N° d'ordre :

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

UNIVERSITE DE M'SILA
-MOHAMMED BOUDIAF-

FACULTE DE TECHNOLOGIE
DÉPARTEMENT D'ELECTRONIQUE

MEMOIRE

Présenté pour l'obtention du diplôme de MASTER

EN : ELECTRONIQUE

Spécialité : **Systèmes des Télécommunications**

Par :
Abdelhafid Oualid
Senouci Abdelkrim.

THEME

L'identification Biométrique Par Les Veines Des Doigts

Soutenu devant le jury composé de :

Mr. LAADJAL Mohammed	**MCA**	Univ M'sila	Président
Mr. ATTALLAH Bilal	**MCA**	Univ M'sila	Directeur de mémoire
Mr. BRIK Youcef	**MCB**	Univ M'sila	Co-Directeur de mémoire
Mr. DJERIOUI Mohammed	**MCB**	Univ M'sila	Examinateur

L'année universitaire
2019 /2020

Dédicace

- *A mon père, à ma mère.*
- *A mes frères et sœurs.*
- *A la mémoire de mes grands parents.*
- *A tout mes amis (es).*
- *A tout mes maîtres et professeurs : du primaire au supérieur.*
- *A tous ceux qui ont contribué au développement des sciences en général et de l'électronique en particulier.*
- *Au Docteur ATTALLAH Bilal.*
- *Au Docteur BRIK YOUCEF.*

Remerciements

Nous adressons toutes nos expressions de remerciements, d'appréciation et de respect au Dr. **ATTALLAH Bilal**, professeur à l'Université de Muhammad Boudiaf et le superviseur de cette mémoire, et au Dr. **BRIK Youcef**, pour toutes les directions qu'ils nous ont fournies pour compléter ce message, ainsi que pour l'inspiration, le traitement aimable et les efforts consentis même à la lumière de cette épidémie mondiale.

Tous nos remerciements et respect aux enseignants qui nous ont accompagnés dans notre parcours académique et n'ont même pas ménagé leurs efforts pour présenter leurs connaissances sur une assiette.

Que Dieu vous accorde le succès, et vous maintiendrez une couronne au-dessus de nos têtes et une lumière pour chaque étudiant du savoir, et vous offrirez une santé et un bien-être durables.

Enfin, nous adressons nos sincères remerciements à tous nos parents et amis qui nous ont toujours soutenus et encouragés à faire ce travail.

Merci à tous.

Table des matières

Table des figures

Table des figures

Table des figures

Liste des tableaux

Liste des abréviations

FV : Finger veines.

LBP : Local Binary Pattern.

BSIF : Binarized statistical image features

SVM : Support Vector Machine (Machine à Vecteurs de Support).

FAR : False Accepted Rate.

FRR : False Rejected Rate.

ERR : Error Rejected Rate.

Introduction Générale

Nous vivons actuellement une véritable révolution d'accès à l'information, dans tous lesdomaines de l'activité humaine. En fait, la sécurité des systèmes d'information est devenue undomaine de recherche d'une très grande importance, l'individu est essentiel pour assurer lasécurité des systèmes et des organismes, la conception d'un système d'identification fiable,efficace et puissant est une étape nécessaire. Dans ce sens, la biométrie est un exemplepratique parce qu'elle est de plus en plus présente dans la vie quotidienne : au travail desopérations bancaires, l'accès à certains endroits militaires ou industriels.La biométrie indique l'ensemble des technologies de reconnaissance physiologiqueset comportementales des individus tels que : l'iris, la voix, les empreintes digitales, le visage,la signature, l'empreinte palmaire, les veines des doigts …etc.

Dans les applications de contrôle d'accès, la biométrie permet d'accéder au niveau de sécuritésupérieur en ce qui concerne les accès logiques (ordinateurs, comptes bancaires, etc.) ou desaccès physiques (bâtiments sécurisés, aéroports, laboratoire s ,etc.) .

La biométrie regroupe deux axes principaux : une **identification** (reconnaissance) et une**Authentification**.

Dans le cas d'identification, le système biométrique demande une information biométrique etcompare avec chaque information stockée dans la base de données.

Alors que pour l'authentification utilisateur annonce son identité par une informationbiométrique, et le système compare les données obtenues à partir de l'information entrée avecla donnée enregistrée.

Il existe plusieurs techniques biométriques qui sont utilisées dans le contrôle d'accès,Chaque technique biométrique a ses avantages et ses inconvénients.

L'usage les veines des doigts en identification biométrique connu pour une augmentation etune utilisation très importantes dans les sociétés et dans les systèmes de gestion d'individus.

Dans le cadre de travail, notre objectif consiste à réaliser un système debiométrique basé sur les veines des doigts en tant que modalité biométrique, lechoix de cette modalité a été motivé par ce qu'elle est considéré comme étant commedomaine, entité unique, stable dans le temps et structure riche d'information.

Objectifs

Dans ce travail, l'un de ces systèmes a été choisi pour l'étude, qui est l'identification despersonnes à travers leurs images, les veines des doigts ou, plus précisément, un système quiutilise les veines des doigts de la main (FV). Cette méthode a été choisie en fonction de sesnombreux avantages, et c'est une technologie acceptable pour les particuliers, simple et facileà utiliser. Enfin, un mélange de tous les doigts (dix doigts dans les deux mains) peut êtreutilisé pour créer un système biologique robuste et précis.

Dans le cadre de ce travail, dans la première série d'expériences, nous avons conçu unsystème biométrique, c'est-à-dire un système qui utilise une seule méthode biométrique. Pourcela, trois algorithmes, BSIF et LBP, RADON, ont été utilisés pour l'étape la plus importante,qui est l'étape d'extraction caractéristique. Ces deux algorithmes sont largement utilisés pourl'analyse des tissus. Dans la deuxième série d'expériences, la fusion multimodale estexaminée pour un système biologique efficace.

L'organisation du manuscrit :

Dans le **premier**chapitre, nous avons identifié les différentes biométries et techniquesbiométriques appliquées dans le cas général. Ce chapitre a été complété par un aperçu des principaux domaines de l'identité vitale et de sa contribution au marché mondial.

Le **deuxième** chapitre, nous décrirons également les différents outils de travail, notamment les algorithmes BSIF, LBP et RADON.

Ensuite, le **troisième** chapitre est consacré à l'utilisation des expériences. Dans la première section de ce chapitre, nous introduisons en appliquant la description de la base de données, puis les critères d'évaluation dans nos systèmes. La deuxième section de ce chapitre examine les résultats expérimentaux obtenus pour les systèmes biologiques. Le scénario de fusion, c'est-à-dire le système dans lequel le système multi-algorithmes a été évalué. Afin de choisir le meilleur système, qui affiche l'identification la plus faible, une comparaison est également effectuée entre les différents systèmes.

Enfin, nous avons terminé notre mémoire avec une conclusion et quelques perspectives visées

Chapitre I

La biométrie

I.1 Introduction

Dans nos jours, la sécurité des individus est devenue un souci majeur, puisque le besoin de se protéger augmente jour après jour. Les méthodes de sécurité classiques des systèmes d'informations ne sont pas efficaces.

En effet, il existe deux manières de cette sécurité :

la première repose sur la connaissance de la personne comme « un mot de passe » ou « un code PIN »; dans ce cas, le mot de passe peut être oublié par son utilisateur ou bien deviné par une autre personne.

La seconde est basée sur ce que possède la personne comme « un badge » ou « une carte à puce », dans ce cas, le badge peut être perdu ou volé.

Pour contourner cette limitation, un autre moyen de sécurité a été développé qui permet d'utiliser, non pas l'information qu'un individu possède ou connait, mais une information intrinsèque à cette personne. Cette nouvelle façon d'identification des individus est dite: « la biométrie ».

Dans ce chapitre, nous commençons par la présentation de quelques généralités sur la biométrie telles que :

Sa définition, ses caractéristiques, et leurs domaines d'application. Ensuite, nous définissons les systèmes biométriques et le principe général de ses fonctionnements. A la fin, nous terminons le chapitre par la présentation de quelques modalités biométriques, une comparaison entre ces modalités, et la motivation de notre choix qui se focalise sur l'utilisation des « les veines des doigts »[1].

I.2 La biométrie

I.2.1 Définition

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

I.2.2 Pourquoi la biométrie…?

Avec l'attention croissante portée aux failles de sécurité et aux fraudes transactionnelles dans les industries et les sociétés, les techniques d'authentification et d'identification personnelleshautement fiables et accessibles deviennent une demande inévitable pour les sociétés humaines. La biométrie a émergé pour répondre à ce besoin et a même évolué vers la sciencecombinant la technologie de la biologie et la technologie de l'information pour utiliser les caractéristiques physiologiques ou comportementales du corps humain pour traiter l'identification des individus. En particulier, les technologies biométriques se concentrent sur les technologies permettant d'authentifier automatiquement les traits immobiles de l'humain tels que l'ADN, les oreilles, l'empreinte palmaire, les géométries des mains et des doigts, l'empreinte digitale, les visages, les iris, l'empreinte, la rétine et la dent ou les traits dynamiques de l'humain. tels que la voix, la démarche, la frappe et la signature. De plus, il semble que la biométrie sera et soit une composante dominante du monde et un nombreremarquablement croissant de systèmes de biométrie ont été développés pour satisfaire les besoins de recherche et commerciaux. Les systèmes biométriques ont été largement appliquésà une variété de domaines gouvernementaux et privés en tant que technologie en ce qui concerne la sécurité et la commodité. En outre, la biométrie a montré sa supériorité écrasante pour remplacer ou améliorer les méthodes d'identification traditionnelles, telles que les approches basées sur les jetons et les approches basées sur les connaissances[2].

I.2.3 Histoire de la biométrie :

Le terme biométrique vient des mots grecs bios et metrikos. La biométrie traite de l'identification des individus en fonction de leurs caractéristiques biologiques ou comportementales (Jain et Ross 2002). La biométrie combine la technologie de la biologie et latechnologie de l'information pour exploiter les caractéristiques physiques ou les caractéristiques comportementales du corps humain afin d'identifier l'identité d'une personne afin de remplacer ou d'améliorer les méthodes traditionnelles d'identification personnelle Avec les préoccupations croissantes concernant les atteintes à la sécurité et la fraude transactionnelle, des technologies de vérification et d'identification personnelles hautement fiables et pratiques sont de plus en plus nécessaires dans nos activités sociales et nos services nationaux. La biométrie est implémentée dans deux applications principales : la vérification d'identité et la reconnaissance d'identité. La vérification d'identité consiste à exiger que le

système dispose d'une option binaire, acceptation ou rejet, en réponse à la demande de la personne lorsque celle-ci revendique une identité. Cependant, la reconnaissance d'identité doit exiger que le système récupère la base de données préexistante des caractéristiques et identifie celle qui correspond aux caractéristiques de l'individu inconnu présenté. Historiquement, le développement des technologies biométriques provient de différents antécédents historiques. L'identification personnelle consiste à associer l'identité à un individu particulier . L'identification peut être considérée comme une forme de reconnaissance ou de vérification connue sous le nom d'authentification (Jain et al. 2000).

