REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
UNIVERSITE KASDI MERBAH OUARGLA
FACULTE DES NOUVELLES TECHNOLOGIES DE L'INFORMATION
ET DE LA COMMUNICATION
DEPARTEMENT DE L'ELECTRONIQUE ET DE TELECOMMUNICATION

Mémoire

MASTER ACADEMIQUE

Domaine : Electronique

Spécialité : Electronique des Systèmes Embarques

Présenté par :

Bechki Amar

Maamri Omar

Thème

Identification des personnes par l'empreinte de l'articulation des doigts

Soutenu le : 14 / 06 / 2022

Devant le jury :

Mr SAMAI Djamel	***MCB***	***President***	***UKM Ouargla***
Mr. MANSEUR Abdelghani	***MCA***	***Examinateur***	***UKM Ouargla***
Mr.CHAA Mourad	***MCB***	***Encadreur /rapporteur***	***UKM Ouargla***

Remerciements

Nous remercions en premier lieu, Dieu tout puissant qui m'a donné la force, la volonté et surtout la patience pour accomplir ce travail.
Nous tenons essentiellement et particulièrement à exprimer nos sincères et profondes gratitude à l'égard de Monsieur **Dr. CHAA Mourad,** d'avoir eu l'aménité d'accepter de diriger ce travail, qui s'est montré d'une générosité sans bornes sur tous les plans, scientifique et humain;
Nous remercions également Monsieur **SAMAI DJAMEL** et Monsieur **MENSEUR ABDELGHANI** d'avoir accepté d'examiner de notre thèse.
Nous tenons à remercier également les responsables et tout le personnel du département d'électronique de la faculté de technologie à l'université kasdi merbah ouargla.
Notre remerciement à tous nos amis ainsi qu'à toutes les personnes que nous avons connues, qui nous ont aidés, soutenu et encouragé.

Dédicace

À l'esprit de mon père Elhadj Hmida
À l'esprit de mon frère Mohamed khaled
À ma chère mère
À mes frères et mes sœurs
À mon frère Lazhar, qui m'a donné
le courage et la force de continuer....
À ma femme, mes filles et mes fils

Amar BECHKI

Dédicace

Je dédie ce travail :

A mes chers parents qui ont donné mon précieux pour arriver ici

A ma femme qui m'encourage en tout

A ma chère fille Lina

A mes frères et soeurs, chacun en son nom

Tous mes amis, surtout Abd el Karim, qui m'ont montré l'idée de master

À tous ceux qui ont donné ne serait-ce qu'un peu pour réussir à terminer mes études

Omar MAAMRI

Résume

Depuis lors, l'homme a cherché à mettre en place des moyens fiables et efficaces pour s'assurer de l'identité des personnes avec lesquelles il interagit. Depuis l'antiquité, le meilleur moyen de s'assurer que la personne que l'on a en face de nous est la bonne restera le partage d'un secret connu uniquement des deux interlocuteurs ou d'un groupe (comme l'utilisation d'un mot de passe par exemple).

La biométrie est l'analyse mathématique des caractéristiques biologiques d'une personne et a pour objectif général de s'identifier. Étant donné que parmi les nombreuses méthodes d'identification biométrique telle que l'utilisation des empreintes des articulations des doigts d'une personne. Le but de ce travail est d'utiliser cette modalité pour réaliser un système de vérification automatique des personnes, Dans notre travail, un bloc « Local Phase Quantification »(LPQ), le codage binaire monogénique (MBC) et le descripteur GIST sont des techniques utilisées pour extraire les caractéristiques discriminantes de la modalité FKP. Bien que des progrès significatifs aient été réalisés pour de tels systèmes, les performances sont encore loin d'être satisfaisantes, ce qui nécessite également le développement de différents systèmes biométriques (comme les descripteurs). Et par la K-Nearest Neighbor Matching avec les différents distances qui consiste à classer un nouveau vecteur d'entrée x, à examiner les k points de données d'apprentissage les plus proches de x et à affecter l'objet à la classe la plus fréquente.

Mots clés : BIOMETRIE-articulations des doigts-LPQ-GIST-MBC-GABOR-KNN.

Abstract

Since then, the man has sought to put in place reliable and effective means to ensure the identity of the people with whom he interacts. Since antiquity, the best way to ensure that the person we have in front of us is the right one will remain the sharing of a secret known only to the two interlocutors or to a group (such as the use of a password for example).

Biometrics is the mathematical analysis of a person's biological characteristics and has the general purpose of identifying. Since among the many biometric identification methods such as the use of finger Knuckle prints, the purpose of this work is to use this modality to realize an automatic people verification system, In our work, a Local Phase Quantification (LPQ), monogenic binary coding (MBC) and GIST descriptor are techniques used to extract the discriminating features of the FKP modality. Although significant progress has been made for such systems, the performance is still far from satisfactory, which also requires the development of different biometric systems (such as descriptors). And by the K-Nearest Neighbor Matching with the different distances which consists in classifying a new input vector x, examining the k training data points closest to x and assigning the object to the nearest class frequent.

Keywords: BIOMETRY-finger knuckle-LPQ-GIST-MBC-GABOR-KNN

ملخص

منذ ذلك الحين، سعى الإنسان إلى إنشاء وسائل موثوقة وفعالة لضمان هوية الأشخاص الذين يتعاملون معهم. منذ العصور القديمة، فإن أفضل طريقة للتأكد من أن الشخص الذي أمامنا هو أن تظل مشاركة سر معروف فقط للمحاورين أو المجموعة (مثل استخدام كلمة مرور على سبيل المثال).

القياسات الحيوية هي التحليل الرياضي للخصائص البيولوجية للشخص وله غرض عام هو تحديد وتعريف الذات. بالنظر إلى أنه من بين العديد من طرق التعرف على القياسات الحيوية مثل استخدام بصمة مفصل الأصبع، فإن الغرض من هذا العمل هو استخدام هذه الطريقة لتحقيق نظام للتحقق التلقائي من الأشخاص، في عملنا، ***Local Phase Quantification (LPQ)***، يعد الترميز الثنائي أحادي المنشأ ***(MBC)*** ، وواصف ***GIST*** من الأساليب المستخدمة لاستخراج الخصائص المميزة لطريقة ***FKP.*** على الرغم من التقدم الكبير الذي تم إحرازه في مثل هذه الأنظمة، إلا أن الأداء لا يزال بعيدًا عن أن يكون مرضيًا، مما يتطلب أيضًا تطوير أنظمة القياسات الحيوية المختلفة (مثل الواصفات). وبواسطة ***K-Nearest Neighbor Matching*** مع المسافات المختلفة والتي تتكون من تصنيف متجه إدخال جديد ***x*** ، وفحص نقاط بيانات التدريب ***k*** الأقرب إلى ***x*** وتعيين الكائن إلى أقرب فئة متكررة.

كلمات مفتاحية : قياسات حيوية – مفصل الاصبع – المرحلة المحلية الكمية – الترميز الثنائي أحادي المنشأ.

Table de Matière

Chapitre III : Résultats et discussions

Liste des figures

Liste des tableaux

Liste des abréviations

.

DIP Articulation Inter Phalangienne Proximale
EER Error Equal Rate
FAR False Acceptante Rate
FKP Figner Knuckle Print
FRR False Reject Rate
GIST Globale Descriptor
KNN K-Nearest Neighbors.
LIF Left Index Finger
LMF Left Middle Finger
LPQ Local Phase Quantization
MBC Monogenic Binary Coding
MCP Articulation Métacarpe Phalangienne
PHD Pretty Helpful Development
RIF Right Index Finger
RMF Right Middle Finger
ROI Region Of Interest

INTRODUCTION GENERALE

INTRODUCTION GENERALE

L'humanité a traversé de nombreux changements importants au fil du temps et dans tous les aspects de la vie, en particulier avec l'arrivée de l'informatique qui a changé le monde, c'était une révolution technologique et surtout dans le domaine de communication [1]. Bien que, Dans le contexte actuel, la sécurité des systèmes d'information soit devenue un domaine de recherche d'une très grande importance, en particulier, concevoir un système d'identification fiable, efficace et robuste est une tâche prioritaire. L'identification de l'individu est devenue essentielle pour assurer la sécurité des systèmes et organisations. Face à cette sollicitation grandissante, plusieurs méthodes de reconnaissance biométriques ont été proposées, reconnaissance du locuteur, reconnaissance faciale, empreinte digitale, reconnaissance de l'iris, de la rétine, de la forme de la main, reconnaissance vocale, dynamique de frappe, Empreinte des Articulations de Doigts,…[2][3]

Ces méthodes ont permis à la biométrie de s'étendre vite à de nombreuses applications destinées à gérer l'accès à des ressources physiques (aéroports, grande magasin, stade,...etc.) et logiques (ordinateurs, comptes bancaires...etc.).[4][5]

Parmi ces méthodes de reconnaissance biométriques Notre travail est axé sur le système qui utilise l'empreinte des articulations des doigts FKP **(Finger-Knuckle-Print)** comme caractéristique biométrique de reconnaissance par image. Son modèle est unique pour chaque individu, aussi, elle ne représente pas un gène pour l'utilisateur. Nous allons focaliser dans ce travail sur l'étude d'un système complet d'identification par FKP comme trait biométrique [5]. Alors que l'objectif visé dans ce travail est la réalisation des systèmes biométriques monomodaux

basés sur les algorithmes d'extraction des caractéristiques : Filtre de Gabor, descripteur (MBC, LPQ, GIST) avec la méthode de classification KNN (K Plus Proche Voisin). [6]

Ce mémoire est composé de trois chapitres :

Le premier chapitre est consacré à la présentation générale de la biométrie, qui inclut sa définition, ses principales modalités, ses différents modes de fonctionnement, ainsi que les objectifs qu'elle cherche à atteindre, aussi les domaines et les applications dans lesquels elle est utilisée, on parle aussi sur les techniques utilisées.

Dans le deuxième chapitre, on va donner une présentation de système FKP, le dispositif d'acquisition des images de l'FKP, les méthodes utilisées pour l'extraction des caractéristiques et la classification des données et quelques distances utilisées.

Le troisième chapitre est consacré à la présentation de la méthode proposée, de la base de données et l'extraction de la région d'intérêt. Ensuite on va discuter les résultats de tests des systèmes monomodaux en utilisant les différents algorithmes de l'extraction des caractéristiques. On termine par la suite par une étude comparative entre les différents systèmes.

Une conclusion générale est présentée à la fin de ce mémoire avec quelques perspectives et recommandations.

Chapitre I : La biometrie

Chapitre *I* : la Biométrie

I.1 Introduction :

L'utilisation de la biométrie s'est répandue énormément dans la vie quotidienne et trouve de nombreuses applications ; pour pénétrer dans un lieu et y circuler librement, pour accéder au poste de travail, retirer de l'argent, …etc. La biométrie tend à remplacer peu à peu les codes d'accès et les mots de passe qui peuvent être changées ou volées. De nombreux travaux de recherche ont été menés et en cherche toujours des nouvelles méthodes.

I.2 Définition de la biométrie

La biométrie est de reconnaître une personne grâce à ses caractéristiques morphologiques pouvant inclure l'iris, l'empreinte digitale, l'empreinte palmaire, les empreintes des articulations des doigts, la géométrie de la main, le visage. Les caractéristiques comportementales incluent la voix, la signature, la démarche ou caractéristiques biologiques incluent l'ADN, les veines de la main, … [7] **(Voir Figure 1**).

Donc, La biométrie recense nos caractères physiques (et comportementaux) les plus uniques, qui peuvent être captés par des instruments et interprétés par des ordinateurs de façon à être utilisés comme des représentants de nos personnes physiques dans le monde numérique. Ainsi, nous pouvons associer à notre identité des données numériques permanentes, régulières et dénuées de toute ambiguïté, et récupérer ces données rapidement et automatiquement à l'aide d'un ordinateur. [8]

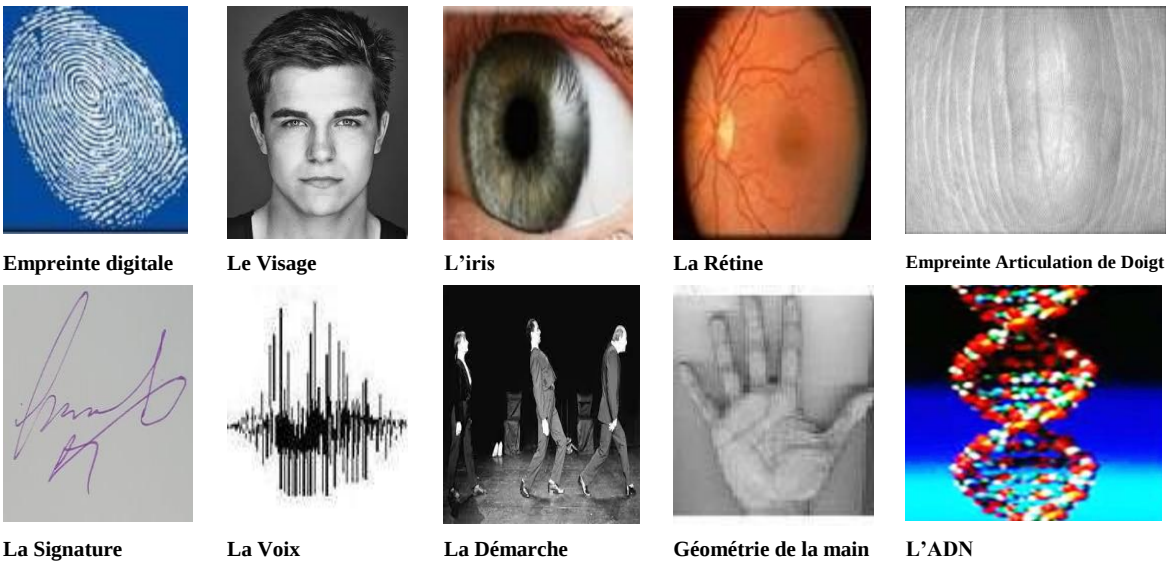


Figure I.1: Exemples de modalités biométriques.

I.3 Les caractéristiques biométriques :

Une caractéristique biométrique est une donnée contenant l'essentiel d'information permettant de différencier d'individus, pratiquement n'importe quelle caractéristique physiologique ou comportementale peut être considérée comme une caractéristique biométrique, dans la mesure où elle est :

Universelle : détermine si la modalité existe et si elle est présente quel que soit l'individu

Unique : définit la probabilité de ne pas trouver de similitudes entre les mesures d'une même modalité sur des personnes différentes.

Collectable : détermine le degré de facilité de l'acquisition, de la mesure et de l'exploitation de la modalité

Permanence : l'information collectée doit être présente pendant toute la vie d'un individu.

Acceptable : indique si la modalité est acceptée sans objection par l'utilisateur.

Performant : caractérise la robustesse, la fiabilité et la vitesse de la mesure.

