.4 -Pour quoi la modalité de la main :

Le trait de la main présente divers avantages par rapport aux autres modalités biométriques. En effet, elle est considérée comme attractive pour les raisons suivantes :

- ✓ La simplicité de l'acquisition de la main avec des appareils peu coûteux
- ✓ L'information sur la main peut être extraite à l'aide d'images à faible résolution
- ✓ Le trait de la main est plus acceptable par le public que les autres modalités

- ✓ Les modalités biométriques supplémentaires, y compris les empreintes palmaires et les doigts, peuvent être intégrées dans un système biométrique développé pour la forme de la main **[29].**

II.5 - Présentation de quelques modalités biométriques de la main :

Plusieurs systèmes de reconnaissance de la main ont été proposés dans le but d'identifier une personne en décrivant différentes parties de la main. Cette section présente un aperçu des caractéristiques de base de la main, y compris sa forme, sa géométrie, ses empreintes de paume et ses doigts **[2].**

II.6 - Aperçu du système biométrique de la main entière :

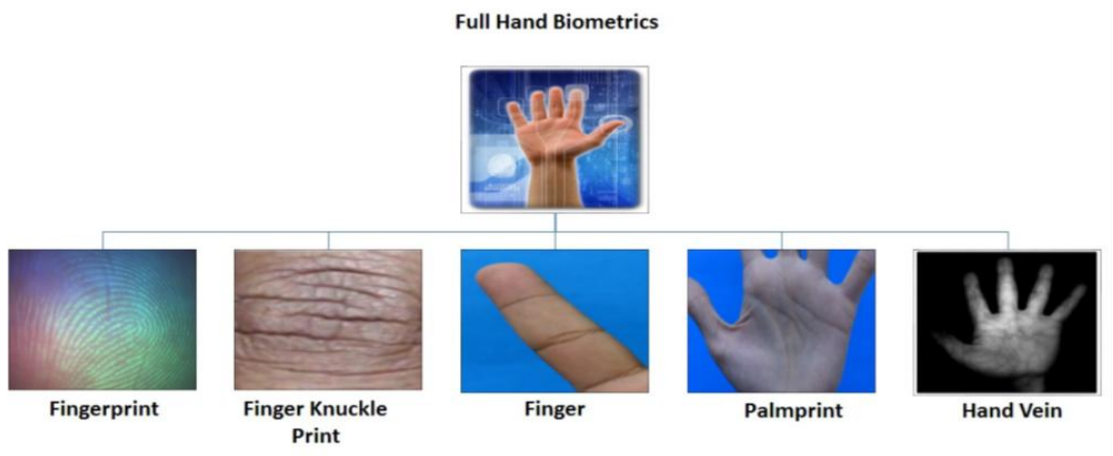

Figure II.2 : Aperçu des sous-composants de la biométrie de la main entière

Un système biométrique basé sur la main entière repose sur l'analyse et la reconnaissance des caractéristiques physiques uniques de la main pour l'identification et l'authentification des individus. Contrairement aux systèmes utilisant uniquement les empreintes digitales ou palmaires, ce type de biométrie exploite une combinaison de plusieurs traits biométriques présents sur toute la surface de la main, améliorant ainsi la précision et la sécurité.

Ce système peut inclure l'analyse des empreintes digitales, des motifs de crêtes de la paume, de la forme des doigts et même de caractéristiques géométriques telles que la structure globale de la main. Avec les avancées technologiques, les solutions biométriques sans contact basées sur la main entière gagnent en popularité, notamment grâce aux caméras haute résolution permettant de capturer des images détaillées sans nécessiter un contact direct **[32].**

Les applications de la biométrie de la main entière sont variées, allant du contrôle d'accès sécurisé aux transactions financières et à l'identification judiciaire. Dans un contexte de sécurité aux frontières et d'analyses criminelles, elle permet une vérification fiable et rapide, réduisant les risques liés à la falsification et l'usurpation d'identité.

L'un des défis majeurs de ces systèmes réside dans l'optimisation des algorithmes de reconnaissance afin de garantir une robustesse face aux variations géométriques et aux conditions d'acquisition des images. Cependant, avec l'évolution des techniques d'intelligence artificielle et de traitement d'image, la biométrie de la main entière pourrait devenir une référence dans les systèmes d'identification biométrique avancés **[32].**

1. La géométrie de la main.
2. Système de reconnaissance des empreintes digitale.
3. Système de reconnaissance des doigts entiers.
4. Système de reconnaissance des empreintes palmaires.
5. Biométrie de la main entière**.**
6. La dynamique du mouvement de la main.
7. Le réseau veineux.

II.6.1 - La géométrie de la main :

La biométrie de la géométrie de la main repose sur l'analyse de dimensions spécifiques telles que :

- La longueur des doigts.
- La largeur de la paume.
- L'angle entre les articulations.

Cette technologie est particulièrement utilisée dans les contrôles d'accès. Cependant, elle est influencée par des facteurs tels que l'âge, les blessures ou la prise de poids, ce qui peut affecter la précision du système **[38].**

Cette technique cantonnée à des usages sans enjeux majeurs de sécurité et concernant un nombre limité d'utilisateurs : accès à des bâtiments privés non stratégiques tels que des entreprises, des écoles **[30].**

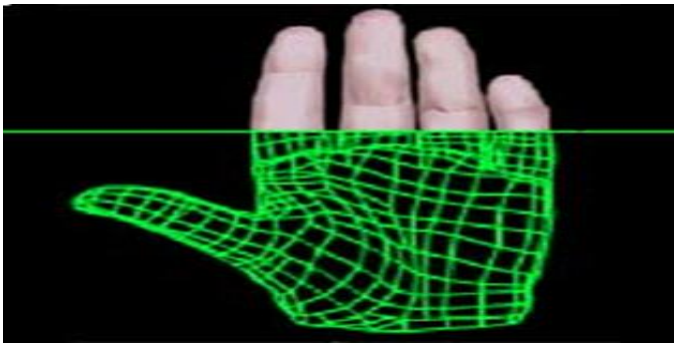

Figure II.3: la géométrie de la main

- **Acquisition de la géométrie de la main :**

En général, une caméra infrarouge prend l'image de la main sous deux angles différents pour obtenir les trois dimensions. Lecteur de la forme de la main.

Cette solution a fait ses preuves tant sur le plan de la simplicité de mise en oeuvre, que de sa fiabilité dans le temps. Mais du fait de la taille de la main, les lecteurs de forme de la main sont en général assez volumineux **[31].**

- **Traitement numérique de l'image de la main :**

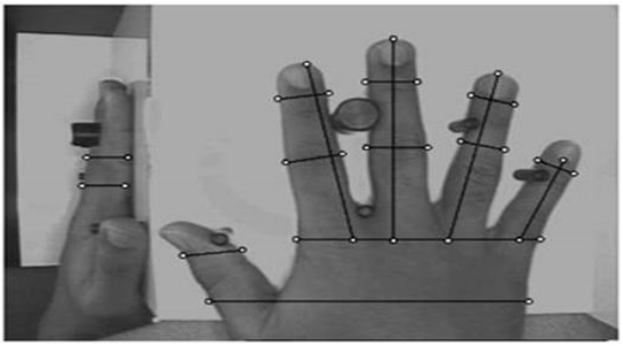

Figure II .4 : Caractérisation de la géométrie d'une main en 3 dimensions.

Les mesures qui sont faites ne prennent que les dimensions de certaines parties de la main (la longueur des doigts, la largeur des articulations, l'épaisseur des doigts, etc.) et non la pigmentation de la peau ou les lignes situées au niveau des articulations. Le gabarit qui en résulte est d'une taille très faible (une dizaine d'octets) et permet de faire de l'authentification **[31].**

II.6.2 - Système de reconnaissance des empreintes digitale :

Est une technologie biométrique avancée qui permet d'identifier ou d'authentifier une personne en analysant les caractéristiques uniques de ses empreintes digitales. Voici une explication approfondie de son fonctionnement et de ses applications **[39].**

Les empreintes digitales-Appelées aussi dermatoglyphes sont une signature que nous laissons derrière nous à chaque fois que nous touchons un objet. Les motifs dessinés par les crêtes et plis de la peau sont différents pour chaque individu ; c'est ce qui motive leur utilisation par la police criminelle depuis le 19è siècle.

Les dermatoglyphes sont des formations de crêtes parallèles présentes sur la peau des paumes et des doigts des mains et sur la plante des pieds et les orteils (Cummins et Midlo, 1926).

Sur le bout des doigts, ces motifs réguliers de crêtes et de sillons forment des empreintes

digitales de trois principaux types de motifs : arc, boucle et verticille. Bien que les empreintes digitales aient probablement évolué pour faciliter la préhension (André et al., 2010 ; Yum et al., 2020) et pour la détection des textures de surface (Loesch et Martin, 1984; Medland et al., 2007; Scheibert et al., 2009), depuis le 19ème siècle, l'empreinte digitale a été largement utilisée pour l'identification personnelle car les motifs sont uniques à chaque individu, présents dès la naissance, et ne changent pas au cours de la vie (Galton, 1892) **[31].**

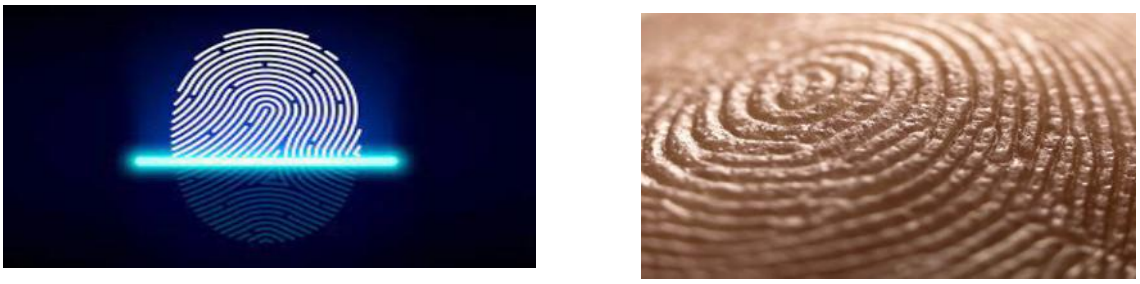

Figure II. 5 : empreinte digitale

II.6.3 - Le système de reconnaissance des doigts entiers :

Est une technologie biométrique avancée qui repose sur l'analyse globale des caractéristiques de l'ensemble du doigt pour l'identification et l'authentification des individus. Contrairement aux méthodes traditionnelles basées sur les empreintes digitales, qui se concentrent sur les minuties telles que les terminaisons de crêtes et les bifurcations, ce système examine la structure complète du doigt, y compris la texture de la peau, les contours et la morphologie **[47].**

Les systèmes biométriques peuvent tirer parti de la modalité FKP en raison de divers avantages. Tout d'abord, l'acquisition de données est relativement simple et économique grâce à l'utilisation de caméras commerciales à faible résolution.

les caractéristiques FKP des adultes sont plus stables dans le temps et ne subissent pas de changements significatifs. Enfin, les informations biométriques basées sur le FKP sont extrêmement fiables et permettent une reconnaissance précise parmi un ensemble de personnes **[50].**

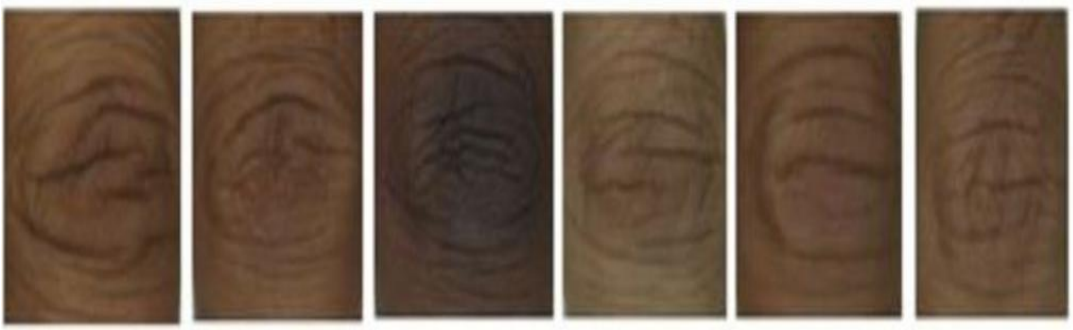

Figure II.6 : Empreintes des articulations des doigts

II.6.4 - Système de reconnaissance des empreintes palmaires :

On appelle paume de la main la partie intérieure de la main (partie non visible lorsque la main est fermée) du poignet aux racines des doigts, comme le montre la Figure II.7.