Les techniques d'identification personnelle basées sur les connaissances et les jetons ont été traitées comme les deux techniques traditionnelles largement utilisées (Miller, 1994). Les approches basées sur la connaissance authentifient l'identité d'un individu selon ce qu'il sait. Toute personne possédant certaines connaissances secrètes, telles que des numéros d'identification personnels ou un mot de passe pour les appels téléphoniques, l'adhésion ou les cartes de crédit, puis des réponses aux questions, recevrait le service associé. Dans l'approche par jeton, l'identité d'une personne est vérifiée en fonction de ce qu'elle possède. Toute personne possédant un certain objet physique (jeton), par exemple des clés ou des cartes d'identité, est autorisée à recevoir le service associé . Cependant, les approches basées sur les jetons et sur les connaissances ont certaines limites inhérentes, car elles ne sont basées sur aucune nature biologique intrinsèque de chaque individu pour une identification personnelle. Ces inconvénients sont généralement fatals et importants pour l'identification personnelle. Par exemple, les jetons peuvent être volés, perdus, oubliés, effacés ou égarés, et même les jetons sont faciles à tromper. Les techniques basées sur la connaissance présentent également des défauts. Par exemple, le numéro d'identification personnel (PIN) peut être oublié par un utilisateur valide ou deviné par une fraude . Parce que les caractéristiques des techniques d'identification personnelle basées sur les connaissances et les jetons ne peuvent pas être uniques, distinctives et distinctes, elles ne peuvent pas répondre aux exigences de sécurité de l'interconnexion électronique de la société de l'information en raison de la vulnérabilité frauduleuse. Afin de faire une percée dans les systèmes de vérification, de puissants systèmes d'identification n'ont jamais été plus demandés. La reconnaissance biométrique est une technologie émergente de reconnaissance personnelle développée pour surmonter les limites inhérentes au personnel traditionnel . approches de reconnaissance (Jain et al. 1999; Zhang 2000, 2002). La biométrie qui exploite l'instinct de caractéristiques physiologiques distinctives a émergé pour améliorer les techniques d'identification en vérifiant ou

reconnaissant automatiquement l'identité d'une personne vivante. Par rapport aux méthodes basées sur les jetons et les connaissances, les identifiants biométriques ne peuvent pas être facilement falsifiés, partagés, oubliés ou perdus, et peuvent ainsi offrir une meilleure sécurité, une plus grande efficacité et un confort d'utilisation accru. L'apparition de la biométrie rend l'authentification plus facile, plus rapide et plus précise. De plus, les identificateurs biométriques sont plus compétents et plus fiables que les techniques d'identification traditionnelles et ont également acquis une grande réputation [2] .

I.3 les Systèmes biométriques :

Généralement, un système biométrique est un système informatique mis en œuvre en exploitant les méthodes, techniques et technologies d'identification biométrique correspondantes. Les systèmes biométriques peuvent être considérés comme des systèmes de reconnaissance de formes, où un ensemble de caractéristiques est d'abord extrait des données acquises, puis comparé à l'ensemble de modèles stocké pour prendre une décision sur l'identité d'un individu. Un système biométrique peut être appliqué à deux domaines, la vérification et l'identification.

En mode vérification, la décision est de savoir si une personne est «qui elle prétend être?» En mode d'identification, la décision est «à qui appartiennent les données biométriques?» Un système biométrique est ainsi formalisé en un système de reconnaissance de formes à deux ou plusieurs classes [2].

- **La phase d'enrôlement ou d'apprentissage :**

Cette phase consiste à créer un modèle biométrique d'un individu qui doit être une référence pour la phase de reconnaissance. Pour ce faire, les caractéristiques biométriques de l'individu sont mesurées par un capteur biométrique, puis représentées sous forme numérique et enfin stockées dans une base de données. Pour assurer une certaine puissance du système aux variations temporelles de données, plusieurs échantillons d'acquisitions la même donnée peuvent être réalisés. Le traitement lié à l'enrôlement n'a pas de contrainte de temps, puisqu'il s'effectue « hors-ligne » [19].

- **La phase de reconnaissance :**

La reconnaissance peut être une vérification ou une identification:

- **Le mode de vérification ou d'authentification :**

La vérification est une comparaison "un à un", dans lequel le système valide l'identité

d'une personne en comparant les données biométriques saisies avec le modèle biométrique de cette personne stocké dans la base de données du système [20].

A ces deux modes de fonctionnement du système s'ajoutent souvent les deux processus suivants[20]:

- **La mise à jour**:le système biométrique peut périodiquement corriger le gabarit de référence lors d'un contrôle de façon à prendre en compte l'évolution de la donnée biométrique de la personne.
- **La fin de vie**:le gabarit et autres données de référence propres à la personne sont détruites pour prendre en compte sa suppression du système de contrôle centralisé.

Tout système biométrique comporte deux processus qui se chargent à réaliser les opérations d'enregistrement et de tests:

- **Processus d'enregistrement:**Ce processus a pour but d'enregistrer les caractéristiques des utilisateurs dans la base de données.
- **Processus de tests (identification /vérification):**Ce processus réalise l'identification ou la vérification d'une personne.

Dans chacun des deux processus précédents, le système exécute quatre opérations fondamentales, à savoir [18]:

- **L'acquisition:**

Cette phase consiste à utilisé un capteur pour acquérir une caractéristique spécifique de l'individu, plusieurs processus peuvent être utilisés pour l'acquisition tels que: le microphone dans le cas de la voix.

- **L'extraction:**

Après l'acquisition d'une image**,** nous réalisons l'extraction des caractéristiques dont le processus d'authentification a besoin. Donc, ce module sert à traiter l'image afin d'extraire uniquement les caractéristiques biométriques, sous forme d'un vecteur, qui peuvent être ensuite utilisées pour reconnaitre les personnes.

- **La classification (comparaison):**

En examinant les modèles stockés dans la base de données (vecteurs), les caractéristiques biométriques extraites sont comparées avec ce vecteur et en marquant le degré de similitude (différence ou distance).

- **La décision:**

En ce qui concerne l'authentification, la stratégie de décision nous permet de vérifier l'identité affirmée par un utilisateur ou déterminer l'identité d'une personne basée sur le degré de similitude entre les caractéristiques extraites et le(s) vecteur(s) stocké(s).

I.4 Les Caractéristiques biométriques :

La caractéristique biométrique est la donnée qui contient les informations de base permettant de distinguer les individus, et en pratique toute caractéristique physiologique ou comportementale peut être considérée comme une caractéristique biométrique, dans la mesure où elle est [3,4] :

- **Universelle :** existe chez tous les individus.
- **Unique :** différente pour chaque individu.
- **Permanente :** stable dans le temps.
- **Enregistrable :** atteignable. Mesurable : une technologie de capteur existe.
- **Utilisable :** acceptation par l'utilisateur.
- **Non imitable :** difficilement copiable.

1.5 Présentation de quelques technologies biométriques:

Aucune biométrie unique ne pouvait répondre efficacement aux besoins de toutes les applications d'identification. Un certain nombre de techniques biométriques ont été proposées, analysées, et évaluées. Chaque biométrie à ses forces et ses limites, et en conséquence, chaque biométrie est utilisée dans une application particulière. Pour les caractéristiques physiques, nous décrirons la reconnaissance de visage, les empreintes digitales, la géométrie de la main et l'iris. Pour les caractéristiques comportementales, nous décrirons les biométries basées sur la voix et la signature .

I.6 Modalités biométriques :

Il n'y a pas de biométrie unique qui puisse répondre efficacement aux besoins de chacunApplications d'identification. Un certain nombre de techniques biométriques ont été réaliséesSuggérer, analyser et évaluer, chaque biométrique a ses propres forces et limitesConséquences, toutes les données biométriques sont utilisées dans une application

spécifique. Les biométriques dépendent en deux techniques [6]:

- **Techniques intrusives :**Ces techniques requièrent un contact physique avec l'individu pour l'identifie tel que les empreintes digitales, la rétine, l'ris ou la forme de la main. Leur usage est généralement mal accepté.

- **Techniques non intrusives :** Ces techniques ne requièrent pas la coopération de l'individu en question. Leur application peut se faire à distance en utilisant des capteurs qui ne nécessitent pas de contact directe avec l'utilisateur (visage, démarche,…).

On peut classer les techniques biométriques en trois catégories :

- **Celles basées sur l'analyse de traces biologiques :**

  ce type de biométrie se fait à l'aide de l'ADN d'une personne, de son sang, ou de sa salive…

- **Celles basées sur l'analyse comportementale :**

  Se base sur l'analyse de certains comportements d'une personne comme le tracé de sa signature, l'empreinte de sa voix, sa démarche et sa façon de taper sur le clavier

- **Celles basées sur l'analyse morphologique:**

  est basée sur l'identification de traits physiques particuliers qui, pour toute personne, sont uniques et permanents. Cette catégorie regroupe la reconnaissance de la forme du visage, de la forme de la main, des empreintes digitales, de la rétine et de l'iris de l'œil .

