الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي

UNIVERSITÉBADJI MOKHTAR-ANNABA
BADJI MOKHTAR– ANNABAUNIVERSITY

جامعة باجي مختار – عنابـــــــــة

Faculté : Science de l'ingénieur
Département : Électronique
Domaine : Sciences et techniques
Filière : Electronique
Spécialité : Instrumentations

Mémoire

Présenté en vue de l'obtention du Diplôme de Master

Thème:

Identification des personnes à l'aide du réseau veineux du doigt

Présenté par : *LAHMER Aissa*
MELLIHI Zakaria

Encadrant : *AMARA Fethi*MCBUBMA

Jury de Soutenance :

BOUSBIA Salah Mounir	PROf	UBMA	Président
AMARA Fethi	MCB	UBMA	Encadreur
AIT IZEM Tarek	MCB	UBMA	Examinateur

AnnéeUniversitaire : 2019/2020

DEDICACE

Je dédie ce modeste travail à mes chers parents, sans eux ce mémoire n'aurait jamais existé « merci de m'avoir permis de vivre ça »

Remerciement :

Je remercie dieu qui m'a donnée la force et la patience pour concrétiser ce travail.

Je tiens à remercier très chaleureusement Dr. AMARA Fethi, mon directeur de recherche pour son écoute, son effort, et ses précieux conseils tout au long de ce travail.

J'adresse aussi mes remerciements aux membres de jury de m'avoir pris la peine de lire et juger mon travail.

Je tiens à saluer tous mes collègues et amis pour leurs conseils prodigués et leurs encouragements.

Je remercie de tout cœur toute ma famille ; qui ont su trouver les mots pour me motiver et me donner la confiance pour réaliser mon travail de recherche.

Finalement, je tiens à remercier infiniment toutes les personnes qui m'ont aidé de prés et de loin.

….Merci

ملخص :

هذا العمل يهدف إلى تقديم نظام تعرف على الأفراد(FVR)، يعتمد على ميزة بيومترية حديثةالاستعمال في مجال التعرف على الأشخاص وهي« عروق الإصبع»

من خلال هذا البحث قمنا بتطبيق ثلاث معلمات مميزة, (LPQ, LBPhist, LPB)وهذا من اجل تحديد افضل مميز للفصل بين الاشخاص. وقد استعملنا المصنف K-NN ,في مرحلة التمرن . تم تطبيق هذا النظام على قاعدتي بيانات عروق الأصابع,FV_USMوSDUMLA .

النتائج المتحصل عليها تبلغ 99,97%كما تبلغ 100%عند استعمال خوارزمية CLAHE

كلمات مفتاحيه:نظام تعرف، ميزة بيومترية،التعرف على الأشخاص،معلمات ومميزة،قاعدتي بيانات،معادلة الرسم البياني ، معالجة أولية,المصنف KNN.

Résumé :

Ce travail vise à présenter un système de reconnaissance des individus qui se base sur un caractère biométrique récemment utilisé dans le domaine d'identification, à savoir « la veine du doigt ».

L'objectif de ce travail est de trouver les paramètres caractéristiques permettant de donner une meilleure discrimination entre les individus. Nous avons établis une étude comparative entre les trois paramètres: LPB,LPQ et l'histogramme de LPB.Ces paramètres ont été utilisés pour entrainer le classificateur K- plus -proche voisins (KNN). Notre système est évalué sur deux différentes bases de données (FV_USM et SDUMLA_HT).

Le taux de reconnaissance atteint 99.97 % en utilisant LBPhist, et il atteint 100% en utilisant l'algorithme CLAHE

Mots clés : Systèmesbiométriques, LPB, LPQ, K-plus proche voisin KNN.

Abstract :

This research paper is an attempt to present a system of recognition of individuals .It is based on a biometric characteristic that is recently used in the domain of identification, which is « Finger Vein».

The objective of this work is to find the more significate parameters giving the best discrimination between individuals. In order to establish a comparative study, three parameters are used LPB, LPBhist, and LPQ. Those parameters are used to train the K-NN classifier. (K nearest neighbors). Two dataset are used; FV-USM and SDUMLA_HT.

Simulation show that the recognition rate can attain 99,97% using LBP hist, and it attains 100% when CLAHE algorithm is used.

Key words: FingerVein Recognition FVR,biometric system, LPB, LPQ, K-voisinsplus proches.

Table des matières :

Chapitre 2 : Système de reconnaissance de la veine du doigt FVR

Chapitre 3 : Résultat et discussion

Liste des figures :

Liste des tableaux :

Liste des abréviations :

PIN : Personal identification Number

ADN : Acide Désoxyribose Nucléique.

FVR : FingerVein Recognition.

ROI : Région Of Intrest.

LPB :Méthode Binaire Locale.

LPQ : Quantification de la Phase Locale.

CLAHE: Contrast Limited Adaptive Histogram.

SVM : Machine à Vecteurs de Support.

KNN:K-Nearest Neighbor.

IRM: Imageries par RésonanceMagnétique.

IBG: International Biometric Group.

PDA: PersonalDigital Assistant.

FIDO: Fast identification Online.

TCAC: Taux de Croissance Annuel Composé.

APAC: AsiéPacifique.

ROW: Rest of World.

AFIS: Automatic Flight Information Service.

Introduction générale :

Ces dernières années, avec la révolution technologique que le monde a connue et l'explosion deréseaux informatiques, la plupart des transactions et des échanges d'informations entre les sociétés internationales et le public, est devenue via le réseau informatique. Elle se fond, particulièrement, sur l'intelligence artificielle de contrôle d'accès. En effet, le besoin de protéger ses sociétés et la vie privé du public devient de plus en plus un souci majeur qui exige une identification précise des personnes, notamment contre l'augmentation des méthodes de fraude, d'espionnages et surtout du piratage des systèmes d'accès.

Malgré l'existence des techniques de sécurité et de contrôle d'accès: code PIN, mot de passe, badge…, elles demeurent classiques et insuffisantes,car elles présentent des lacunes facilitant le vol d'identité. Dans le but de pallier certaines failles inhérentes à ces systèmes, les spécialistes représentants de ce domaine ont réussi à développer une technique qui est apparue au 19èmesiècle, à savoir la biométrie.

La biométrie c'est une technique qui détermine l'identité des individus ; elle est fondé sur la mesure de leurs caractéristiques: physiologique (l'empreinte digitale, l'iris, visage, géométrie de la main, réseau des veines…), comportementale (la voix, la démarche, la signature…) ou biologique (ADN). Dès l'émergence des systèmes d'identification biométrique, sa demande par les sociétés modernes est en perpétuelle croissance.Cela revient à sa performance supérieure et le niveau haut de la sécurité que ces systèmes garantissent. Ce qui a contribué, de ce fait, à diminuer le recours aux systèmes d'authentifications traditionnelles.

Aujourd'hui la biométrie c'est l'une des nouvelles technologiques qui occupe une place importante dans les diverses applications de la vie quotidienne tels que : le contrôle d'accès sécurisé, le passeport, applications policiers, payement électronique, etc. La biométrie fait également appel aux outils médicaux dans l'opération d'authentification des individus, et ce à partir des trais inaccessibles : motif cerveau, la texture de l'OS, les impulsions cardiaque, etc. C'est ce qu'on appelle '' la biométrie caché'' : ce type est en cours d'exploration et constitue une préoccupation primordiale des chercheurs criminalistiques.

Dans le cadre de ce travail, nous nous sommes concentrées sur un caractère physiologique, à savoir le motif vineux du doigt, ce caractère biométrique est récemment découvert pour une meilleur identification des personnes, le système de la reconnaissance de veine du doigt **FVR** (FingerVein Recognition) a été développé et utilisé pour la première fois au japon, et elle a connu un grand succès dans les entreprises financières japonaises. Le modèle biométrique de veine du doigt, contrairement aux autres modalités biométriques tels que : l'empreinte digitale, visage,.., se cache sous la surface de la peau ce qui fait de lui un modèle invisible, et c'est cette dernière propriété qui renforce son niveau de sécurité (la difficulté de reproduire ou falsifier).

Actuellement les systèmes de FVR deviennent une technologique prometteuse pour les gestions d'identités dans des applications distinctes: contrôle aux frontières, carte de crédit, guichet automatique …etc.

Dans le premier chapitre, nous présentons la définition des notions de base et la biométrie, le principe de fonctionnement des systèmes biométriques (généralités sur la biométrie et système biométrique), les critères d'évaluation des performances des systèmes biométriques, le domaine d'application et les lacunes des modalités biométrique, et enfin nous parlons de marché biométrique.

Dans le deuxième chapitre, nous présentons les éléments principaux de fonctionnement du système de reconnaissance de veines du doigt, tels que : processus d'acquisition et de prétraitement, extraction la région d'intérêt. Nous allons voir les différentes approches d'extraction des caractéristiques et on définit quelques paramètres (Algorithme) appartenant à ces approches: le motif binaire locale LPB, la quantification de la phase locale LPQ. Nous définissons aussi la méthode de classification K- voisins plus proches.

Dans le troisième et le dernier chapitre ''Résultats et discussions'', nous réalisons une simulation sur Matlab pour tester et comparer les performances des 3 algorithmes d'extraction caractéristiques appliqués sur deux bases de données de motif vineux de doigt , et nous testons l'influence de la méthode d'égalisation de l'histogramme adaptée à contraste limité CLAHE sur le taux de reconnaissance.

Finalement, nous clôturons par une conclusion générale en se référant aux résultats obtenus et nous donnons, parallèlement quelques perspectives sur les travaux futurs.

Chapitre 1

Généralités sur la biométrie.

1.1.Introduction :

Aujourd'hui, avec l'augmentation de la communication internationale et la croissance des transactions à l'échelle mondiale tels que :les échanges commerciales entre les pays les transactions bancaires, financières et les manifestations internationales sportifs (olympiade), l'identification des êtres humains devienne une préoccupation majeur pour l'évaluation des réglementations internationales en terme de sécurité, notamment pour le contrôle d'accès aux frontières, le vol de l'identité et la réduction de la cyber criminalité.