Ainsi, l'empreinte palmaire n'est autre que l'impression (image) de la paume de la main faite par la pression de cette dernière sur une surface donnée. En d'autres termes, elle peut être définie comme étant le modèle de la paume de la main illustrant les caractéristiques physiques du motif de sa peau tel que les lignes (principales et rides), points, minutie et texture **[11].**

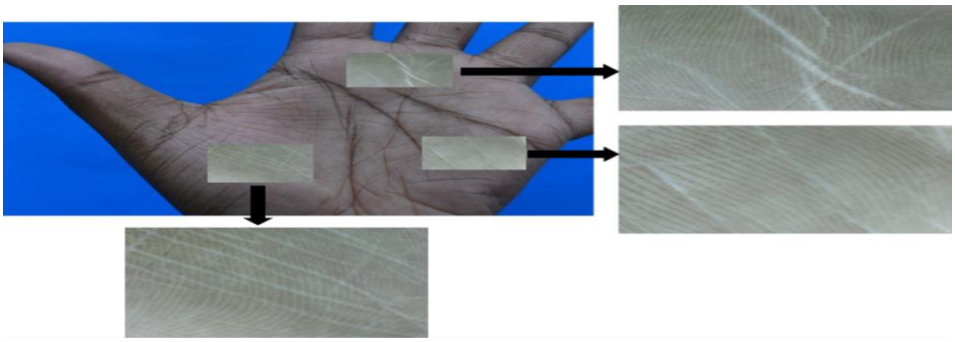

Figure II.7: Représentation du motif des crêtes dans une paume sans contact.

II.6.5 - Biométrie de la main entière :

La biométrie de la main entière est une méthode de reconnaissance qui analyse l'ensemble de la structure et des caractéristiques uniques de la main pour identifier ou authentifier une personne. Cette technique biométrique est reconnue pour sa simplicité, son efficacité et sa capacité à capturer plusieurs traits distinctifs simultanément. Cet article explore les principes fondamentaux, les technologies utilisées et les applications pratiques de cette méthode **[16].**

Figure II .8 : biométriques de la main entière

II.6.6 - La dynamique du mouvement de la main :

L'étude du mouvement de la main permet d'analyser la manière dont une personne interagit avec un système. Cela inclut :

- La vitesse de déplacement des doigts et de la paume.
- La pression exercée sur un écran tactile ou un capteur.

- Les trajectoires suivies lors de la saisie ou du dessin d'une signature.

Ce type de biométrie est particulièrement utile pour détecter les comportements frauduleux et renforcer le cyber sécurité **[41].**

II.6.7 - Le réseau veineux :

Figure II.9 : Reconnaissance des veines.

On a longtemps considéré que le modèle des veines dans l'anatomie humaine peut être unique aux individus. En conséquence, il y a eu de diverses réalisations du balayage de

veineux cours des années, du balayage de main, au Balayage de poignet et, plus récemment, au balayage de doigt. La plupart de ces techniques ont été utilisées sur terrain et ont pu certainement former la base d'un système biométrique viable de vérification d'identité.

Le problème auquel elles font face n'est pas un problème de possibilités ou d'efficacité technique, mais plutôt un problème de réalité du marché. La prépondérance de système d'empreinte digitale, de visage et d'iris, facilement disponibles à une large gamme de couts, ne permet pas à une technique distincte de gagner la part de marché sans avantage Clair et irrésistible.

Même les techniques primaires, telles que la géométrie de main, ont une base qui est peu susceptible d'être réalisée par une technique plus récente de performance comparable. En conséquence, pour n'importe quelle nouvelle technique biométrique prenant place dans le marché, elle doit gagner le terrain et offrir des avantages clairs qui ne peuvent pas are réalises par des méthodes contemporaines.

Les diverses réalisations de balayage des veines. Bien qu'assurément intéressantes, ne peuvent Lutter que peu dans ce contexte. Cependant, le temps peut s'avérer un niveleur intéressant dans ces contextes et les demandes de la technique de balayage de veines peuvent s'accroitre **[11].**

II.7 – Conclusion :

La biométrie de la main représente une approche diversifiée et efficace pour l'identification et l'authentification des individus. Elle repose sur plusieurs modalités, allant des empreintes digitales aux veines de la main, en passant par la géométrie et les caractéristiques comportementales.

Chaque modalité possède des avantages spécifiques : les empreintes digitales offrent une fiabilité éprouvée, la reconnaissance des veines garantit une sécurité renforcée, et l'analyse de la géométrie de la main propose une alternative rapide et intuitive. Toutefois, la précision et la robustesse de ces systèmes varient en fonction de l'environnement, des conditions physiologiques de l'utilisateur et des exigences de sécurité propres à chaque application.

CHAPITRE III

L'EMPREINTE DES ARTICULATIONS DES DOIGTS (FKP)

III.1- Introduction :

L'identification biométrique est devenue une technologie incontournable dans divers domaines, allant de la sécurité aux applications commerciales et gouvernementales. Parmi les nombreuses caractéristiques biométriques utilisées, l'empreinte des articulations des doigts, connue sous le nom de **Finger Knuckle Print (FKP)**, représente une modalité innovante et prometteuse.

Contrairement aux empreintes digitales classiques, les empreintes FKP exploitent les motifs uniques présents sur les articulations des doigts. Ces motifs sont formés par des crêtes dermiques qui restent stables tout au long de la vie d'un individu, offrant ainsi une fiabilité et une précision accrues dans les systèmes d'identification.

L'intérêt croissant pour cette technologie repose sur plusieurs avantages : une facilité d'acquisition des empreintes, une résistance aux altérations dues à l'usure des doigts, et une sécurité renforcée contre les tentatives de falsification. De plus, les empreintes FKP peuvent être utilisées en complément des empreintes digitales classiques pour améliorer la robustesse des systèmes biométriques.

III. 2 - La biométrie FKP :

Récemment, les chercheurs en biométrie ont découvert que l'empreinte de l'articulation de doigt (FKP), qui fait référence aux motifs inhérents à la surface externe autour de l'articulation phalangienne de doigt, est très unique et peut servir d'identificateur biométrique distinctif. En plus Les rides et les ridules peuvent également être clairement visibles à l'FKP dans les images de faible résolution. Dans un système biométrique FKP, un individu est vérifié par l'extraction des lignes, des plis et de la texture sur l'impression de jointure qui se trouvent à proximité des trois articulations. La surface externe d'un doigt a trois jointures classées en articulations majeure et mineure **[1] :**

✓ Première FKP mineure.

✓ FKP majeur.

✓ Deuxième FKP mineure.

III. 3 - Etat de l'Art de l'empreinte des articulations des doigts :

Récemment, on constate que l'empreinte d'articulation du doigt, qui se réfère aux formes inhérentes de la surface externe autour du doigt et spécialement la partie haute du doigt, est fortement unique et peut servir à une modalité biométrique distinctive. L'articulation du doigt est encore à la phase de développement et peut être considérée comme nouvelle tendance dans la biométrie **[34].**

Woodard and Flynn (2005), ont tout d'abord étudié la surface du doigt pour l'authentification individuelle. Ils ont utilisé un capteur Minolta 900/910 pour acquérir la surface du dos du doigt 3D. Leur étude valide le caractère unique de la surface arrière du doigt

en tant que caractéristique biométrique pouvant être utilisée. Cependant, leur travail n'est pas totalement centré sur les points d'articulation et ils ont utilisé toute la surface du dos des doigts pour l'authentification. De plus, le prétraitement de la surface du doigt en 3D et augmente le temps et la complexité du système ce qui limite son utilisation pour les applications biométriques en ligne **[26].**

En 2009, Kumar et Ravikanth, a présenté une description plus détaillée de l'acquisition et de l'extraction des points d'articulation de la partie dorsale de la main. Ils utilisent un appareil photo numérique à moindre coût (Canon Powershot A620-) pour capter le dos de la main. L'image de la main captée est ensuite utilisée pour extraire les points d'articulation comme une région d'intérêt (ROI). La PCA, Linear Discriminant Analysis (LDA) et Independent Component Analysis (ICA) sont des traits extraits de points d'articulation. Ce travail a mis beaucoup d'efforts pour valider le caractère unique de la surface externe supérieure du doigt, mais il n'a pas apporté de solution pratique **[10].**

Malgré le développement d'un nouvel appareil d'acquisition, le temps d'exécution reste un problème et ce problème est dû au matching et à la mesure de similarité (le temps total d'exécution pour une seule vérification prend environ une seconde), comme résultat ils ont trouvé un taux de reconnaissance de 97% et un FAR de 0.02% et un EER de 1.09%. Le centre biométrique de recherches à l'université polytechnique de Hong Kong a développé un appareil en temps réel pour la capture de l'empreinte d'articulation et l'utiliser pour la construction d'une base de données à grande échelle **[26].**

Dans, les images de l'empreinte de l'articulation contiennent plus de bruit que les empreintes de la paume. Dans ce cas, ils ont proposé deux étapes : l'application du filtre 2D de Gabor pour améliorer les lignes de l'empreinte de l'articulation et les descripteurs SIFT (Scale-Invariant Feature Transform). Après le filtre de Gabor, l'algorithme CLAHE (Contrast Limited Adaptive Histogram Equalization) est appliqué pour corriger le contraste des lignes de l'articulation **[10].**

ZHU Le-qing, utilise la base de données PolyU. Dans un premier temps, une normalisation du ROI FKP a été utilisée, après l'application de l'algorithme SURF (Speeded Up Robust Features) pour l'extraction des caractéristiques en vue d'une comparaison ultérieure avec RANDOM SAMPLE Consensus (RANSAC). Ils ont obtenu 90,63 % comme pourcentage de vérification et 96,91 % pour l'identification **[34].**

Yang Wankou, propose une autre méthode qui consiste à utiliser le filtre de Gabor et l'analyse discriminante linéaire orthogonale (OLDA) pour identifier les individus à partir de leurs empreintes articulaires. Tout d'abord, la représentation des caractéristiques obtenues à partir du filtre de Gabor est calculée après l'utilisation d'un ACP, et après le calcul d'une OLDA de transformation. Ce travail également basé sur la base de données PolyU, les résultats montrent que cette méthode est plus performante que les algorithmes qui utilisent uniquement LDA ou PCA **[34].**

Zahra S. et al., utilisent une banque de filtre de Gabor pour l'extraction des caractéristiques, la combinaison des PCA et LDA pour la fragmentation de la dimension de l'espace et la distance euclidienne pour la classification. Ce travail regroupe quatre empreintes d'articulation du même individu au niveau des caractéristiques. La base de données PolyU a été utilisée pour examiner la performance de la méthode proposée. Les résultats obtenus sont 98.79% pour l'identification et 91.8% pour la vérification **[34].**

Chetana Hegde et al, proposent trois algorithmes différents pour la reconnaissance des empreintes d'articulation. La première approche utilise la transformée de Radon pour l'extraction des caractéristiques et pour la phase de prétraitement, la détection du contour et le filtre médian ont été utilisé. Après l'application de la morphologie mathématique et la dilatation, un taux FAR de 1.55% est obtenu et 1.02% pour le FRR. Dans la deuxième méthode, les ondelettes de Gabor sont utilisées pour l'extraction des caractéristiques. Dans la première étape, ils éliminent le bruit et incrémentent l'intensité avec les coefficients de corrélation. Les résultats obtenus sont le FAR : 1.24% et le FRR : 1.11%. Pour le dernier algorithme, celui-ci reconnait les parties endommagées des FKP. Ils ont créé 450 FKP endommagés pour introduire le bruit et aléatoirement éliminer quelques valeurs des pixels de l'image des FKP. Un taux de reconnaissance de 95.33% est obtenu **[34].**

La méthode par la fusion de plusieurs algorithmes pour l'extraction des caractéristiques est présentée. Ils utilisent LG (Log Gabor), LPQ (Local Phase Quantization), PCA et LPP (Locality Preserving Projections) pour l'extraction des caractéristiques. Dans la première expérience, ils utilisent un seul algorithme pour extraire les caractéristiques. Les résultats de cette étude montrent que l'algorithme de LG est d'une grande précision par rapport aux autres algorithmes. Une fusion entre deux algorithmes a été utilisée. La meilleure fusion est la fusion entre LG et LPP avec un taux de reconnaissance de 89,67%. Dans cet article, ils se concentrent uniquement sur la phase d'extraction des caractéristiques **[34].**

III. 4 - Signification de l'utilisation des articulations des doigts :

Les méthodes basées sur la géométrie de la main, qui incluent les empreintes digitales, les empreintes de paume et d'autres identifiants similaires, sont les plus courantes parmi les caractéristiques biométriques, car elles bénéficient d'un taux d'acceptation plus élevé auprès des utilisateurs. Récemment, après une analyse approfondie, il a été découvert que les plis et les creux de la peau au niveau des articulations des phalanges externes sont distincts. Par conséquent, ils peuvent être utilisés comme identifiant biométrique unique. Cette découverte est relativement récente. Comparées aux empreintes digitales, les articulations des doigts offrent des avantages supplémentaires, notamment leur moindre susceptibilité aux dommages.