Le contournement : représente la difficulté de contourner le système, par usurpation d'identité ou d'autres techniques de fraude. [9]

I.4 Les différentes techniques biométriques

Parmi les différentes techniques biométriques existantes on distingue trois catégories :

L'analyse morphologique : les empreintes digitales, l'iris, la forme de la main, les traits du visage, le réseau veineux de la rétine

L'analyse des traces biologiques : l'ADN, le sang, la salive, l'urine, l'odeur, la thermographie

L'analyse comportementale : la reconnaissance vocale, la dynamique de frappe au clavier, la dynamique de signature, la manière de marche

I.4.1 L'empreinte digitale :

Une empreinte digitale est le motif de crêtes et de sillons à la surface du bout du doigt. Sa formation est déterminée pendant la période fœtale. Les empreintes digitales de vrais jumeaux sont différentes et il n'y a pas de corrélation entre les empreintes sur les différents doigts d'un individu. Les empreintes digitales sont l'un des éléments biométriques les plus compris et les plus étudiés. Les humains utilisent les empreintes digitales pour l'identification personnelle depuis des siècles et la validité de l'identification par empreintes digitales est bien établie. Avec le développement des capteurs à semi-conducteurs, le coût marginal de l'incorporation d'un système biométrique basé sur les empreintes digitales pourrait bientôt devenir abordable dans de nombreuses applications. Bien que, Les empreintes digitales contiennent suffisamment d'informations pour permettre une identification à grande échelle. Un problème avec la technologie des empreintes digitales est son acceptabilité par un utilisateur typique, car les empreintes digitales ont traditionnellement été associées aux enquêtes criminelles et au travail de la police. Les gens peuvent se sentir mal à l'aise d'utiliser les empreintes digitales dans des applications civiles. Un autre problème avec la technologie des empreintes digitales est que l'identification automatique des empreintes digitales nécessite généralement une grande quantité de ressources de calcul. Les empreintes digitales d'une petite fraction de la population peuvent être inutilisables pour l'identification automatique pour des raisons génétiques, de vieillissement, environnemental ou professionnel.[10]

Figure I.2: Images de L'empreinte digitale**.**

Après la capture de l'image de l'empreinte, on fait un rehaussement de l'image. Ensuite on identifier et on extrait les minuties, qui vont être comparées avec l'ensemble des minuties sauvegardées des autres utilisateurs. C'est l'une des technologies biométriques les plus étudiées et les plus utilisées, surtout dans le contrôle d'accès. [11]

I.4.2 La Géométrie de La main :

Une variété de mesures de la main humaine, y compris sa forme et les longueurs et largeurs des doigts, etc. peuvent être utilisées comme caractéristiques biométriques. Des systèmes biométriques basés sur la géométrie de la main ont été installés dans des milliers d'endroits à travers le monde. La technique est très simple, relativement facile à utiliser et peu coûteuse. Les facteurs environnementaux opérationnels (par exemple, le climat sec) ou les anomalies individuelles (par exemple, la peau sèche) n'ont généralement aucun effet négatif sur la précision de l'identification. Cela ne semble pas être un problème pour les gens d'accepter cette technologie. Le principal inconvénient de cette technique est sa faible discrimination.[10]

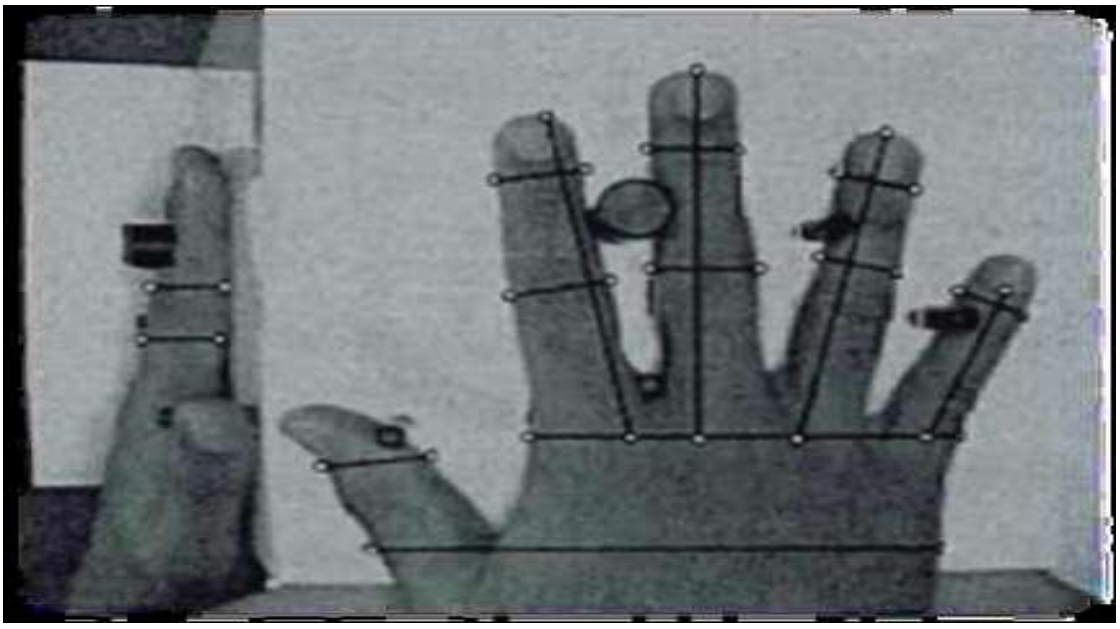


Figure I.3 : Géométrie de la

I.4.3 Empreinte des articulations des doigts :

C'est une technologie biométrique basée sur la surface arrière de doigt, elle contient des caractéristiques distinctives, telles que les lignes principales, les lignes secondaires et les crêtes, qui peuvent être extraites à partir des images à basse résolution. La main contient plusieurs doigts, pour cela, il faut conserver les informations à chaque doigt pour une reconnaissance précise dans le domaine d'identification. [12]

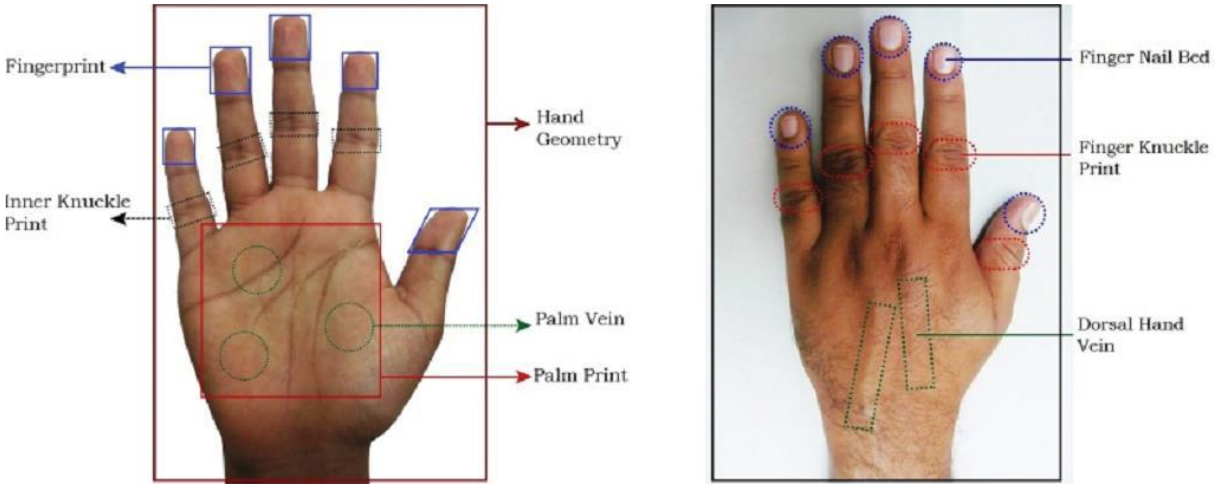


Figure I.1: Vue avant et arrière de la main

Dans ces dernières années seulement, un intérêt considérable a été accordé aux caractéristiques biométriques liées à la main en raison de sa grande acceptation par les utilisateurs. Ils ont une anatomie très particulière et fournissent donc des informations très distinctes pour reconnaître les individus. De plus, ils peuvent être capturés avec des équipements de capture d'image de petite taille et à faible coût sans nécessiter de matériel supplémentaire, ce qui conduit à des modèles de plus petite taille, et sont appropriés pour les pratiques de grande population [13]. La main est la partie du corps à l'extrémité de votre bras qui comprend vos doigts et votre pouce, elle est composée de parties contenant des informations riches en texture qui ont fourni les bases des systèmes de reconnaissance rapide. La main est une région particulièrement riche en informations pouvant être utilisées pour l'authentification ou pour l'identification des individus. Parmi les divers types d'identifiants biométriques, la biométrie de la main a suscité une attention considérable et disponible l'empreinte digitale est certainement une des modalités les plus utilisés dans les systèmes biométrique notamment grâce à son invariance dans le temps. Hormis l'empreinte digitale, d'autres caractéristiques plus ou moins robuste mais aussi plus moins acceptable pour l'utilisation peuvent être considérée, nous peuvent citer par exemple :

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 interne et saisissante de la main. Les attributs biométriques largement utilisés extraits de cette partie sont :

- Empreinte digitale (fingerprint)
- Empreinte palmaire (palmprint)
- Les réseaux veineux (palm vein, fingervein)

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 des doigts (Figner géométriy)
- Les réseaux veineux (dorsal hand vein)
- Les motifs d'articulation du doigt sur la face dorsal de la main (Finger dorsal knuckle print FKP)
- Les motifs d'articulation du doigt sur la face de la paume de la main finger inner knuckle print IKP)
- Finger Nail Bed. [13]

Anatomie des doigts :

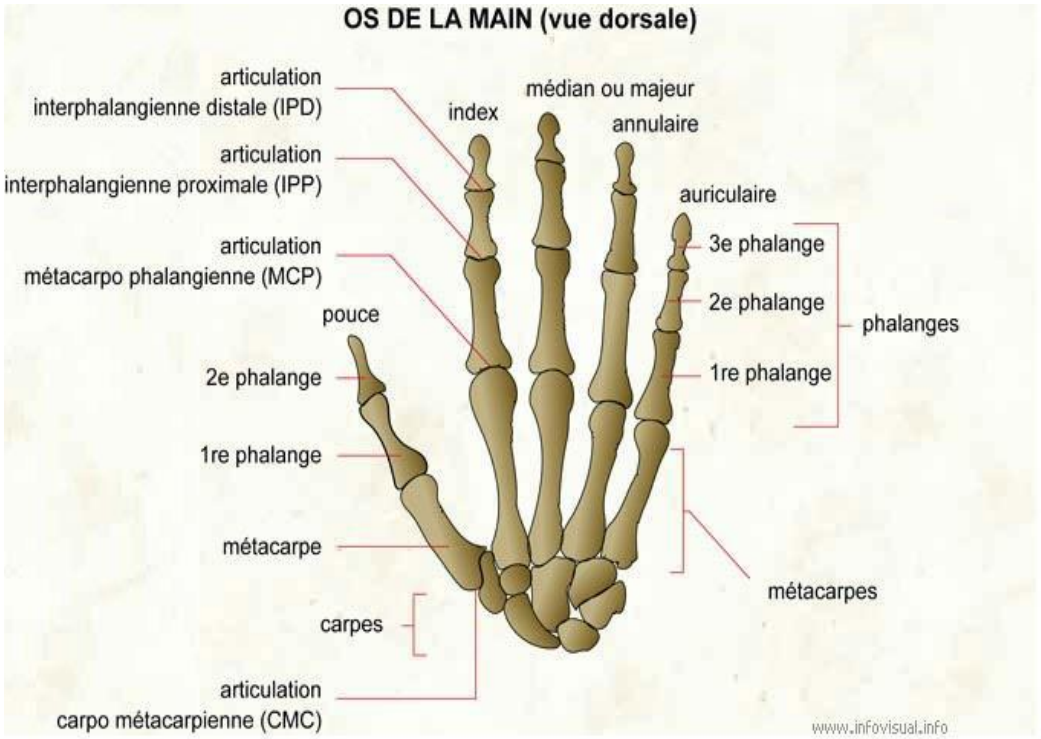


Figure I.2: OS de la main (vue dorsale)

La main est constituée d'une face palmaire (ou antérieure) et d'une face dorsale (ou Postérieure), ainsi que d'une extrémité proximale (ou supérieure) et d'une extrémité Distale

(ou inférieure). Elle comporte sur sa face palmaire la paume, trois plis de Flexion et les lignes de la main. Sur cette même face, les doigts possèdent deux plis de flexion à l'exception du pouce qui n'en a qu'un seul. La partie dorsale de la main se caractérise par la présence de l'ongle sur l'extrémité distale des doigts. Les cinq Doigts de la main sont raccrochés à sa partie proximale et forment son extrémité Distale. Ils sont appelés le pouce, l'index, le majeur, l'annulaire et l'auriculaire (également appelé petit doigt), en partant du côté latéral (côté de L'éminence thénar) pour se diriger vers le médial (celui de l'éminence hypothénar).

Les quatorze OS formant le squelette des doigts sont longs et appelés les phalanges. Les doigts comportent trois phalanges, l'une proximale, l'autre intermédiaire (ou Médiane) et enfin une dernière distale, qui forme l'extrémité des doigts. Hormis le Pouce, qui n'a pas de phalange intermédiaire, tous les doigts sont concernés. Ces Phalanges sont reliées entre elles par des articulations. Il existe deux types d'articulations ; les métacarpo-phalangiennes, qui se situent entre les métacarpiens et Les phalanges proximales correspondantes, soit au niveau de la jonction entre les doigts et la main et l'inter phalangiennes, entourées de chaque côté par une phalange. Pour tous les doigts sauf le pouce, on décrit les articulations inter phalangiennes proximale et distale. En plus des OS vue précédemment, il existe également de petits OS présents dans les articulations ou les tendons, les OS sésamoïdes. [13]

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.

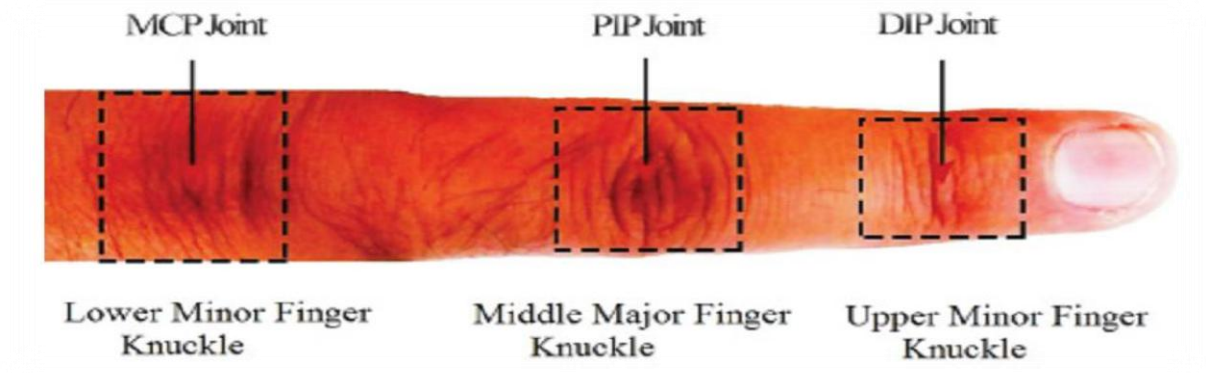


Figure I.3: La surface externe d'un doigt a trois jointures.

La surface externe d'un doigt a trois jointures comme illustré à la **Fig. 6** classé en articulations majeure et mineure :

- Une articulation inter phalangienne distale (DIP) (première FKP mineure).
- Une articulation inter phalangienne proximale (PIP) (FKP majeur).