De ce fait, les méthodes des identifications traditionnelles (code PIN, mot de passe, badge ….etc.) deviennent insuffisantes, du fait qu'elles présentent de plusieurs risques (le vol, l'oubli, la duplication, perte…..etc.) ce qui a diminué son utilisation. Dans le but de surmonter ces obstacles et répondre aux lacunes de ces méthodes classiques, les chercheurs ont met en œuvre des nouvelles technologies, qui représententl'ensemble de systèmes électroniques assurant l'identification/authentification automatiques des personnes de manière fiable et plus rapide, et ce en fonction de ses propres caractéristiques : morphologiques (empreinte digitale, l'iris, visage, réseaux de veines ….etc.), Biologiques(ADN) et comportementales (démarche, signature, la voix, on appelle ces nouvelles technologies « la biométrie ».

1.2 Généralités sur la biométrie :

1.2.1Définition :

Le terme biométrie est issu d'une combinaison de deux mots grecs « **bio** » signifie la vie « **métrie**» signifie la mesure.

D'après Roethenbagh *''La biométrie s'applique à des particularités ou des caractères humain unique en leur genre est mesurables, permettant de reconnaitre ou de vérifier automatiquement l'identité »* [4].

Donc la biométrie c'est la science qui permet l'exploitation des caractéristiques physiques (empreinte digitale, l'iris, les veines, etc.), comportementales (démarche, la voix, la signature, etc.) ou biologiques (ADN) mesurables d'humain dans des systèmes électroniques intelligents pour l'objectif de l'identification/authentification automatiques des personnes, on appelle ces systèmes « les systèmes biométriques)[3].

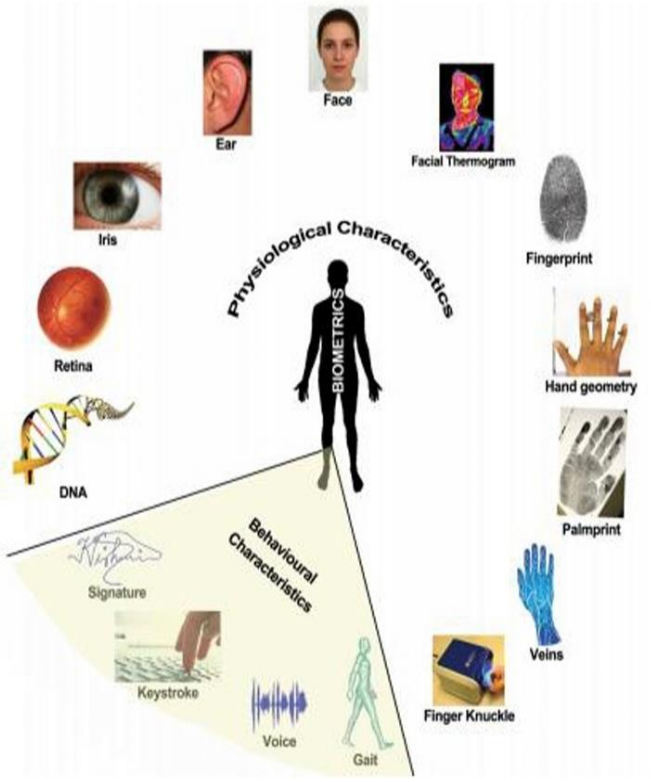


Figure1.1 : Déférentes modalités biométriques.

1.3 Modalités Biométriques :

Les modalités biométriques renvoient à l'ensemble des caractéristiques qui sont propres et spécifique à chaque personnes aux monde, et qu'on peut à partir desquelles vérifier l'identité des individus. De manière générale, il ya trois catégories de modalités biométriques : physiques, Comportementale, biologique [5] **Figure (1.2) :**

1. La biométrie morphologique (physique): se base sur l'analyse des trais physiques liées aux personnes (empreinte digitale, l'iris, visage, géométrie de la main réseaux de veines…etc.).

2. La biométrie comportementale : cette catégorie se base sur l'analyse des comportements des personnes (la voix, signature, démarche….etc.).
3. La biométrie biologique : se fond sur l'analyse des caractéristiques biologiques (ADN : salive, odeur.. etc.).

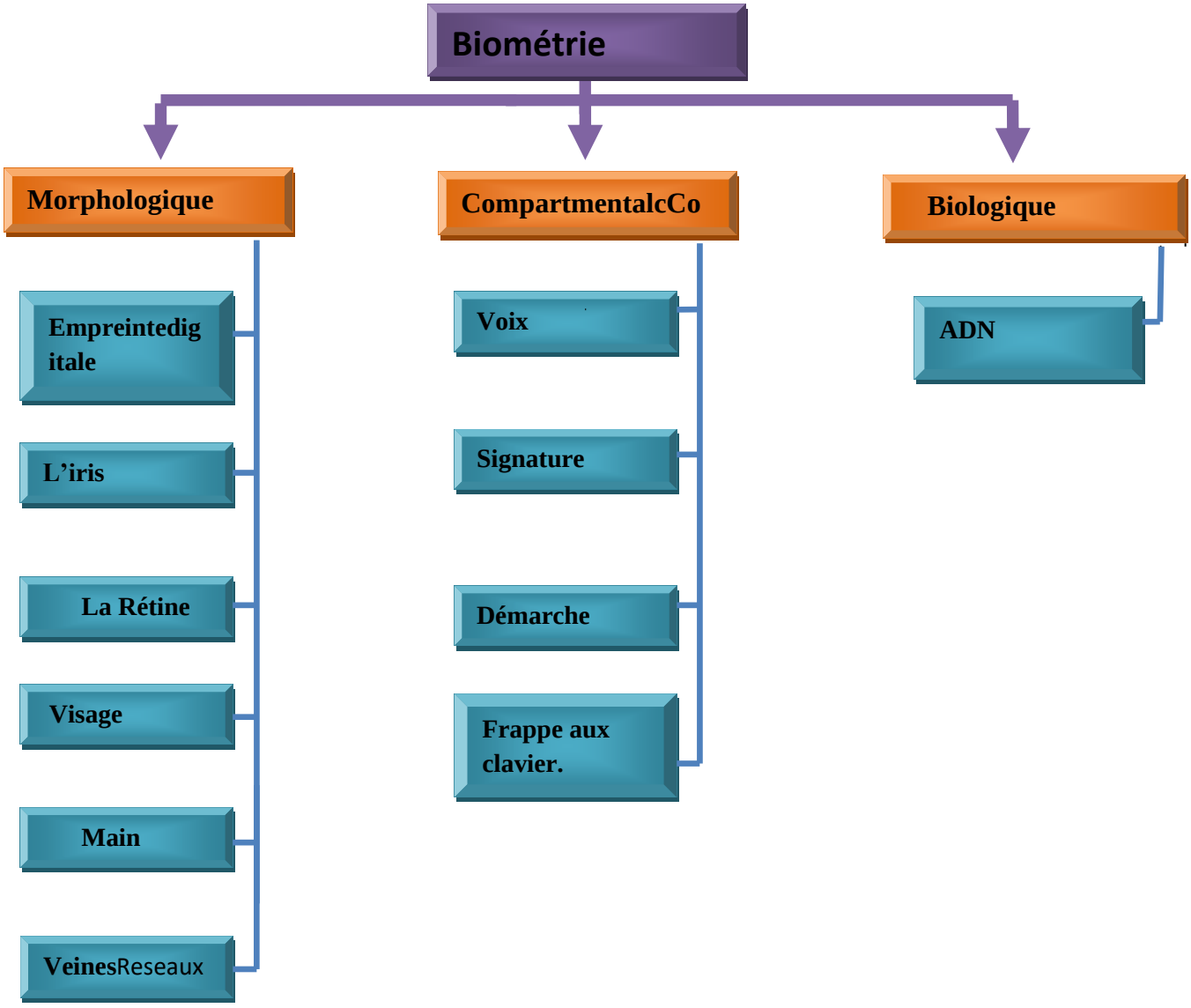


Figure1.2 : Différentes modalités biométriques

1.3.1 Biométrie morphologique :

a. Empreinte digitale :

La surface au bout des doigts de l'être humain se forme des extrémités intérieures « vallées » et des extrémités latérales « crêtes », ces deux composants (vallées et crêtes) sont

nommés « empreinte digitale ». Depuis plus de 100 ans les policiers utilisés le motif d'empreinte digitale comme une technique d'identification des criminelles.

Aujourd'hui la reconnaissance par l'empreinte digitale est la plus utilisée, notamment dans le domaine policier et judiciaire. Cela revient à son efficacité et sa facilité quant à l'usage. En effet, l'empreinte digitale est unique pour chaque personne : laprobabilité de rassemblement de deux empreinte est une fois pour 64 milliards,cette ressemblance est moins présente même entre les empreintes desdoigts d'une personne identique. Ils existent trois grands types de motif d'empreintes :

- **Boucle : Les** lignes de replient sur elle-même à travers la gauche ou à travers la droite formant des bifurcations.C'est le motif le plus courant.
- **Spirales :** Les lignes d'enroulement autour d'un point en formant une espèce de tourbillon.
- **Arc :**Les lignes sont disposés les unes au-dessus des autres et forment un ''Arc'' le motif le plus rare.

➢ **Avantages :**

- Technique plus fiable et inchangeable: à partir d'un petit nombre de minutes le système est capable d'identifier une empreinte parmi plusieurs millions d'échantillons
- Facile à utiliser.
- Rapidité de traitement et taille de lecteur peu volumineuse.
- Moins cher.

➢ **Inconvénients :**

- L'obligation du contact direct.
- la saleté constitue un obstacle au niveau du lecteur d'empreinte.
- la fiabilité de l'identification dépend de la qualité de l'image.

b. Iris :

L'iris est la partie la plus intérieur de tunique vasculaire qui contient un disque avec un trou centrale '' la pupille'' ; lorsque on observe un œil nous pouvons constater que l'iris c'est la zone colorée (la couleur de

l'œil dépend de l’iris).

La reconnaissance de l'iris c'est l'application biométrique la plus fiable (côté résultat), car elle recueille nombre infinid'informations.