La partie externe est rarement utilisée, car seule la zone interne de la paume est sollicitée lorsque nous plions nos mains. De plus, elle n'est impliquée dans aucune activité illégale, ce qui la rend parfaitement adaptée à une utilisation sécurisée. Un autre avantage est qu'elle ne

peut pas être falsifiée, car personne ne laisse son empreinte d'articulation sur les surfaces qu'il touche ou manipule **[35].**

III. 5 - Système de reconnaissance des articulations des doigts :

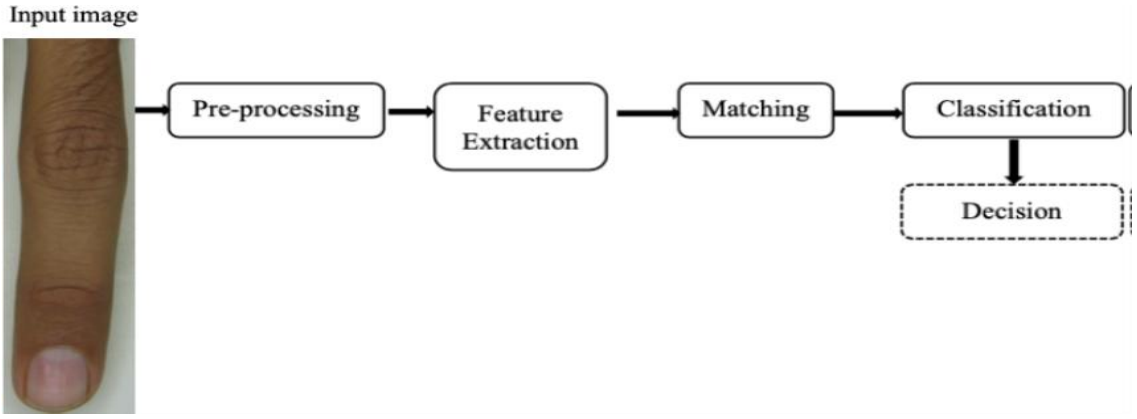

Figure III.1 : Système de reconnaissance des articulations des doigts

III.6 – Acquisition :

Le module d'acquisition des images FKPs est composé d'un support de doigt, d'une source de lumière LED sous forme d'un anneau, d'une lentille, d'une caméra CCD et d'une carte d'acquisition. La source de lumière LED et la caméra CCD sont enfermés dans une boîte de sorte que l'éclairage soit presque constant. Un bloc basal et un bloc triangulaire sont utilisés pour fixer la position de l'articulation du doigt.

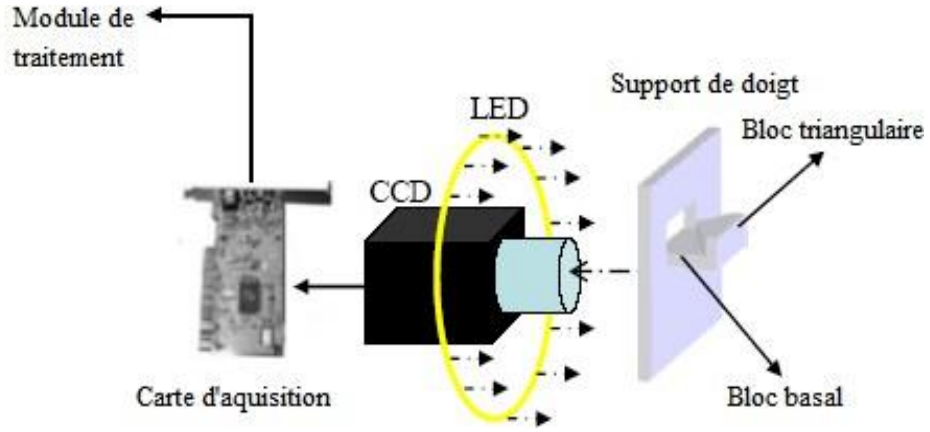

Figure III.2 : Structure du module d'acquisition.

Dans acquisition de données, l'utilisateur peut facilement mettre son doigt sur le bloc basal en touchant les deux pentes du bloc triangulaire. Une telle conception vise à réduire les variations de position du doigt dans différentes sessions de capture.

Dès que, l'image est capturée elle est envoyée au module de traitement de données pour le prétraitement et l'extraction de caractéristiques **[10].**

III.7 – Prétraitement :

La phase de prétraitement vient après la phase de détection. Elle permet de préparer l'image de l'articulation de doigt de telle sorte qu'elle soit exploitable dans la phase d'enrôlement. On l'appelle aussi phase de normalisation puisqu'elle ramène à un format prédéfini toutes les images extraites de l'image brute afin d'extraire la région d'intérêt (Region Of Interest ROI) qui contient les textures autour de l'articulation. Cette opération a pour but d'éliminer le fond (réduction de la taille d'image) et d'avoir des résultats plus précis **[13].**

III.7.1 - Extraction du ROI des empreintes des articulations des doigts (FKP) :

L'objectif principal de l'extraction du ROI des empreintes des articulations des doigts (FKP) est de déterminer le rectangle qui couvre la région contenant les caractéristiques FKP. Ce processus est considéré comme une étape de prétraitement visant à obtenir les informations utiles des traits FKP. La Figure(III.3) illustre les étapes du processus permettant d'extraire le ROI à partir des caractéristiques FKP.

La procédure décrite les étapes suivantes :

1. Appliquer une opération de lissage gaussien à l'image originale (Fig.III.3a).
2. Déterminer l'axe X du système de coordonnées fixé à partir de la limite inférieure du doigt (Fig. III.3b). Ainsi, la limite inférieure du doigt est extraite à l'aide du détecteur de contours de Canny.
3. Déterminer l'axe Y du système de coordonnées en utilisant le détecteur de contours de Canny sur la région (Fig. III.3c). Cet axe est extrait de l'image originale selon l'axe X. Cette étape permet de localiser la direction convexe.
4. Enfin, déterminer le système de coordonnées du ROI, où le rectangle couvre la région contenant les informations du ROI **[37].**

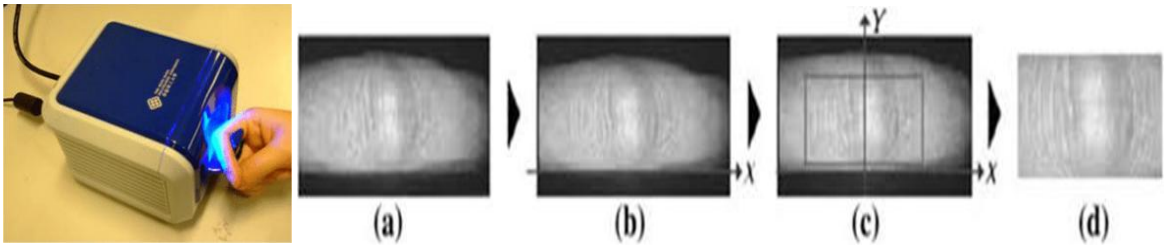

Figure III.3: Le processus d'extraction de la région d'intérêt (ROI) de l'image FKP.

III.7.2 - Segmentation des Empreintes Articulaires (Finger- Knuckle - Print):

Les échantillons FKP peuvent être acquis dans un environnement sans contact et sans contrainte. Ces échantillons contiennent généralement l'image de tout le doigt ainsi que des informations de fond inutiles. Par conséquent, il est nécessaire d'extraire la partie pertinente de

l'image, appelée Région d'Intérêt (ROI), qui contient la zone articulaire avec peu ou pas de bruit de fond pour une meilleure extraction des caractéristiques **[44].**

III.7.3 - L'orientation des Empreintes Articulaires (Finger- Knuckle - Print) :

L'orientation des doigts/articulations décrit la position des doigts ou des articulations de la main lors de la production d'un signe ; en d'autres termes, la direction dans laquelle les doigts ou les articulations pointent pendant la formation d'un signe.

Dans les descriptions écrites de la formation des signes, nous incluons souvent l'orientation des doigts ou des articulations, car l'orientation de la paume seule peut ne pas être suffisamment précise. Par exemple, considérez ce qui suit (une main plate est utilisée pour les illustrations, vues du point de vue de l'observateur).

- **Paume vers le bas, doigts pointant vers l'intérieur** : position de la main lorsque la paume est tournée vers le sol et les doigts pointent vers le signataire.
- **Paume vers le bas, doigts pointant vers le côté (gauche)** : position de la main lorsque la paume est tournée vers le sol et les doigts pointent vers le côté gauche du signataire.
- **Paume vers le bas, doigts pointant vers le côté (droit)** : position de la main lorsque la paume est tournée vers le sol et les doigts pointent vers le côté droit du signataire.
- **Paume vers le bas, doigts pointant en diagonale vers l'avant et vers le côté opposé (gauche)** : position de la main droite lorsque la paume est tournée vers le sol et les doigts pointent en diagonale vers l'avant et vers le côté opposé (gauche).
- **Paume vers le bas, doigts pointant en diagonale vers l'avant et vers le côté opposé (droit)** : position de la main gauche lorsque la paume est tournée vers le sol et les doigts pointent en diagonale vers l'avant et vers le côté opposé (droit).

En général, l'orientation la plus naturelle de la main lors de la production d'un signe devant le corps est avec les doigts pointant en diagonale vers l'avant et vers le côté opposé.

III.8 - Extraction des caractéristiques :

Les caractéristiques d'une image sont ses propriétés intrinsèques et distinctives, extraites afin de représenter son unicité par rapport aux autres images et d'illustrer son contenu sous une forme plus condensée avec moins de dimensions. Les caractéristiques sont également appelées attributs d’image.

Pour construire les caractéristiques d'une image, on extrait ses aspects globaux et locaux. Ces attributs incluent les informations spatiales, la forme, le contraste, les contours et la couleur de l’image. Une autre approche est la fusion des caractéristiques, qui consiste à combiner plusieurs aspects pertinents d’une image afin d’obtenir des attributs plus robustes **[35].**

Le traitement d’image utilise diverses stratégies et algorithmes d’extraction de caractéristiques, parmi lesquels les plus notables sont le BSIF et LPQ.