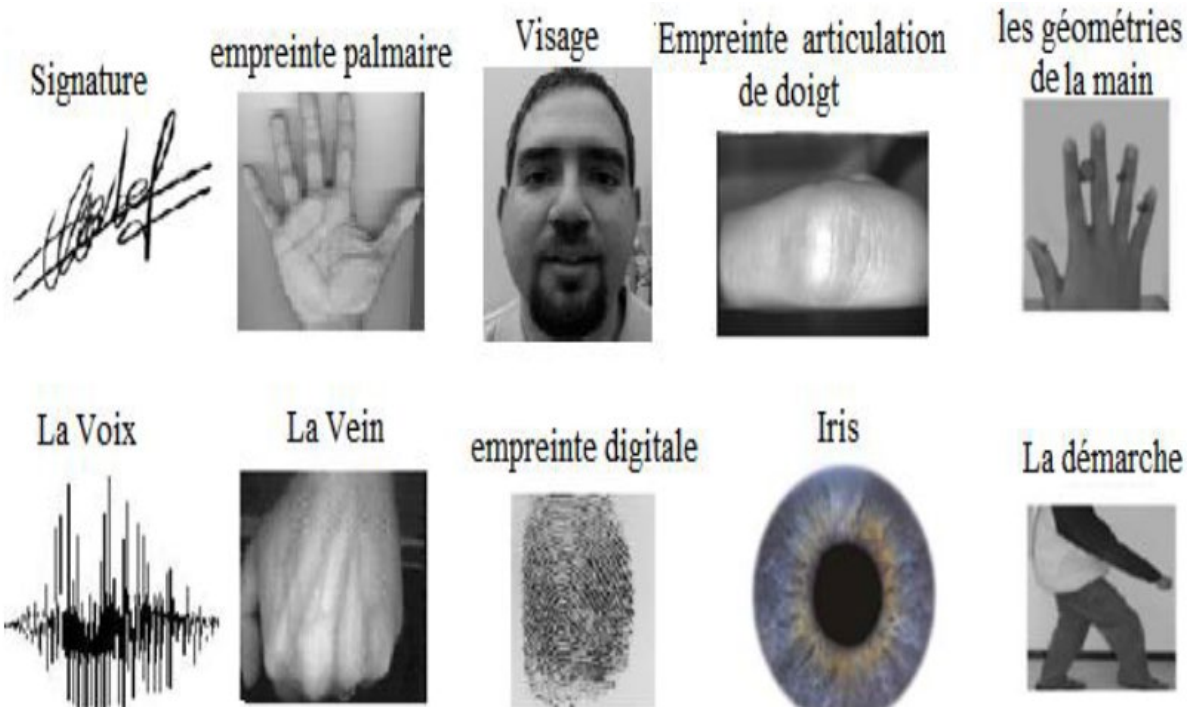


figure I.1:les techniques biométriques .

I.6.1 Analyse et mesure des caractéristiques biométriques :

L'identification biométrique consiste à analyser l'une des caractéristiques comportementales ou morphologiques de l'individu.

On distingue dans la pratique trois technologies biométriques :

A. Analyse comportementale :

L'individu possède plusieurs éléments liés à son comportement qui lui sont propres :

❖ **La dynamique des frappes au clavier (Key stroke-scan) :**

C'est un système de reconnaissance d'un individu basé sur la manière de ses écritures par un dispositif logiciel qui calcule la vitesse de la frappe, la suite des lettres, le temps de frappe et la pause entre chaque mot [7] (Figure I.2).

Généralement les facteurs comportementaux pris en compte son :

•Les durées entre les frappes.

•La fréquence des erreurs.

•La durée de la frappe elle-même.

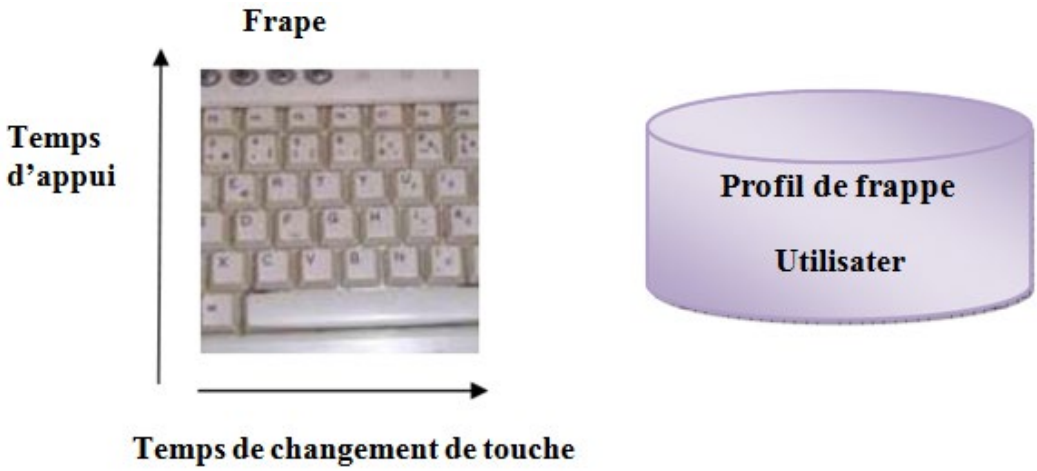


Figure I.2 : Reconnaissance par la dynamique du clavier .

❖ La reconnaissance vocale (Voice-scan) :

La voix humaine varie d'une personne à une autre et peut se constituer de composantes physiologiques et comportementales. L'identification par la voix est basée sur la forme et la taille des appendices (bouche, cavités nasales et les lèvres) et utilisées dans la synthèse du son [7]. La reconnaissance des locuteurs est plus utilisée par les téléphones, les corps policiers, les hôpitaux…etc. (Figure I.3).

Figure I.3 : Spectre d'un signal voix.

❖ La dynamique des signatures (signature-scan):

C'est une écriture personnelle d'un individu (Figure I.4), la vérification de la signature est basée sur deux modes: Mode statique: la vérification de la signature statique met l'accent sur les formes géométriques de la signature, dans ce mode, en générale, la signature est normalisée à une taille connue ensuite décomposer en élément simple. Mode dynamique: il utilise les caractéristiques dynamiques telles que l'accélération, la vitesse et les profils de trajectoire de la signature .[8]

Figure I.4: Signature .

lors de la signature, Ce dispositif va mesurer (la vitesse, l'ordre des frappes, la pression et les accélérations, le temps total…) Les difficultés liées à la capture d'une signature viennent du fait qu'une personne ne signe jamais deux fois de la même façon, même à quelques secondes d'intervalle. En effet suivant les émotions ou la fatigue, une signature peut fortement évoluer. D'où la mise au point d'algorithmes très complexes capables de prendre en compte ces évolutions possibles .

- **Démarche**

Chaque personne a une façon particulière de marche, nous pouvons identifier les individus de la nature du mouvement des jambes, des bras et des articulations ou le mouvement spéciale obtenus par un caméra vidéo afin de l'envoyer à un ordinateur pour l'analyse afin de déterminer la vitesse et l'accélération de chaque individu .[7]

Figure I.5: Démarche.

B.Analyse morphologique :

Il existe plusieurs caractéristiques physiques qui se révèlent être uniques pour un individu , et il existe également pour chacune d'entre elles plusieurs façons de les mesurer :

- **Reconnaissance par empreintes digitales (finger –scan) :**

La reconnaissance des individus par empreintes digitales est la technique biométrique la plus utilisée. Les empreintes digitales sont composées de lignes localement parallèles

présentant des points singuliers (minuties) et constituent un motif unique, universel et permanant, comme montré dans la Figure I.6. Les lecteurs d'empreintes digitales scannent puis relèvent des éléments permettant de différencier les empreintes. Il existe plusieurs types de minuties. Ce type de technique biométrique est utilisé par les institutions financières pour leurs clients et se trouve en même temps dans les hôpitaux, les écoles, les aéroports…etc . [4,8].

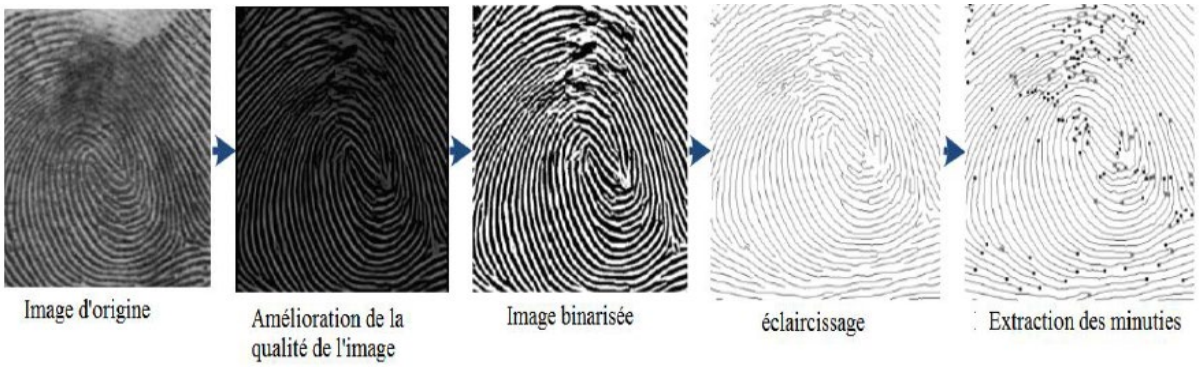


Figure I.6 : Le processus de reconnaissance par empreinte digitale.

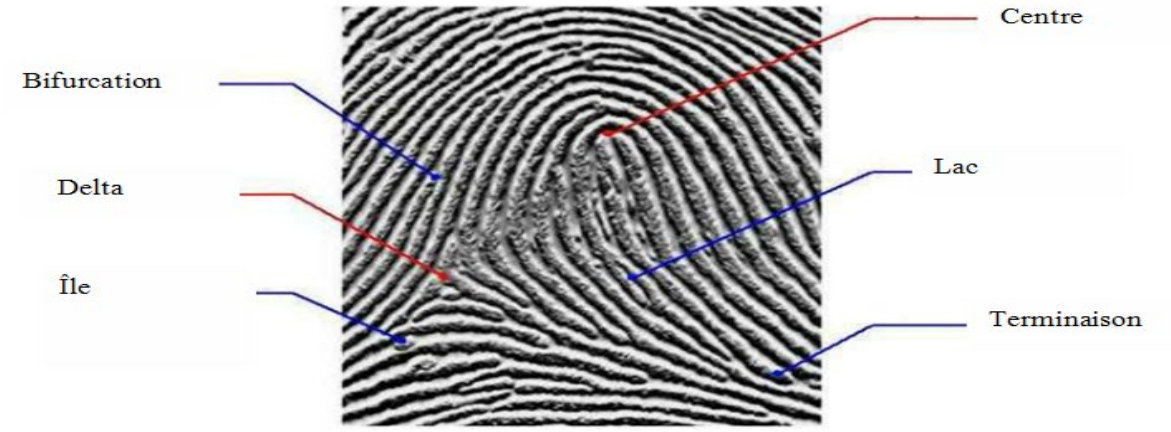


Figure I.7 : Représentation d'une empreinte digitale .[34]

il existe plusieurs techniques d'acquisition de l'empreinte digitale (capteur optique, thermique, ultrason…), le procédé consiste former une image à partir des points de contact du doigt sur le capteur .