L’acquisition de l’iris s'effectué à l'aide d'unecamera pour pallier le mouvement indépendant de la pupille.

- **Avantages**

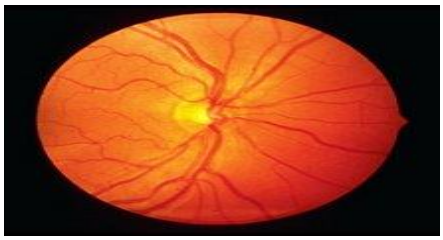
  - Le nombre important des informations qu’on peut extraire.
  - La fiabilité des résultats permet le passage de l’identification àl’authentification.

- **Inconvénients :**

  - Technique difficile à mettre en œuvre dans le marché.
  - Nécessite des dispositifs plus chers.
  - L’obstacle de l’utilisation à chaque fois scanné l’œil

c. La rétine :

La rétine est la cloison interne et opposée de l’œil formée de tissue nerveux « réseaux nerveux» avec une structure très complexe. Elle contient des cellulesde vision appelées « photo réceptrice », qui capte la lumière et transforme en impulsion nerveuse.



La rétine tapissée par un réseau sanguin, qui forme un motif unique pour chaque individu.La technique de la rétine basé sur l’émission de faisceaux lumineux à travers de l’œil de l'utilisateur jusqu’à éclairer le fond. L’image de réseaux veineux rétinienne est capturée sous formes des lignes ou des points, le système de reconnaissance rétinienne numérise et cartographie l’image pour extraire les caractéristiques distinctifs.

- **Avantages :**

  - Technologies plus précise.
  - Lecteur de rétine capable d’identifier jusqu’à192 pts de repère
  - On peut recenser Jusqu’à 400 points caractéristiques.

- .**Inconvénients :**

  - Difficile à mettre en œuvre.
  - La fiabilité d’identification s’influence par la distance entre l’œil et le Capteur.

- Mal accepter par le grand public.

D. visage :

Aux cours de la vie quotidienne nous pouvons distingués et reconnaître facilement les gens à partir de leurs traits des visages, cette modalité est la plus commune pour la reconnaissance naturelle.La technique de la reconnaissance faciale s'appuie sur les caractéristiques de visage qui sont : les yeux, la bouche' la forme du visage …etc.Dans un système de la reconnaissance faciale, l'image présenté sont capturé par web Cam, puis on numérise cette photo pour extraire un ensemble de caractéristiques propre qui permet de distinguer l'individu.

- **Avantages :**

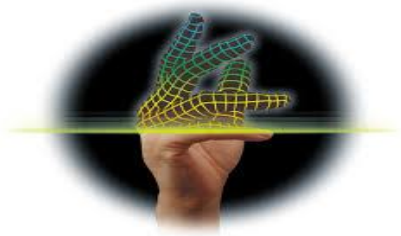
  - Très simples à utiliser et elle a reçus une bonne acceptation par les gens.
  - Technique capable d'effectuer l'identification à distance.
  - Peu couteuse.

- **Inconvénients :**

  - la biométrie faciale relativement fiable puisque le caractère à mesurer est soumis à des variations (maquillage, barbe, l'existence ou absence de lunettes, pilosité,…etc.) Plus élèves que d'autre caractéristiques.
  - l'identification est sensible à des facteurs extérieurs (éclairage, position de visage…etc.).

e. Géométrie de la main :

Cette technique basé sur la forme de la main(la longueur et la largeur de cour de la main, …etc.). Elle nous permet de relever jusqu'à 90 points caractéristiques pour l'identification des individus, Dans le système de la géométrie de la main on peut scanner la main de l'utilisateur à deux déférents angles pour obtenir une image à deux dimensions.Le système analyse l'image numérisé pour extraire les points caractéristiques et réaliser l'identification.



- **Avantages :**
  - Simple à utiliser
  - Apprécier l'utilisateur.

- Les images numérisées sont peu volumineuses.

➢ **Inconvénients :**

- La forme de la main est moins stable.
- Le scanner plus encombrant.
- Echec de l'acquisition quand les mains sont sales

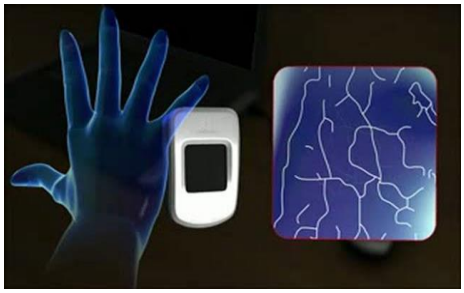
f. Réseaux veineux :

Les artères sont celles qui transfèrent du sang saturé en oxygène à la main et qui se propagent ensuite dans les veines jusqu'à la paume de la main et jusqu'aux doigts.Le sang dans les veines absorbe la lumière à des longueurs d'ondes plus proche à l'infrarouge (760 micromètres).Le système veineux basé sur l'éclairage de la main ou de doigt avec une lumière infrarouge puis il fait apparaître le réseau comme des lignes en noir. En effet, les prolongements des veines sont variés d'une personne à l'autre autre. C'est pour cette raison que nous avons opté pour ce système comme base de données pour la comparaison et l'identification des personnes.

➢ **Avantages :**

- Difficile à falsifier
- L'utilisation sans contact.

➢ **Inconvénients :**



-les dispositifs d'acquisition très sensible aux bruits (température, luminosité).

1.3.2 Biométrique comportementale :

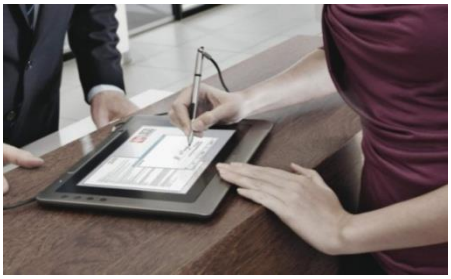
a. La voix :

La voix est constituée des caractéristiques physiques et comportementales, la voix produite par la bouchecausée par les vibrations de la gorge sous pression de l'air qui émit par les poumons, La voix des individus dépend à des caractéristiques physiques (la taille et la forme d'appendices ….etc.) qui sont unique pour chaque personne, par contre les caractéristiques comportementales qui se change en même personnes au cours de temps de l'âge ou sous l'effet à des conditions médicales.

Les techniques de la reconnaissance vocale basées sur la relève et la synthèse des caractéristiques de la voix (latonalité, l'intensité et la fréquence …etc.).

Il ya 2 méthodes de reconnaissance vocale :

- Texte – dépendent : basée sur la reconnaissance de phrase prononcer par l'utilisateur.
- Texte – Independent : l'utilisateur peut prononcer n'importe quelle phrase pour être reconnue du système.



- **Avantages :**
  - Très acceptable
  - Simple à mis en œuvre
  - Identification sont contact.
- **Inconvénients :**
  - Moins permanente.
  - La voix s'influence par différents facteurs (la grippe, tabagisme, le bruit).
  - La variation de caractéristiques de la voix variées aux cours de temps.
  - Vulnérable à la fraude**.**

b. Signature :

Parmi les premières techniques de la biométrie qui ont étéutilisées avant des centaines des années dans les documents des transactions la signature. C'est un style d'écriture différent d'un individu à un autre. Aujourd'hui, les systèmes de la signature se sont utilisable beaucoup plus pour l'authentification des documents dans le domaine judicaire ou administratif aussi dans les transactions bancaires ou commerciales.

Géométriquement, il est facile de trouver deux signatures assemblables mais on peut distinguer entre les deux signatures on se focalise sur ensemble des caractéristiques (l'inclination de stylo, …etc.)

La technique consiste à prendre des captures de la signature et extraire l'ensemble des caractéristiques et l'analyse numériquement pour réaliser la reconnaissance.

- **Avantages :**
  - Protection des fichiers personnels
  - Acceptable par le public
- **Inconvénients :**
  - Moins sécurisé (facile à recopier).

c. Démarche :

Chaque personne marche d'une façon spécifiques, nous pouvons reconnaitre les individus à partir de ces manières particulières pendant la marche : mouvement du corps et de la main, position des jambes etc. On obtient les séquences de démarche à l'aide d'une caméra.

- **Avantages :**
  - Acceptable par le public.

- **Inconvénients :**
  - N'est pas permanent.
  - La façon de marcher s'influence par l'endroit.

d. Frappe au clavier :

C'est la techniqueparticulière d'écriture des individus sur un dispositif logiciel qui calcule la vitesse de la frappe des doigts, le temps entre la frappe et la pause entre chaque mots…etc.

Les séquences des frappes ont construit un mot de passe, le système fait la comparaison et détermine la similarité avec les données de références.

- **Avantages :**
  - Ne nécessite pas des équipements particuliers.
  - Facile à utiliser.
  - Plus acceptable par le public.
  - Moyen précis.
- **Inconvénients :**
  - Permanence faible.
  - Facile à falsifier.
  - N'est pas plus pratique.

1.3.3 Biométrie biologique :

a)ADN :

L'empreinte génétique ou l'empreinte d'acide nucléaire (ADN), qui existe dans toutes les cellules des êtres humains telles que : cheveux, salive,les gouttes de sueur et de sperme…etc. qui découverte la première fois en Angleterre université de « leicester » à Londres par le généticien '' ALEC JEFRIES'' en 1984, c'est la technique la plus extrêmement précise pour l'identification dans le domaine de médecine légiste. Malgré sa fiabilité d'identification qui atteint 99,99%, la décision des tests d'ADN est malheureusement prend beaucoup de temps (plusieurs semaines) par rapport aux autres techniques biométriques.

1.5.Les propriétés des caractéristiques biométriques :

Le choix des caractéristiques biométriques est important, et que le choix de n'importe quelcaractère doit être soumis aux propriétés [6] suivantes :

Unicité : les caractéristiques biométriques des individus doivent être variées d'une personne à une autre.

Permanence : les caractéristiques biométriques doivent être stable au cours du temps et ne doivent pas changer.

Acceptabilité : l'acceptabilité de public dépend de la qualité de l'acquisition en prenant en considération des conditions et contraintes de la capture de modalités.