III.8.1 - LPQ (Local Phase Quantization) :

L'opérateur de quantification de phase locale LPQ a été initialement proposé par Ojansivu et Heikkila pour décrire les textures. L'opérateur LPQ est avéré robuste et performant plus que l'opérateur LBP dans la classification des textures .LPQ est conçu pour conserver une image dans les informations locales invariantes aux artefacts générés par différentes formes de flou. Inspirés par cette idée, nous proposons le LPQ comme méthode efficace pour résoudre le problème de variations d'expressions. Le descripteur LPQ est construit sur le concept de quantification de la phase autour d'un bloc M×M de voisinage Nx pour chaque pixel x de l'image f(x) en utilisant la transformée de Fourier à court terme STFT. Le STFT (u, x) pour chaque position de pixel x à la fréquence u est donnée par :

$$F\,(\mathrm{u}, x) = \sum_{\mathrm{b}\in Na} \mathrm{f}\,(x - x)\, e^{-2j\pi u^T y} = W_u^T\, f_x \qquad \text{(III.5)}$$

Où $W_u$est le vecteur de base de la transformée discrète de Fourier 2D à la fréquence u, et fx est un autre vecteur contenant tous les échantillons d'image M^2 de N_x. Seuls les quatres coefficients de basse fréquence correspondant aux fréquences 2D sont pris en compte u_1 = $[a, 0]$, u_2 = $[0, a]$ T, u_3 = $[a, a]$ T et u_4 = $[a, -a]$ T, où a est un suffisamment petit scalaire pour satisfaire (u_i) > 0. Pour chaque position de pixel, il en résulte un vecteur :

$$F_a^c = [\mathrm{F}\,(u_1, x), F\,(u_2, x), F\,(u_3, x), F\,(u_4, x)] \qquad \text{(III.6).}$$

Les informations de phase dans les coefficients de Fourier sont enregistrées en observant les signes des parties réelles et imaginaires de chaque composant dans F_x. Ceci est fait par :

$$q_j = \begin{cases} 1 & si\ g_{i(x)} > 0 \\ 0\,, & si\ non \end{cases} \qquad \text{(III.7).}$$

Où $g_i(x)$ est le $j^{ième}$composant de G (x) = [Re $\{F\ (x)\}$, $\{(x)\}$] et $q_j(x)$ sont les huit coefficients binaires représentés sous forme de valeurs entières comprises entre 0 et 255 en utilisant un codage binaire similaire à la méthode LBP comme suit :

$$f_{LPQ}\,(x) = \sum_{j=1}^{8} q_j\, 2^{j-1} \qquad \text{(III.8).}$$

En conséquence, nous obtenons l'image d'étiquette f_{LPQ} dont les valeurs sont les étiquettes LPQ invariantes de flou. La Figure III.4 représente la structure de générer le code LPQ **[19].**

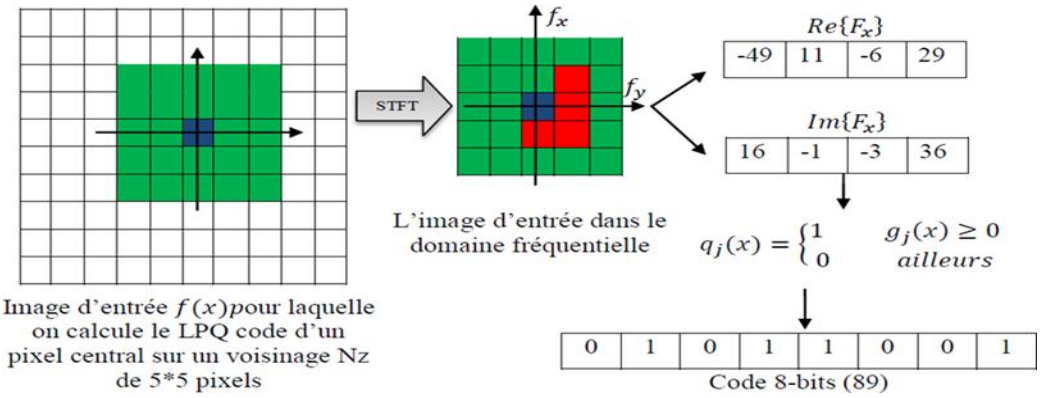

Figure III.4 : Organigramme de l'ensemble des étapes nécessaires du descripteur LPQ.

III.8.2 - Caractéristiques statistiques des images binarisées (BSIF) :

BSIF est un descripteur local récent pour reconnaître des textures. BSIF descripteur a été mentionné pour la première fois par J. Kannala et E. Rahtu en 2012. Ce descripteur est basé sur un ensemble de filtres linéaires de taille fixe. BSIF filtre une image donnée I de taille NxNpixels avec un ensemble de filtres $\varphi N\times N$alors les réponses ri sont binarisée.

J. Kannala et E Rahtu utilisent un ensemble des images naturelles (ȶ- à-dire-appliqué les concepts introduites dans) (voir Figure 3.14) pour former un ensemble des filtres φN×N, ces filtres sont estimés en maximisant l'indépendance statistique des répons ri par ICA. Également, nous avons utilisé les filtres open-source qui sont appris à partir de 13 images naturelles différentes. La réponse du filtre est obtenue comme suit:

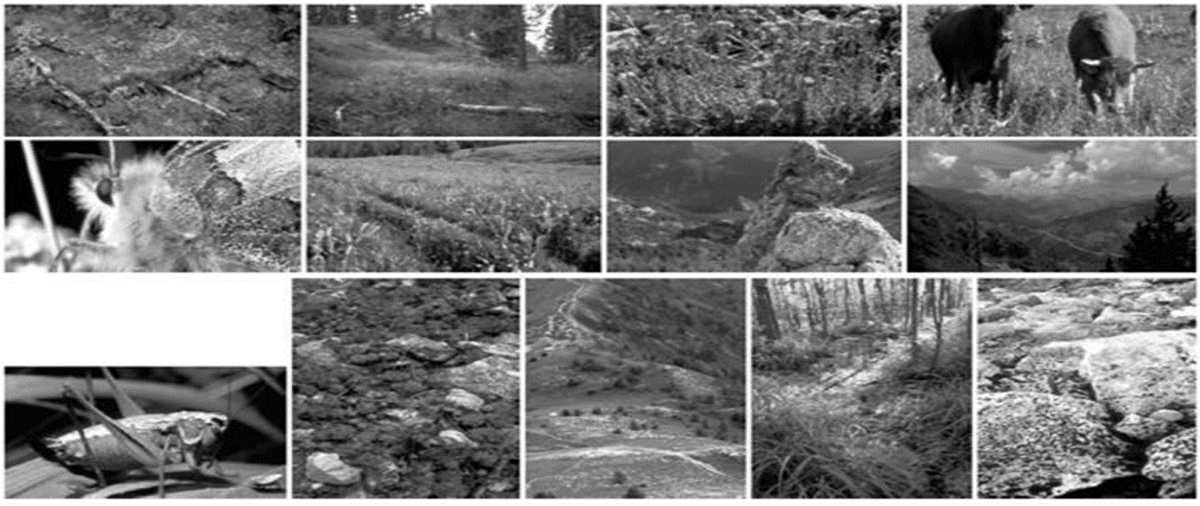

Figure III.5 : Les 13 images naturelles utilisées pour l'apprentissage des filtres dans le descripteur BSIF.

$$r_{i=} \sum \varphi_i^{N\times N}(x,y)\, I\,(x,y) \text{.....(III.9).}$$

Où $\varphi_i N \times N$ est un filtre linéaire de taille N et i = {1, 2… n} indique le nombre de filtres statistiquement indépendants dont la réponse peut être calculée ensemble et binarisée pour obtenir la chaîne binaire comme suit :

$$b_i = \begin{cases} 1 & si \ r_i > 0 \\ 0 & si \ r_i \leq 0 \end{cases} \quad \text{.....(III.10).}$$

Enfin, les fonctions BSIF sont extraies comme l'histogramme des codes binaires de chaque pixel. BSIF caractérise efficacement les composants de texture de l'image. Il existe deux facteurs importants dans le descripteur BSIF: la taille du filtre N et n la longueur du filtre. L'image et l'image filtrée par BSIF correspondantes sont représentées sur la Figure (III.6). La Figure (III.6.a) indiqué un exemple d'image FKP. La Figure (III.6. b) représente le filtre BSIF de taille 11x11 et de longueur 12. La Figure (III.6.c) montre les résultats de la convolution de l'image FKP avec un filtre BSIF. La Figure (III.6.d) montre image filtrée par BSIF filtre **[53].**

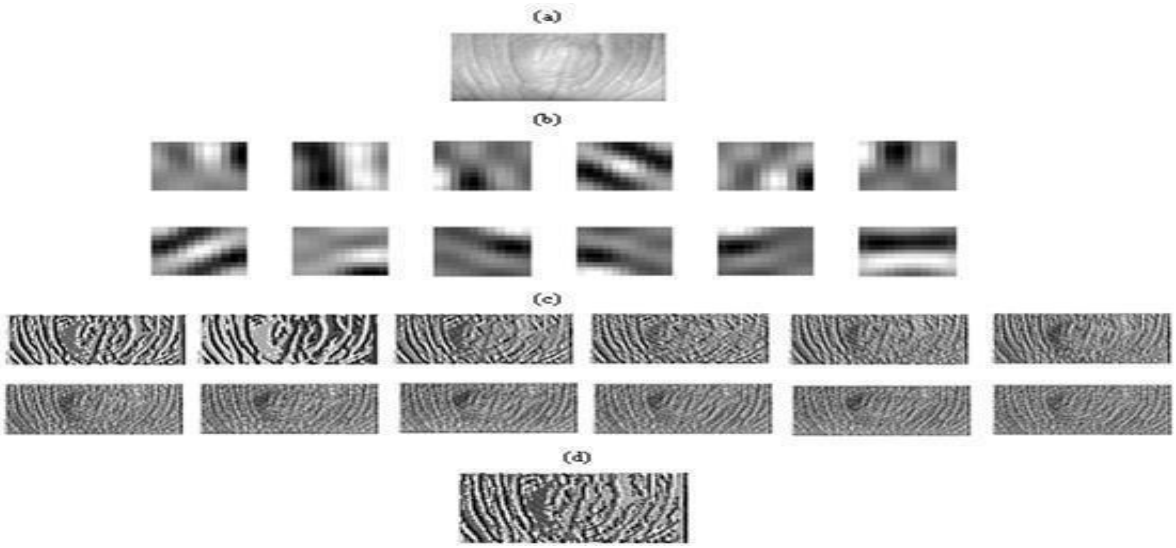

Figure III.6: (a) Exemple d'image FKP. (b) Filtre BSIF de taille 11x11 et de longueur 12. (c) Les résultats de la convolution de l'image FKP avec un filtre BSIF. (d) Image finale FKP filtrée par BSIF filtre.

III.8.3 - Les ondelettes de Gabor :

Hegde et al ont proposé un système d'authentification basé sur l'image FKP d'une personne en utilisant l'ondelette de Gabor. Dans la technique proposée, ils ont appliqué la transformée en ondelettes de Gabor sur l'image FKP prétraitée. Ensuite, ils ont tracé un graphe d'ondelette de Gabor et des points pics ont été identifiés. L'algorithme proposé est simulé sur la base de données PolyU FKP.

Avoir la base de données d'images FKP de tous les membres d'une organisation consomme plus d'espace et la complexité du système augmente. Ainsi, ils ont proposé d'avoir le numéro d'identification d'utilisateur (UID) pour chaque personne.

Les caractéristiques de l'image FKP comme le nombre de pics dans le diagramme en ondelettes de Gabor et les distances successives entre ces pics sont stockées dans la base de données correspondant à un UID particulier. Lors de l'authentification, la personne doit fournir son UID et son image FKP est capturée. Si les caractéristiques de la nouvelle image conviennent aux caractéristiques correspondantes dans la base de données, la personne peut être authentifiée.

Dans un premier temps, un prétraitement est effectué. L'image acquise en RVB est convertie en niveaux de gris. Ensuite, la région d'intérêt (ROI) est extraite de l'image FKP. Les bords sont détectés par recherche de maxima locaux du gradient de l'image. Le gradient est calculé en utilisant la dérivée d'un filtre gaussien.

Le procédé utilise deux seuils pour détecter les bords forts et faibles, et inclut les bords faibles dans la sortie si elles sont reliées à des bords forts. Ensuite des filtres de rang sont utilisés, dont la réponse est basée sur la commande (classement) des pixels contenus dans la zone d'image englobées par le filtre. La réponse du filtre à un point quelconque est alors déterminée par le résultat de classement. L'algorithme actuel utilise le filtre médian.