❖ Reconnaissance par Iris :

L'iris est une région sous forme d'anneau, située entre la pupille et le blanc de l'œil, elle 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 a été développée dans les années 80, elle est donc considérée comme une technologie 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 (Figure 1.8). [9]

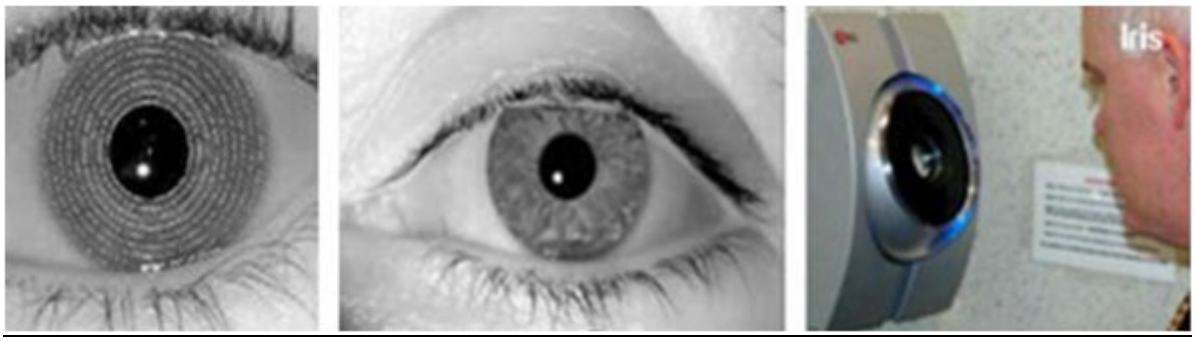


Figure I.8 : Photo d'iris.

L'individu se place en face du capteur (caméra CCD/CMOS) qui scanne son iris. L'iris présente une quasi-infinité de points caractéristiques qui ne varient pas pendant la vie d'une personne contrairement à la couleur de l'iris qui, elle, peut changer. Des problèmes peuvent se poser à cause des reflets qui nécessite d'avoir un éclairage restreint et maitrisé, et lors de la détection des faux yeux (photos) et autres fraudes.

❖ Reconnaissance faciale :

Nos visages sont des objets complexes avec des traits qui peuvent varier dans le temps, comme montré dans la Figure 1.9. L'écart entre les deux yeux, l'écartement des narines ou encore la largeur de la bouche peuvent permettre d'identifier un individu. Cette méthode doit pouvoir tenir compte de certain changement de la physionomie (lunettes, barbe, chirurgie esthétique) et de l'environnement (conditions d'éclairage). Parfois, il est impossible de différencier deux jumeaux. [9,10]

Figure I.9 : Reconnaissance faciale .

❖ Empreintes des articulations des doigts :

C'est une technologie biométrique basée sur la surface arrière du doigt, elle contient des caractéristiques distinctives telles que les lignes principales, les lignes secondaires et les crêtes, qui peuvent être extraites à partir des images à basse résolution (Figure 1.5). La main contient plusieurs doigts, pour cela, il faut conserver les informations à chaque doigt pour une reconnaissance précise dans le domaine d'identification. [8,33]

Figure I.10: système biométrique basé sur les articulations des doigts.

❖ La géométrie de la main :

Cette technique utilise la surface intérieure de la paume pour l'identification et/ou la vérification des personnes (Figure I.8). Elle est bien adaptée pour les systèmes à moyenne sécurité telle que le contrôle d'accès physique ou logique .[8,]

Figure I.11:Géométrie de la main.

❖ Empreintes Palmaires « Palmprints » :

Palmprint est l'une des nouvelles modalités biométriques les plus efficaces et qui s'appuie sur la texture de la paume de la main. Récemment, il a été montré que les lignes principales et les

rides dans une image palmprint sont uniques [35,36]. En général, la plupart des gens ont trois lignes principales: la ligne du cœur, la ligne de tête et la ligne devie.

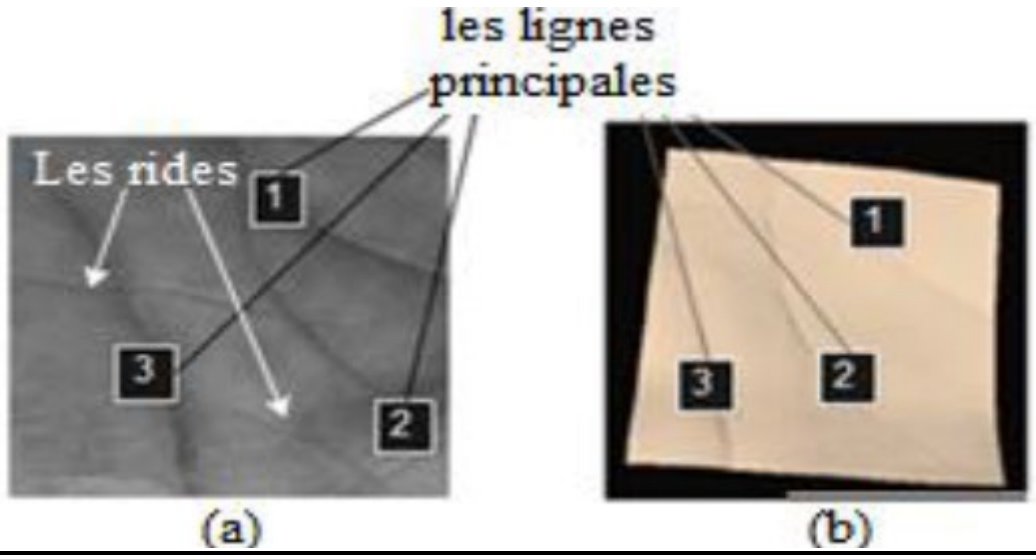


Figure 1. 12 : Empreinte palmaires : (a) 2D (b) 3D

C. Analyses biologiques

❖ L'odeur corporelle :

Chaque personne dégage une odeur qui lui est particulière. Les systèmes biométriques qui exploitent cette technologie analysent les composantes chimiques contenues dans l'odeur pour ensuite les transformer en données comparatives.

❖ L'A.D.N. (Support matériel de l'hérédité) :

Il est la façon la plus précise pour déterminer l'identité de la personne. Il est impossible de trouver deux personnes qui ont le même ADN. Cette modalité possède l'avantage d'être unique et permanant durant toute la durée de vie.[8]

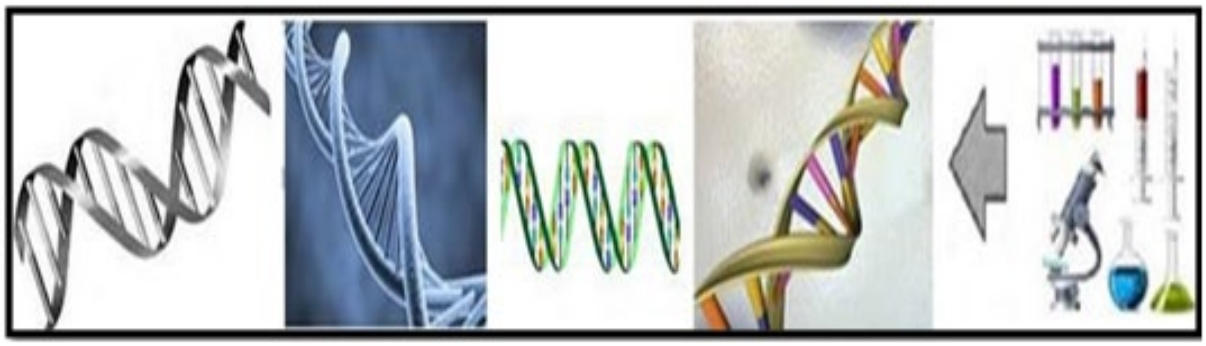


Figure I.13 : L'A.D.N.

❖ La reconnaissance de la thermographie faciale :

Une caméra infrarouge capte la chaleur émise par la peau. contrairement àReconnaissance faciale, afin que nous puissions l'utiliser même dans l'obscurité ou dans de mauvaises conditions de vision. Mais les conditions de prise de vue peuvent entraîner des erreurs.[8]

Figure I.14:la thermographie faciale.

❖ Veines de la main :

Les veines de la main sont des réseaux qui varient d'une personne à une autre (Figure I.11).

L'analyse de cette différence permet de maintenir des points pour différencier une personne à une autre .

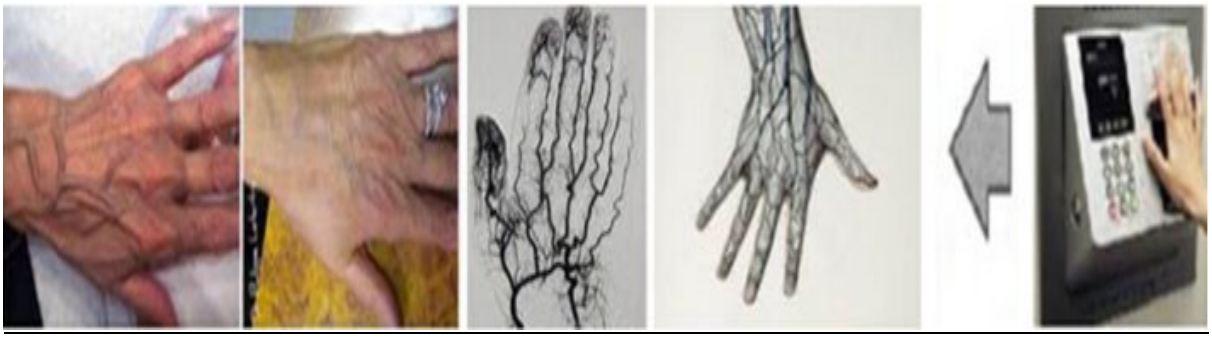


Figure I.15 : Système biométrique basé sur les veines de la main.

Techniques biométriques	universelles	uniques distinctif	Permanente	Enregistrable Mesurable	Performance Acceptabilité
Empreintes digitales	Moyenne	Haute	Haute	Moyenne	Moyenne
Visage	Haute	Faible	Moyenne	Haute	Haute
Iris	Haute	Haute	Haute	Moyenne	Faible
Rétine	Haute	Haute	Moyenne	Faible	Faible
ADN	Haute	Haute	Haute	Faible	Faible
Signature	Faible	Faible	Faible	Haute	Haute
Voix	Moyenne	Faible	Faible	Moyenne	Haute
Démarche	Moyenne	Faible	Faible	Haute	Haute
Frappe clavier	Faible	Faible	Faible	Moyenne	Moyenne
Veines d main	Moyenne	Moyenne	Moyenne	Moyenne	Moyenne

Tableau I.1: Comparaison entre les modalités biométriques .[9]

Il existe de nombreuses technologies biométriques au travail dans différentes applications.