- Une articulation métacarpe phalangienne (MCP) (deuxième FKP mineure)

La plupart des recherches se sont concentrées sur des algorithmes de reconnaissance des motifs de texture des articulations PIP et ont évalué ses performances à l'aide d'une base de données d'images publique. **[13]**

Bien que, les systèmes biométriques basé sur la modalité FKP ont la possibilité de fonctionner dans des conditions météorologiques extrêmes et des conditions d'éclairage médiocres. Aussi, les caractéristiques FKP chez les adultes sont plus stables au fil du temps et ne sont pas sujettes à des changements majeurs. Plus que, les informations biométriques basées sur le FKP sont très fiables et peuvent être utilisées avec succès pour reconnaître des personnes parmi plusieurs individus. **[14].**

Figure I.4: Empreintes des articulations des doigts**.**

I.4.4 La reconnaissance faciale (Le Visage) :

Les images faciales sont probablement la caractéristique biométrique la plus couramment utilisée par les humains pour établir une identification personnelle. La reconnaissance faciale est l'un des domaines de recherche les plus actifs avec des applications allant de la vérification statique et contrôlée des photos d'identité à l'identification dynamique et incontrôlée des visages dans un arrière-plan encombré. La reconnaissance faciale est une technique non intrusive et les gens n'ont généralement aucun problème à accepter le visage comme caractéristique biométrique. Au cours de ces dernières années, de nombreux efforts de recherche ont été consacrés à la reconnaissance faciale. Les approches de la reconnaissance faciale sont généralement basées sur (i) l'emplacement et la forme des attributs faciaux tels que les yeux, les sourcils, le nez, les lèvres, la forme du menton, etc. et leurs relations spatiales ou (ii) l'analyse globale de l'image du visage et la décomposition du visage en un certain nombre de visages canoniques. Un certain nombre de systèmes commerciaux de reconnaissance faciale sont disponibles. Bien que les performances de ces systèmes soient raisonnables, on peut se demander si le visage lui-même, sans aucune information contextuelle, est suffisamment efficace pour effectuer une identification personnelle avec un

niveau de confiance élevé. En outre, les systèmes de reconnaissance faciale actuels imposent un certain nombre de restrictions sur la manière dont les images faciales sont acquises (par exemple, arrière-plan simple, éclairage uniforme et fixe). Pour que la reconnaissance faciale soit largement adoptée, ils doivent être automatiquement (1) détecter s'il existe un visage dans l'image acquise, (2) localiser le visage s'il y en a un, et (3) reconnaître le visage d'un point de vue général. Ces problèmes mettent en évidence certaines difficultés de la reconnaissance faciale. **[10]**

Figure I.5: Reconnaissance faciale.

I.4.5 **L'iris :**

L'iris est la région, sous forme d'anneau, située entre la pupille et le blanc de l'œil, il est unique. L'iris a une structure extraordinaire et offre de nombreuses caractéristiques de texture qui sont uniques pour chaque individu. La reconnaissance de l'iris est développée dans les années 80 c'est pour cela elle est une technologie plus récente .l'image de l'iris est capturée par un appareil qui contient une caméra infrarouge, lorsque la personne se place à une courte distance de l'appareil**. [12]**

I.4.6 La rétine :

La rétine est située à l'arrière de l'œil et est une pellicule très photosensible. Cette technique utilise le style des dessins formés par les vaisseaux sanguins d'une rétine par individu et est totalement stable pendant la vie d'une personne. La reconnaissance de la rétine est actuellement considérée comme une des méthodes biométriques les plus sûres. Les motifs formés par les veines sous la surface de la rétine sont uniques et stables dans le temps. La biométrie par la rétine procure également, un haut niveau en matière de reconnaissance. Cette technologie est bien adaptée pour des applications de haute sécurité. Aussi, cette technologie, très précise [7].

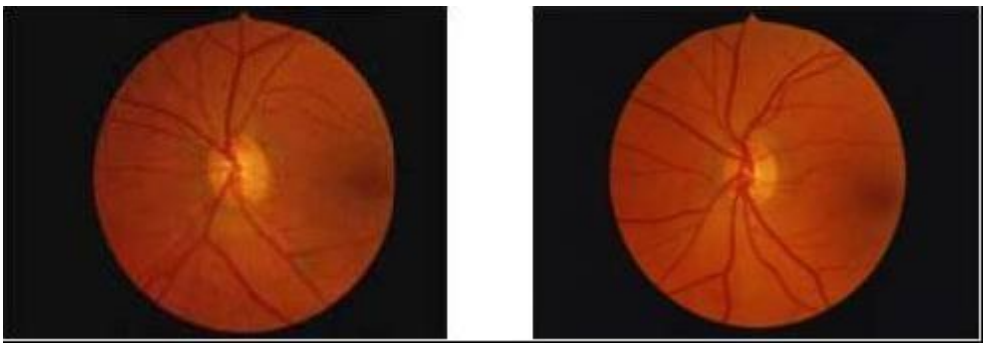


Figure I.7: **Photographies des deux rétines d'un individu.**

I.4.7 L'ADN :

L'authentification d'un individu par analyse de son ADN s'avère complexe, coûteuse et lente à réaliser compte tenu des nombreuses manipulations biologiques (amplification + électrophorèse). Ceci explique qu'il n'existe toujours pas de solution technologique grand public qui permette de réaliser automatiquement cette analyse, d'autant plus qu'elle nécessite un prélèvement d'échantillon (sang, salive, sperme, cheveux, urine, peau, dents, etc.) qui rend cette technique très intrusive. [15]

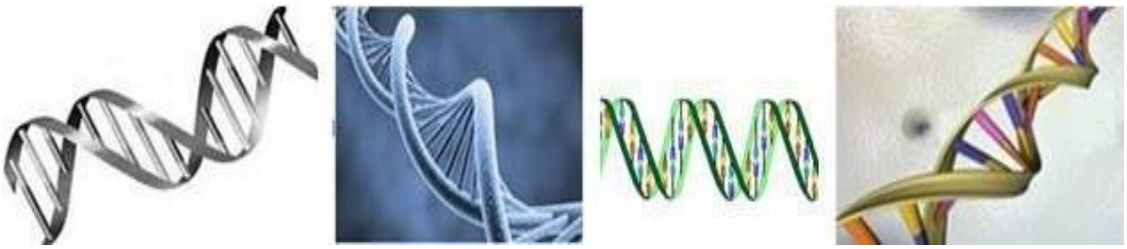


Figure I.8 : Exemple de l'ADN

I.4.8 La signature :

Chaque personne a un style d'écriture unique. Il n'y a pas deux signatures d'une personne exactement identiques ; les variations par rapport à une signature typique dépendent également de l'état physique et émotionnel d'une personne. Malgré les variations dans les signatures d'un individu, quelques systèmes d'authentification basés sur la signature ont été conçus et réussis à identifier les individus. La précision d'authentification des systèmes biométriques basés sur la signature est raisonnable mais ne semble pas suffisamment élevée pour conduire à une identification à grande échelle. Il existe deux approches de vérification de signature : statique et dynamique. La vérification de signature statique utilise uniquement les caractéristiques géométriques (forme) d'une signature. La vérification de signature dynamique utilise à la fois les caractéristiques géométriques (forme) et les caractéristiques dynamiques telles que les profils d'accélération, de vitesse et de trajectoire de la signature. Un avantage inhérent d'un système biométrique basé sur la signature est que la signature a été établie comme une forme acceptable de méthode d'identification personnelle et peut être intégrée dans les processus commerciaux existants. (par exemple, les transactions par carte de crédit). Un autre avantage de la signature est qu'il est impossible pour un imposteur d'obtenir les informations dynamiques d'une signature écrite. **[10].**

Les données peuvent être analysées à l'aide d'une tablette électronique et/ou d'un stylo lecteur. Ce système est facile à utiliser, mais sa fiabilité est qualifiée de moyenne. Il n'est pas possible de comparer la saisie d'une signature avec un gabarit préalablement stocké dans une base de données. Les systèmes d'authentification sont donc à privilégier pour la saisie dynamique de la signature**. [16]**

Figure I.9: Signatures

I.4.9 La reconnaissance vocale (La voix) :

La reconnaissance vocale ou de la parole est une technologie biométrique comportementale qui évalue les aspects de la voix d'une personne pour reconnaître son identité. Elle est qualifiée de non intrusif et facile à utiliser. L'un des avantages de cette technologie est d'autoriser une reconnaissance à distance. De plus, cette technique a une bonne acceptabilité, mais présente, à l'évidence, un niveau de sécurité inférieur aux autres

techniques. Il est relativement facile d'enregistrer et de reproduire une voix. Il est possible de s'affranchir de ce problème en faisant varier la phrase à prononcer, ou en couplant cette technique avec la prononciation d'un mot de passe. **[16]**

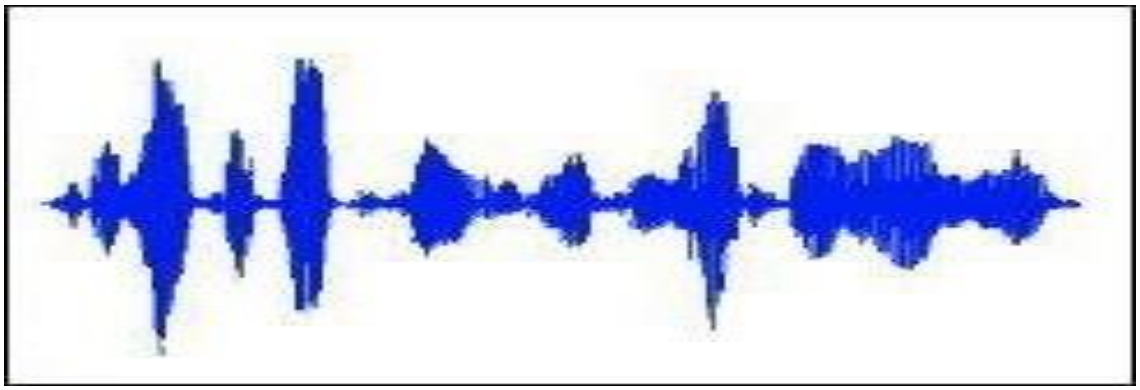


Figure I.10: Reconnaissance vocale

I.4.10 L'Analyse de la marche :

Cette technique biométrique est utilisée afin de reconnaître un individu par sa façon de marcher et de bouger. En analysant les déformations des jambes et bras au niveau des articulations. La démarche serait en effet étroitement associée à la musculature naturelle, donc, elle est très personnelle, l'intérêt de cette technologie réside que l'identification de démarche se situe dans la capacité d'identifier un individu à distance. Elle peut, aussi, détecter les comportements suspects (par vidéo-surveillance), on l'utilise pour le contrôle d'accès aux bâtiments ou aux zones réglementées mais elle est facilement modifiable par l'individu. **[15]**

Figure I.11: La Démarche.

Le tableau en dessous résume une comparaison des traits biométriques. A noté que, Chaque technologie biométriques possède des avantages, mais aussi des inconvénients, acceptables ou inacceptables suivant les applications utilisées. Ces technologies n'offrent pas les mêmes niveaux de sécurité ni les mêmes facilités d'emploi ou encore pas la même précision. [15]

Tableau I.1: **Comparaison de quelques modalités biométrique**

Technologie	*Avantages*	*Inconvénients*
Visage	Coût moyenne Bonne acceptabilité	-Jumeaux, déguisement Vulnérabilité aux attaques(facile falsifier)
Iris	-Fiabilité	Acceptabilité très faible Contrainte d'éclairage
Géométrie de la main	Très ergonomique Bonne acceptabilité	Système en comburante coûteux Perturbation possible pardes blessures
Empreintes des articulations des doigts	• facilité d'acquisition • ces images ayant une basse résolution	Très similaire pour les jumeaux Posent correct de doigt sur le lecteur provoque une grande erreur
Empreinte digitale	Coût faible Ergonomie(Facilité d'utilisation) moyenne	Acceptabilité moyenne Possibilité d'attaque
Rétine	Fiabilité Pérennité	Acceptabilité très faible Contrainte d'éclairage
Signature	-Ergonomie	- Dépendant de l'état émotionnel delà personne peu fiable
Reconnaissance Vocale	Facile	Vulnérable aux attaques
Démarche	Facile Très ergonomique Bonne acceptabilité	Dépendant de l'état De la personne
ADN	- Une Très grande précision.	Acceptabilité très faible Très cher

I.5 Les Modes de fonctionnement d'un système biométrique

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

I.5.1 Le mode enrôlement :

Quelle que soit la modalité, il est nécessaire de passer par une phase d'enrôlement (ou entraînement du modèle biométrique). À acquérir un échantillon et d'en extraire les caractéristiques puis d'entraîner un classifieur à les reconnaitre. C'est une phase d'apprentissage qui a pour but de recueillir des informations biométriques sur les personnes à identifier. Pendant cette phase, les caractéristiques biométriques des individus sont saisies par un capteur biométrique, puis traitées et représentées sous forme numérique et enfin stockées dans une base de données. [9]. (Voir Figure 15)

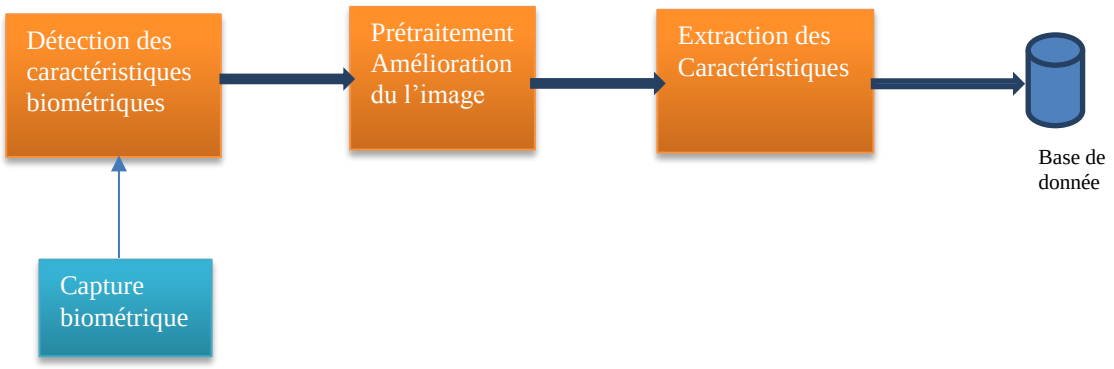


Figure I.12: **Mode enrôlement d'un système biométrique.**

I.5.2 Mode vérification (authentification) :

Lorsqu'un système biométrique opère en mode vérification, l'utilisateur affirme son identité et le système vérifie si cette affirmation est valide ou non, généralement via un code PIN (Personal Identification Number), un nom d'utilisateur, une carte à puce, etc., le système effectue alors une comparaison on appariement (1 : 1) afin de déterminer si la déclaration est vraie ou non [7].