L'Ouverture morphologique est appliquée pour lisser le contour des bords et éliminer des protubérances minces. L'image est ensuite dilatée pour élargir les bords obtenus. Ensuite, nous appliquons la transformée en ondelettes de Gabor sur l'image obtenue après traitement préalable. L'ondelette de Gabor est une onde plane complexe limitée par une enveloppe gaussienne bidimensionnelle. L'ondelette de Gabor contient deux composants à savoir réel et imaginaire. En dehors de l'échelle et l'orientation, la seule chose qui diffère deux ondelettes de Gabor est le rapport entre la longueur d'onde et la largeur de l'enveloppe gaussienne. Chaque ondelette de Gabor a une certaine longueur d'onde et une orientation, et peut être convoluée avec une image pour estimer l'amplitude des fréquences locales de cette longueur d'onde approchée et l'orientation dans l'image.

Pour authentifier la personne en question, nous comparons tout d'abord le nombre de points pics dans le graphe d'ondelettes de Gabor et celui dans la base de données pour un UID donné. S'ils ne correspondent pas à la valeur du seuil prédéfinie, la personne est refusée. Dans le cas contraire, les distances entre les sommets successifs stockées dans la base de données et celles de cette nouvelle image sont comparées. Chaque similarité pour un seuil donné est considérée comme le nombre de succès et une non-similarité comme un échec. La probabilité de succès est alors calculée. Si la probabilité calculée est supérieure à 0.60, la personne peut être acceptée. Sinon, elle sera rejetée **[23].**

III.9 - Appariement et classification :

L'appariement des distances est effectué à l'aide de métriques de distance, qui constituent un élément clé de plusieurs algorithmes d'apprentissage automatique. Ces métriques de distance, telles que la distance Euclidienne, Manhattan, Minkowski et Hamming, sont utilisées

dans l'apprentissage supervisé et non supervisé, principalement pour mesurer la similarité entre des points de données.

Une métrique de distance efficace améliore la performance de notre modèle d'apprentissage automatique, que ce soit pour des tâches de classification telles que les plus proches voisins (Nearest Neighbors), les machines à vecteurs de support (SVM), les réseaux de neurones artificie, les k-plus proches voisins (k-NN) **[35].**

III.9.1 - Algorithme du K-voisin le plus proche (KNN) :

L'algorithme K-Nearest Neighbour ou algorithme du K-voisin le plus proche est une méthode d'apprentissage supervisé non paramétrique qui a été développée pour la première fois en 1951 par Joseph Hodges et Evelyn Fix, et qui a ensuite été développée par Thomas Cover.

L'algorithme KNN est utilisé pour résoudre les problèmes de classification et de régression. Il calcule les distances entre une requête et tous les exemples des données, sélectionne le nombre spécifié d'exemples (K) les plus proches de la requête, puis vote pour l'étiquette la plus fréquente ou fait la moyenne des étiquettes dans le cas de la classification ou dans le cas de la régression respectivement. Dans le cas de la classification et de la régression, le choix du bon K pour les données se fait en essayant plusieurs K différent, puis en choisissant celui qui fonctionne le mieux en fonction de nos besoins **[48].**

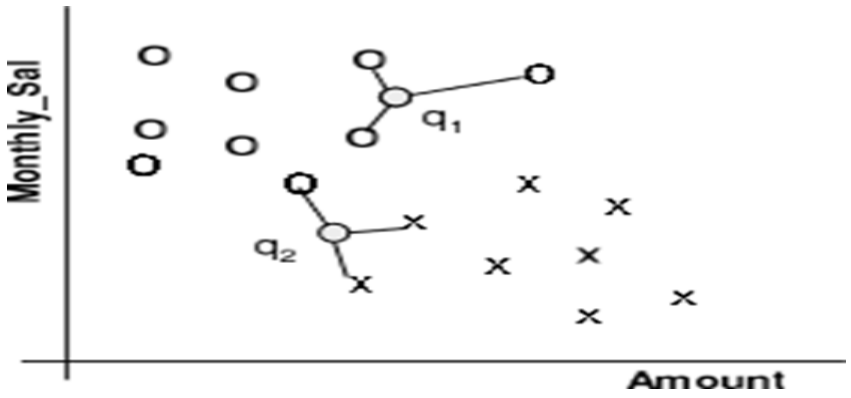

Figure III.7 : Un exemple simple de classification par 3 plus proches voisins

K-NN st l'un des plus simples algorithmes du ML basé sur une technique d'apprentissage supervisé.

Proposé par [Fix and Hodges, 1951], puis modifié par [Cortes and Vapnik, 1995], le K-NN est utilisé aussi bien pour la régression que pour la classification, mais il est surtout utilisé pour les problèmes de classification.

Dans le NN chaque échantillon est affecté à la classe de son plus proche voisin, ou à la classe la plus commune parmi ses *k* plus proches voisins dans la variante K-NN. Le NN pur est utilisé lorsque $K = 1$, mais souvent $K > 1$ où un vote majoritaire a lieu. L'algorithme utilise la distance euclidienne entre un échantillon de test x_i et un échantillon d'apprentissage y_i **[49] :**

$$D(x_i, y_i) = \|xi - yi\|_2^2 \quad \text{..... (III.11).}$$

III.9.2 - Machine à vecteurs de support (SVM) :

Les machines à vecteurs de support (SVM, ou réseaux de vecteurs de support) sont des modèles d'apprentissage supervisé avec des algorithmes d'apprentissage associés qui analysent les données utilisées pour la classification et l'analyse de régression. Étant donné un ensemble d'exemples d'apprentissage, chacun marqué comme appartenant à l'une ou l'autre de deux catégories, un algorithme d'apprentissage SVM construit un modèle qui affecte les nouveaux exemples à l'une ou l'autre catégorie, ce qui en fait un classificateur linéaire binaire non probabiliste.

Un modèle SVM est une représentation des exemples sous forme de points dans l'espace, cartographiés de manière à ce que les exemples des différentes catégories soient divisés par un espace clair aussi large que possible. Les nouveaux exemples sont ensuite cartographiés dans ce même espace et leur appartenance à une catégorie est prédite en fonction du côté de l'écart où ils se situent **[48].**

Le SVM est l'un des algorithmes les plus populaires de la littérature sur l'apprentissage supervisé [Cortes and Vapnik, 1995].
Étant donné un ensemble de données de classification binaire.

$$(xi\ yi) \quad i = 1. . . \ N, \text{ ou } \quad xi \in R^n \text{..... (III.12).}$$

R^n est le vecteur de caractéristiques représentant le $i^{ième}$ exemple d'apprentissage et $y^{(i)} \in \{-1, 1\}$ est l'étiquette de classe correspondant au $i^{ième}$ exemple d'apprentissage. L'algorithme SVM trouve les paramètres (w, b) de l'hyperplan de séparation linéaire à marge optimale comme l'indique la figure (III.6) **[49].**

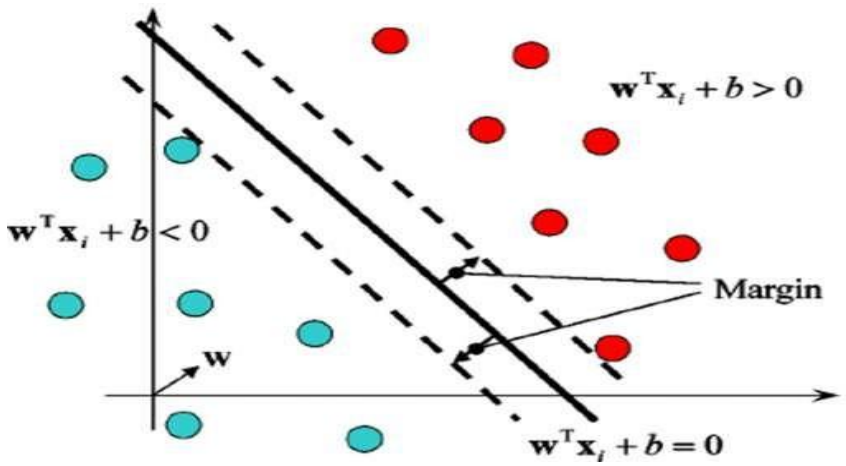

Figure III.8 : Marge optimale de l'hyperplan de séparation linéaire

III. 10 - La décision :

C’est l’étape qui fait la différence entre un système d’identification d’individus et un autre de vérification. Dans cette étape, un système d’identification consiste à trouver le modèle qui correspond le mieux au FKP pris en entrée à partir de ceux stockés dans la base de données, il est caractérisé par son taux de reconnaissance. Par contre, dans un système de vérification il s’agit de décider si FKP en entrée est bien celui de l’individu (modèle) proclamé ou il s’agit d’un imposteur, il est caractérisé par son EER (equal error rate) **[42].**

III.11 - CONCLUSION :

L’empreinte digitale FKP (Finger-Knuckle Print) représente une avancée significative dans le domaine de la biométrie. Elle offre une méthode d'identification unique, fiable et sécurisée, basée sur les caractéristiques distinctives des plis des articulations des doigts. Grâce à sa robustesse et à sa précision, cette technologie trouve des applications variées, notamment dans les systèmes de sécurité, les dispositifs de contrôle d'accès et l'identification personnelle. Avec le développement rapide des technologies biométriques, l'empreinte FKP pourrait jouer un rôle essentiel dans l'avenir des solutions d'identification numérique.

CHAPITRE IV

RÉSULTATS EXPÉRIMENTAUX ET DISCUSSIONS

IV.1 - Introduction :

Ce chapitre regroupe les résultats expérimentaux de la reconnaissance des images FKP et puis l'identification des personnes, faites avec les algorithmes LPQ et BSIF sur la base de données qui contient plusieurs images des empreintes de plusieurs personnes.

Donc sur cela, on voit que notre travail consiste à concevoir un système d'identification biométrique des individus par la reconnaissance FKP en se basant sur LPQ et BSIF. qui sont essentiellement utilisées pour extraire les caractéristiques des images.

IIV.2. Environnement matériel :

Afin de mener à bien ce projet, il a été mis à notre disposition un ensemble de matériels dont les caractéristiques sont les suivantes :

- Un ordinateur DELL- 2170p avec les caractéristiques suivantes :
- Processeur: Intel® core (TM) i5- 4210U CPU @ 3.10Ghz 1.70 GHz
- RAM : 8.00 Go de RAM.
- Disque Dur : SSD 256 GB.
- OS: Microsoft Windows 13 64 bits.

IV.3 - Outils de développement :

Nous avons eu recours lors de l'élaboration de notre système au logiciel Matlab R2021b que nous présenterons ci-dessous.

MATLAB (MATrix LABoratory) est un environnement de calcul numérique et un langage de programmation développé par MathWorks. Il est largement utilisé pour des tâches telles que l'analyse de données, le développement d'algorithmes, la création de modèles, et la simulation. MATLAB se distingue par sa capacité à manipuler facilement des matrices, son vaste ensemble de fonctions mathématiques et son interface conviviale pour la visualisation de données. Il est couramment employé dans des domaines tels que l'ingénierie, la finance, la recherche scientifique, et l'enseignement.