Chaque technologie biométrique a des avantages et des inconvénients, le choix dépend donc de l'application. L'utilisation des **veines des doigts** pour identifier la biométrie est une nouvelle manière de porter des qualités exceptionnelles qui la qualifient pour être l'une des méthodes idéales d'identité biométrique, ce qui en fait une entité unique, stable dans le temps, et une structure riche en informations.

I.7 Architecture et fonctionnement des systèmes biométriques :

Un système biométrique est un système de reconnaissance des personnes qui ne procède en premier pas par l'acquisition des données biométriques de l'individu à reconnaître, puis extrait un ensemble de caractéristiques à partir de celles-ci, enfin il compare ces caractéristiques avec les modèles de la base de données. L'architecture d'un système Biométrique est illustrée sur la Figure. I.12.

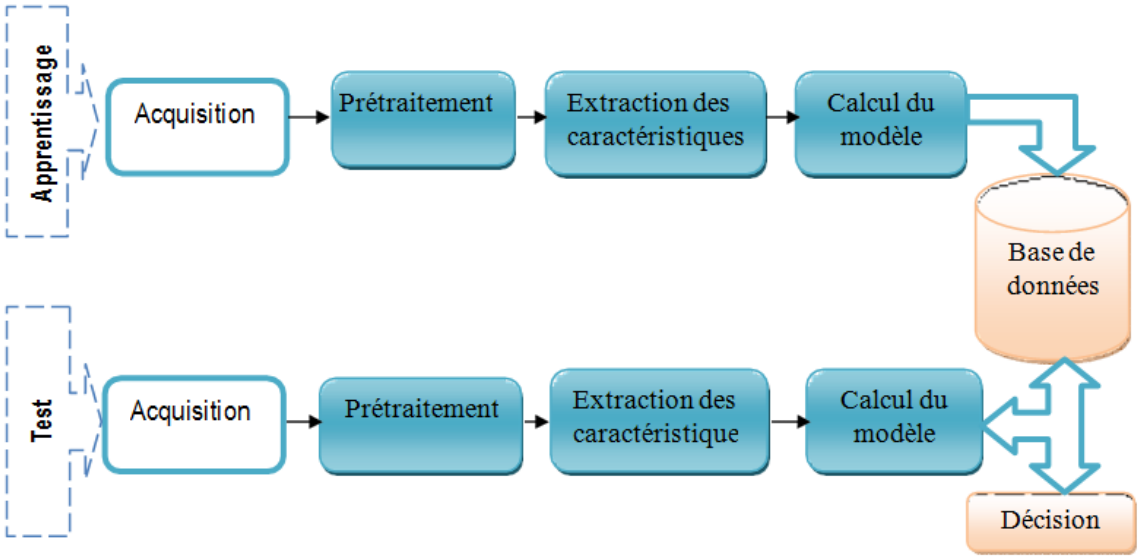


Figure I.16 : Architecture d'un système biométrique **.**

En effet, il existe deux phases , la phase d'entrainement et la phase de test :

Pendant la phase d'entrainement les données biométriques d'un individu client appartenant au système sont stockées dans une base de données. Typiquement, les données biométriques acquises par module de capture (une caméra de sécurité, un lecteur d'empreintes digitales, etc.) sont traitées par le module d'extraction de caractéristiques afin d'extraire des traits saillants et distinctifs pour chaque individu. Pendant la phase de reconnaissance, la donnée biométrique acquise par personne de test est comparée avec les données stockées par le

module de comparaison. La détermination de l'identité de l'utilisateur se fait par le module de décision. Un système biométrique peut fonctionner soit en mode vérification ou identification.

I.7.1 Mode Vérification

Dans ce cas, le système compare la donnée de test (de la personne de test) avec la donnée biométrique stockée dans la base de données pour vérifier l'identité déclarée. Dans ce genre de système, la comparaison n'est faite qu'une fois et sert ensuite à prendre une décision à partir de la sortie du module de comparaison, appelée aussi one-to-one (1:1) (voir Figure. I.13).

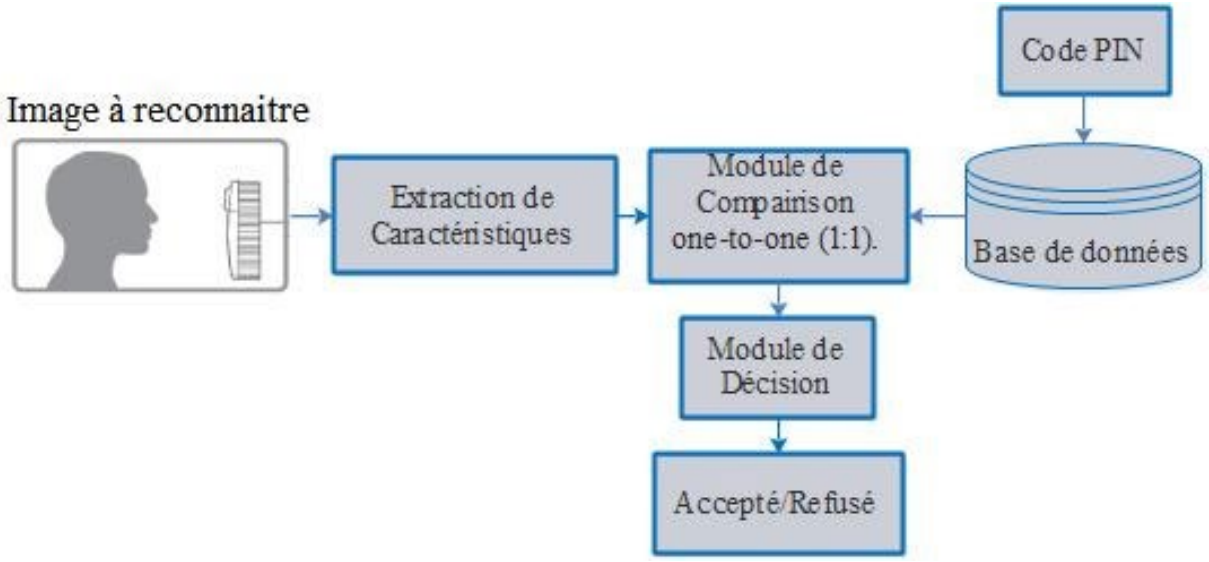


Figure I.17 :Architecture duMode Vérification **.**

I.7.2 Mode identification

Dans ce cas, le système compare la donnée de test avec toutes les références stockées dans la base de données et sert ensuite à prendre une décision à partir de la sortie du module de comparaison (voir Figure I.14), appelée aussi one-to- many (1:N) .

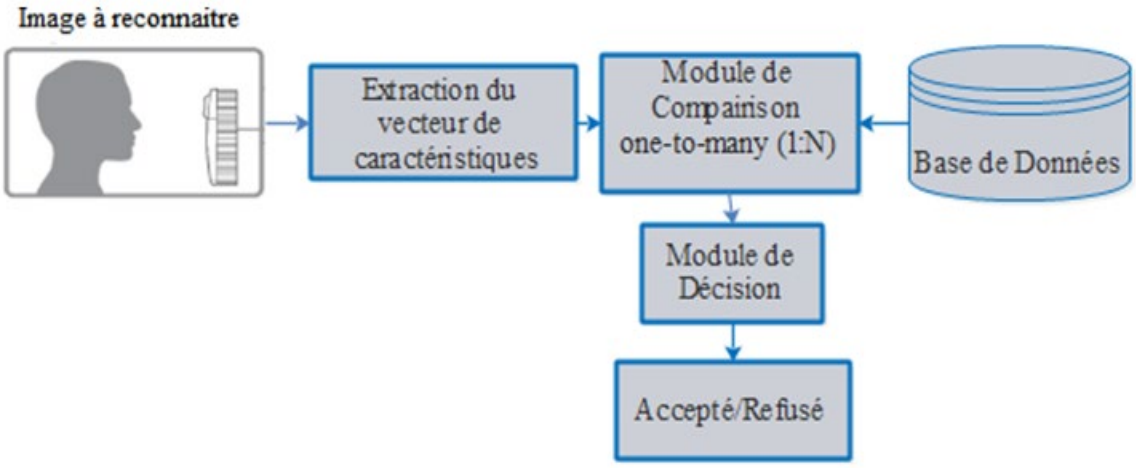


Figure I.18 : Architecture du mode identification.

I.8 Principaux Modules

Le système biométrique est un système pour identifier les tendances et le stockage des données à sauvegarder ou de les identifier dans la forme de matrices. Ensuite, le système est prêt à identifier les intrus. Ce système se compose de quatre unités : l'acquisition, l'extraction des caractéristiques, la comparaison (mesure de similarité) et la décision. L'inscription ou l'enrôlement est utilisé pour une future comparaison tandis que la décision est de reconnaître la personne ou non.

- **Le module de capture :** est 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, etc.,).
- **Le module d'extraction de caractéristiques :** 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. Généralement, cette nouvelle représentation est censée être unique pour chaque personne et relativement invariante aux variations intra-classes .
- **Le module de correspondance** : 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**.**
- **Le 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).

I.9 Évaluation d'une performance

En comparant avec les systèmes d'authentification basés sur des objets ou mot de passe qui retournent des réponses absolues (Oui ou Non), les systèmes biométriques sont plus fluctuantes donnent des réponses en termes de pourcentage de similitude (entre 0% et 100% et le 100% n'étant jamais atteint) . La solution était donc de définir un seuil de décision (acceptation ou refus) compris entre 0% et 100% de similitude au sein des applications. Ce seuil peut être différent pour chaque personne.Les performances des systèmes d'authentification biométriques s'expriment par :

❖ **Taux d'erreurs :** Lorsqu'un système en mode de vérification ou identification ensemble ouvert, il existe deux types d'erreur qui peuvent être utilisés pour évaluer leur performance. La première erreur mesure le taux de faux rejet (False Rejection Rate ou**FRR**) et la deuxième erreur mesure le taux d'acceptation des imposteurs, on parle alors à la Fausse acceptation (FalseAcceptance**Rate** ou **FAR**).