Performance: la vitesse de discrimination et la décision exacte de système dans un temps raisonnable.

Confidentielle : Ne pas violer la vie privé des personnes.

Presque toutes les modalités biométriques possèdent ces propriétés mais à des degrés différents et comparables selon le **Tableau1.1** :

Modalités biométriques	Universalité	Unicité	Permanence	Acceptabilité	Confidentialité	Performance

Empreinte digitale	M	E	E	M	M	E
Iris	E	E	E	F		E
Rétine	E	E	M	F	E	E
Visage	E	F	M		F	F
Main						M
Réseaux de Veines	M	M	M	M	E	M
Voix	M	F	F	E	F	F
Signature	F	F	F	E	F	F
Démarche	M	F	F	E	F	F
Dynamique de frappe	F	F	F	M	F	F
ADN	E	E	E	F	E	E

Tableau 1.1: Tableau comparatif de différentes modalités biométriques.
(E : Elevé, F: Faible, M: Moyen) [7][8].

- Nous citons un autre type des modalités biométriques, qui s'appelle la biométrie caché : ce type consiste à utiliser les outilsmédicaux (IRM, Rayon X, Electrocardiogramme ECG, Electromyogrammes EMG) dans l'application de l'authentification. En effet les modalités cachées sont inconvenables, en raison de la difficulté d'implémentation ces trais inaccessibles dans un système pour le contrôle d'accès à un réseau informatique.
Ce type biométrique est encore à explorer et suscite l'intérêt des chercheurs criminalistiques.

1.5. Systèmes biométriques :

1.5.1 Définition :

En générale, un système biométrique est un système automatisé capable d'acquérir des données comportementales et physiologiques d'une personne et extraire un ensemble des caractéristiques qui lui permet d'identifier / Authentifie l'individu en se référant à l'ensemble de base des données établi dans ce systèmes [9].

1.5.2 Architecture d'un système biométrique :

L'Architecture d'un système biométrique se compose en générale de cinq 5 modules détaillé ci-dessus [5][10][11].

:

a. Module d'acquisition : Il s'agit d'un capteur biométrique qui permet de réaliser une représentation numérique à partir de l'acquisition des données biométriques.

b. Module de traitement : permet l'amélioration de la qualité du signal (image, voix) provenant du capteur.

c. Module d'extraction des caractéristiques : dans lequel, on applique des méthodes pour l'extraction des informations utiles pour la discrimination et l'identification.

d. Module de stockage : contient des modèles biométriques des utilisateurs (base des données).

e. Module de la décision : au niveau de ce module le système fait la décision de l'authentification ou l'identification à partir de la comparaison entre la base des données et le modèle biométrique capturé**.**

1.5.3. Modes de fonctionnement :

On a 3 modes de fonctionnement du système biométriques : mode d'enrôlement, mode d'authentification, mode d'identification [12].

1.5.3.1. Mode d'enrôlement :

C'est la première phase dans quelques systèmes biométriques, l'enrôlement c'est le mode pendant lequel on stocke les modalités biométriques pour la première fois de l'utilisateur.

1.5.3.2. Mode authentification / vérification:

Le système biométrique vérifier la validité de l'identité d'individu à partir d'une comparaison « one to one ». Comparer le modèle biométrique acquis par le système avec la base des données

Le système fait une décision qui répond à la question « suis-je réellement la personne X ou non ».

1.5.3.3. Mode d'identification :

Dans ce mode, le système établit l'identité de la personne à partir d'une comparaison. « one to many » entre le modèle biométrique de personne et la base des données de plusieurs personnes qui est établi dans le système.

La décision répond à la question « qui êtes-vous ».

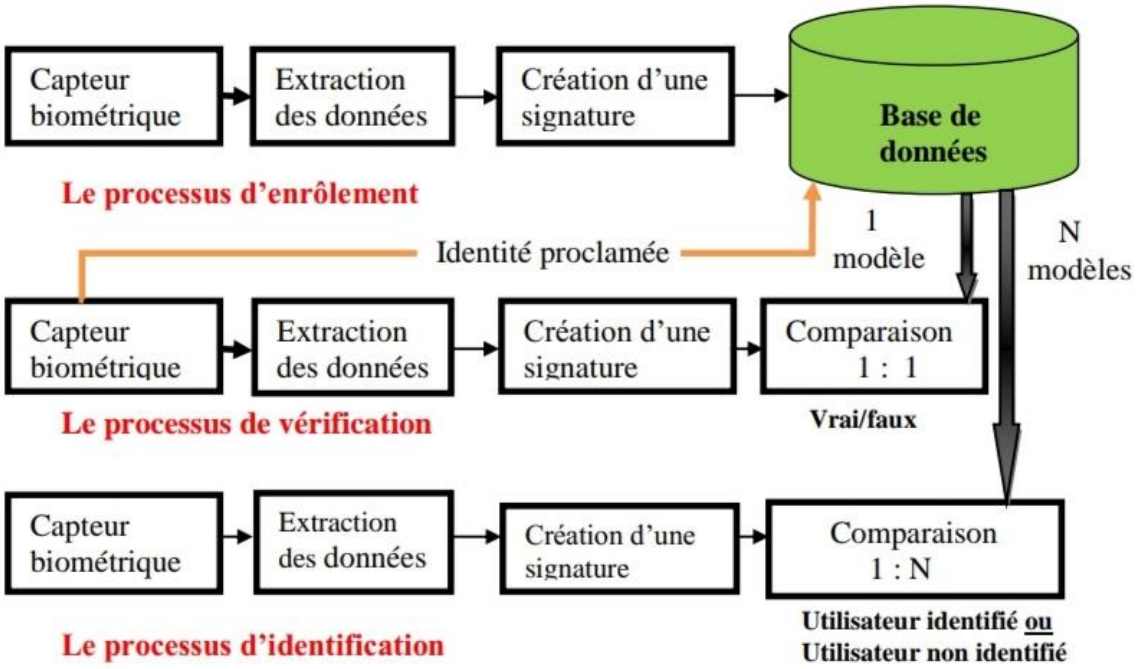


Figure 1.3: Les modes d'un système biométrique [13].

1.6. Les Applications de la biométrie :

La biométrie c'est une technologie d'application polyvalente qui est appliquée dans divers domaine, on peut diviser les applications de la biométrie en 3 groupes :

- **Application commerciales :**
  - contrôler les transactions commerciales.
  - protéger le paiement électronique.
  - l'accès au réseau informatique.
  - la carte crédit.
  - Le PDA.
  - L'ATM.

- **Application de gouvernement :**

-les pièces d'identité (carte d'identité nationale, permis de conduire, passeport...etc.)

- la sécurité sociale.
- contrôle aux frontières.

❖ **Applications légale ou juridiques :**

- La lutte contre les crimes.
- l'identification de terroriste.

1.8. Comparaison entre les modalités biométriques :

IBG (International Biometric Group) a procédé une comparaison entre des différentes technologies biométriques Analyse Zéphyr. Les résultats de cette comparaison sont illustrés dans la figure, d'après 4 critères :

Effort : effort fourni par l'utilisateur lors de l'identification.

Intrusion : information sur l'acceptation du système par les usagers.

Cout : cout de la technologie.

Précision : efficacité de la méthode**.**

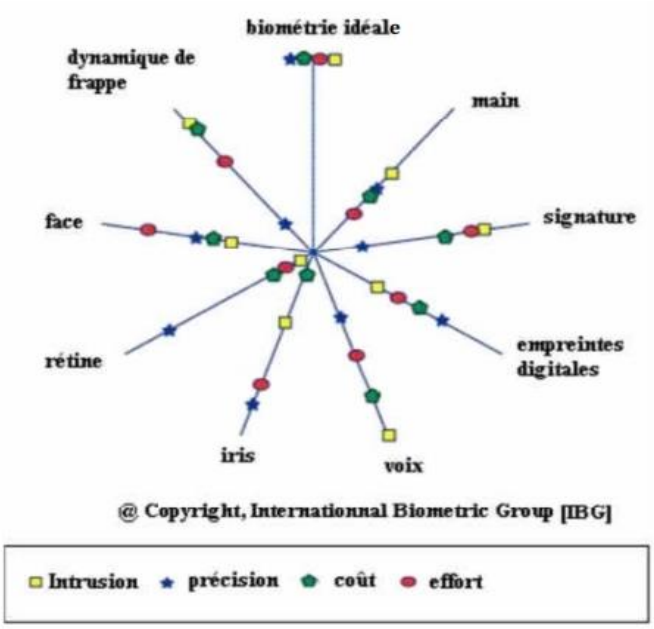


Figure1.7 : Comparaison des techniques biométriques selon les critères :
Effort, intrusion, cout, précision.

1.9. Les limites de la biométrie :

Malgré ces grands avantages qu'elle présente, la biométrie contient aussi un nombre considérable d'inconvénients tels que :

- le bruit sur les modèles acquis.
- Les caractéristiques biométriques ne sont pas toujours simple à acquérir à cause des maladies ou handicap.
- La qualité d'authentification des systèmes biométriques moins fiables que les méthodes d'authentification classique et la précision d'authentification des systèmes biométriques s'effectue à certain nombre des erreurs du rejet et fausses acceptation et n'atteint jamais les 100%.
- La possibilité de falsifier quelques modalités biométriques ces dernières années, comme les empreintes digitales qui laissent les traces sur le passage d'individus et le visage qui est facile à fabriquer un visage 3D de gélatine.
- l'impossibilité de l'accèdes au système à cause des conditions imparfaites de l'acquisition des données biométriques.
- la difficulté d'acceptabilité de quelques modalités biométriques par le public comme : l'iris, la rétine.

Conclusion :

A partir du premier chapitre, nous avons présenté un état de l'art sur la biométrie, ses propriétés, les trois différentes catégories des modalités biométriques et nous avons cité quelques avantages et inconvénients de ses modalités, nous avons aussi définit c'est quoi un système biométrique et ses différents mode de fonctionnements (mode d'entrainement, mode d'apprentissage, module de test). Les domaines d'applications des systèmes biométriques, les limites de ces systèmes.