IV .4 - Les bases de données :

IV.4.1 - Base de Données IIT Delhi Finger Knuckle :

Cette base de données a été constituée en capturant la région dorsale des articulations des doigts à l'aide d'une caméra numérique à basse résolution, et ce, sans contact physique. Elle contient des images d'articulations digitales collectées auprès de 158 utilisateurs âgés de 16 à 55 ans. Au total, la base de données comprend 790 images d'articu-

lations digitales. Ces images sont numérotées de manière séquentielle à l'aide d'un identifiant entier propre à chaque utilisateur. Étant donné que l'ensemble de la région dorsale du doigt a été capturé, la région d'intérêt (ROI) correspondant à la phalange proximale est extraite à l'aide d'algorithmes de détection de bords et de lignes **[52].**

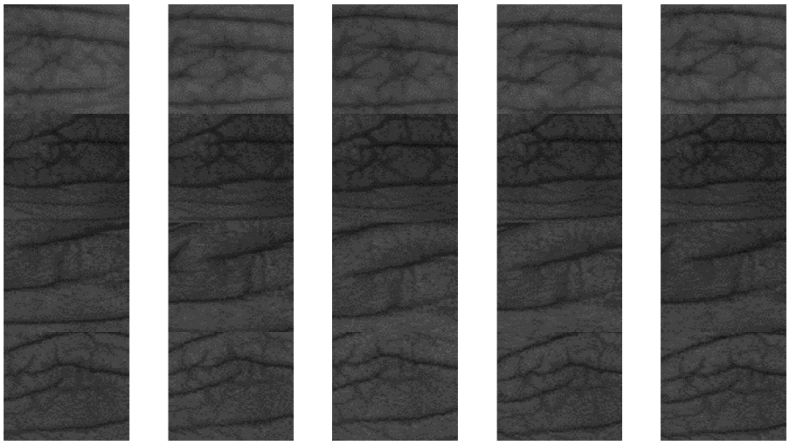

Figure IV.1 : Échantillon provenant de la base de données des articulations des doigts de L'IIT Delhi.

IV .4.2 - Base de Données PolyU Finger Knuckle Print (ROI) :

Dans cette base de données PolyU Finger Knuckle Print, des images d'articulations des doigts ont été collectées auprès de 165 individus, comprenant 125 hommes et 40 femmes, à l'aide d'une caméra automatisée à basse résolution dans un environnement sans guide physique pour les doigts.

Ce système de capture d'images des articulations digitales recueille les données en deux sessions distinctes. Lors de chaque session, chaque participant soumet six images de quatre surfaces articulaires différentes de ses doigts. Ces images concernent les articulations de l'index gauche, du majeur gauche, de l'index droit et du majeur droit. Ainsi, 24 images sont collectées par personne et par session, ce qui porte à 48 le nombre total d'images soumises par individu au cours des deux sessions.

La base de données comprend au total 7920 images, correspondant à 660 surfaces articulaires digitales différentes. L'intervalle moyen entre les deux sessions de capture est d'environ 25 jours. Cette base de données fournit également des images de la région d'intérêt (ROI) extraites des images initiales, en construisant un système de coordonnées propre à chaque image FKP (Finger Knuckle Print). Ces sous-images de la ROI contiennent les caractéristiques les plus saillantes, idéales pour l'authentification personnelle **[51].**

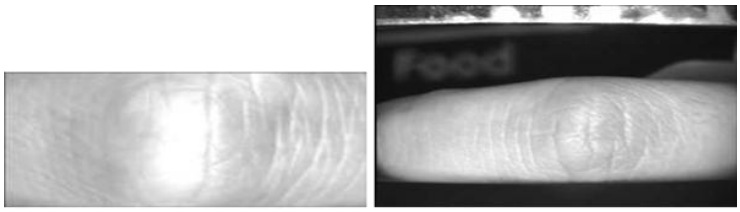

Figure IV .2 : Deux échantillons biométriques des ensembles de données Poly U FKP

IV.5 - Protocole de test :

L'identification par l'empreinte FKP est une procédure de comparaison un contre plusieurs pour identifier une image FKP de test.

- **Base de Données IIT Delhi Finger Knuckle :**

Les 10 images de l'empreinte FKP sont divisées en deux groupes

✓ Images d'apprentissages : Les 04 premières images de chaque personne servent pour la phase d'apprentissage.

✓ Images de Tests : Les 06 restantes images de chaque individu servent pour la réalisation des différents tests (phase de test).

- **Base de Données PolyU Finger Knuckle Print (ROI) :**

Les 12 images de l'empreinte FKP sont divisées en deux groupes :

✓ Images d'apprentissages : Les 04 premières images de chaque personne servent pour la phase d'apprentissage.

✓ Images de Tests : Les 08 restantes images de chaque individu servent pour la réalisation des différents tests (phase de test).

IV.6 - Présentation du système :

Cette section présente notre système de reconnaissance basé sur l'FKP qui est conçu en base sur la fonction LPQ, BSIF au niveau de la phase d'extraction des paramètres.

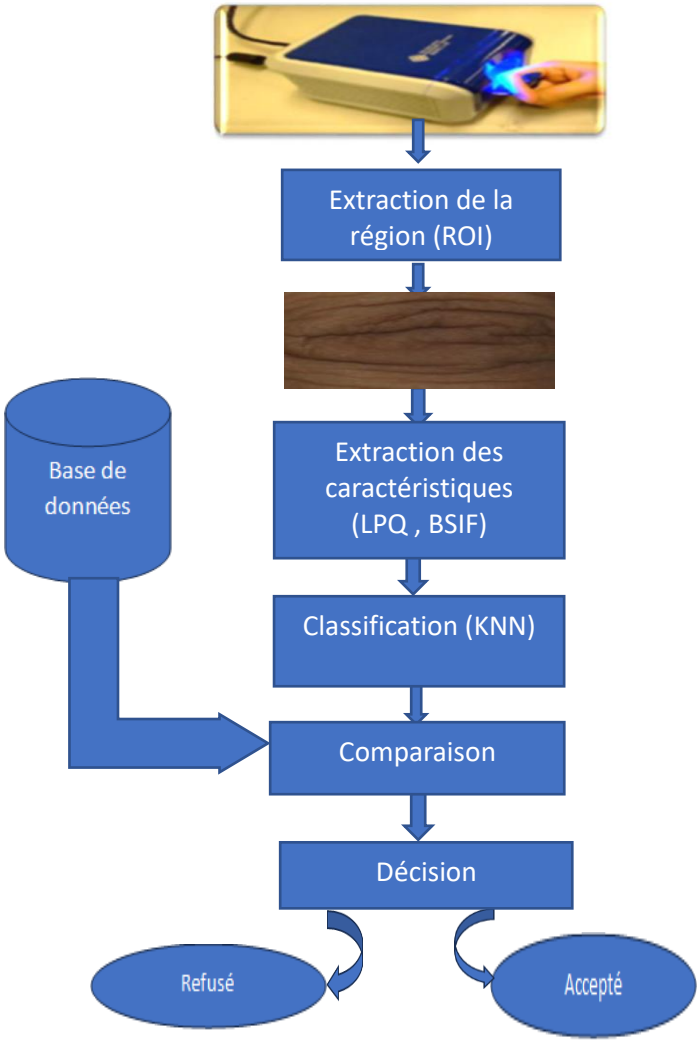

Figure IV.3 : Schéma proposé du système de reconnaissance de FKP

IV .7 - Taux de reconnaissance :

Le taux de reconnaissance permet d'évaluer la qualité de l'algorithme par rapport au problème pour lequel il a été conçu. Cet algorithme a été évalué grâce à une base de test qui contient des formes décrites dans le même espace de représentation que celles utilisées pour l'apprentissage. Elles sont aussi étiquetées par leur classe réelle d'appartenance afin de pouvoir vérifier les réponses du classifieur.

En général, quand les échantillons étiquetés à disposition sont suffisamment nombreux, ils sont séparés en deux parties disjointes et en respectant les propositions par classes de la base initiale. Une partie sert pour former la base d'apprentissage et l'autre pour former la base de test. Le découpage le plus courant est de 1/2 pour l'apprentissage et le 1/2 restant pour la base de test.

Les performances en termes de taux de reconnaissance sont alors déterminées en présentant au classifieur chacun des exemples de la base de test et en comparant la classe donnée en résultat à la vraie classe **[1].**
Le Taux de Reconnaissance Totale (TR) est simplement défini par :

$$\mathbf{TR(\%)} = \frac{\textbf{Nombre d'empreinte bien classé}}{\textbf{Nombre total d'empreinte de test}} \quad \text{.....(IV.13).}$$

IV.8 - Résultats expérimentaux et discussion :

Dans cette partie nous allons expliquer les différentes expérimentations effectuées pour évaluer la performance des méthodes que nous proposons. Avant cela, nous allons expliquer les différentes bases de données utilisées dans le travail actuel.

Pour obtenir les résultats des tests, chaque vecteur de l'image de test a été comparé avec tous les vecteurs dans la base des références. Si les deux vecteurs sont de la même classe (même personne), la mise en correspondance entre eux serait comptée comme un client, sinon il aurait considéré comme un imposteur, l'objectif est d'évaluer le taux de reconnaissance de l'algorithme utilise, en suivant un protocole de test se base sur la mesure du taux de reconnaissance.

IV.8.1- Performance de la Base de données IIT Delhi Finger Knuckle :

- **Les résultats pour diffèrent taille d'image de FKP avec la méthode LPQ** :

La méthode LPQ est basée sur quatres paramètres importants : la taille de fenêtre (windows size), le nombre des blocs et le nombre des filtres. Pour cela, des tests empiriques ont été exécutés afin d'en choisir les meilleurs paramètres de cette méthode. Dans le tableau suivant, nous avons mis les résultats de cette expérience en calculent à chaque fois erreur (EER) des différentes empreintes (FTP) des mains droite et gauche.

Tableau IV.1 : Résultat du taux de reconnaissance de la base de données IIT Delhi Finger Knuckle par la méthode LPQ :

filtre / image	3×3	5×5	7×7	9×9	11×11
96×64	**88.10**	99.66	99.83	**100**	**100**
64×64	90.15	**100**	**100**	**100**	**100**
32×32	99.15	**100**	**100**	**100**	**100**

Une augmentation remarquable du taux de vérification est observée, passant de 88,10 % à 100% quand on a diminué la taille de l'image et on augmente la taille de filtre. Il convient également de noter que le descripteur LPQ offre les performances les plus élevées dans les grandes tailles des filtres

- **Les résultats obtenus avec BSIF :**

Dans cette expérimentation, nous avons appliqué la méthode BSIF, nous avons utilisé respectivement 4 échantillons pour l'entraînement et 6 échantillons pour le test.

Le tableau IV.2, présente les performances du système utilisant par défirent filtre avec le descripteur BSIF, évaluées sur la base de données IIT Delhi Finger Knuckle Les métriques de performance incluent le taux de vérification et le taux d'identification.

Tableau IV.2 : Résultat du taux de reconnaissance de la base de données IIT Delhi Finger Knuckle par la méthode BSIF :

Filtre / Nombre De bits	3×3	5×5	7×7	9×9	11×11	13×13	15×15	17×17
5 bits	95.75	97.79	99.15	98.98	98.98	99.15	99.15	99.32
6 bits	91.16	98.98	99.66	**100**	99.83	99.83	99.66	**100**
7 bits	97.96	99.83	99.83	**100**	**100**	**100**	**100**	**100**
8 bits	98.94	99.83	**100**	**100**	**100**	**100**	**100**	**100**
9 bits	/	99.15	100	99.83	99.83	100	100	100
10 bits	/	98.47	99.66	100	99.83	100	99.83	100
11 bits	/	89.46	99.66	99.83	100	99.32	100	99.83
12 bits	/	**50.34**	87.59	84.01	96.77	99.83	100	99.83

Les résultats présentés dans le Tableau IV.2 montrent que les meilleurs taux de reconnaissance sont obtenus avec des tailles de filtre allant de **9×9 à 17×17** et un nombre de bits compris entre **7 et 9**. En particulier, l'utilisation de **7 ou 8 bits** combinée à des

filtres de taille moyenne à grande permet d'atteindre des performances optimales, souvent **égales à 100 %**. À l'inverse, une augmentation excessive du nombre de bits (notamment **11 ou 12 bits**) entraîne une dégradation notable des performances, surtout lorsque la taille du filtre est faible. Cela suggère qu'un **compromis optimal** entre la complexité du codage (nombre de bits) et la richesse de l'information capturée (taille du filtre) es e PolyU FKP.