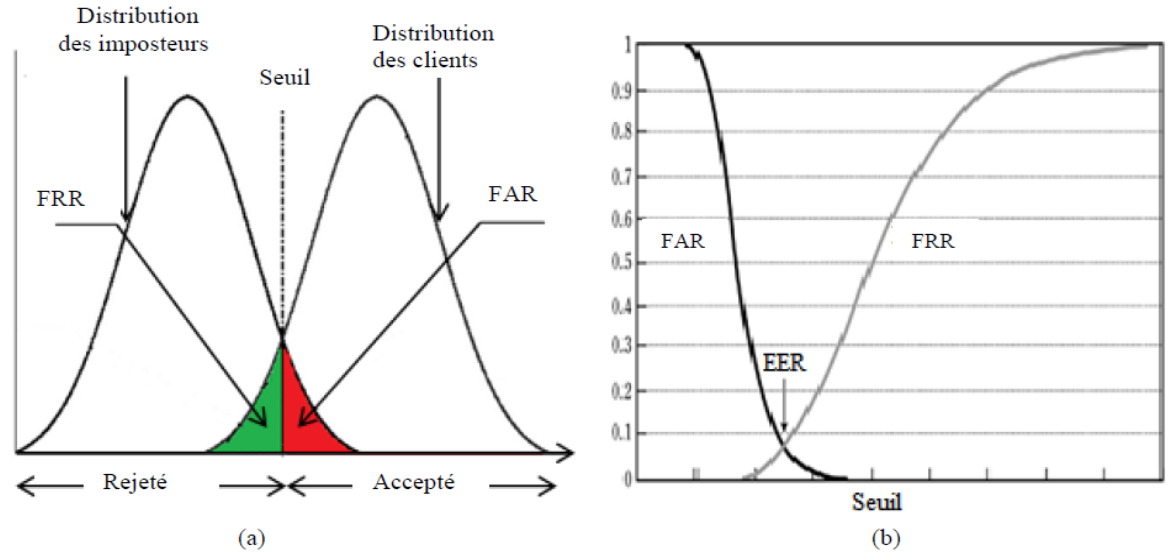


Figure I.19: Distribution des scores et les taux d'erreurs pour un seuil donné :(a) Distributions des Scores client et des scores imposteur ; (b) Variation des FRR et des FAR en fonction du seuil [11].

- ❖ Le **F.R.R** (False Rejection Rate) : Taux de Faux Rejets : Pourcentage de personnesrejetées par erreur.[11]
- ❖ Le **F.A.R** (False Acceptance Rate) : le Taux de Fausses Acceptations donne le pourcentage d'acceptations par erreur.

- Le **E.E.R** (EqualError Rate): le Taux d'Egale Erreur donne un point sur lequel le F.R.R. est égal au F.A.R. Ces taux vont dépendre de la qualité des systèmes, mais aussi du niveau de sécurité souhaité.

I.10 Domaines d'applications :

Le champ d'application de la biométrie est très vaste. En effet, tous les domaines qui nécessitent de vérifier ou déterminer l'identité d'une personne sont concernés. D'où les applications de la biométrie peuvent être divisées en trois groupes principaux [5]:

- ✓ **Applications commerciales :** telles que l'ouverture d'un réseau informatique, la sécurité de données électroniques, l'e-commerce, l'accès Internet, les cartes de crédit, le contrôle d'accès physique, le téléphone cellulaire, la gestion des registres médicaux, l'étude à distance … etc. [14]

- ✓ **Applications gouvernementales :** telles que la carte d'identité nationale, le permis de conduire, la sécurité sociale, le contrôle des frontières, le contrôle des passeports, etc .

- ✓ **Applications légales :** telles que l'identification de corps, la recherche criminelle, l'identification de terroriste… etc.

I.11 Choix d'une caractéristique biométrique

Le choix d'une modalité dépend de sa nature d'un côté et niveau de sécurité qu'elle apporte aux applications (certain modalités présentent des contraintes d'ergonomie, de cout d'acceptabilité) ainsi que l'environnement de leur usages (facilité d'emploi, d'analyse, de stockage, et de vérification).

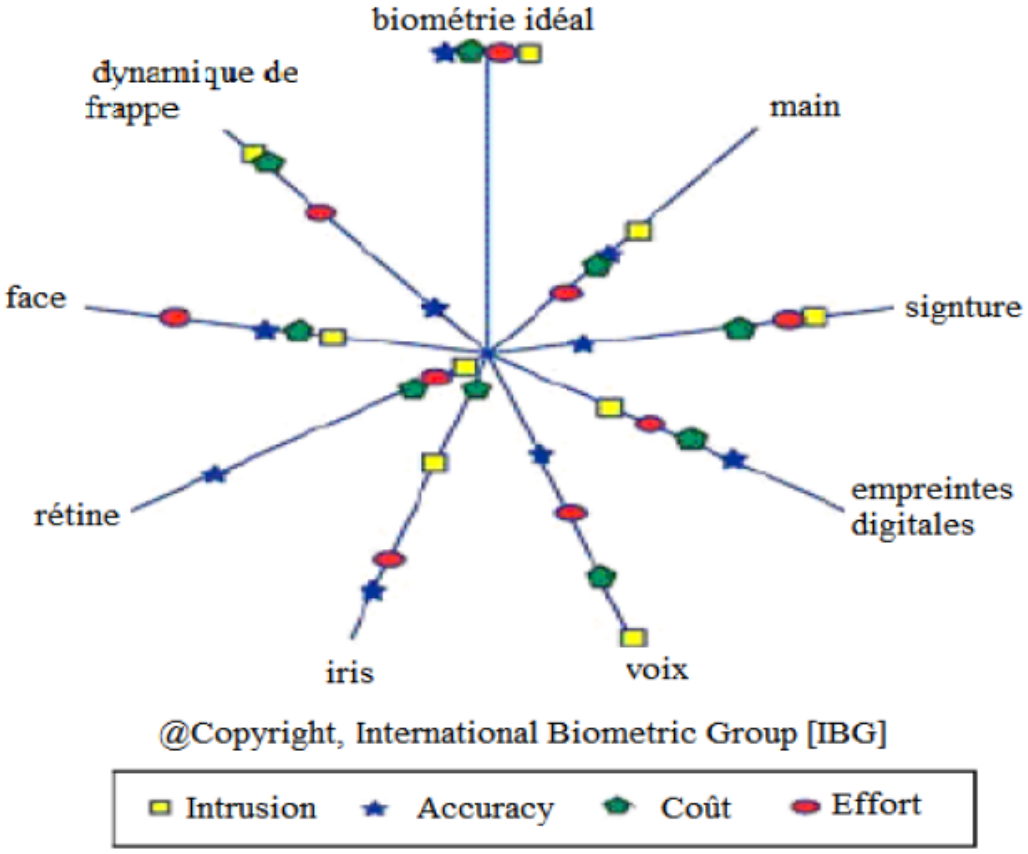


Figure I.20: Critères de choix des caractéristique biométriques.

Nous remarquons dans la figure I.21 que l'empreinte digitale est proche d'être une modalité idéale par rapport aux autre caractéristique biométrique, de par son efficacité, son cout minimal de mise en œuvre avec un moindre effort requis par l'utilisateur, ce ci rend intrusive la méthode surtout que c'est la plus ancienne et la plus nature.

I.12 Le marché de la biométrie

La biométrie connaît un engouement sans précédent. La croissance mondiale de la biométrie depuis quelques années est incontestable, tant le nombre d'intervenants est grand, même s'il existe peu d'informations publiques concernant ce marché.

On peut toutefois considérer certaines données et certains chiffres sur son évolution au fil des années, tant à l'échelle mondiale, qu'américaine, européenne ou française.

Le marché de la sécurité informatique est encore atomisé, peu de fournisseurs peuvent prétendre offrir une gamme complète de produits. Les spécialistes estiment que ce marché est en pleine croissance et qu'il va également se concentrer.[18]

Dans son rapport intitulé « Sen sors for Biométrie and Recognition 2016 », l'Institut d'études Yole Développement estime que les technologies d'empreintes digitales dominantes évolueront progressivement vers des solutions multimodales. La conclusion la plus importante souligne que le secteur des applications smart phone constitue le moteur majeur du développement de la biométrie à près de 66% du marché total de la biométrie.

La biométrie pour le consommateur bénéficiera sans doute d'une croissance de l'ordre de 10% de 2016 à 2021, selon les analystes de Yole.[15]

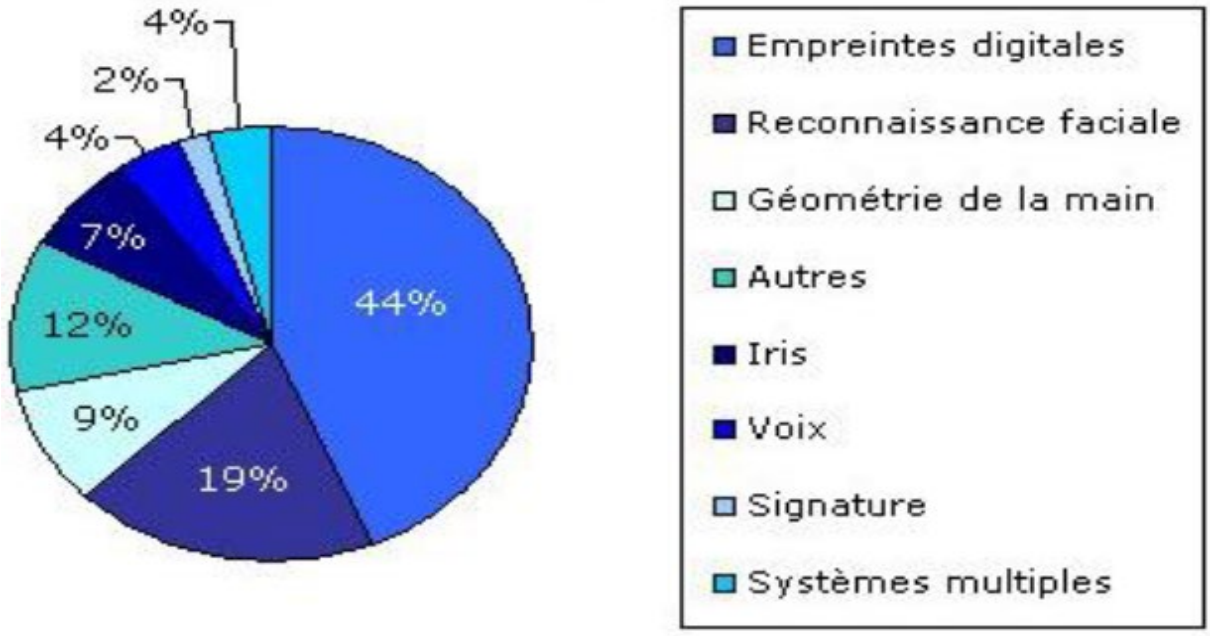


Figure I.21 : Les parts de marché par technologie[15].