Chapitre 02

La reconnaissance via les réseaux de veines du doigt

2.1. Introduction :

En effet, la biométrie preuve une grande efficacité dans diverses applications et l'utilisation des systèmes intelligents biométriques surpasser tous les systèmes d'authentification classique (l'empreinte digitale domine la grande part dans le marché des systèmes d'authentification…), car était plus sécurisé et acceptable par le public. Mais malheureusement ces dernières années, quelques modalités biométriques ont subi des attaques par des imposteurs qui finalement ont réussi sont piratage.

Dans le but de combler les lacunes de certaines modalités biométriques les chercheures ont proposé un motif hautement sécurisé, à savoir le motif de veine des doigts qui présente des caractéristiques hautement discriminants, qui propre à chaque personne même entre les jumeaux identiques et en même entre les doigts de la même personne; le réseau de veines du doigt est un motif invisible qui se cache à l'intérieur de la peau et ne laisse pas des traces ce qui fait de lui un modèle difficile à falsifier contrairement aux autres modalités biométriques qui sont souvent susceptible d'être falsifié, comme les experts en données numériques searchsecurity disent : ' contrairement à certains systèmes biométriques ,les modèles de vaisseaux sanguins sont presque impossible a contrefaire … ,les systèmes biométriques basés sur les empreintes digitales peuvent être trompé comme les empreintes digitales qui ont laissé des traces ou les traits de visage qui sont visibles et faciles à se substituer par un masque 3D avec le gélatine.

Aujourd'hui, la veine du doigt devient une technique biométrique prometteuse et un domaine d'étude important pour l'identification des personnes, car la fiabilité et commodité a été déployée dans diverses applications de sécurité: bancaires,financière et présenter un grand potentiel dans le domaine de criminalistiques, l'idée de la technique de la veine du doigt consiste à éclairer le doigt avec une lumière proche de l'infrarouge (NIR) et extraire l'image de motif de veine comme des lignes ombres. Certaines techniques de reconnaissance de veine du doigt identifient seules les veines du doigt vivantes se la rend plus efficace.[18].

2.2. Système de la reconnaissance de veine du doigt :

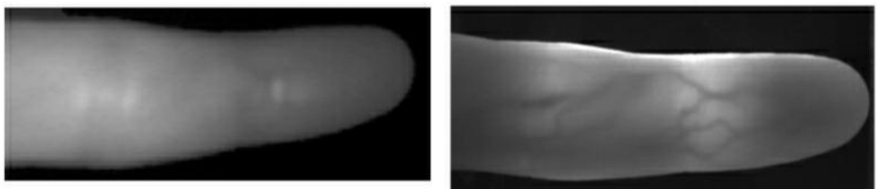
Le système de reconnaissance des veines du doigt se compose de 4 modules comme tout système biométrique :

2.2.1 Acquisition d'une image IR du doigt :

L'acquisition ou l'extraction de motifs de réseau de veines du doigt est la première étape dans le système FVR, principalement on a 3 méthodes utilisées pour l'acquisition d'image des veines [20] :

- **Méthode de la transmission lumineuse :** le doigt est placé entre le capteur d'image et la source lumineuse.
- **Méthode de réflexion de la lumière :**La source lumineuse et le capteur sont placés du même côté du doigt.
- **Méthode de rayonnement bidirectionnel :** la nouvelle méthode qui a combiné les avantages des deux méthodes, se compose de 2 sources lumineuses qui sont placées aux deux côtes du doigt.

Généralement, on utilise la méthode de la transmission de la lumière pour obtenir une image a contraste élève comme le montre la **Figure 2.1.**



(a) Image utilise la réflexion de la lumière

(b) image utilise la transmission de la lumière

Figure 2.1 : comparaison entre les méthodes de luminosité.

2.2.1.1. Méthode de la transmission de la lumière :

Principe de fonctionnement : Une LED émet une lumière proche de l'infrarouge (NIR) (longueur d'onde 700 à 1000 nanomètres) à travers l'emplacement du doigt l'hémoglobine dans le sang au contraire d'autres tissus absorbent la lumière (NIR). Une camera CCD capture le motif des veines comme des lignes sombres

L’intensité de la lumière du LED est ajustée en fonction de la luminosité de l’image.

La transmission de la lumière IR varie en fonction de l’épaisseur de doigt.

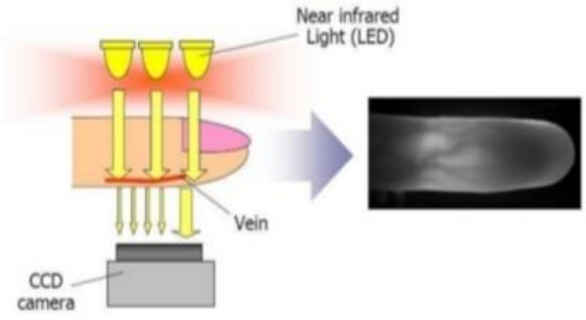


Figure 2.2 : Capteur de transmission de la lumière.

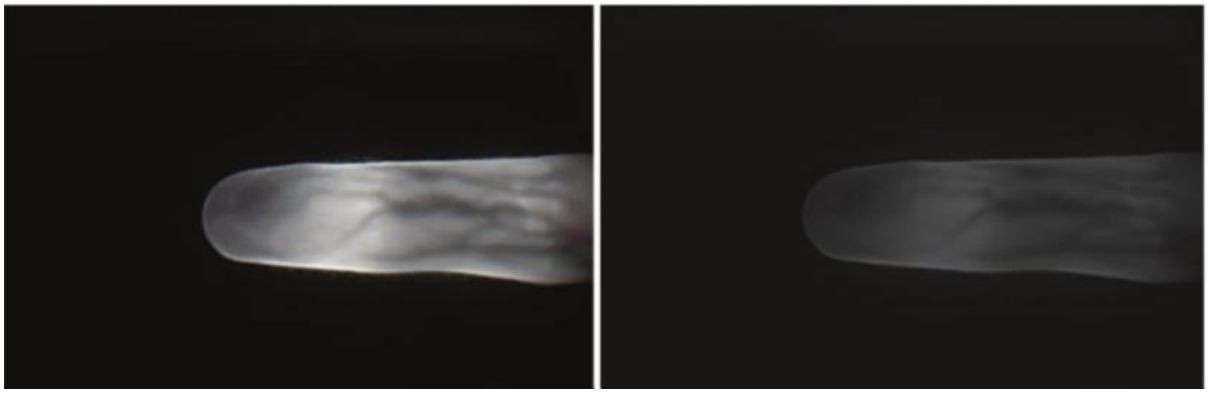
2.2.2 Prétraitement :

L’étape du prétraitement suit toujours l’étape de l’acquisition d’image, le prétraitement c’est un processus crucial dans tous les systèmes d’identification biométrique. Il intervient pour l’objectif de résoudre les problèmes au niveau de l’appareil de l’acquisition de l’image, généralement l’image acquise de la veine se compose de bruit, de nuance et de faible contraste à cause de la lumière reflétée et la variation de l’emplacement de doigt à chaque fois.

Dans le prétraitement en appliquent des algorithmes classiques du traitement d’image et du filtre numérique pour fournir une image robuste pour la fonctionnalité de l’extraction de ROI et l’extraction des caractéristiques généralement, le prétraitement contient à 3 étapes :

- ✓ **Réduction de bruit :** le bruit produit par la numérisation est de la transmission de l’image originale, on ne peut pas toujours éliminer le bruit. On utilise le filtre médian comme technique pour la réduction de bruit.
- ✓ **Normalisation :** la normalisation c’est uneopération utilisée dans le traitement d’image qui modifie la plage des pixels dont l’objectif est obtenir une image de sortie avec une moyenne ou une variation souhaitable.

- L’image à éclairage uniforme est normalisée par la formule ce dessus[21] :



(a). Image normalisée de la veine du doigt. (b) Image originale de la veine du doigt

Figure 2.3 : Le résultat de la normalisation d'image.

2.2.3. Extraction du ROI :

L'extraction précise du ROI joue un rôle principal pour l'amélioration de la fonctionnalité de l'extraction des caractéristiques est donc pour l'amélioration des performances du système FVR.

Dans cette étape on élimine l'arrière-plan de l'image qui se compose des régions indésirables et on intègre seule la zone utile pour la reconnaissance qui contient les informations discriminantes qui s'appelle ''la région d'intérêt''.

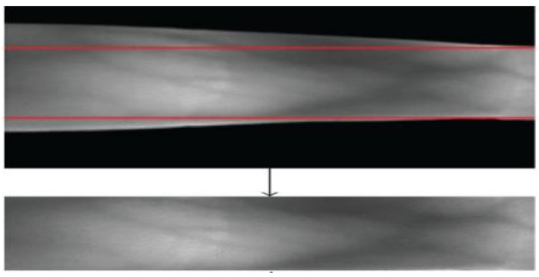


Figure 2.4 : l'extraction de la région d'intérêt « ROI ».

2.2.4. Extraction des caractéristiques :

L'étape d'extraction des caractéristiques représente le cœur du système de reconnaissance des veines, est le facteur critique qui améliore la capacité de discrimination.

Plusieurs méthodes et des algorithmes ont étaient proposés dans le domaine d'extraction des caractéristiques, on a divisé les méthodes d'extraction des caractéristiques en trois (3) grandes approches [10][14] :

2.2.4.1 Les approches globales : (statiques)

Dans laquelle, on utilise les techniques de l'analyse statique bien connues, les images sont traitées sous forme des matrices ou des vecteurs dans des sous-espaces de plus faibles dimension (pixellisation).

On peut séparer les méthodes globales en deux différentes techniques distinctes : les techniques linéaires et les techniques non linéaires.

2.2.4.2 Les approches locales : (géométriques)

Dans laquelle, on analyse l'image des veines géométriquement, les techniques utilisées détectent les différents morphologies des veines (bifurcations…etc.).

2.2.4.3. Les approches hybrides :

Les méthodes hybrides présentent l'association des techniques de la détection de caractéristiques locales de motif des veines avec les techniques de l'extraction des caractéristiques d'apparence statistiques. Ces approches essayent de combiner les avantages des deux précédentes méthodes.