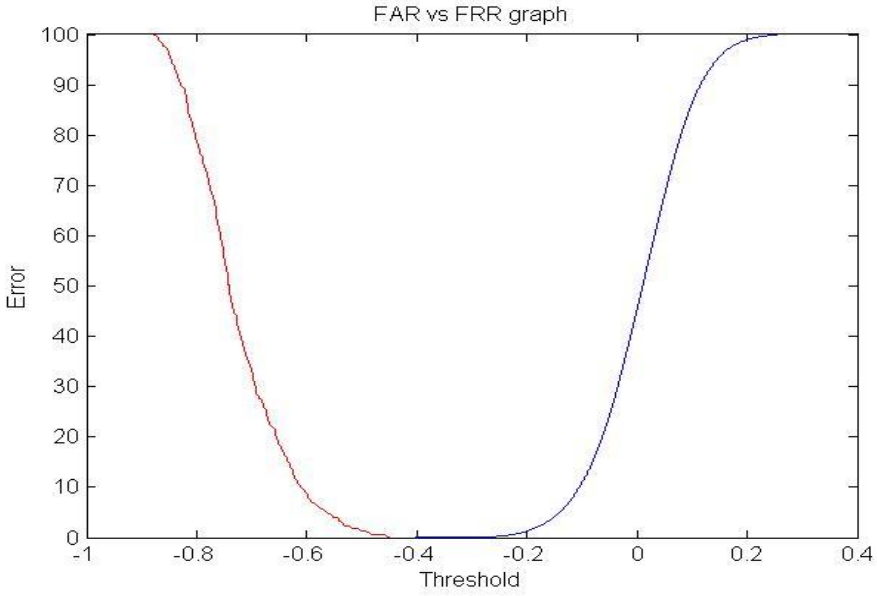

Figure IV .4 : illustre FRR et FAR avec descripteur LPQ.

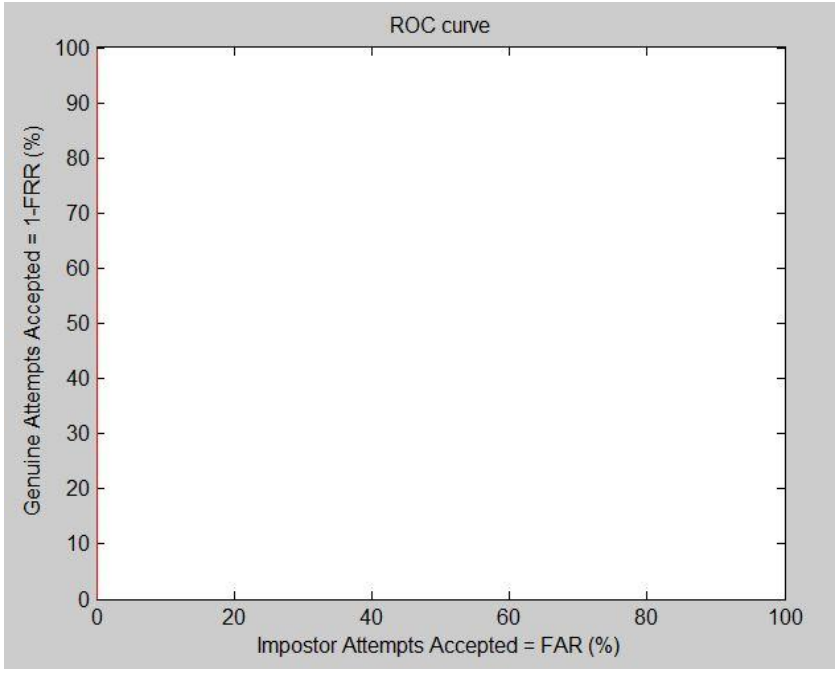

Figure IV .5 : courbe ROC

IV.8.2- Performance de la base de données PolyU Finger Knuckle Print (ROI) :

- **Les résultats obtenus avec BSIF :**

Dans cette expérimentation, nous avons appliqué la méthode BSIF, nous avons utilisé respectivement 4 échantillons pour l'entraînement et 8 échantillons pour le test.

Tableau IV.3 : Résultat du taux de reconnaissance de la base de Données PolyU Finger Knuckle Print (ROI) par la méthode BSIF :

Filtre / Nombre De bits	3×3	5×5	7×7	9×9	11×11	13×13	15×15	17×17
5 bits	93.41	94.68	95.19	94.76	94.93	94.34	93.58	92.99
6 bits	95.78	96.88	97.89	97.72	97.80	97.47	96.11	95.86
7 bits	96.45	98.31	97.89	98.73	98.48	97.89	97.64	97.38
8 bits	97.38	98.48	98.65	98.73	**98.99**	98.40	98.48	97.97
9 bits	/	97.13	97.72	98.73	98.40	98.40	97.97	97.97
10 bits	/	95.35	96.79	96.79	96.79	96.54	96.79	96.45
11 bits	/	91.89	95.35	95.61	95.69	96.45	95.02	94.09
12 bits	/	**80.74**	89.70	93.75	94.43	94.17	90.88	88.94

On observe une amélioration progressive des taux de reconnaissance avec l'augmentation du nombre de bits, atteignant des performances optimales autour de **8 et 9 bits**. Le meilleur taux de reconnaissance, soit **98,99 %**, est obtenu avec un filtre de taille **11×11** et **8 bits**, ce qui indique que ce paramétrage permet une extraction efficace des caractéristiques discriminantes.

Au-delà de 9 bits, les performances commencent à diminuer, en particulier à partir de 11 et 12 bits, suggérant qu'un excès d'informations peut introduire du bruit ou de la redondance, nuisant ainsi à l'efficacité du système. Par ailleurs, les filtres de taille moyenne à grande (notamment de 7×7 à 13×13) montrent globalement de meilleurs résultats par rapport aux filtres plus petits.

Les résultats obtenus dans l'expérimentation avec LPQ:

Dans cette expérimentation, nous avons appliqué la méthode LPQ. Et on a utilisé le nombre de train 4 et le nombre de teste 8.

Pour augmenter les paramètres on a divisé l'image originale on sous images (sub - image) comme la figure IV.6 M'entre après on extraire les paramètres pour chaque sous image et on concaténé ces vecteurs sur un seul vecteur.

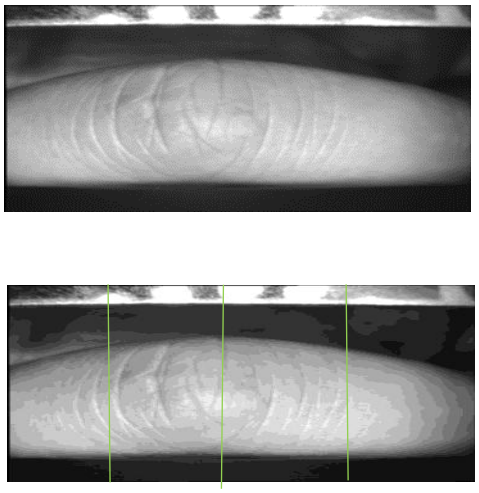

Figure IV .6 : la méthode de division de l'image on sous-images.

Tableau IV.4 : Résultat du taux de reconnaissance de la base de donne polyU FKP(ROI) avec LPQ :

Filtre / Image	**3×3**	**9×9**	**11×11**	**13×13**	**15×15**
220×110	97.97	98.23	**98.82**	98.48	98.40

On constate que les valeurs varient légèrement selon le filtre utilisé. Par exemple, le filtre **11** donne les résultats les plus élevés (**98,82**), ce qui peut indiquer qu'il préserve mieux certaines caractéristiques de l'image. En revanche, le filtre **9** semble donner la valeur la plus basse (**23**), ce qui pourrait signifier une perte d'information ou une mauvaise performance selon le critère mesuré.

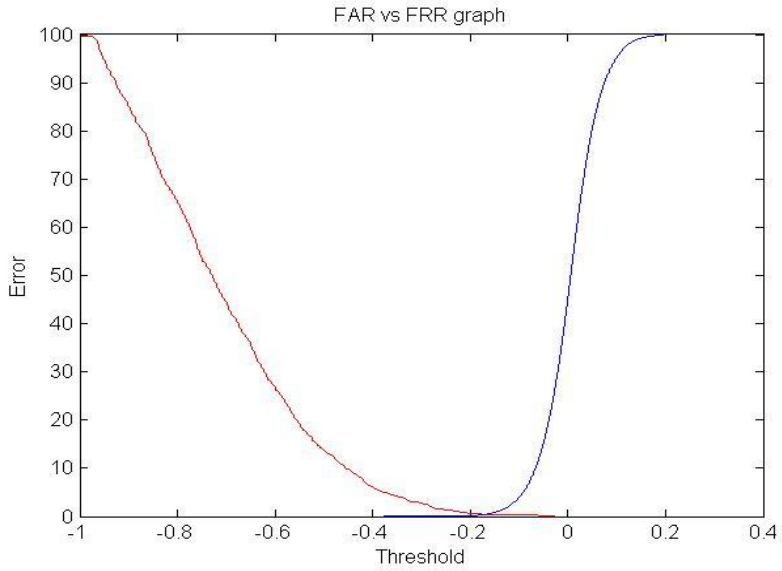

Figure IV .7 : illustre FRR et FAR avec descripteur LPQ.

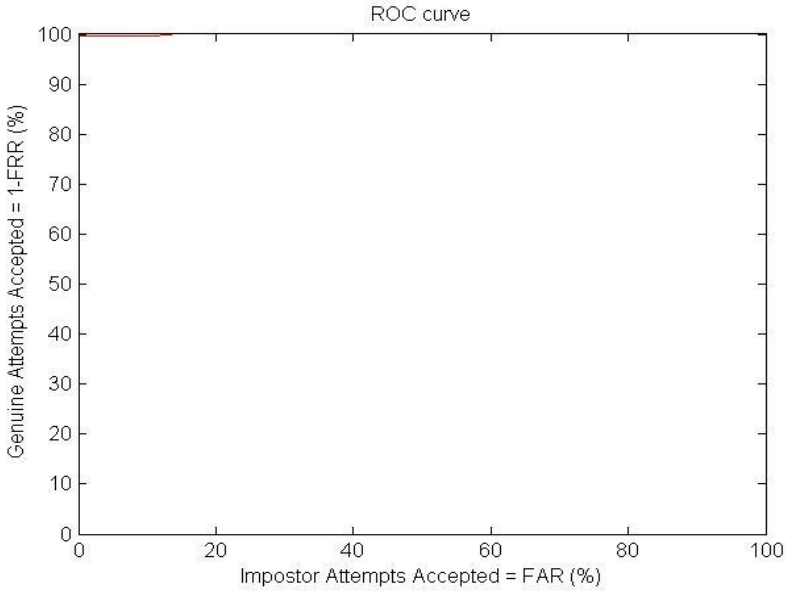

Figure IV .8 : courbe ROC.

IV.8.3 – Comparaison :

Nous avons comparé notre résultat utilisant le descripteur LPQ et BSIF avec ceux des autres méthodes proposées par différentes études. Les résultats obtenus sont présentés dans le tableau suivant :

Tableau IV.5 : Etude comparative de l'approche proposée avec des méthodes récentes sur la base de données PolyU-FKP.

Références	Extraction de caractéristiques	Base de donne	Taux de reconnaissance
Shehu Ha-midu - 2023	AlexNet BSIF and PCA.	PolyU Knuckle V1	Multimodal : 100% Unimodal : 98.25%
A. Attia, Z. Akhtar, and Y. Chahir - 2021	BSIF .PCA+LDA.	PolyU Knuckle V1	Multimodal : 99.60% Unimodal : 95.43%
S. Trabelsi et al – 2020	Convolutional Neural Network (CNN).	PolyU-FKP	Multimodal : 100% Unimodal : 99.93%
[1] – 2020	LPK RI-LPQ	PolyU-FKP	96.75% 98.25%
Attia et al.2022	PCANet+SVM	PolyU-FKP	98%
Gao et al - 2024	CNN multi-echelle+textures 1er et 2em ordre.	PolyU-FKP	99.60%
Système Proposé	LPQ BSIF BSIF LPQ	polyU FKP (ROI) polyU FKP(ROI) IIT Delhi Finger Knuckle IIT Delhi Finger Knuckle	Unimodal: 98.40% Unimodal: 98.99% Unimodal: 100% Unimodal : 100%

Le Tableau IV.4 présente une comparaison des approches de reconnaissance biométrique basées sur les empreintes des articulations. Les méthodes combinant des techniques d'extraction de caractéristiques comme **BSIF**, **LPQ**, **PCA**, et les réseaux de neurones (**CNN**) ont obtenu des taux de reconnaissance très élevés, notamment en mode multimodal.