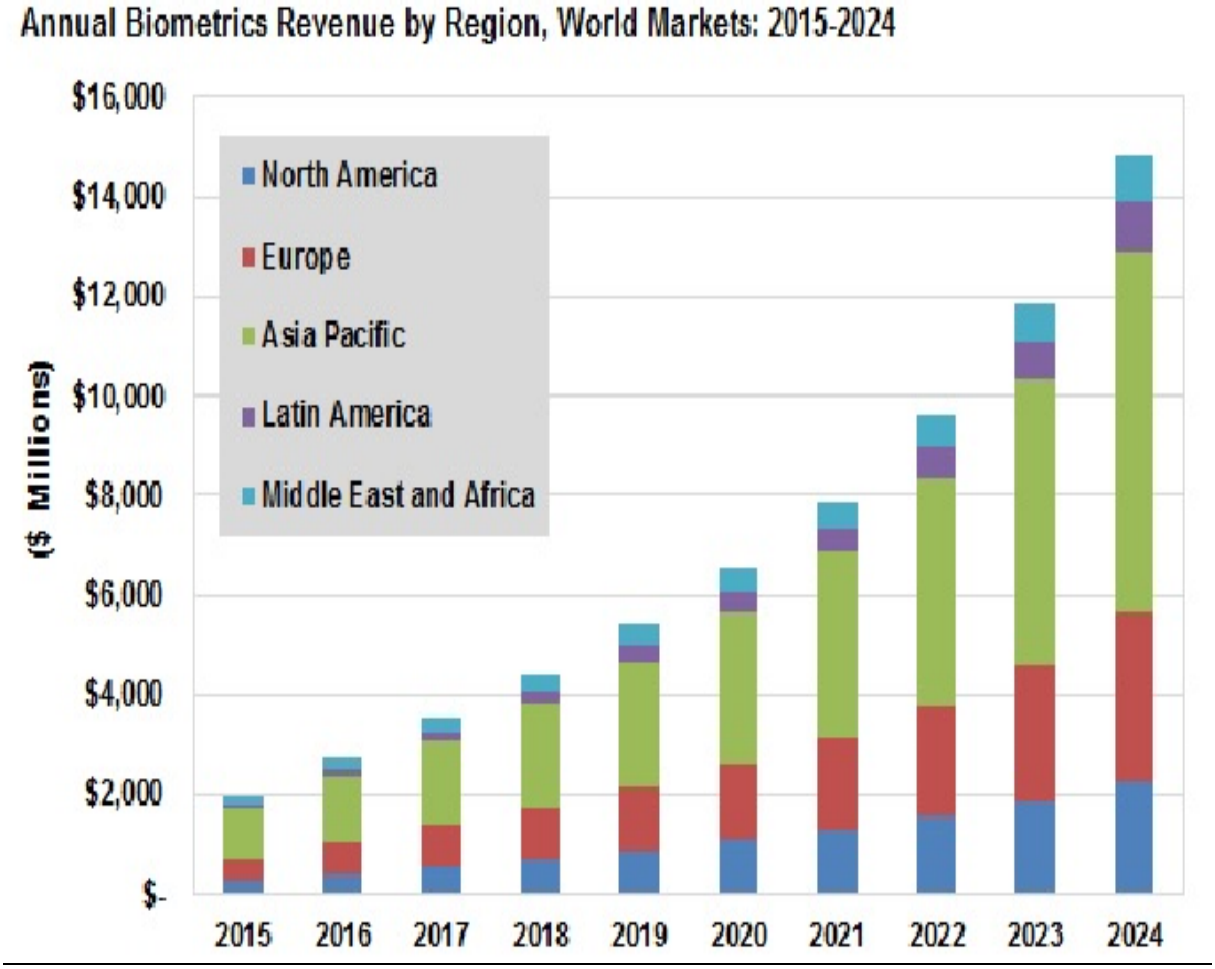


Figure I.22 : La croissance de la biométrie [15].

I.13Conclusion :

Dans ce chapitre, nous décrivons les techniques utilisées dans les systèmes biométriques Connaître les gens et leurs différentes structures et applications Nous avons fourni un aperçu des techniques d'analyse comparative des systèmes Différentes modalités biométriques sont présentées avec mise en évidence Les avantages et les inconvénients de chacun.

Chaque technologie biométrique possède des avantages mais aussi des inconvénients, acceptables ou inacceptables suivant les applications. Ces technologies n'offrent pas les mêmes niveaux de sécurité ni les mêmes facilités d'emploi ou encore pas la même précision.

Nous avons également constaté que la performance des systèmes critiques dépend de Plusieurs facteurs diffèrent d'un système à l'autre.

Chapitre II

LE SYSTEME DE RECONNAISSANCE DES VEINES DES DOIGTS PROPOSE

II.1 Introduction

Nous connaissons tous les processus de reconnaissance de la rétine ou même les processus de reconnaissance d'empreintes digitales, et les technologies utilisées à des fins d'authentification regroupées sous le terme de «biométrie».

Ils sont utilisés pour diverses applications, notamment dans le domaine de la sécurité. Cependant, la biométrie a considérablement progressé ces dernières années. Ainsi, un nouveau système de sécurité biologique est apparu, basé sur l'identification des doigts intraveineux.

Au cours des années 1990, les scientifiques ont identifié un nouveau composant pour chaque individu: leur réseau veineux. Cependant, cet élément morphologique n'a pas été utilisé à des fins d'identification. Il a fallu plusieurs années avant d'être utilisé à des fins différentes. Certains professionnels de la sécurité ont suggéré son «infaillibilité». Ils soutiennent surtout le fait qu'il s'agit de "biométrie sans trace", et qu'il est donc presque impossible de les répéter. En effet, il est basé sur une comparaison d'images d'enchevêtrement vasculaire avec son caractère «invisible».

Comme il ne peut pas être pris, tout comme les empreintes digitales, qui se déposent partout sur différents objets (verre, poignée de porte, etc.), le risque de fraude est complètement éliminé. Aussi, s'appuyer sur le réseau de veines du doigt est une technologie qui peut être un coup dur pour le secteur bancaire et le secteur public, car certaines institutions bancaires s'intéressent désormais à ce processus biométrique, qui doit révolutionner les procédures de certification. Ainsi, il doit permettre aux clients d'accéder à leurs comptes bancaires et d'effectuer diverses transactions sans avoir à saisir de code PIN ou à utiliser un lecteur de carte.

A travers ce chapitre, nous allons présenter la méthode de prétraitement utilisée pour les FV (Finger-vein), ainsi que les méthodes d'extraction des caractéristiques. En particulier et leur classification, A la fin, nous terminons par une conclusion[21].

II.2 Architecture globale du système FV (Finger-vein) :

Pour déterminer l'identité de la personne avec la reconnaissance de FV, il faut nécessairement référencer les images FV, sous la forme d'une base de données de FV de toutes les personnes connues par le système. A chaque image est associé un vecteur des caractéristiques. Ces caractéristiques sont supposées être invariantes pour une même personne, et différentes d'une personne à l'autre. La reconnaissance consiste alors à comparer

le vecteur de caractéristiques du FV à reconnaitre avec celui de chacun des FV de la base de données.[22]

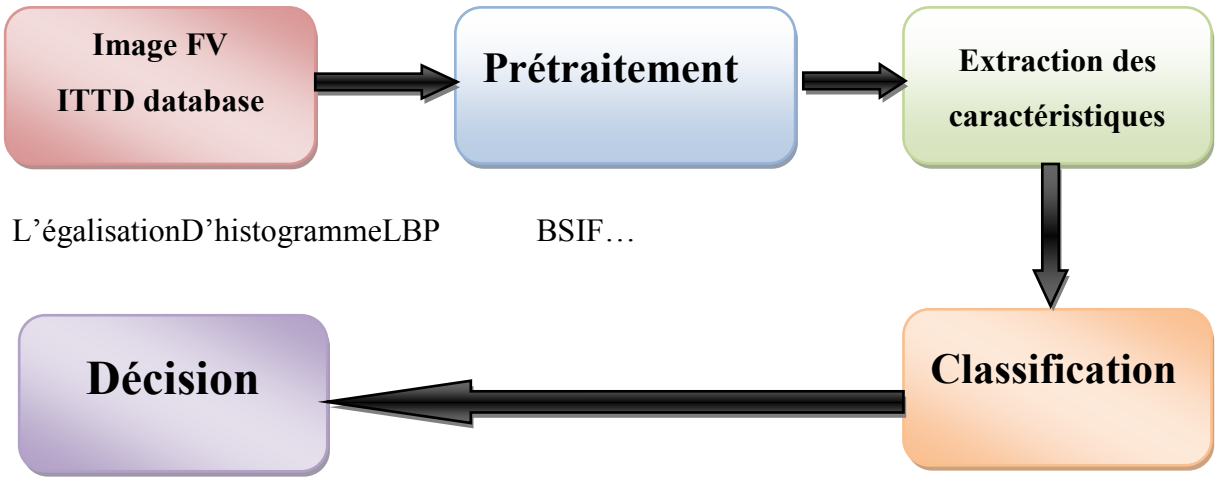


Figure II.1 : Architecture globale du système FV.

II.2.1 Le prétraitement d'une image :

L'étape de prétraitement vient après l'étape de détection. Il aide à préparer l'image FV afin qu'elle puisse être utilisée dans la phase d'enregistrement. Elle est également appelée étape de normalisation car elle renvoie toutes les images extraites de l'image brute dans un format prédéterminé. Il consiste généralement à centrer la zone principale de l'image et à supprimer les zones non multimédias.Pour améliorer le contraste, nous avons appliqué **légalisation d'histogramme**.

L'histogramme d'une image mesure la distribution des niveaux de gris dans l'image. Pour un niveau de gris x, l'histogramme permet de connaître la conversation de tomber sur un pixel de valeur x en tirant un pixel au hasard dans l'image.

Concrètement, l'histogramme d'une image à valeurs entières est construit de la manière suivante: pour chaque niveau de gris x, on compte le nombre de pixels ayant la valeur x.