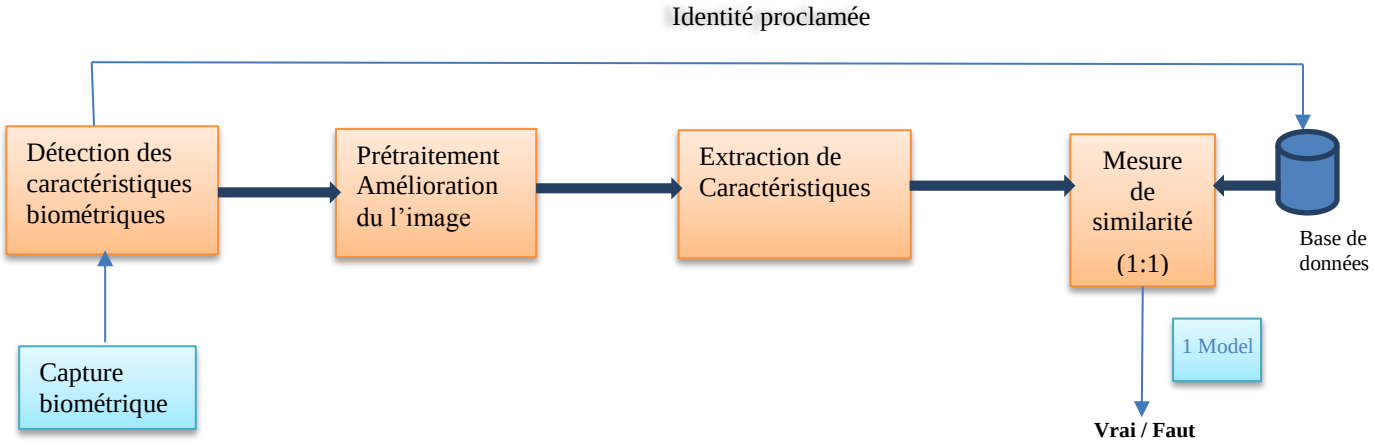


Figure I.13: **Mode vérification d'un système biométrique.**

I.5.3 Mode identification :

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

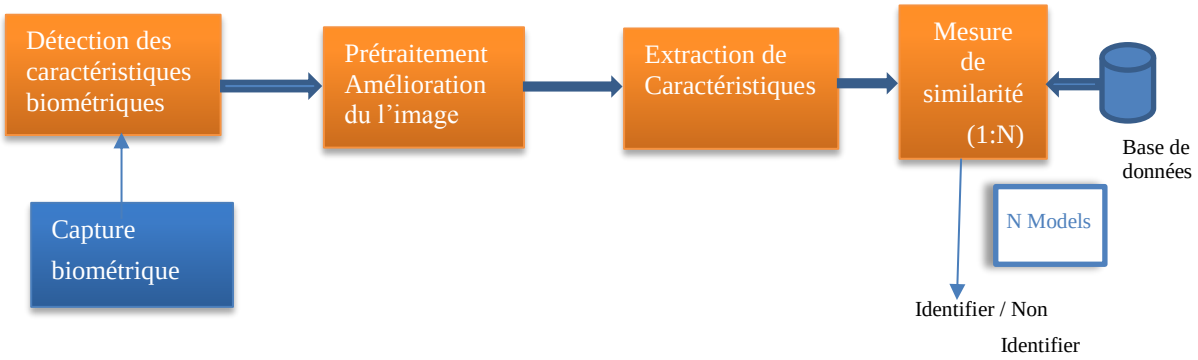


Figure I.14: **Mode identification d'un système biométrique.**

1.6 Les Principaux modules du système biométrique

Un système biométrique peut être représenté par quatre modules principaux. Ces modules sont :

I.6.1 Module capture :

Responsable de l'acquisition des données biométriques d'un individu (cela peut être un appareil photo, un lecteur d'empreintes digitales, une caméra de sécurité...). **[11]**

I.6.2 Module d'extraction des caractéristiques :

Qui prend en entrée les données biométriques acquises par le module de capture et extrait seulement l'information pertinente afin de former une nouvelle représentation des données. Idéalement, cette nouvelle représentation est censée être unique pour chaque personne et relativement invariante aux variations intra-classe. **[11]**

I.6.3 Module de correspondance :

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

I.6.4 Module de décision :

Vérifie l'identité affirmée par un utilisateur ou détermine l'identité d'une personne basée sur le degré de similitude entre les caractéristiques extraites et le(s) modèle(s) stocké(s). **[18]**

I.7. Evaluation des performances des Systèmes biométriques

Chaque caractéristique (ou modalité) biométrique a ses forces et ses faiblesses, et le choix dépend de l'application visée. On s'attend ce qu'aucune modalité biométrique ne répond efficacement aux exigences de toutes les applications, plusieurs études ont été menées afin

d'évaluer les performances des systèmes biométriques. Ces études sont basées sur quatre critères d'évaluation :

Intrus : Ce critère permet de classifier les systèmes biométriques en fonction de l'existence d'un contact direct entre le capteur utilisé et l'individu à reconnaître.

Fiabilité : Dépend de la qualité de l'environnement (éclairage par exemple) dans lequel l'utilisateur se trouve. Ce critère influe sur la reconnaissance de l'utilisateur par le système considérablement.

Coût : Doit être modéré. À cet égard nous pouvons dire que la reconnaissance faciale ne nécessite pas une technologie coûteuse. En effet, la plupart des systèmes fonctionnent en utilisant un appareil à photo numérique de qualité standard

Effort : Requis par l'utilisateur lors de la saisie de mesures biométriques, et qui doit être réduit le plus possible.

Un système biométrique peut faire l'objet de deux types d'erreurs. Il peut rejeter un utilisateur légitime et dans ce premier cas on parle de faux rejets (false rejection). Il peut aussi accepter un imposteur et on parle dans ce second cas de fausse acceptation (false acceptante). La performance d'un système se mesure donc à son taux de faux rejet (False Rejection Rate ou FRR) et à son taux de fausse acceptation (False Acceptante Rate ou FAR). [5].

Le FAR (False Acceptante Rate):

Proportion des imposteurs acceptés par le système biométrique, ce système classe alors deux caractéristiques provenant de deux personnes différentes, comme appartenant à la même personne. [11].

$$\text{FAR} = \frac{\text{Nombre des imposteurs acceptées}}{\text{Nombre totale d'accés imposteurs}} \quad \textbf{(I.1)}$$

Le FRR (False Reject Rate):

Ce taux représente le pourcentage des véritables clients censés être reconnus par le système mais qui sont rejetés, le système indique la probabilité qu'un utilisateur connu soit rejet [11].

$$FRR = \frac{\text{Nombre des clients rejetés}}{\text{Nombre totale d'accés clients}} \quad \textbf{(I.2)}$$

Une diminution du FAR entraîne systématiquement une augmentation du FRR (et inversement) [7].La performance du système ne peut pas être mesurée en utilisant séparément les taux d'erreur (FAR / FRR) mais on utilise le taux d'erreur égale (EER).

Le EER (Error Equal Rate):

La valeur au point de croisement des courbes de taux FRR et FAR sera la valeur du taux EER (Equal Error Rate). Il est couramment utilisé pour une comparaison rapide entre deux systèmes si nécessaire et le meilleur compromis entre les faux rejets et les fausses acceptations. Plus le taux EER est faible, plus le système biométrique est considéré comme étant précis [9].

$$EER = \frac{\text{Nombre de fausses acceptations} + \text{Nombre de faux rejet}}{\text{Nombre totale d'accés}} \quad \textbf{(I.3)}$$

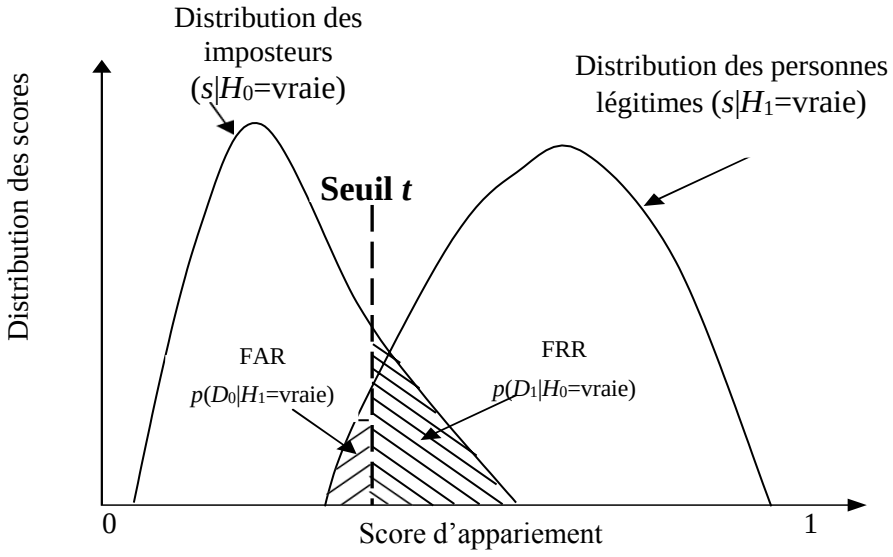


Figure I.15: Illustration de FRR et du FAR

Uncompromis est à rechercher entre FAR et FRR dans chaque système biométrique. En effet, FAR et FRR sont fonctions du seuil de décision t du système et, plus rigoureusement, elles devraient être notées comme FAR(t) et FRR(t), respectivement. Leurs courbes respectives (voir figure 18) permettent d'estimer les performances du système pour différentes valeurs du seuil de décision.

Tandis que le choix du seuil de similarité est important car il influe directement sur les performances du système. Un seuil trop petit entraîne l'apparition d'un grand nombre de faux rejets, tandis qu'un seuil trop grand engendre un taux important de fausses acceptations. La statistique la plus simple pour mesurer la performance d'un algorithme dans le contexte de la vérification est de calculer le point d'équivalence des erreurs (Equal Error Rate - EER). Le point d'équivalence des erreurs, ou taux d'exactitude croisée, est déterminé par le point d'intersection entre la courbe du taux de fausses acceptations et la courbe du taux de faux rejets. Un exemple de courbes d'erreurs croisées est donné à la figure (19). [20]

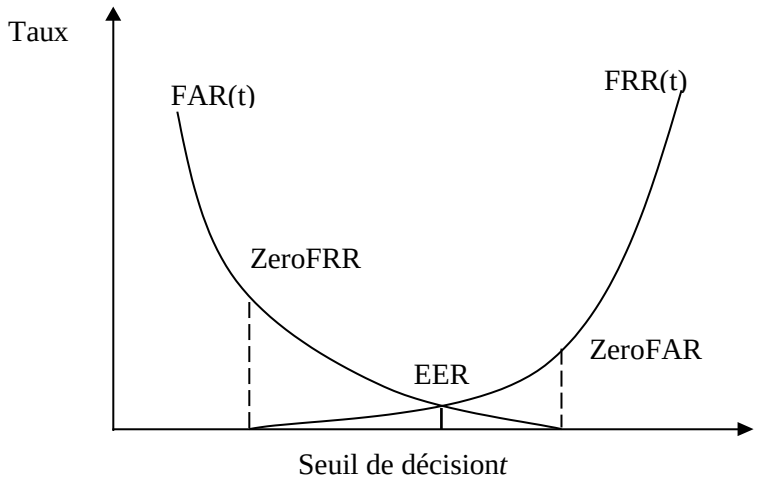


Figure I.16: Courbe du point d'équivalence des erreurs dans un système biométrique.[20]

La représentation du FRR en fonction du FAR pour les différents points opérationnels du seuil t, permet de tracer la courbe DET « Detection Error Tradeoff » largement répandue pour l'évaluation de tels systèmes d'authentification.

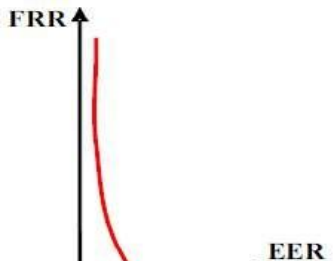


Figure I.17: Courbe DET.

1.8. Domaines d'applications :

La biométrie répond aux exigences de sécurité par les secteurs particuliers et les entreprises dans tous les pays. La sécurité biométrique couvre presque tous les domaines. Aujourd'hui, La sécurité biométrique est utilisée dans l'accès aux réseaux et aux systèmes d'informatique, paiement électronique et cryptage des données. Généralement, les applications de la sécurité biométrique peuvent être classées en quatre sections principales [11].

1.8.1 Service public

- Le contrôle et la sécurité des bâtiments gouvernementaux frontière.
- Contrôle les immigrants qui entrent et sortant pays.
- Utilisés dans les aéroports et la santé.
- Aidant à passer de la carte d'assurance sociale.

1.8.2 Pouvoir judiciaire

- L'utilisation des empreintes digitales pour prouver certains faits concernant les infractions pénales.

- L'utilisation de l'ADN extrait du sang ou des cheveux dans la scène du crime pour obtenir le criminel.

8.3 Secteur des banques

- Les transactions bancaires (retraits en espèces, les cartes bancaires, paiement par le téléphone et internet).

- La réduction de la proportion de la fraude grâce à l'intégration des cartes à puce avec

reconnaissance des empreintes digitales

1.8.4 Accès physique et logique

Ceci se rapporte au contrôle d'accès physique comme la sécurisation des lieux (bâtiment ou une pièce) ou le contrôle d'accès logique comme la sécurisation d'une session informatique (ordinateur ou base de données).

I.9 La multi modalité :

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

Le bruit des capteurs, la non-universalité, le manque d'individualité, le manque de représentation invariante et la sensibilité aux attaques.

Ainsi, à cause de tous ces problèmes pratiques, les taux d'erreur associés à des systèmes biométriques unimodaux sont relativement élevés, ce qui les rend inacceptables pour un déploiement d'applications critiques de sécurité. Pour pallier ces inconvénients, une solution est l'utilisation de plusieurs modalités biométriques au sein d'un même système, on parle alors de système biométrique multimodal.

En outre, La recherche dans le domaine de la biométrie multimodale est relativement récente. Depuis 1995, date à laquelle les premiers travaux de fusion du visage et de la voix ont été menés, de nombreuses études ont été conduites en associant différentes modalités, en faisant varier le niveau de fusion des données et en testant plusieurs règles de fusion. [21].