Le système proposé atteint un taux de reconnaissance de **100 %**, démontrant son efficacité et sa supériorité par rapport aux approches précédentes. L'étude met en évidence l'importance du choix des descripteurs et de la stratégie de fusion dans la performance globale du système.

IV.9 – Conclusion :

Dans ce chapitre nous avons présenté notre système global de reconnaissance par l'empreinte des articulations des doigts FKP basée sur les algorithmes LPQ et BSIF, on a présenté aussi les différents résultats obtenus pour chaque algorithme.

Notre système de reconnaissance par l'empreinte des articulations des doigts FKP, est appliquée sur les bases de donné de polyU FKP(ROI) et la base de données IIT Delhi Finger Knuckle Pour conclure, Nous pouvons noter que les expérimentations ont montré que la méthode de reconnaissance FKP base sur la méthode LPQ est la plus efficace que la méthode BSIF. Cependant, nous avons également vu que de nombreux facteurs extérieurs influent sur la qualité de la reconnaissance.

CONCLUSION GÉNÉRALE

Conclusion Générale

La reconnaissance biométrique et l'identification des personnes basées sur l'utilisation de ses caractéristiques physiques ou comportementales ou biologies.

Parmi les modalités les plus utilisées dans la reconnaissance biométrique est l'empreinte FKP par ce qu'elle est permanente et unique. Les chercheurs essayent toujours de développer les systèmes de reconnaissance à travers des outils mathématiques habituellement complexes pour faire la discrimination entre les individus.

L'objectif suivis dans ce mémoire propose une démarche qui consiste à améliorer la performance de l'identification biométriques via l'empreinte FKP par plusieurs méthodes avec un ensemble d'opérations. 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 pour notre problème. Suivant les résultats obtenus, nous avons opté pour le choix des méthodes LPQ et BSIF.

Enfin, le système proposé est appliqué sur les bases de données connues dans le domaine des empreintes polyU FKP (ROI) et la base de donneé IIT Delhi Finger Knuckle et les résultats obtenus, sont intéressants. En effet on est arrivé à un taux de reconnaissance acceptable. Ce taux est intéressant ce qui rend notre système fiable où il répond bien à l'objectif que nous nous sommes fixés au départ, à savoir la mise en œuvre d'un système permettant la reconnaissance d'individus.

Comme travail futur, nous proposons de concentrée sur l'évaluation de la performance dans les deux phases (vérification et identification) en utilisant une base de données de grande taille et de l'intégration d'autres traits biométriques pour obtenir les performances du système avec une grande précision.

BIBLIOGRAPHIES

Bibliographies

[1] REZZOUG Balkis BASSIMANE Rayane, &SLAOUI Abderrahim Mémoire Master Académique Thème « Identification des individus par l'empreinte de l'articulation de doigt (FKP) » 2019/2020.

[2] BENCHENNANE Ibtissam « Etude et mise au point d'un procédé biométrique multimodale pour la reconnaissance des individus » THÈSE En vue de l'obtention du Diplôme de Doctorat, Université des Sciences et de la Technologie d'Oran Mohamed Boudiaf.

[3] CHARGHI Fatima Zohra Thème de Doctorat en sciences en Electronique « Fusion de Techniques Biométriques pour une amélioration de reconnaissance de personnes » 11/06/2023.

[4] HALIMI Abir, SEDDIKI Amel. « Système Biométrique pour la Reconnaissance des Articulations des Doigts et la Méthode de Quantification de phase Local ». UNIVERSITÉ KASDI MERBAH OUARGLA 2019/2020.

[5] CHIHEB Amira https://www.memoire online.com/02/13/6979/Reconnaissance-de-Visages-par-Analyse-Discriminante-Linéaire LDA. Université du 8 mai 45 de Guelma.Algérie - Licence en informatique /2003. Academia.

[6] S.Boudjallel « Détection et Identification de personne par méthode biométrique » Mémoire de Magister en Electronique, Université de Tizi-Ouzou / 2014.

[7] T.Hafs « Reconnaissance Biométrique Multimodale basée sur la fusion en score de deux Modalité », Mémoire de Doctorat en Electronique, Université de Annaba /2016.

[8] Arun A.Ross, Karthik Nandakumar, Anil K. Jain « Handbook of Multibiometric » /2006.

[9] A.Benagga, L. Telbi « Reconnaissance des personnes basée sur l'empreintes de L'articulation de doigt » Mémoire de Master, Université KASDI Merbah Ouargla, 2016.

[10] BERREDJEM Achref « reconnaissance des individus par leur empreinte des Articulations des doigts » Université 08 Mai 1945-Guelma /2019.

[11] SADALAH Khedija « identifation biométrique des personnes par les empreintes palmaires » UNIVERSITE ANNABA /2019.

[12] KABBARA Yeihya « caractérisation des images a Rayon-X de la main par des modèles mathématiques : application à la biométrie » thèse de doctorat université paris-Est Université libanaise.

[13] ADJAINE Elmechri, BENSLIMAN Abdelkarim « Authentification et Identification Biométrique des personnes par les empreintes palmaires ». Université KASDI Merbah Ouargla, 2018/2019.

[14] BETTAYEB Nadjla. Razika BOUZAR « conception d'un système biométrique FKP ». ECOLE NATIONALE POLYTECHNIQUE /2013.

[15] A. Meraoumia « Modèle de Markov caché applique à la multi biométrie » USTHB / 2014.

[16] A. Ross and A. K. Jain « Information Fusion in Biometrics » Pattern Recognition Letters, Vol. 24, Issue 13, pp. 2115-2125 / 2003.

[17] K. Nanda kumar, A. Ross, and A. K. Jain « Biometric Fusion: Does Modeling Correlation Really Matter? » Proc. 3rd Int`l Conf. on Biometrics: Theory, Applications and Systems, Washington DC, Sept / 2009.

[18] S.Jidong, L.Xiaoming « Fusion of Radar and AIS Data » 7th International Conference on Processing-ICSP'04, Beijing, China, Vol.3, 2004, p p, 2604- 2607.

[19] ADEL SAOUD « Reconnaissance Biométrique par Fusion Multimodale de Visages » Université Mohamed Khider Biskra /2022.

[20] Julian Fièrrez - Aguilar, Javier Ortega-Garcia, Daniel Garcia-Romero, and Joaquin Gonzalez-Rodriguez « A comparative evaluation of fusion strategies for multimodal biometric varication » 4th International Conference on Audio-and Video-Based Biometric Person Authentication-AVBPA, Guildford, UK, Jun 2003.

[21] DEHACHE Ismahène & Labiba Souici-meslati « UNE APPROCHE MULTIMODALE POUR LÀ VERIFICATION BIOMETRIQUE » 2011.

[22] Lorène Allano « stratégies de fusion de scores et mesures de dépendance appliquées aux bases de personnes virtuelles » UNIVERSITE D'EVRY-VAL D'ESSONNE / 2009.

[23] BETTAYEB Nadjla, Razika BOUZAR « Conception d'un système biométrique FKP » ECOLE NATIONALE POLYTECHNIQUE / Juin 2013.

[24] BENMAZA Oussama et ABDESSEMED Salim « identification de perssononnes basée sur les articulations des doigts 3D » UNIVERSITE KASDI MERBAH OUAR-GLA. 2021/2022.

[25] BENOUAER Aichouche .TAHRINE Soumia « systéme biométrique basé sur les motifs locaux binaires orientés (LBP). UNIVERSITE KASDI MERBAH OUARGLA / 2016.

[26] BECHKI Amar. Maamri Omar. Thème « Identification des personnes par l'empreinte de l'articulation des doigts » UNIVERSITE KASDI MERBAH OUARGLA / 2022.

[27] NAIT ALI Amine, Régis Fournier « traitement du signal et de l'image pour la biométrie » LAVOISIER / 2012.

[28] https://www.abiova.fr/biométrie.

[29] CHRAIR Amina et LAROUI Fella Hayat (La biométrie de la main sans contact) Université Aboubakr Belkaïd – Tlemcen 2022 /2023.

[30] https://www.cite-sciences.fr/archives/francais/ala_cite/expositions/biometrie/nonvoyants/programme_details_6_3.htm.

[31] (https://www.biometrie-online.net/technologies/volume-de-la-main).

[32] Akmal Jahan Mohamed Abdul Cader « Finger Biometric System using Bispectral Invariants and Information FusionTechniques" Doctor of Philosophy Queensland University of Technology / 2019.

[33] https://hal.science/hal-03655718/file/attia_mtap_2022.pdf.

[34] https://123dok.net/article/etat-l-art-l-empreinte-articulations-doigts.z3d9x99y.

[35] Hasan Erbilen ≪ Finger Knuckle Patterns For Person Identification≫. Eastern Mediterranean University September /2022 Gazimağusa, North Cyprus.

[36] file : // C:/Users/Win-10/Downloads/Biometric_Recognition_of_Finger_Knuckle_Print_Base.pdf.

[37] https://hal.science/hal-03655718/file/attia_mtap_2022.pdf.

[38] Kumar et al, ≪L'analyse morphologique de la main≫ /2010.

[39] Helala Fouad ≪Identification des personnes par les empreintes digitales≫, Université Mohamed Khider de Biskra / 2018.

[40] Hasnaoui Nassim Aboubakr ≪ La reconnaissance automatique des empreintes digitales≫.

[41] Revett ≪La dynamique du mouvement est une modalité prometteuse pour la sécurité numérique ≫ / 2009.

[42] BETTAHAR Abdessettar SABER Fathi ≪Extraction des caractéristiques pour l'analyse biométrique d'un visage ≫ UNIVERSITE KASDI MERBAH OUARGLA.

[43] Mohamed Y. Bouhaddaoui, Christophe Rosenberger, Mohamed T. El-Allam , Julien Mahier, Baptiste Hemery, ≪ Performance Evaluation in Biometrics ≫ GREYC Laboratory ENSICAEN University- France.

[44] Geetika Aroraa , Avantika Singhb , Aditya Nigamb , Hari Mohan Pandeyc , Kamlesh Tiwaria aBirla≪ Finger-Knuckle-Print Database Indexing to Boost Identification≫ Institute of Technology and Science Pilani, Rajasthan, INDIA.

[45] Melle.Bouaka Halim .Mme. Bazzine Oum El kheir. ≪Estimation Automatique de L'âge des Patients à Partir des Images Faciales≫. UNIVERSITE KASDI MERBAH OUARGLA : 2018 /2019.

[46] NAAM RANIA et NAAM IMANE ≪ Finger knuckle print using ResNet 50 method Evaluation ≫ university kasdi Merbah OUARGLA /2021.

[47] Derawi, M. O, & Bours, P. « Biometric recognition with the full hand using 3D sensors ». In Handbook of Remote Biometrics (pp. 27–45). Springer / 2013.

https://doi.org/10.1007/978-1-4471-4402-5_2.

[48] BOUMAZZA Abdennour ≪ Identification des personnes par les empreintes palmaires ≫ Université du 8 mai 45 de Guelma.Algérie / 2023.

[49] Mr. CHERRAK Abdenasser Mr BOUKLI HACENE Adel. ≪Conception et Réalisation d'un Système Intelligent de Surveillance basée sur Raspberry Pi dans le Contexte du Covid-19≫ Université Ain Temouchent- Belhadj Bouchaib 2021/2022.

[50] Mili Aya et Machene Imed Eddine ≪ Reconnaissance automatique des personnes par les veines de la main ≫ Université 08 Mai 1945-Guelma/2024.

[51] <http: //www.comp.polyu.edu.hk/biometrics/FKP.htm>. « PolyU Finger Knuckle Print Database ».

[52] <http: //www.comp.polyu.edu.hk/csajaykr/knuckle/iitdknuckle.htm>.

« IIT Delhi Finger Knuckle Database ».

[53] Mr. Mourad CHAA « SYSTÈME DE RECONNAISSANCE DE PERSONNE PAR DES TECHNIQUES BIOMÉTRIQUES ».Université Ferhat Abbas – Sétif -1- UFAS (ALGERIE) / 2017.