Les approches	**Vitesse de réponse**	**Mis en œuvre**	**Réponse**
Globales	Très bien	Simple	Médiocre
Locales	Moyen	Complexe	Bien
Hybrides	Mauvais	Très complexe	Très bien

Tableau2.1 : Comparaison entre les différentes approches d'extractions des caractéristiques.

2.3 Algorithmes d'extraction des caractéristiques :

2.3.1 Motifs binaire locaux (en anglais : Local Binary Pattern ou LBP).

Le motif binaire local (LBP) est un motif efficace d'extraction des caractéristiques quia été proposé par Ojala et al en 1996 afin de représenter les caractéristiques de texture dans l'image en niveaux de gris, le processus de cet opérateur de texture sert à attribuer à chaque pixel de l'image un code binaire dépendant des valeurs de niveaux de gris des pixels voisins, on compare le niveau de pixel central avec les pixels voisins en utilisant la formule suivante :

$$\text{LBP(xc ,yc)}== \sum_{n=0}^{p} \text{U(ic} - \text{in)}2^n$$

U=1 si x $\geq$ 0

Sinon :

U=0

in et ic sont respectivement les niveaux de gris d'un pixel voisin et du pixel central.

Dans le cas de voisinage de 8 bits, si la valeur d'intensité de pixel voisin supérieur ou égalà la valeur de l'intensité de pixel centrale donc le voisin prend une valeur de ''1'' si non il prend la valeur '' 0'', on obtient un code binaire a 8 bits on multiplie les valeurs binaire par ces poids et on les somme pour obtenir des valeurs d'intensité entre 0 à 255.

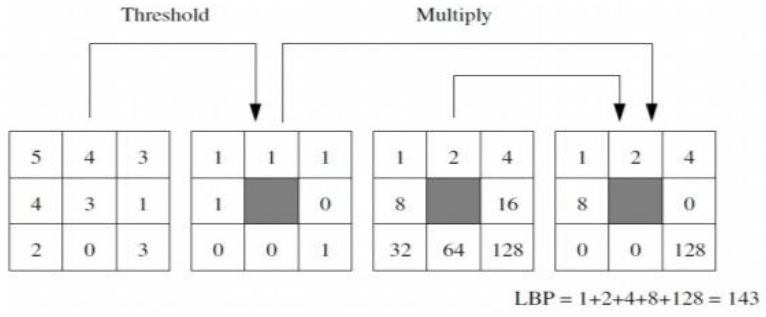


Figure 2.5 : Exemple de l'analyse de l'opérateur LBP a simple voisins.

L'opérateur LBP peut être étendu à des voisinages de taille supérieure différente à 8 (multi _ échelle), dans ce cas les pixels voisins se trouvent sur un cercle autour du pixel central et construit par deux paramètres :

R : Représente la distance entre le point centrale est les points voisins.

P : Nombre des pixels voisins.

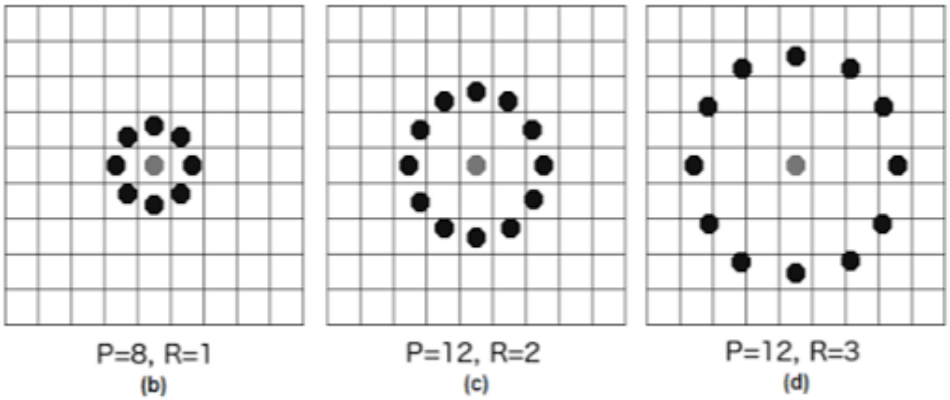


Figure 2.6 :LPB multi-échelle. Différents voisinages pour différentes valeur de RetP.

Les coordonnées de N points voisins sont établit selon l'équation suivante :

$$X = Xc + R\cos(2\pi n/N).$$

$$Y = Yc + R\sin(2\pi n/N) .$$

Le motif LBP ne s'influe pas par la variation de l'intensité.

2.3.2 Quantification de la phase locale :(local phase quantization ou LPQ)

La quantification de la phase locale est une méthode d'extraction des caractéristiques très utilisée dans plusieurs technologies biométriques. L'algorithme de LPQ permet d'extraire des informations locales, pour chaque région de l'image, après avoir devisé cette dernière en petite région de même taille $M * M$.

LPQ extrait l'information par l'utilisation de la transformée de Fourier discrète de chaque pixel x, illustré dans l'équation suivante :

$$Fu(x)=\sum_{m\ni Nx} h(m-x)\, f(m) e^{-2j\pi mu^T} = Eu^T f(x)$$

On résume la méthode de LPQ en quatre étapes distinctes. Dans la première étape, on labélise l'image, puis on devise cette image en petites régions de même taille, ensuite on construit des vecteurs des caractéristiques locaux et l'histogramme des codes de chaque pixel et enfin on représente le vecteur des caractéristiques globales (image entière) par la combinaison de tous les vecteurs.

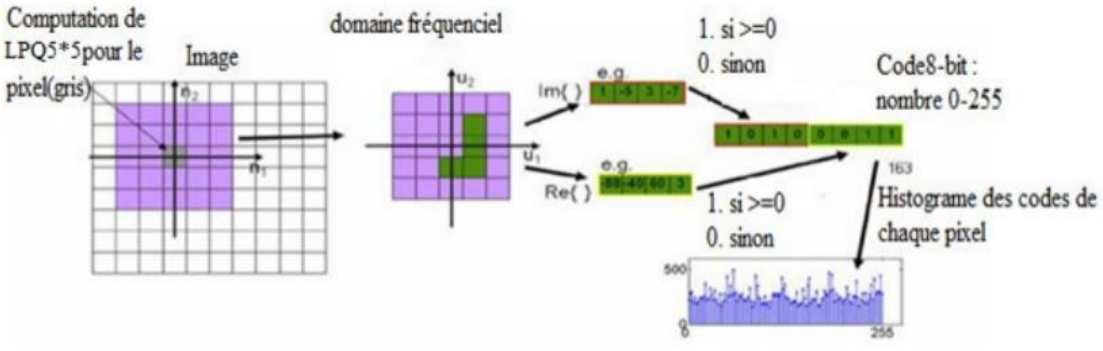


Figure2.7 : Organigramme de l'ensemble des étapes nécessaire à la construction du descripteur LPQ.

2.4 Apprentissage :

C'est l'étape dans laquelle on stocke les paramètres traitant des caractéristiques d'un ou plusieurs modèles des veines d'un utilisateur, dans une base de données bien ordonnée dont l'objectif est améliorer la phase de reconnaissance et la prise d'une décision.

On définit deux types d'apprentissages : apprentissage supervisé, et l'apprentissage non supervisé.

2.4.1 Apprentissage supervisé :(supervised Learning)

L'apprentissage supervisé c'est une forme de l'apprentissage machine (Machine learning).

Préalablement, il faut importer les exemples de ce qu'il faut apprendre (ensemble des modèles d'apprentissage) avec leurs étiquettes d'appartenances aux classes, ensuite le système doit être capable d'expliquer et de prédire l'appartenance des nouveaux modèles à une classe bien connue.

2.4.2 Apprentissage non supervisé :

L'apprentissage non supervise contient des exemples sans aucune étiquette de classe. En général, l'algorithme essaie de trouver les caractéristiques entre les exemples pour faire la classification.

2.5 La décision :

Dernière étape dans un système de reconnaissance ou de vérification de l'identité des individus, la prise de la décision dépend de la similarité entre les caractéristiques extraites et les modèles stockés dans la base de données.

2.5.1 La classification :

La classification c'est le dernier processus dans un système de reconnaissance, dans laquelle on classe ou on regroupe les caractéristiques biométriques extraites selon le degré de la similitude entre ces caractéristiques et les modèles stockés, la classification est un processus crucial pour la prise de la décision.

On peut définir certaines méthodes de classification :

2.5.1.1. K- plus proche voisin(KPPV) ou KNN (k-nearestneighbour) :

La méthode KNN est un algorithme de classification automatique, est parmi les algorithmes la plus couramment utilisés dans l'apprentissage supervisé, il permet de traiter des nuages de points non linéairement séparables.

K le plus proche voisin est une extension de l'idée du voisin le plus proche(NN), NN est une méthode utilisé pour un seul plus proche, ou K=1.

Principe de fonctionnement :

Le fonctionnement de KNN consiste à calculer la distance d'un nouvel échantillon d'entrée X, par rapport aux échantillons d'apprentissage (classe majoritaire), donc pour sélectionner la classe de X, en détermine le K la plus proches voisins parmi tous les échantillons de la classe majoritaire.

La valeur de K doit être sélectionnée par l'utilisateur, généralement nous choisirons une valeur petit de cas pour rendent les frontières entre les classes plus distinctes.

Nous définissons différents types de formules pour mesurer la distance, soit L l'ensemble de données à disposition ou échantillon d'apprentissage :

La distance euclidienne :

- Calcule la racine carrée de la somme des différences carrées entre les cordonnées de deux points x,y :
- $D_e((x_1,x_2....x_j),(y_1,y_2, ...,y_j))=\sqrt{(x1 - y1)\,2 + (x2 - y2)\,2 + ... + (xj - yj)\,2}$.