I.9.1 Les différentes multimodalités possibles :

Dans le spectre de la biométrie, l'utilisation de plusieurs modalités biométriques au sein d'un même système diminuent les contraintes des systèmes biométriques monomodaux en combinant plusieurs systèmes. On peut différencier Cinq (5) types de systèmes multimodaux selon les systèmes qu'ils combinent. (Figure 21) [21]

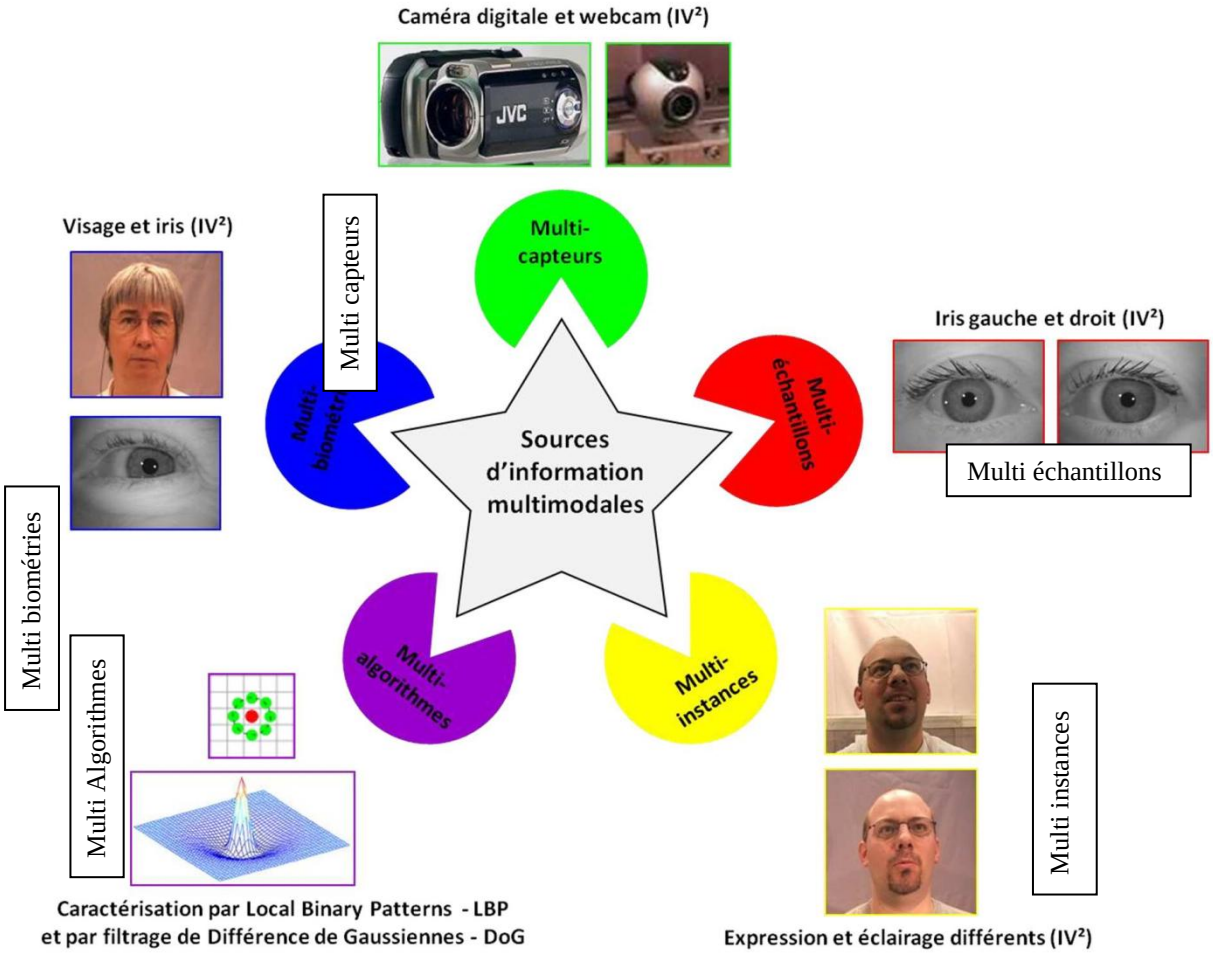


Figure I.18: Les différents systèmes multimodaux. [22]

Systèmes multi-instances : il s'agit d'utiliser un seul capteur pour extraire des instances du même caractère biométrique, afin d'obtenir plusieurs variations de ce trait en enrichissant le modèle biométrique de l'individu. Par exemple l'acquisition de plusieurs images de visage en changeant la pose, l'expression, et/ou l'illumination. **[22]**

Systèmes multi-capteurs : dans ce système nous utilisons plusieurs capteurs pour acquérir la même modalité, afin d'extraire plusieurs informations de même trait biométrique. Exemple la capture de la texture 2D, de la surface 3D, ainsi que l'image infrarouge de visage de l'individu avec différentes gammes de capteurs. **[22]**

Systèmes multi-algorithmes : dans ce genre de système plusieurs algorithmes sont utilisés, dans la phase d'extraction de caractéristiques et/ou dans la phase de la mise en comparaison pour traiter la même donnée. Exemple l'utilisation des algorithmes pour analyser la texture et les minuties de l'empreinte digitale afin d'extraire des caractéristiques pouvant améliorer la performance du système **[22].**

Systèmes multi-échantillons : ce type de système associent plusieurs échantillons de la même biométrie. C'est le cas par exemple de l'iris gauche et droit, ou deux empreintes

digitales de doigts différents. Ce genre de système ne nécessite ni plusieurs algorithmes, ni plusieurs capteurs, cependant il exige plusieurs références contrairement au système multi-instance qui n'utilise qu'une seule. **[22]**

Systèmes multi-biométries : (ou système multimodale au sens strict) ici on combine différents traits biométriques d'un individu par exemple le visage et l'iris, le visage et l'empreinte digitale etc. Il faut noter ici que l'utilisation des biométries décorrélés (comme la rétine et la démarche) peut donner un système plus performant que celui obtenu en fusionnant deux biométries corrélés (comme la voix et le mouvement des lèvres). **[22]**

Tous ces types de systèmes peuvent pallier à des problèmes différents et ont chacun leurs avantages et inconvénients. Les quatre premiers systèmes combinent des informations issues d'une seule et même modalité ce qui ne permet pas de traiter le problème de la non-universalité de certaines biométries ainsi que la résistance aux fraudes, contrairement aux systèmes "multi-biométries".

En effet, les systèmes combinant plusieurs informations issues de la même biométrie permettent d'améliorer les performances en reconnaissance en réduisant l'effet de la variabilité intra-classe. Mais ils ne permettent pas de traiter efficacement tous les problèmes des systèmes monomodaux. C'est pour cette raison que les systèmes multi-biométries ont reçu beaucoup d'attention de la part des chercheurs. **[7]**

I.10 Conclusion

Dans ce chapitre, nous avons passé en revue les principales technologies biométriques. Ensuite, nous avons présenté l'architecture de base d'un système biométrique et leurs différentes applications. Nous avons aussi enregistré que les performances des systèmes biométriques dépendent de plusieurs facteurs et qu'elles varient d'un système à un autre. Parmi les critères d'évaluation de la qualité du système biométrique, nous avons présenté les taux des erreurs (FAR, FRR et ERR), nous avons parlé aussi de la biométrie multimodale et ses différents types.

Chapitre II :

Etat de l’Art de l’empreinte des articulations des doigts et les algorithmes utilisés.

II.1. Introduction :

L'objectif de l'état de l'art est de pouvoir analyser les techniques et les méthodes existantes afin de sélectionner celles qui vont être intégrées dans la méthodologie d'analyse de systèmes biométriques que nous cherchons à concevoir. Nous allons parler dans ce chapitre des bases de données FKP, des phases de prétraitement, extraction des caractéristiques et de classification. Aussi nous allons donner des définitions des quelques algorithmes utilisés dans les systèmes biométriques, les algorithmes qu'on va parler ce sont principalement les descripteurs et les filtres utilisés pour l'extraction des caractéristiques, Les filtres de Gabor, Descripteurs MBC, GIST, LPQ [6]. Ainsi, pour la classification on parle de la méthode des K plus proches voisins.

II.2 Etat de l'Art de l'empreinte des articulations des doigts :

L'articulation du doigt est à la phase de développement et peut être considérée comme nouvelle tendance dans la biométrie.

Woodard and Flynn (2005) [23], 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.

FigureII. 1 : capteur d'Acquisition d'images FKP

En 2009, Kumar et Ravikanth [24], 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 (Principal Component Analysis) , 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.

Alors que, la méthode [23], utilise principalement l'information de la forme 3D du dos du doigt mais n'utilise pas toutes les informations de texture. Alors que les méthodes d'analyse sous-espace utilisées dans [24], ne peuvent extraire efficacement les lignes et les caractéristiques distinctes du dos de la surface du doigt. D'autre part, dans l'article [23], ils ont élaboré un système de reconnaissance d'empreinte d'articulation incluant plus spécifiquement le dispositif d'acquisition, puis une détection de la région qui les intéresse a été réalisée et ensuite un filtre de Gabor 2D a servi pour extraire les informations de l'orientation locale. Pour la comparaison, ils ont utilisé la distance angulaire pour mesurer la similitude entre deux codes qui correspondent aux images.

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.

Dans [25], 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.

ZHU Le-qing [18], 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.

Yang Wankou [25], 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'une 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.

Zahra S. et al. [26], 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.

Guangwei Gao et al [27], développent le code compétitif pondéré (W-CompCode) pour une extraction des caractéristiques effective. En premier lieu, ils proposent une matrice pondérée pour chaque ROI des images de FKP basée sur le filtre de Gabor. Pour le matching des W-CompCode, la distance de Hamming normalisée est utilisée en se basant sur la distance angulaire. L'EER obtenu est 1.203 pour la base de données PolyU FKP.

Chetana Hegde et al [28], 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.

Dans **[29],** une 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.

II.3 Prétraitement de l'empreinte d'articulation de doigt FKP :

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 [7] 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].

Etape 1 : Filtrage et sous-échantillonnage

La taille de chaque image de la base des données est d'un nombre de pixels important avec une résolution importante. Il n'est pas nécessaire d'utiliser cette résolution pour l'extraction des caractéristiques (une faible résolution peut représenter bien les lignes principales et secondaires autour de l'articulation). Par conséquent, l'image du doigt subit une opération de filtrage suivi par une opération de sous-échantillonnage. L'objectif de l'opération de filtrage est de réduire le bruit dans l'image. Un filtre passe-bas (filtre gaussien), peut être appliqué pour réduire ce bruit et améliorer la qualité de l'image originale. L'opération de sous-échantillonnage permet de réduire la résolution de l'image. L'avantage de cette opération est de réduire considérablement le coût de calcul en réduisant la quantité de données. Nous notons ID l'image résultante. Le résultat de cette étape est illustré dans la figure (23).

Figure II.2: filtrage et sous-échantillonnage de l'image de doigt.

Etape 2 : Détermination de l'axe :

Une fois que l'image de l'empreinte a été filtrée et sous échantillonnée, l'algorithme détermine l'axe horizontal X. La limite inférieure du doigt peut être facilement extraite par un détecteur de contour de type Canny. Le filtre de Canny est utilisé en raison de ses avantages (bonne détection, bonne localisation). En fait, cette limite inférieure est presque conforme à toutes les images parce que tous les doigts sont mis sur le bloc de base dans l'acquisition de l'image. En adaptant cette frontière comme une ligne droite, l'axe X est déterminé. La figure (24) montre l'axe X dans la frontière basse du doigt.

Figure II. 3 : Présentation de l'axe X dans la frontière basse du

Etape 3 : Extraction d'une sous-image

Les informations utiles qui peuvent être utilisées pour une identification biométrique ne réside que dans une partie de l'image du doigt. Donc ça nécessite une coupure d'une sous-image IS, à partir de l'image originale.

Figure II.4 : sous-image extraite avant l'extraction de la ROI.

Les limites gauche et droite d'IS sont deux valeurs axées empiriquement. Les limites hautes et basses sont estimées selon la limite de vrais doigts. La figure (25) montre un exemple d'une sous-image. Cette sous-image est utilisée pour calculer l'axe Y.

Etape 4 : Détection de contour

L'application d'un détecteur de contour de type Canny sur l'image IS, nous permet d'obtenir l'image des contours IE. (Voir figure 26)

Figure II.5: Image des contours obtenue.

Etape 5 : Codage des directions convexe

Cette étape basée sur les caractéristiques des courbes des contours dans l'image IE, ainsi que, le codage de cette image, nous permet d'obtenir une image codé ICD qui représente les directions convexes des courbes. Dans cette étape, chaque pixel dans IE sera donc désigné par un code afin de représenter la direction (convexe) locale de ce pixel. On se basant sur l'observation des images de doigt, la figure (27) illustre un modèle idéal des courbes dans l'image de doigt comme Dans ce modèle, une courbe dans l'image soit convexe vers la gauche Ou convexe vers la droite.

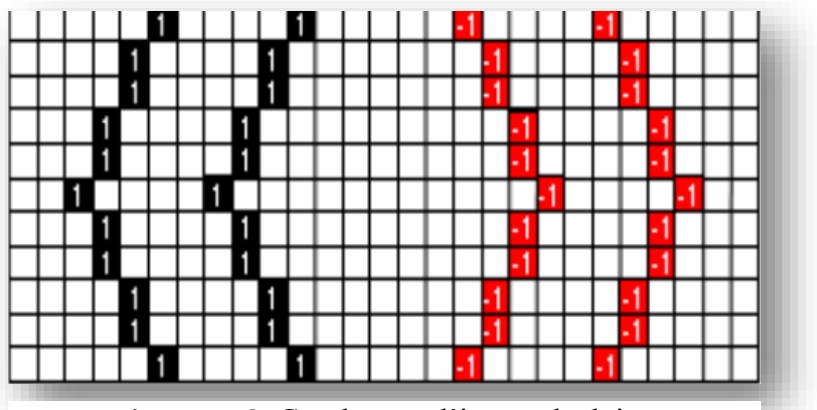


Figure II.6: Courbes sur l'image de doigt.

Nous pouvons, donc, coder les pixels sur les courbes convexes (vers la gauche) par

« -1 », les pixels sur les courbes convexes (vers la droite) par « 1 » et les autres pixels (n'appartiennent pas à ces deux courbes) par « 0 ». La figure (27) montre les directions convexes ICD.

Figure II.7 : Image obtenue par l'application de codage de la direction

Etape 6 : Détermination de l'axe Y

Pour une image de doigt, la plupart des courbes sur la partie gauche de l'image sont dirigées vers la gauche et ceux sur la partie droite sont dirigés vers la droite. Cependant, il n'y a pas des directions convexes évidentes dans une petite zone autour de l'articulation.

Cette position peut être utilisée pour définir l'axe Y. La figure (29) montre la position de l'axe Y dans l'image du doigt.

Figure II.8: détermination de l'axe Y.

Etape 7 : Localisation de la ROI

Après avoir localisé les axes X et Y, nous pouvons déterminer une zone dans l'image ID, nommée IROI, qui représente la région d'intérêt. D'après la figure (30) la ROI, avec une taille fixe, peut être extraite à partir de l'image ID.

Figure II.9: localisation de la ROI dans l'image de doigt**.**

Etape 8 : Extraction de ROI

Une région d'intérêt de l'empreinte est définie et découpée autour du l'axe Y (comme le montre la figure (31) Une région rectangulaire, qui correspond au ROI, avec une dimension fixe et contenant la majorité de l'empreinte, est ensuite extraite.

Figure II.10: Extraction de la ROI à partir de l'image de doigt**.**

Enfin, nous pouvons constater que la méthode de localisation des axes X et Y, ainsi que la méthode d'extraction de la ROI, peuvent aligner efficacement les différentes images des doigts, en normalisant la zone qui fait l'objet des différents traitements pour extraire les caractéristiques biométriques du doigt. Ces opérations réduisent considérablement les variations causées par les différentes poses du doigt dans le système d'acquisition.

II.4. Extraction Des Caractéristiques

L'extraction des caractéristiques à partir de l'image de modalité (dans notre cas c'est FKP) représente une phase très importante pour concevoir un système d'identification efficace. Cependant, le choix de la méthode d'extraction des caractéristiques est basé sur trois informations essentielles à savoir la texture, les lignes et l'apparence de l'empreinte [13]. Donc, cette étape représente le cœur du système de reconnaissance, on extrait de l'image les informations qui seront sauvegardées en mémoire pour être utilisées plus tard dans la phase de décision. On distingue deux approches pour l'extraction des caractéristiques :

II.4.1. Extraction basé sur la texture

II.4.1.1 Descripteur de base LPQ (Local phase quantization) :

L'information de LPQ peut être extraite en utilisant la transformée discrète de Fourier à fenêtre à deux dimensions (2DWFT).

$$\sum_{\mathbf{m}\in\mathbf{Nxh}}(\mathbf{m}-\mathbf{x})\mathbf{f}(\mathbf{m})\mathbf{e}^{-\mathbf{j2\pi uTm}} = E_u^T f_x \qquad \textbf{(II.3)}$$

Ou $\boldsymbol{E_u}$, de taille=1xM2, est un vecteur de base de **2DWFT** avec la fréquence **u** , et **Fx**, taille = $M^2 \times N$ est un vecteur contenant les valeurs des pixels d'image dans **Nx** a chaque position **x**.

La fonction fenêtre**, h(x)** est une fonction rectangulaire.

La transformation est calculée a quatre valeurs de la fréquence, u = [u0, u1, u2, u3] ou u0= [a,], u1= [0,], u2 = [a,] et u3 =[a, $-$a]^T .

La valeur **a** est la plus haute fréquence scalaire pour laquelle Hui> 0. Ainsi, seuls quatre fonctions complexes comme un banc de filtres sont nécessaires pour produire huit images résultantes, composées de 4 images de la partie réelle et 4 images de la partie imaginaire de la transformée.

Chaque pixel de l'image complexe résultant peut-être code en une valeur binaire représentée dans l'équation (II.4) en appliquant (the quadrant bit coding) [32].

$$\mathbf{B}_{\mathbf{Ui}}^{\mathbf{Re}}(\mathbf{x}) = \mathbf{f}(\mathbf{x}) = \begin{cases} \mathbf{1}, si\ \mathbf{F}_{\mathbf{Ui}}^{\mathbf{Re}}(\mathbf{x}) > 0 \\ \mathbf{0}, si\ \ \mathbf{F}_{\mathbf{Ui}}^{\mathbf{Re}}(\mathbf{x}) \leq \mathbf{0} \end{cases} \mathbf{B}_{\mathbf{Ui}}^{\mathbf{Im}}(\mathbf{x}) = \begin{cases} \mathbf{1}, si\ \mathbf{F}_{\mathbf{Ui}}^{\mathbf{im}}(\mathbf{x}) > 0 \\ \mathbf{0}, si\ \ \mathbf{F}_{\mathbf{Ui}}^{\mathbf{im}}(\mathbf{x}) \leq \mathbf{0} \end{cases} \quad \textbf{(II.4)}$$

Ce procédé de codage attribue deux bits pour chaque pixel pour représenter le quadrant dans lequel se trouve l'angle de phase. En fait, il fournit également la quantification de la fonction de phase de Fourier. En général, LPQ est une chaîne binaire, présentée dans l'expression (II.5), obtenue pour chaque pixel par la concaténation des codes quadrant bits réelles et imaginaires des huit coefficients de Fourier de U_i

$$\boldsymbol{LPQ(X)} = \left[\boldsymbol{B_{U0}^{Re}(X), B_{U0}^{Im}(X), \ldots\ldots, B_{U3}^{Re}(X), B_{U3}^{Im}(X)}\right] \quad \textbf{(II.5)}$$

La chaîne binaire est convertie en nombre décimal par l'expression (II.6) pour produire une étiquette de LPQ. (La figure 31) résume l'ensemble de ces étapes.

$$\boldsymbol{LPQ(X)} = \left[\boldsymbol{B_{U0}^{Re}(X) + B_{U0}^{Im}(X) \times 2^{1} + \cdots + B_{U3}^{Re}(X) \times 2^{k-1} + B_{U3}^{Im}(X) \times 2^{k}}\right] \quad \textbf{(II.6)}$$

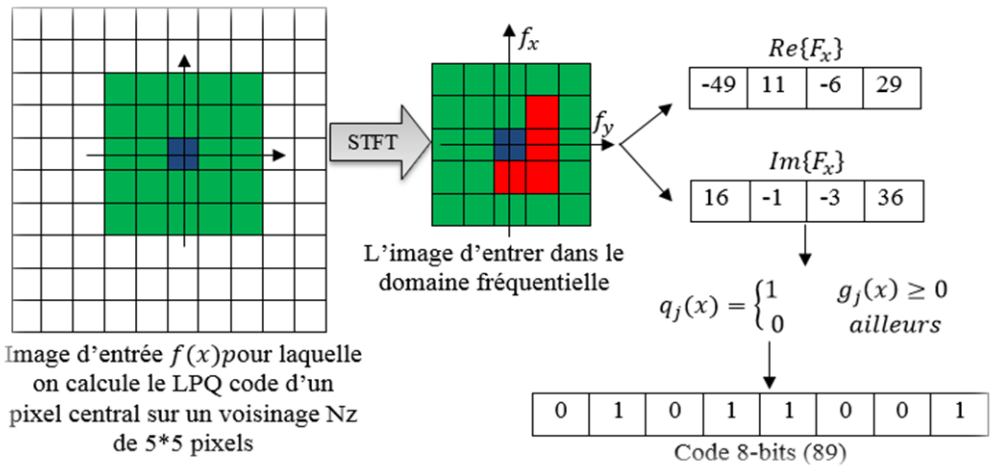


Figure II.11: Organigramme de l'ensemble des étapes nécessaire à la construction du descripteur LPQ.

II.4.1.2 GIST (global descriptor)

Dans le domaine de la vision par ordinateur, le descripteur GIST est une représentation d'une image en basse dimension qui contient suffisamment d'informations pour identifier une scène. Il a été introduit par les chercheurs Oliva et Torralba dans [33] dans le but d'une classification automatique des images. Ces deux auteurs ont défini le descripteur GIST de l'image en analysant les fréquences spatiales et les orientations. Il est issu d'une suite de travaux

de recherche à la fois psychologiques et informatiques sur la classification automatique de scènes. Il y a plusieurs présentations différentes de ce descripteur.

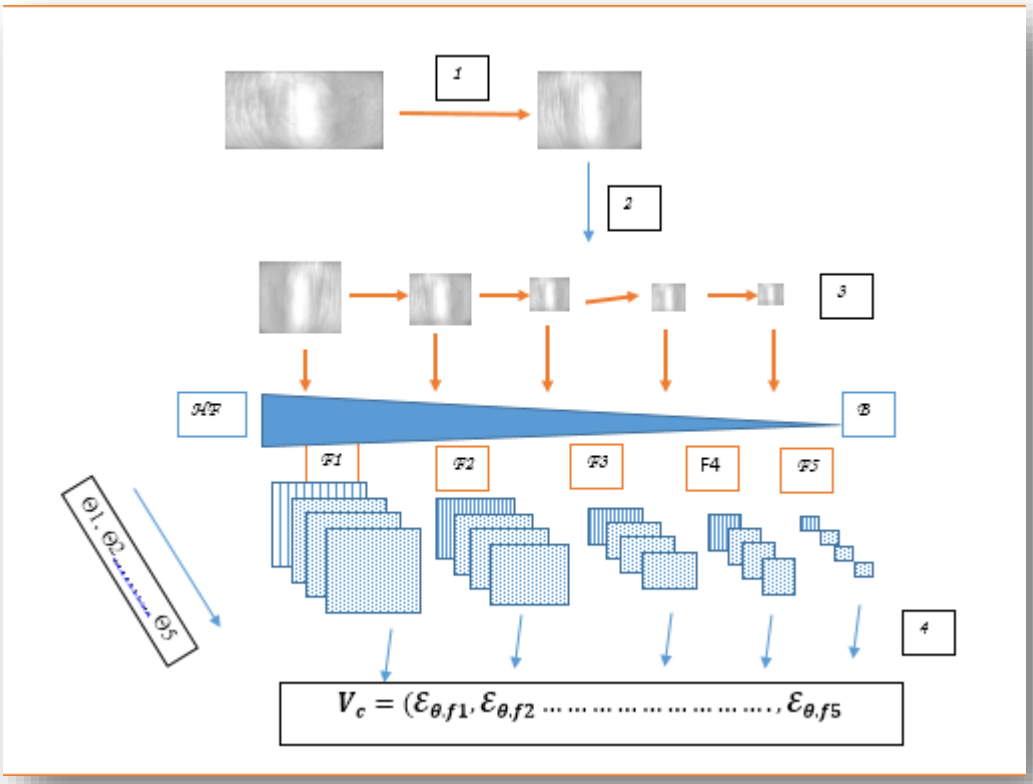


Figure II.12 : Principe du descripteur GIST.[33]

D'après Torralba et Oliva, le descripteur GIST peut être considéré comme une bonne solution pour des problèmes de catégorisation de scènes . Le succès du descripteur GIST s'est rapidement propagé vers d'autres applications, d'abord il a été réutilisé efficacement pour résoudre des problèmes de reconnaissance de lieux [35], ensuite il a été appliqué dans le domaine de la recherche d'image à l'échelle du web .

Le descripteur GIST se calcule suivant les étapes montrées dans la Figure (33) :

- D'abord, les images d'entrée sont réduites en imagettes carrées, d'une taille comprise entre 32x32 et 128x128, quelles que soient leur proportions.

- Ensuite elles sont convoluées avec un banc de filtres de Gabor avec $N\theta$ orientations et $N\sigma$ échelles.

II.4.1.3 Descripteur (monogenic binary coding) MBC:

Pour chacune des amplitudes, phase et composantes d'orientation de la représentation du signal monogénique, on peut avoir un code binaire monogénique (MBC). Nous désignons par MBC-A, MBC-P et MBC-O les cartes de code pour l'amplitude, la phase et orientation,

respectivement. À chaque emplacement, MBC-A, MBC-P et MBC-O sont formés en combinant les codes d'intensité d'imagerie et le code de variation locale comme suit :

$$\mathbf{MBC\text{-}A}(zc) = [CIx(zc), Cy(zc), CA(zc)]\mathbf{binary} \quad \textbf{(II.7)}$$

$$\mathbf{MBC\text{-}P}(zc) = [CIx(zc), CIy(zc), CP(zc)]\mathbf{binary} \quad \textbf{(II.8)}$$

$$\mathbf{MBC\text{-}O}(zc) = [CIx(zc), CIy(zc), CO(zc)]\mathbf{binary} \quad \textbf{(II.9)}$$

Tableau II.1: Le nombre de modèles dans les méthodes de codage MBC-X (X∈{A,P,O}), LBP et Gabor (par exemple, LGBP,HGPP et LGXP) lorsque les 8 plus proches voisins d'un pixel sont impliqués dans le codage.

Tableau II.1: Le nombre de modèles dans les méthodes de codage MBC-X [37]

Methode	**MBC-X**	**LBP**	**Méthodes de codage liées à Gabor**
Nombre de motifs	1024	256	256

On peut voir que lorsque les 8 plus proches voisins d'un pixel sont impliqués dans le codage à variation locale, chacun Le modèle MBC aura 10 bits. Ensuite, le nombre de modèles possibles pour chaque MBC est de 1024, ce qui est plus grand que celle des méthodes de codage binaire précédentes telles que LBP, LGBP, HGPP et LGXP (voir le tableau 2 s'il te plaît).

Plus il y a de motifs pour caractériser plus précisément la structure du signal local ; en même temps, il rendra également l'histogramme généré dans chaque sous-région un peu plus clairsemé. Cependant, cet histogramme plus clair peut encore avoir une capacité de discrimination suffisante (encore plus élevée) et donner de très bonnes performances FR (veuillez se référer à la section des résultats expérimentaux). [37]

Les trois cartes MBC ci-dessus peuvent être utilisées individuellement comme fonction de classification des images, et elles peuvent également être utilisées ensemble pour améliorer les performances FR.

II.4.2. Extraction basé sur le filtrage

II.4.2.1 Filtre de Gabor :

Pour les applications nécessitant une analyse par orientations, les fonctions de Gabor qui produisent une décomposition en ondelettes est très utilisée. De nombreuses applications en traitement d'images font appel à l'utilisation ces types des fonctions, comme par exemple

l'analyse de textures ou objets par attributs fréquentiels. En effet, les lignes de l'empreinte sont caractérisées par leur fréquence locale et leur orientation. En utilisant des filtres de Log Gabor, bien choisis, il est possible d'en extraire les caractéristiques biométriques. Cependant, lorsque ceux-ci sont correctement paramétrés, ils permettent de préserver les lignes et fournissent des informations sur l'orientation locale de la texture. Dans le domaine fréquentiel, la réponse f(G) de filtre log-Gabor 1D se définit comme :

$$\boldsymbol{f(G) = exp\left[\frac{-(\log\left(\frac{f}{f0}\right))^2}{2(\log\left(\frac{\sigma}{f0}\right))^2}\right]} \qquad \textbf{(II.10)}$$

Ou **f0** est la fréquence centrale et dénote la variance.

Pour l'application du filtre de Log-Gabor, il faut un choix empirique de paramètres de filtre (**f0 et σ**).Ces paramètres empiriques sont très difficiles à déterminer et c'est l'un des inconvénients des approches basées sur ce filtre [8].

II.5. La décision

La dernière étape dans le processus de reconnaissance est de déterminer l'identité d'une personne qui se base sur le degré de similitude entre les caractéristiques extraites et le(s) modèle(s) stocké(s) [39].

II.5.1 La Classification :

La classification est l'élaboration d'une règle de décision qui transforme les attributs caractérisant les formes en appartenance à une classe (passage de l'espace de codage vers l'espace de décision).Rappelons que la classification automatique est un processus qui permet de regrouper des données dans des ensembles ou classes tel que les éléments d'une classe aient les mêmes caractéristiques alors que la séparation entre les classes doit être totale. Pour réaliser une classification automatique, il existe plusieurs méthodes que le nous pouvons distinguer selon que le nous disposons de toutes les informations a priori sur les données. Dans ce cas, la classification automatique est dite supervisée.

Dans ce cas, les méthodes utilisées tentent d'apprendre à partir d'images étiquetées (pour les quelles la classe est connue), constituant un échantillon d'apprentissage, une fonction de classification. Cette fonction permettra d'associer une valeur de la classe de chaque image ou objet non étiqueté (non connu). Dans le cas où l'information n'est pas complète ou sans

information a priori, nous parlerons de classification non- supervisée.[40]

II.5.2 K nearest neighbors (KNN)

K plus proche voisins ou K- Nearest Neighbors (KNN) en Anglais est l'un des méthodes d'apprentissage supervisé le plus simple, utilisé pour résoudre des problèmes de classification et de la régression. Son fonctionnement est de classer les nouveaux points de données en fonction de la similarité aux points de données voisins [41].

KNN est un algorithme qui ne fait aucunes hypothèses sur la structure des données et de la distribution, ce qui signifie qu'il s'agit d'un algorithme non paramétrique. Il est également appel algorithme de l'apprenant paresseux, car il n'apprend pas immédiatement de l'ensemble d'apprentissage, mais stocke l'ensemble de données et, au moment de la classification, il exécute une action sur l'ensemble de données. KNN fonctionne par classification ou prédiction sur la base d'un nombre fixe (K) de points de données les plus proches de point d'entrée. Cela signifie que pour une valeur choisie de K, un point d'entrée serait classée ou devrait appartenir à la même classe que la classe la plus proche des nombre des points K voisins [42]. Voici une illustration simplifie est présentée dans la Figure 34 en-dessous.