La distance Manhattan :

- Calcule la somme des valeurs absolues des différences entre les coordonnées de deux points :

$D_m(x,y)=\sum_{i=1}^{k} |xi - yi|$

La distance Hamming :

- la distance entre deux points donnés est la différence maximale entre leurs coordonnées sur une dimension :

$\mathbf{D}_h(x,y)=\sum_{i=1}^{k} |xi - yi|$

Avec :

$$x=y \Rightarrow D=0$$

$$x \neq y \Rightarrow D=1$$

Il existe plusieurs formules pour calculer la distance, mais la distance euclidienne reste la plus utilisée.

Conclusion :

Dans ce chapitre, premièrement nous avons expliqué les différents modules de système FVR,les méthodes de l'acquisition d'image des veines, quelques processus du prétraitement, les différentes approches de l'extraction des caractéristiques, est nous définissons deux descripteurs LPQ et LPB qui sont des descripteurs lesplus utilisés. Nous avons présenté le classificateur K voisins les plus proches.

Chapitre 3

Résultats et discussions

3.1 Introduction :

Dans ce chapitre, nous allons effectuer une simulation sur le logiciel ‘’**MATLAB**’’ pour tester et comparer ces algorithmes sur des images de motif veineux du doigt sur les deux différentes bases de données, à savoir : ‘’**FV-USM** et **SDUMLA-HT** ‘’ avec l’utilisation de l’algorithme **CLAHE** pour l’amélioration le contraste des images et la méthode K- la plus proche voisine (**KNN :** K- Near Neighbors), c’est une méthode largement utilisée pour la classification supervisée Multi-Classe.

3.2 Bases de données :

Il existe plusieurs bases de données accessibles au public pour la reconnaissance des veines des doigts. Dans ce travail on utilise deux différentes bases de données pour évaluer notre système : la base de données (FV-USM) et la base de données (SDUMLA-HT).

3.2.1 FV_USM (Finger Vein USM):

La base FV-USM d’images de motif de veine se compose à d’ensemble des données des veines des doigts, collectées auprès des étudiants et des membres personnels de l’université Sain Malaysia. Cette base de données contient des images de veine de quatre doigts (l’index gauche, le milieu gauche, l’index droit et le majeur droit) de 123 personnes (83 hommes et 40 femmes). L’âge des sujets (personnes) variait de 20 à 52 ans et chaque sujet fournier volontairement 6 échantillons (images) par doigt, les échantillons ont été capturé dans deux sessions, séparer par plus de deux semaines lors de la première session, un total de 2952 images (1 4 6), à partir de deux sessions nous avons collecté un total de 5904 images de 492 classes de doigts.

3.2.2 SDUMLA_HT :

La base SDUMLA_HMT c’est base de données biométrique multimodale (visage, iris, empreinte digitale et veine de doigt), contient des images de veines recueillies auprès de 106 personnes, ces images sont acquises par Joint Lab pour l’informatique intelligente et les systèmes intelligents de l’Université de Wuhan. Lors du processus de capture, l’ensemble de

données des veines des doigts contient des images de six doigts par personne (annulaire, majeur, l'index des deux mains). Et chaque personne contribue a 6 images de chacun de doigt, à partir de ces contributions on collecte un total de 3816 images, on stocke chaque image au format 'bmp' avec une taille de 320 240 pixels.

3.3 Méthodologie :

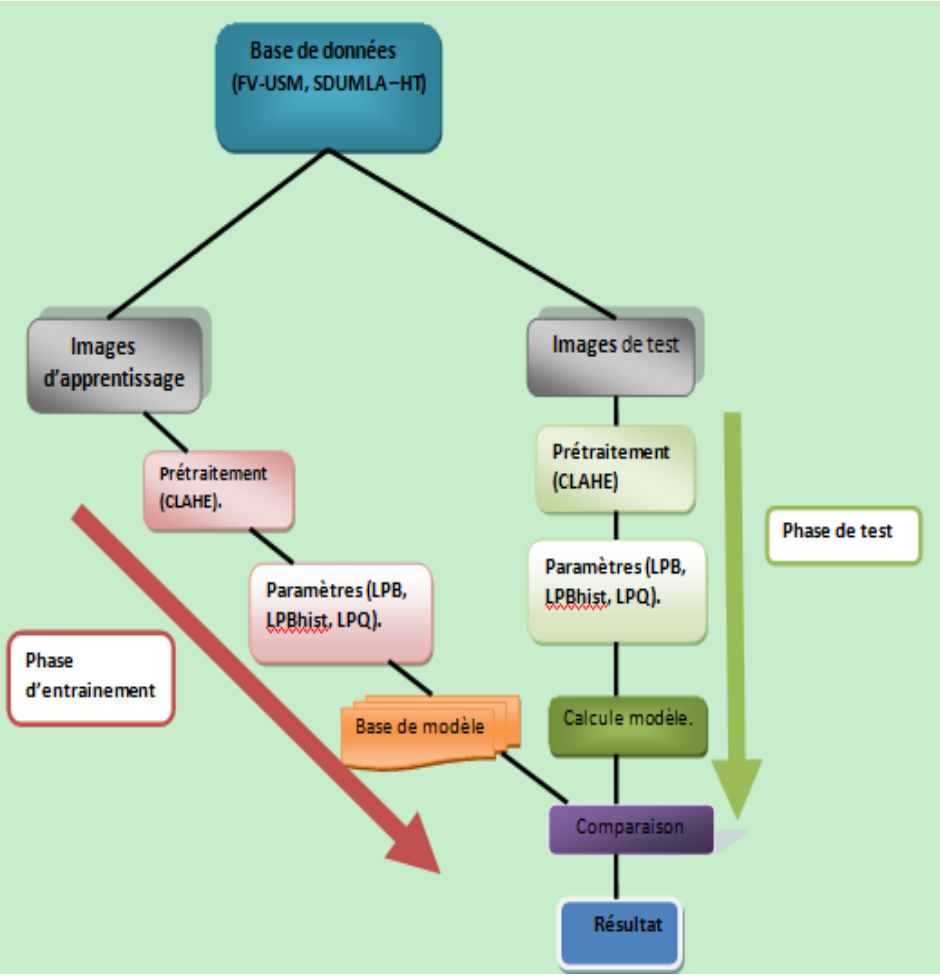


Figure 3.1 : Schéma synoptique de notre système d'identification FVR.

Le fonctionnement de notre système nécessite deux phases opérationnelles. La phase d'apprentissage et la phase de test, donc on a besoin de séparer la base de données (FV-USM, SMDULA-HT).

3.3.1 Séparation de la base de données :

Soit dans la base des données (FV-USM) ou (SDMULA-HT) : chaque doigt a été capturé 6 fois (une répétition de 6 fois d'imageslemême doigt de chaque personne).

On divise ces images on deux groupe : un groupe pour l'apprentissage et le deuxième groupe pour effectue le test. La séparation de la base de données FV-USM ou SDMULA-HT s'effectue avec la façon suivante :

Images d'apprentissage:

Les trois premières images de chaque personne s'utilisent pour l'apprentissage.

Images de teste :

Les 3 dernières images restantes de chaque individu servent pour le test.

Tableau (3.1) distribution d'images entre l'apprentissage/ tests.

Base de données	FV-USM	SMDULA-HT
- Nombres des personnes	123	106
- Nombres des images	738	636
- Images utilisées dans l'apprentissage.	369	318
- Images utilisées dans le test.	369	318

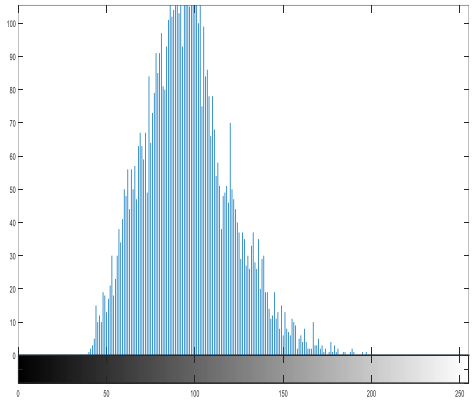
Donc on a utilisé 229personnes pour l'évaluation de notre système 123 dans FV-USM et 106 dans SMDULA-HT.

3.3.2. Prétraitement :

3.3.2.1 Egalisation de l'histogramme Adaptive à Contraste Limité CLAHE :

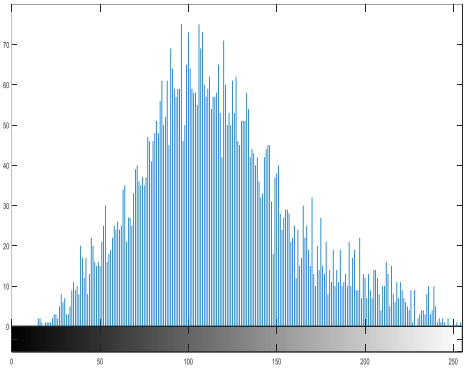
L'étape de prétraitement c'est une étape prépondérante dans la phase d'apprentissage et la phase de test, dans laquelle on implémente des techniques pour l'objectif d'améliorer la qualité des images. Dans notre système on applique l'histogramme adaptatif à contraste limité (CLAHE)

C'est une opération d'ajustement du contraste d'une image utilise l'histogramme, cette technique normalise la luminosité de l'image en augmente le contraste des petites régions on appliquant une transformation sur chaque pixel de l'image Figure (3.2).



(a) image ROI originale de SDUMLA. **(b)** l'histogramme de l'image ROI originale.

Figure (3.1) : image et l'histogramme de ROI de SDUMLA-HT sans CLAHE



(c) histogramme étiré de l'image originale.**(d)** l'image après l'étirement d'histogramme.

Figure 3.2 : Les résultats de l'algorithme CLAHEsur l'image ROI de la base SDUMLA-HMT.

3.3.3. Paramètre d'extractions des caractéristiques :

Dans notre travail, nous utilisons 03 différentes méthodes pour l'extraction des caractéristiques LPB, LPQ et LPBhist. Les deux descripteurs LPB et LPQ sont les méthodes les plus couramment utilise pour l'extraction les caractéristiques.

3.4 Protocole d'évaluation :

3.4.1. Environnement matériel :

Un Ordinateur hp aves les caractéristiques suivantes :

- Processeur : Intel (R) celeron ® CPU N3060 @ 1.60 GHZ 1.60 GHZ

- RAM: 4.00 GO

- Disquedur : 500 Go.