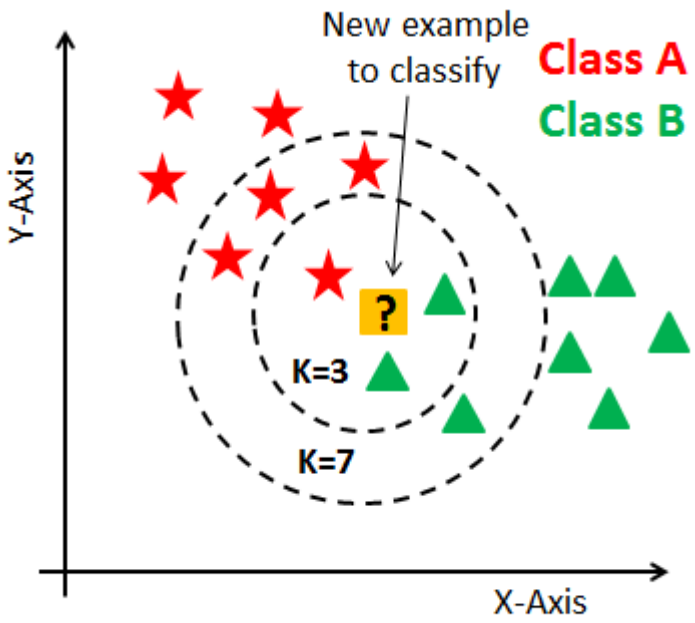


Figure II.13 : Fonctionnement de l'algorithme 'KNN'

II.5.2.1 Calcul de similarité dans l'algorithme KNN

L'algorithme K-NN a besoin d'une fonction de calcul de distance entre deux données. Pour en

faire Il existe plusieurs fonctions de distance à savoir : la distance euclidienne, Manhattan, …etc. le choix de la distance utilisée dans l'algorithme KNN dépond fortement de types des données en cours.

D'après les expérimentations, la distance euclidienne semble plus adéquate lorsqu'il s'agit des données de même type ainsi que pour les données quantitatives. De l'autre côté, la distance de Manhattan est une bonne mesure et qui peut-être appliquer sur des données de diffèrent type. En-dessous on va présenter les définitions de quelques distances les plus utilisées.

II.5.2.2 Les distances

La distance de Minkowski

Considérons deux vecteurs X = (x1, x2, ..., xN) et Y = (y1, y2, ..., yN), la distance de Minkowski d'ordre p notée Lp est définie par :

$$L_p = \left(\sum_{i=1}^{N} |x_i - y_i|^p\right)^{1/p} \quad \textbf{(II.11)}$$

la distance City-Block

Pour p = 1, on obtient la distance City-Block :

$$L_1 = \sum_{i+1}^{N} |x_i - y_i|^2 \quad \textbf{(II.12)}$$

La distance euclidienne:

Pour **p=2,** on obtienne la distance euclidienne qui calcule la racine de la différence carrée entre les coordonnées de la paire d'objets **:**

$$L_2 = \sqrt{\sum_{i=1}^{N} |x_i - y_i|^2} \quad \textbf{(II.13)}$$

II.6 Conclusion

la reconnaissance automatique de l'empreinte de l'articulation des doigts FKP est considérée comme un processus de reconnaissance de forme. Dans ce sens nous avons présenté les techniques de prétraitement de la modalité concernée et les techniques d'extraction de ses caractéristiques, ensuite on a abordé l'explication de la classification toutes en présentant quelques modèles de classifieur utilisé dans le processus de classification.

Chapitre III :
Résultats et discussions

III.1 Introduction :

Dans cette partie du mémoire, nous allons présenter notre étude expérimentale basée sur la reconnaissance de personnes par leurs empreintes des articulations des doigts en utilisant les méthodes : Filtre de Gabor, LPQ, Gist et MBC. Cette étude expérimentale est réalisée sur la base de données de PolyU [45], largement utilisée.

III.2 Environnement du travail

L'environnement matériel et le logiciel dans lesquels notre travail a été effectué est décrit comme suite :

III.2.1 Environnement matériel :

Les caractéristiques techniques de la machine utilisées dans la partie expérimentale de notre mémoire sont :

Tableau III.1 : Caractéristiques de la machine utilisée

Processeur	**Intel(R) Core (TM) i5-6300U CPU @ 2.40GHz 2.50 GHz**
RAM	8,00 Go
Disque dur interne	250 Go / SSD
Système d'exploitation	Windows 10 Professionnel 64 bits
Graphiques	Intel(R) HD Graphics 520

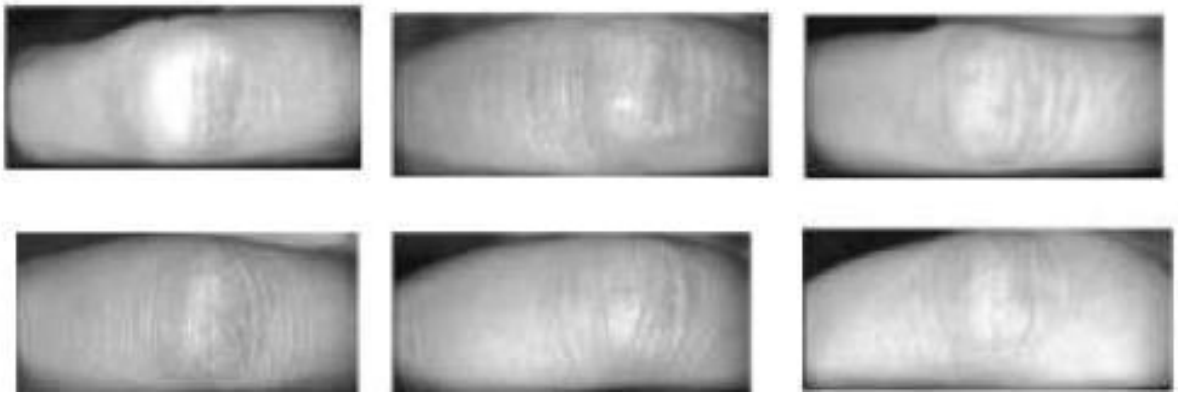
III.2.2 Logiciel MATLAB :

Entre 1970 et 1990, de nombreux programmes informatiques interactifs sont apparus sur le marché électronique, notamment le programme MATLAB, conçu par « Cleve Moler » à la fin des années 1970. MATLAB « Matrix Laboratory » est un langage de développement informatique spécialement conçu pour les applications scientifiques, utilisé pour développer des solutions nécessitant une puissance de calcul très élevée, et permettant d'effectuer de multiples simulations basées sur des algorithmes d'analyse numérique [9]. (Version utilisée 2021)

III.3 Description de la base de données :

La base de données PolyU FKP contient 7 920 images FKP collectées par 165 personnes volontaires dont 125 mâles et 40 femelles [44]. Ces images sont obtenues à au moyen d'un dispositif de capture FKP en temps réel élaboré par le Centre de recherche biométrique (UGC / CRC) de l'Université polytechnique de Hong Kong. Chaque personne est invitée de fournir 48 images en deux sessions séparées par un intervalle de temps d'environ 25 jours à partir de 4 doigts. Pour chaque session, la personne fournit 24 images pour chaque index gauche, majeur gauche, index droit et majeur droit. Par conséquent, la base de données PolyU FKP se compose

de 7 920 (165*48) échantillons de 660 (165x4) doigts différents. [45]



FigureIII.1: Exemple d'images de FKPs dans la base de données **PolyU** [45]

III.4 Structure da la base de données :

La base de données contienne plusieurs dossiers. Chaque dossier est nommé XXX-finger type représente l'identité de la personne. Par exemple « 001_left index ». Dans chaque dossier, les 6 premières images (01~06) ont été capturées lors de la première session et les 6 dernières images (07~12) lors de la seconde session. La base de données contient toutes les images FKP originales collectées avec le dispositif de capture FKP. En plus elle contient également les images ROI extraites en utilisant l'algorithme d'extraction de ROI décrit dans [44].

III.5 Protocole d'évaluation :

L'identification par l'empreinte FKP est une procédure de comparaison un contre plusieurs pour identifier une image FKP de test. Dans cette étude, nous avons sélectionné les premières n (n=2,....,6) images pour chaque doigt comme un ensemble d'apprentissage et nous avons utilisé le reste comme des images de test. Le Taux l'identification de rang a été calculé afin d'évaluer la performance d'identification de la méthode proposée.

III.6 Résultats expérimentaux sur le système monomodal :

Les performances de chaque doigt présenté dans cette expérience sont évaluées en utilisant les techniques proposées. Le taux de reconnaissance est calculé et présenté dans les tableaux indiqués en dessous.

Dans notre expérience, 6 images de la première session, de chaque modalité (LMF, RMF, LIF, RIF) sont utilisées dans la phase d'entrainement. Les autres 6 images de la deuxième session ont été utilisées dans la phase de test. Il y a donc un total de 990 images d'entrainement et 990 images de test.

III.6.1 Les résultats obtenus par la méthode Filtre de Gabor :

Variation de l'échelle et l'orientation:

Le filtre de Gabor est appliqué séparément sur chaque image FKP pour chacune des modalités. Nous avons varié la valeur de l'échelle et l'orientation du filtre Gabor afin de fournir les meilleurs taux de reconnaissance (TR) de système. Le Tableau III.2 présente Les résultats de cette expérience :

Tableau III.2 : Résultats obtenus pour différentes valeurs de l'échelle et de l'orientation.

Modalité Echelles/Orientation	LMF	LIF	RMF	RIF	Temps Moyen d'execusion
Echelle = 1 / Orientation = 2	51.11%	48.89%	61.21%	53.74%	38 sec
Echelle = 2 / Orientation = 3	73.03%	70.00%	73.43%	67.37%	1 min 10 sec
Echelle = 3 / Orientation = 5	84.95%	83.43%	83.64%	81.21%	2 min 21 sec
Echelle = 4 / Orientation = 6	90.61%	89.29%	88.69%	86.46%	3 min 28 sec
Echelle = 5 / Orientation = 7	92.32%	92.63%	90.51%	89.70%	4 min 45 sec
Echelle = 5 / Orientation = 8	93.54%	**94.44%**	92.02%	90.40%	5 min 53 sec
Echelle = 7 / Orientation = 9	**94.14%**	94.24%	**93.43%**	91.52%	8 min 25 sec
Echelle = 7 / Orientation = 10	93.84	94.14%	93.13%	91.62%	9 min 5 sec
Echelle = 8 / Orientation = 11	94.14%	94.34%	93.33%	**92.32%**	11 min 10 sec
Echelle = 8 / Orientation = 12	93.84%	94.04%	93.33%	92.22%	12 min 53 sec

Commentaires :

On observe d'après les résultats obtenus que les meilleures valeurs de l'échelle et de l'orientation soient respectivement : 5 et 8. Ces valeurs donnent un taux de reconnaissance de 94,44 % pour le doigt index gauche qui est meilleur par rapport aux autres valeurs.

Donc, les paramètres de filtre de Gabor qu'on a fixés sont : 5 échelles et 8 orientations.

Variation de la distance:

Différentes distances ont été employées dans la méthode proposée. Les résultats obtenus sont présentés dans le tableau III.3

Tableau III.3 : Résultats obtenus pour différentes méthodes de distance « Gabor ».

Modalité / Distance	LMF	LIF	RMF	RIF
Euclidean	91.92 %	91.52 %	88.79 %	87.78 %
Cosine	93.54 %	94.44 %	92.02 %	90.40%
Cityblock	89.80 %	91.11 %	88.08 %	87.78%
MahCos	**93.54 %**	**94.44 %**	**92.02 %**	**90.40%**

Commentaires :

On observe d'après les résultats obtenus que la meilleure méthode de calcul de distance est la méthode MahCosine qui donne un taux de reconnaissance de 94,44 % pour le doigt index gauche meilleur par rapport aux autres méthodes (Euclidien ou Cityblock).

Variation de la fréquence Fmax :

Nous avons varié la valeur de la fréquence fmax (paramètre de la fonction Filtre banc) afin de fournir les meilleurs taux de reconnaissance (TR) de système. Le Tableau III.4 présente Les résultats de cette expérience :

Tableau Ⅲ.4 **:** Résultats obtenus du TR pour différentes valeurs de Fmax.

Modalité Fmax	LMF	LIF	RMF	RIF
0.35	92.02%	93.74%	91.31%	**90.71%**
0.3	93.54%	93.84%	91.31%	**90.10%**
0.25	93.54%	94.44%	92.02%	**90.40%**
0.2	**93.03%**	**93.23%**	**91.92%**	**90.61**

Commentaires :

On observe d'après les résultats obtenus que la meilleure valeur de fmax soit 0,25. Cette valeur donne un taux de reconnaissance de 94,44 % pour le doigt index gauche qui est meilleur par rapport aux autres valeurs.

Variation de la valeur ‘ ni ’ netteté de l’axe Y :

Différentes valeurs de ni ont été employées dans la méthode proposée. Les résultats obtenus sont présentés dans le tableau III.5

Tableau Ⅲ.5 **:** Résultats obtenus du TR pour différentes valeurs de ni « Gabor ».

Modalité Ni	LMF	LIF	RMF	RIF
1	92.02%	92.93%	91.21%	89.09%
Sqrt(1.5)	92.73%	93.74%	91.62%	89.60%
Sqrt(2)	93.54%	94.44%	92.02%	90.40%
Sqrt(3)	93.23%	94.44%	92.32%	90.91%
Sqrt(4)	93.13%	93.84%	92.12%	91.31%

Commentaires :

On observe d'après les résultats obtenus que la meilleure valeur de ni est sqrt(3) qui donne un taux de reconnaissance de 94,44 % pour le doigt index gauche meilleur par rapport aux autres valeurs.

III.6.2 Les résultats obtenus par la méthode LPQ :

Variation de la valeur SIGMA:

Nous avons examiné plusieurs valeurs de Sigma pour comparer les taux de reconnaissances obtenus et fixé le meilleur taux. Les résultats des tests sont montrés dans le Tableau III.6.

Tableau III.6: Résultats obtenus pour différentes valeurs de Sigma.

Modalité Sigma	LMF	LIF	RMF	RIF
0.3	94.24%	94.14%	95.66%	93.43%
0.5	96.97%	97.27%	97.68%	96.57%
0.6	97.07%	97.37%	97.58%	96.67%
0.632	96.97%	**98.69%**	97.58%	96.67%
0.65	97.17%	97.88%	**98.18%**	96.36%
0.7	97.07%	97.47%	97.58%	94.95%

Commentaires :

On observe d'après les résultats que la meilleure valeur de Sigma est comprise entre [0.632 et 0,65] qui donne un taux de reconnaissance de 98,69% pour le doigt index gauche meilleur par rapport aux autres valeurs.

***Variation* de la distance:**

Différentes distances ont été employées dans la méthode proposée. Les résultats obtenus sont présentés dans le tableau III.7.

Tableau III.7 : Résultats obtenus pour différentes méthodes de distance « LPQ »

Modalité / Distance	LMF	LIF	RMF	RIF
Euclidean	96.06 %	97.47%	96.87%	95.56 %
Cosine	97.17 %	**98.69 %**	**98.18 %**	96.67 %
Cityblock	94.95%	95.35%	96.87%	95.25%
Mahcos	96.67%	98.38%	97.47%	96.67%

Commentaires :

On observe d'après les résultats que la meilleure méthode de calcul de la distance est la méthode « Cosine » qui donne un taux de reconnaissance de 98,69% pour le doigt index gauche, ainsi que cette méthode est meilleur par rapport aux autres méthodes (Euclidien ou Cityblock).

III.6.3 Les résultats obtenus par la méthode GIST :

***Variation* de la distance:**

Différentes distances ont été employées dans la méthode proposée. Les résultats obtenus sont présentés dans le tableau III.8

Tableau III.8: Résultats obtenus pour différentes méthodes de distance « GIST ».