- OS: Microsoft Windows 10 64 bits.

3.4.2. Logiciel de développement:

Matlab (matrix laboratory). (R2015a) :

C'est un langage de programmation de quatrième génération émulé par environnement de développement du même nom, utilise pour le calcul numérique, développé par la société Math Works. Il permet de manipuler des matrices, d'afficher des courbes et des données, mettre en œuvre des algorithmes et de créer des interfaces utilisateurs.

3.5. Résultats et interprétations:

Dans nous système, on essaye d'évaluer le taux de reconnaissance de 3 différents algorithmes d'extractions des caractéristiques : **LPB, LPBhist, LPQ** appliquer sur les bases de données **FV-USM** et **SMDULA-HT,** On utilise le classificateur K-NN qui est détaillé dans le deuxième chapitre. Puis on essaye d'implémenter un algorithme de prétraitement dans le but d'améliorer les performances du système. Les simulations sont reparties en deux parties :

1ère Partie :

Dans la première partie d'expérimentation on applique les 3 différents algorithmes d'extractions des caractéristiques LPB, LPBhist, LPQ sans aucun prétraitement :

$$\text{Le taux de reconnaissance} = \frac{\text{Nombre d'images de test reconnus.}}{\text{Nombre totale d'images de test}} \text{x100 .}$$

- **Index gauche :**

Tableau (3.2) : Taux de reconnaissance (%) en utilisant index gauche :

Base de données	FV-USM	SMDULA-HT
LPBhist	99,45%	97,16%
LPB	98,37%	95,91%
LPQ	94,03%	94,33%

- **Annulaire gauche :**

Tableau (3.3) : Taux de reconnaissance en utilisant l'annulaire gauche

Base de données	FV-USM	SMDULA-HT
LPBhist	97 ,28%	90,27%
LPB	96,48%	78,93%
LPQ	85,09%	78,30%

- **Index droite :**

Tableau (3.4) Taux de reconnaissance en utilisant index droit

Base de données	FV-USM	SMDULA-HT
LPBhist	99,73%	97,48%
LPB	95,66%	95,91%
LPQ	89,43%	92,76%

- **Discussion :**

D'après les trois tableaux précédentes de résultats on remarque que :

- Les meilleurs résultats sont obtenus en utilisant la base FV-USM, cela est dû à la qualité des images de cette base d'une part. D'autre part, le ROI est fourni avec cette base, par contre.

- Les meilleurs résultats sont obtenus en utilisant le descripteur LBP hist avec un taux de reconnaissance qui atteint 99,93%.
- En remarque une grande différence entre les différents doigts. Ce qui explique que le réseau veineux de chaque personne est unique.

2 émé Partie : Simulations avec prétraitement

Dans la deuxième partie, nous appliquons l'algorithme CLAHE dans la phase de prétraitement, dont l'objectif est améliorer le contraste des images.

- **Index gauche :**

Tableau (3.5) Taux de reconnaissance en utilisant index gauche

Base de données	FV-USM	SMDULA-HT
LPB-hist	100%	98,11%
LPB	98,92%	97,79%
LPQ	96,2%	97.79%

- **Annulaire gauche:**

Tableau (3.6) : Taux de reconnaissance en utilisant annulaire gauche

Base de données	FV-USM	SMDULA-HT
LPB-hist	98,64%	92,76%
LPB	95,93%	92,35%
LPQ	98,10%	86,47%

- **Index droite :**

Tableau (3.7) Taux de reconnaissance en utilisant index droit

Base de données	FV-USM	SMDULA-HT
LPB- hist	100%	100%
LPB	97 %	98,42%
LPQ	100%	99,05%

Discussion :

- En remarque clairement que l'utilisation de l'algorithme CLAHE ; qui jeu le rôle d'améliorer le contraste ; permet d'obtenir une amélioration des taux de reconnaissance. Le taux de reconnaissance attient les 100%.
- Une image claire permet d'avoir des descripteurs exacts, ce qui améliore la discrimination entre les individus.

Conclusion Générale :

Le travail illustré dans notre mémoire, s'inscrit dans le cadre générale de la biométrie, et plus spécifiquement l'identification automatique des individusà partirdes veines du doigt. Cette dernière est considérer comme une modalité biométrique récemment utilisée pour une identification très précise et plus sécurisée, le motif de veine du doigt parmi les modalités biométriques les plus distinctives mêmes entre les jumeaux identiques. En effet, l'efficacité de l'utilisation des motifs veineux réside dans l'impossibilité de sa falsification, grâce àson positionnement à l'intérieur de la peau. Donc, après avoir introduit les notions de base de la biométrie et des systèmes biométriques et leurs fonctionnements, nous avons présenté quelques paramètres et des outils mathématiques pour l'analyse et l'extraction des caractéristiques.

Notre travail s'appuie sur l'évaluation des trois algorithmes LPB, LPBhist, LPQ en termes de taux de reconnaissance.Nousavons aussitesté l'influence de la méthode CLAHE du prétraitement sur le taux de reconnaissance de notre algorithme. En Effet, les résultats obtenus nous permettent de conclure quele paramètreLBPhistest meilleur que les deux autres algorithmes (LPQ, LPB). Les meilleurs résultats atteint un taux de reconnaissance de 99,73% et de 100 % sans et avec prétraitement respectivement.

Perspectives :

Finalement et en guise de perspectives, nous essayerons dans les futurs travaux de :

- Construire un système multi-modèle, combinaison de systèmes d'empreinte digitale et le motif de veine du même doigt.
- Développer des approches hybrides pour une meilleure méthode d'extraction des caractéristiques.
- Utiliser le deeplearning.

Bibliographie :

[1] W. Hizem « capteur intelligent pour la reconnaissance de visage ». Thèse de doctorat, l'institut Nationale des technologies et l'université Piérre de Marie Curie-paris 6 2009.

[2] N. Galy « Etude d'un système complet de reconnaissance digitale pour un capteur microsystme à balayage ». Thèse de doctorat, Institut Nationale polytechnique de Grenoble (France), Soutenance le 14/04/ 2005.

[3] Le Duc Bao « Authentification des empreinte digitales dans un système, Bio PKI ». Travail d'intérêt personnel encadré, l'institut de Francophonie pour l'informatique, Hanoi le 20 /01/2007.

[4] G. Roethenbagh « An Introduction to Biométrics and General History », Biometrics Explained, Section 1, 1998.

[5] S.L Padme, D.C Jain, V.P. Pawar, H.S. Fadewar, and G.P.Khetri: « Humain Computer Interpreting with Biometric Recognition »International journal of Advenced Research in computer Science and SoftWar Enginering.Vol.02, issue.02, PP12, 2012.

[6] M. El Abed « Evaluation de Système Biométrique ».Thèse de doctorat Université de Caen /Basse-Normandie (France). Soutenance le 09 /12 /2011.

[7] H. Hezil « Identification de personne par signature manuscrite ». ThèsedoctoratUniversité 8 mai 1945- Guelma (Algérie). Soutenance 2018.

[8] R.P.Wilds, «A System for Automated Iris Recognition». Proc. Of 2nd IEEE Workshop on Applications of Computer Voisin, pp.121-128, Décater 1994.

[9] L.Manssoura, «identification des visages Basé sur la JAVA CARD», Mémoire fin d'étude d'ingéniorat en informatique, Institut Internationale de formation en informatique(I.N.I) ,2011.

[9] Anil K Jain, Ling Hong, et al, «»in proccecing of the IEEE, Vol.85 NO, S (1997).

[10] D.Dahbia&G.Soumia « Identification et Reconnaissance Biométrique par l'utilisation des empreintes palmaires».Thése Académique Université AkilmohandOulhadj, Bouira(algerie), Soutenance le 24/09/2017.

[11] S.Probhakav,S.Pankami,andA.K.jain:BiometricRecognition:Security and Privacy Concerns .IEEE Security and Privacy.Vol.03,No.02.pp.33-42,2003

[12] A.BettahardF.Saber , «Extraction des caractéristiques pour l'analyse biométrique d'un visage» . Thèse master université KASDI MERBAH OUERGLA soutenance. Soutenance, le 15/06/2014.

[13] S, Lio,M. Silveman, «A practical guide to biometric security technology »,IEEE Computer society ,ITPRO-SECURITY ,January,2001.

[14] D. Youssef .Hamza«Réalisation d'un Système de reconnaissance biométrique sur des images 2D d'un visage » .Thème fin d'étude master université Akli Mohand Oulhadj .de Bouira , (soutenance le 24/09/2017)

[15] ISO/IEC 19795-1 : information technology-biometric performance testing and reporting-part: principles and framework ,2006.

[16] S.G Ababsa . « Authentification d'individus par reconnaissance d'un visage 2D/3D

[17]http://www.biometrie-online.net/biometrie/le-marche.

[18]http://www.marketsandmarkets.com/Market-Reports/biometric-market-278.html.

[19]http://www.usinenouvelle.com/article/gemalto-mise-sur-la-biometrie-en-rachentant-l-activite-securite-de-l-americain-3m-N475079Thèse doctorat, université soutenance le 03/10/2008.

[20] Naoto Miura, Akio Nagasaka, TakafumiMiyataka, « Feature extraction of finger-vein patterns based on repeated line tracking and its application to personal identification», Hitachi, ltd 1-280 Higashi-Koigakubo,

[21] Kejun Wang, Hui Ma, Oluwatoyin P. Popoola and JingyuLui(2011). Finger vein recognition, Biometrics, Dr. Jucheng Yang(Ed) , ISBN :978-953-307-618-8, In Tech.

[22] S.AKBAR, A.AHMAD, H.MAQSOUD et A.FAHEEM, ''Face Recognition Hybrid Feature Space in Conjunction With Support Vector Machine''. Journal of Applied Envirenmental and Biological Sciences, Vol.5, No.7, pp.28-36, 2015.

[23] http://mla.sdu.edu.cn/info/1006/1195.htm.

[24] http://drfendi.com/fv_usm_database/.