Modalité / Distance	LMF	LIF	RMF	RIF
Euclidean	84.14%	83.43%	82.42%	78.79%
MahCos	**91.11%**	86.97%	87.47%	83.64%
Cityblock	88.99%	85.35%	85.76%	83.13%
Cos	80.81%	81.52%	80.10%	77.47%

Commentaires :

On remarque d'après les résultats obtenus que la meilleure méthode de calcul de distance est la méthode MahCosine qui donne un taux de reconnaissance de 91,11 % pour le doigt middle gauche et un taux de reconnaissance de 86.97% pour le doigt index gauche. Cette méthode de calcul de distance est meilleur par rapport aux autres méthodes (Euclidien ou Cityblock).

Variation de Nombre du bloc :

Dans cette phase, nous avons effectués plusieurs variations de nombre de bloc pour comparer les taux de reconnaissances obtenus et fixé le meilleur taux. Les résultats des tests sont montrés dans le Tableau III.9

Tableau Ⅲ.9 : TR obtenus pour différentes valeurs de N_{bre} du bloc« GIST ».

Modalité / Nbre Bloc	LMF	LIF	RMF	RIF
3	91.62%	89.39%	90.61%	**88.69%**
4	91.11%	86.97%	87.47%	**83.64%**
5	**79.49%**	**78.18%**	**80.10%**	**75.45%**

Commentaires :

On remarque d'après les résultats obtenus que l'utilisation de 3 ou 4 blocs dans la méthode proposée donne des taux de reconnaissances comprises entre 91,62 % et 91.11% pour le doigt middle gauche et un taux de reconnaissance entre 89.39 % et 86.97% pour le doigt index gauche.

Variation de échelle l'orientation par échelle :

Nous avons varié la valeur de l'orientation dans les paramètres de la méthode proposée afin de fournir les meilleurs taux de reconnaissance (TR) de système. Le Tableau III.10 présente Les résultats de cette expérience :

Tableau Ⅲ.10 : Résultats obtenus du TR pour différentes valeurs de l'orientation « GIST ».

Modalité / Orientation	LMF	LIF	RMF	RIF
8	91.62%	89.39%	90.61%	**88.69%**
7	91.31%	88.89%	89.70%	**87.98%**
6	**90.81%**	**86.16%**	**89.09%**	**86.67%**

Commentaires :

On observe d'après les résultats obtenus que la meilleure valeur de l'orientation soit la valeur 8. Cette valeur donne un taux de reconnaissance de 91,62 % pour le doigt middle gauche qui est meilleur par rapport aux autres valeurs.

III.6.4 Les résultats obtenus par la méthode MBC :

Variation de la valeur SIGMA:

Pour évaluer les performances de cette méthode. Nous avons examiné plusieurs variations de la valeur de Sigma afin de comparer les taux de reconnaissances obtenus et fixé le meilleur taux. Les résultats des tests sont montrés dans le Tableau III.11

Tableau III.11 : Résultats obtenus du TR pour différentes valeurs de Sigma « MBC ».

Modalité Sigma	LMF	LIF	RMF	RIF
0.5	98.59%	98.18%	99.39%	98.48%
0.6	98.59%	98.28%	99.19%	97.58%
0.632	**98.59%**	98.08%	**99.39%**	**98.48%**
0.65	98.28%	98.69%	99.29%	98.38%
0.66	97.88%	**98.79%**	**99.39%**	98.18%
0.7	98.08%	98.08%	98.99%	98.28%

Commentaires :

On observe d'après les résultats que la meilleure valeur de Sigma est comprise entre [0.632 et 0,66] qui donne un taux de reconnaissance de 99,39 % pour le doigt middle droit meilleur par rapport aux autres valeurs.

Variation* de la distance *:

Différentes distances ont été employées dans la méthode proposée. Les résultats obtenus sont présentés dans le tableau III.12

Tableau 12 : Résultats obtenus du TR pour différentes méthodes de distance « MBC ».

Modalité / Distance	LMF	LIF	RMF	RIF
Euclidean	97.47%	97.68%	98.99%	97.37%
Cosine	**98.59%**	**98.79%**	**99.39%**	**98.48%**
Cityblock	96.87%	96.87%	98.48%	96.46%
Mahcos	98.28%	98.59%	99.29%	98.28%

Commentaires :

On observe d'après les résultats que la meilleure méthode de calcul de la distance est la méthode Cosine qui donne un taux de reconnaissance de 99,39 % pour le doigt middle droit, ainsi que cette méthode (Cosine) est meilleur par rapport aux autres méthodes (Euclidien ou Cityblock).

III.6.5 Comparaison entre notre travail et les travaux existants dans la Littérature :

Tableau III.13 : comparaison entre notre travail et des travaux existes.

	LMF (%)	LIF (%)	RMF (%)	RIF (%)
GABOR	93.54	94.44	92.32	91.31
LPQ	96.97	98.69	98.18	96.67
GIST	91.62	89.39	90.61	88.69
MBC	98.59	98.79	99.39	98.48
Réf [70]	82.48	92.64	85.92	88.26
Réf [71]	88.59	89.90	88.48	89.49

Conclusion :

Dans ce chapitre, nous concluons a partir les résultats obtenus que l'approche appliquée d'identification biométrique en utilisant les articulations des doigts (FKP) avec des algorithmes LPQ, GABOR, MBC et GIST soit tres efficace pour obtenu un taux de reconnaissance très fiable .

Les résultats ont été considérablement améliorée via le choix des modalités et avec les variations des différents paramètres des algorithmes tel que : la distance, sigma, orientation et l'échelle. En remarque que les meilleurs résultats sont obtenus par la valeur de SGMA=0.632 pour de la méthode LPQ+Cosine et SGMA= [0.632 et 0,66] pour de la méthode MBC+Cosine.

Conclusion generale

Conclusion générale

La biométrie est un domaine à la fois passionnant et rigoureux. Elle utilise, des outils mathématiques souvent très développés, pour identifier et reconnaître des individus, nous obligeant à travailler dans un contexte d'immense diversité. Cette diversité se manifeste également dans beaucoup d'algorithmes qui ont été mis pour la reconnaissance par l'empreinte d'articulation de doigts.

Notre travail consiste à construire un système biométrique pour la reconnaissance des individus par ses empreintes d'articulation (FKP). Les algorithmes LPQ, MBC et GIST sont utilisés pour extraction des caractéristiques de FKP images. L'algorithme KNN avec les différentes distances ont été utilisé dans le module de comparaison. Les comparaisons des différents résultats par ses algorithmes (LPQ, MBC et GIST) ont été faites dans ce travail. De cette étude, nous avons conclu, sur la base de nos résultats, qu'il existe de bons résultats et jugés satisfaisants, en particulier pour l'algorithme LPQ avec la valeur SIGMA =0632 un taux de reconnaissance 98.69% et pour l'algorithme MBC avec l'utilisation de distance COSINE un taux de 99.39%. Cette étude a permis la validation et l'évaluation des performances de la technique présentée.

Comme perspectives, nous suggérons aux futures promotions de faire des études et des travaux de simulation sur d'autres modalités biométriques utilisant différentes technique de classification comme CNN et des autres algorithmes, et de faire une conception finie par une réalisation d'un système biométrique bénéfique par exemple pour le contrôle des accès aux locaux de notre faculté.

Bibliographies

[1] Chakour Alla Eddine, Identification Biométriques des Personnes par les Empreintes d'Articulation du Doigt. Université Badji Mokhtar Annaba, Mémoire de Master en Electronique, 2019.

[2] Arun A. Ross, K. Nandakumar and A. K. Jain, "Handbook of Multibiometrics", Springer Science+Business Media, LLC, New York, 2006.

[3] A.O.LAZOUL et I. CHETIOUI, Identification Des Personnes Par Utilisant Un Descripteur De Texture, Universite Kasdi Merbah Ouargla, Mémoire de Master en Electronique, 2017.

[4] Lin Zhang, Lei Zhang, and David Zhang, "Finger-Knuckle-Print Verification Based on Band-Limited Phase-Only Correlation", CAIP 2009, LNCS 5702, pp. 141-148, 2009

[5] A. AMROUN et M. S. AMRAOUI, Identification des personnes par système multimodale, Université Kasdi Merbah Ouargla, Mémoire de Master en Electronique, 2018.

[6]Personal Identification Based on Single Knuckle-print Image", AsiaPacific Conference on Information Processing, APCIP, 2009.

[7] S. Boudjellal, " Détection et identification des personnes par méthode biométrique", Thèse de Magister, Université Mouloud Mammeri, Tizi-Ouzou.2012.

[8] LEMMOUCHI Mansoura, Reconnaissance Biométrique par Fusion Multimodale, Thèse de Doctorat de l'Université Batna 2 – Mostefa Ben Boulaïd, 2020.

[9] Pierre Bonazza. Système de sécurité biométrique multimodal par imagerie, dédié au contrôle d'accès, Thèse de Doctorat de l'établissement université Bourgogne Franche-Comté, 2019.

[10] A.K. Jain, L. Hong and S. Pankanti, « Biometrics: Promising Frontiers for Emerging Identification Market », Comm. ACM, pp. 91-98, February. 2000.

[11] GASMI Lynda. Deep Learning for face Recognition, Universite Mohamed Boudiaf - M'Sila, Mémoire de Master en informatique, 2020.

[12] F. Z. MAHDI et F. TABI. Caractérisation d'empreinte de l'articulation de doigt pour l'authentification des personnes, Université Mohamed Boudiaf - M'Sila, Mémoire de Master en Génie Electronique, 2019.

[13] BENAGGA Abderahmane , TELIB Lina « Reconnaissance des personnes basée sur l'empreinte de l'articulation de doigt » mémoire de master université KASDI MERBAH OUARGLA .2016.

[14] MERAOUMIA, Abdallah, CHITROUB, Salim, et BOURIDANE, Ahmed. "Fusion of finger-knuckle-print and palmprint for an efficient multi-biometric

system of person recognition". In : Communications (ICC), IEEE International Conference.2011.

[15] F .Douali, Identification biométrique des personnes par les veines des doigts, Universite Badji Mokhtar Annaba, Mémoire de Master en Télécommunication, 2019.

[16] AWARE, Livre Blanc, WP_WhatareBiometrics_0114_v01, Document en PDF Téléchargé le 24 Février 2022.

[17] Diallo.N « La reconnaissance des expressions faciales », Thèse de Master en informatique, Université 8 Mai 1945 de Guelma, 2019

[18] ZHU Le-qing, « Finger knuckle print recognition based on SURF algorithm » , Eighth International Conference on Fuzzy Systems and Knowledge Discovery (FSKD),IEEE, 2011.

[19] CNIL, Communication de la CNIL relative à la mise en œuvre de dispositifs de reconnaissance par empreinte digitale avec stockage dans une base de données, Document en PDF Téléchargé le 27 Février 2022.

[20] Anis CHAARI, "L'identification dans les bases de données biométriques basée sur une classification non supervisée", Nouvelle approche Pour obtenir le diplôme du doctorat, Université d'Evry-Val d'Essonne, 2009

[21] N. MORIZET, Reconnaissance Biométrique par Fusion Multimodale du Visage et de l'Iris, École Doctorale d'Informatique, Télécommunications et Électronique de Paris, 2009.

[22] Mohamad El-Abed, Évaluation de système biométrique, Thèse de Doctorat de l'Université de CAEN/BASSE-NORMANDIE, 2011.

[23] D.L. Woodard and P.J. Flynn, « Finger surface as a biometric identifier ».CVIU, vol. 100, pp. 357–384, 2005.

[24] C. Ravikanth and A. Kumar, « Biometric Authentication using Finger-Back Surface », CVPR'07, pp. 1-6, 2007.

[25] A. Morales et al, « Improved finger-knuckle-print authentication based on orientation enhancement », electronics letters, Vol. 47 No. 6 , 17th March 2011.

[25] YANG Wankou, « Finger-Knuckle-Print Recognition Using Gabor Feature and OLDA » Proceedings of the 30th Chinese Control Conference, Yantai, China, July 22-24, 2011.

[26] Zahra S. Shariatmadar, Karim Faez, « A Novel Approach for Finger-Knuckle-Print Recognition Based on Gabor Feature Fusion » ,4th International Congress on Image and Signal Processing, IEEE, 2011.

[27] Guangwei Gao and Jian Yang, « Weight Competitive Coding for Finger-Knuckle-Print Verification » pp. 185–192, Springer International Publishing Switzerland, 2013.

[28] Chetana Hegde et al, « Authentication using Finger Knuckle Prints », Springer-Verlag London, 2013

[29] Harbi AlMahafzah et al, « Multi-Algorithm Decision-Level Fusion Using Finger-Knuckle-Print Biometric ».Springer India 2014.

[30] BENOUAER Soumia, TAHRINE Aichouche. « Système biométrique basé sur les motifslocaux binaires orientés (LBP) ».université Kasdi merbah Ouargla, 2016.

[31] Julie M. Gauthier, Cadre juridique de l'utilisation de la biométrie au Québec : sécurité et vie privée, Université de Montréal, Centre de recherche en droit public Faculté de Droit, 2014.

[32] OUAMANE Abdelmalik « Reconnaissance Biométrique par Fusion Multimodale du Visage 2D et 3D » Thèse de doctorat.Université Mohamed Khider, biskra 2015.

[33] A. BOHI. « Descripteurs de Fourier inspirés de la structure du cortex visuel primaire humain », these de doctorat.universite de toulon.2017.

[34] https://www.math.univ-toulouse.fr/~besse/Wikistat/pdf/st-m-Intro-ApprentStat.pdf.

[35] BRIK Youcef « Reconnaissance des chiffres Manuscrits par les Modèles de Markov Cachés Continus » mémoire de magister université des sciences et de la technologie Houari Boumediene 2010.

.[37]A.chouchane. « analyse d'image d'expression faciales et orientation de la tete base sur la profendeur »,these doctorat en informatique ,université de biskra .2016.

[38] Belahcen. M « Système de reconnaissance de visage », Thèse de Master en informatique, Université de Biskra, juin 2013.

[39] M. Amraoui et al, "Finger-Knuckle-Print Recognition Based on Local And Global Feature Sets", Journal of Theoretical and Applied Information Technology 15th December 2012. Vol. 46 No.1.

[40]T.mensink, " distance-based image classification generalizing to new classes at near-zero cost". IEEE publication .2013.

[41] Z. hanen- B. ichrak, « Classification du diabète avec l'algorithme KNN ».these master en informatique,b.b.arridej.2021.

[42] https://datascientest.com/knn.

[43] https://www.mathworks.com/matlabcentral/fileexchange/35106-the-phd-face-recognition-toolbox. (Février 2022)

[44]M.chaa, « système de reconnaissance de personne par des techniques biométriques ».these doctarat ,setif.2017.

[45] http://www4.comp.polyu.edu.hk/~csajaykr/IITD/iitd_knuckle.htm. (Mars 2022)

[46] S.Altaher* and S. Taha " Personal authentication based on finger knuckle print using quantum computing ». Int. J. Biometrics, Vol. 9, No. 2, 2017.

[47] SHARIATMADAR, . An efficient method for fingerknuckle-print recognition by using the information fusion at different levels. In: Hand-Based Biometrics (ICHB), International Conference on. IEEE, 2011.