Cela se fait par les étapes suivantes:

- **Etape 1** : Calcul de l'histogramme $h(i)$ $i \in [0,255]$
- **Etape 2** : Normalisation de l'histogramme $h_{n=}\frac{h(i)}{Nbp} i \in [0,255]$
  - Nbp **:** nombre de pixels de l'image.
- **Etape 3** : Densité de probabilité normalisé $c(i) = \sum_{j=0}^{i} h_{n\,(j)}$ $i \in [0,255]$
- **Etape 4** : Transformation des niveaux de gris de l'image $f'(x,y) = c(f(x,y)) \times 255$

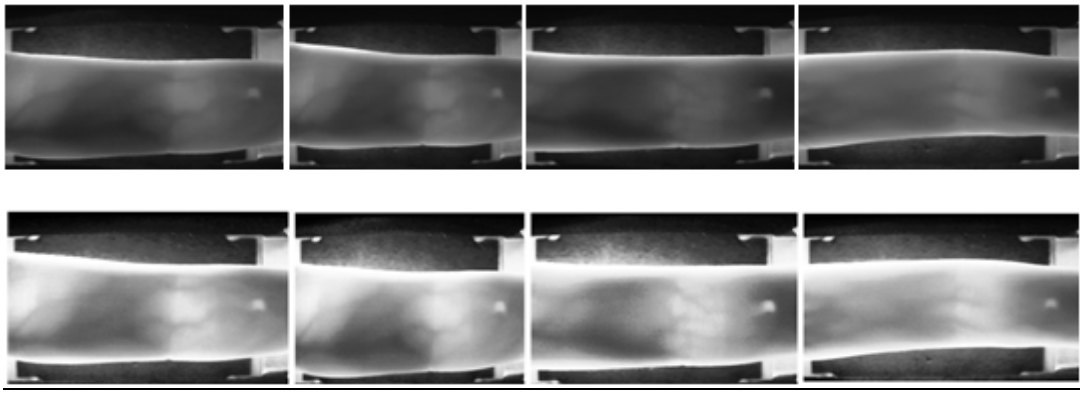


Figure II.2: leprétraitement des images de veines des doigts.

II.2.2 Génération des caractéristiques :

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. L'extraction des caractéristiques utilise plusieurs méthodes, Parmi lesquelles on cite **LBP, BSIF** et **T RADON**[22].

II.3 Etat De L'art Sur Les Méthodes d'Extraction Des Caractéristiques :

La génération des caractéristiques est une étape cruciale dans tout système de reconnaissance. Généralement on peut distinguer deux approches:

- Approche statistique.
- Approche géométrique.

II.3.1 Approche statistique [24]

Les caractéristiques statistiques représentent la densité et la distribution des pixels dans une image. Parmi les caractéristiques statistiques les plus utilisés, on peut citer :

- **Moyenne :** représente le nombre des pixels noirs sur le nombre des pixels de la fenêtre.

$$\bar{X}=\frac{1}{N}\times\sum_{i=1}^{N} x_i$$

- **Variance :** mesure donc la dispersion autour de la moyenne**.**

$$\sigma^2 \frac{1}{N\text{-}1}\sum_{i=1}^{N}(x_i\text{-}\bar{X})^2$$

- **Entropie :** mesure la quantité d'information contenue dans le champ des données extraites. Elle est calculée selon l'équation :

$$E= -\sum_i p_i . \log(p_i)$$

Où $\boldsymbol{p_i}$ est la probabilité d'occurrence des pixels.

Une entropie faible informe sur l'uniformité de la zone alors qu'une entropie forte informe sur l'hétérogénéité.

II.3.2 Approche géométrique :

Plusieurs méthodes ont été proposées pour générer un vecteur caractéristique en tenant compte de la géométrie de la forme [25]. Nous pouvons citer : les concavités, moments géométriques. [26]

Dans notre cas, nous avons choisi la transformée de Radon pour ses propriétés intéressantes. Pour cela nous rappelons dans les sections suivantes ses principales propriétés ainsi la méthodologie retenue pour générer le vecteur caractéristique.

II.4 Extraction Des Caractéristiques Avec La T.RADON :

II.4.1 Définition :

En mathématiques, la transformation du radon est la transformation intégrale qui prend une fonction f spécifique au niveau en une fonction RF spécifique à l'espace (bidimensionnelle) pour les lignes dans un plan, dont la valeur dans une ligne donnée est égale à l'intégrale de la ligne sur la ligne. La conversion a été introduite en 1917 par Johan Radon, qui a également fourni une formule pour la conversion inverse. Le radon a également inclus des formules de transformation en trois dimensions, où l'intégration dépasse les aéronefs (appelée intégration transversale en tant que conversion aux rayons X). Il a ensuite été généralisé aux espaces euclidiens de dimensions supérieures, et plus largement dans le contexte de l'ingénierie intégrée. L'analogue complexe de la conversion du radon est connu sous le nom de conversion de Pen rose. La conversion du radon est largement applicable à la tomodensitométrie et à la création d'une image à partir de données de projection associées à des scans d'objets.

II.4.2 Propriétés de La T.RADON :

La transformée de Radon consiste à projeter l'image sur une droite :

$(\Delta : \rho = \mathrm{x}.cos\theta + \mathrm{y}.sin\theta)$

pour n'importe quelle valeur de ($\boldsymbol{\rho}$, θ) avec **ρ** la distance de Δ à l'origine du repère et θ l'angle entre l'axe des abscisses et la normale à (Δ). La transformée de Radon d'une fonction I(x , y) est définie par :

$$T_{R^I}(\rho\,,\theta) = \int_x \int_y f(x,y)\delta(x.cos\theta + y.sin\theta - \rho)\,dx\,dy$$

Où : est la fonction de Dirac.

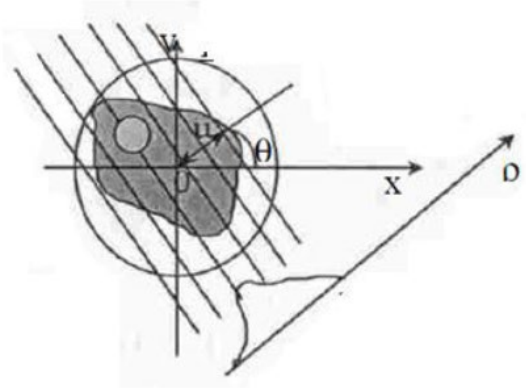


Figure II.3 : Définition de la transformée de Radon [27]

La rotation de l'objet entraîne un déphasage dans l'espace de Radon qui peut être corrigé simplement. La difficulté de l'utilisation de la transformée de Radon réside surtout dans la translation (qui modifie la transformée de manière non-linéaire) et le changement d'échelle (qui implique des modifications sur les coordonnées radiales et les amplitudes de la transformée).[28]

II.5 Extraction Des Caractéristiques Avec LesLBP:

II.5.1 Définition :

Les modèles binaires locaux (LBP) sont un type de descripteur visuel utilisé pour la classification en vision par ordinateur. Le LBP est le cas particulier du modèle Texture Spectrum proposé en 1990. Le LBP a été décrit pour la première fois en 1994. Il s'est depuis avéré être une caractéristique puissante pour la classification des textures; il a en outre été déterminé que lorsque LBP est combiné avec le descripteur Histogramme de gradients orientés (HOG), il améliore considérablement les performances de détection sur certains ensembles de données. Une comparaison de plusieurs améliorations du LBP d'origine dans le domaine de la soustraction de fond a été réalisée en 2015 par Silva et al.[29]

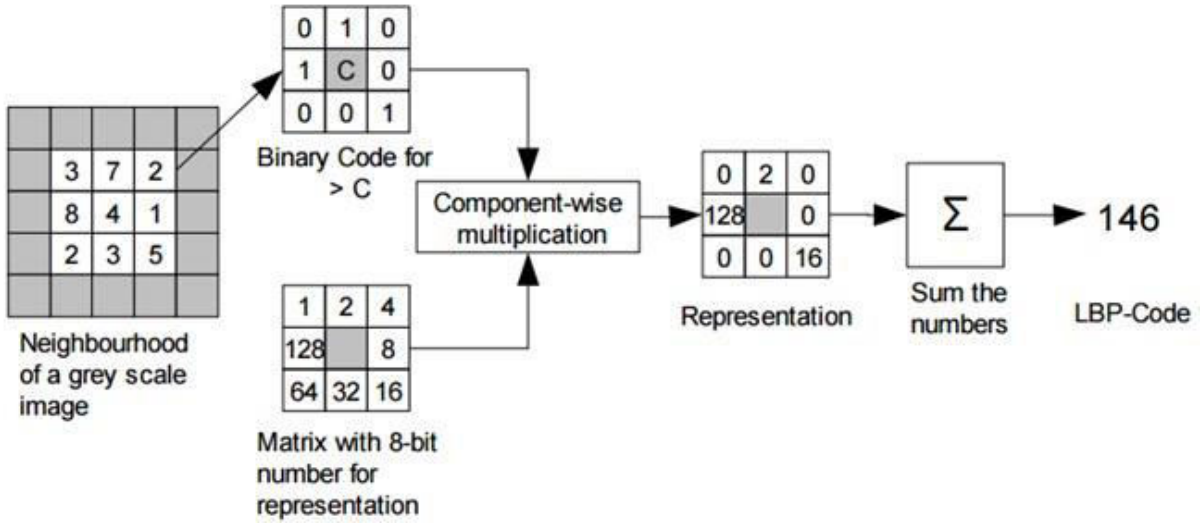


Figure II.4: Une illustration de LBP basique**.**

Soit g*c* un pixel dans l'image d'entrée, ses p pixels voisins sont (g0,g1,…,g$P-1$).

La réponse LBP du pixel g*c* est calculée comme suit :

$$\text{LBP}\ (xc,) = \sum p-1\ f(x)(gi - gc\ ).\ 2i$$

Où f(x) est la fonction de seuillage, donnée par :

$$(x) = \begin{cases} 1\ six \geq 0 \\ 0\ \ x < 0 \end{cases}$$

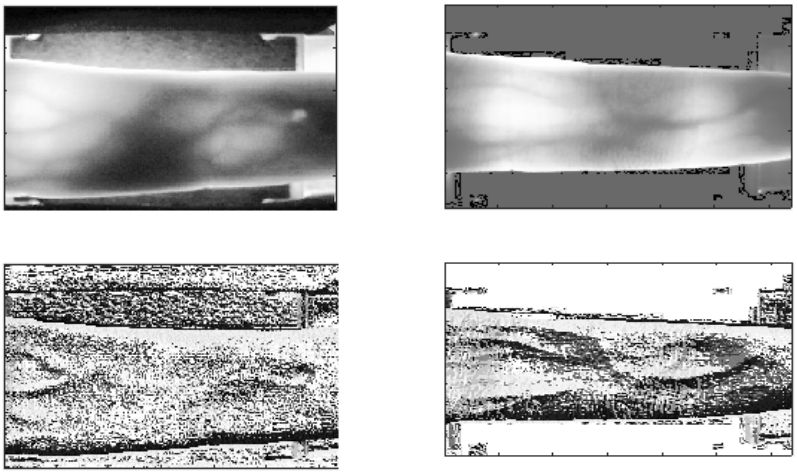


Figure II.5 : Quelque modalité et leurs images LBP.

LBP a été étendu ultérieurement basant sur des voisinages de taille différente (un voisinage de P pixels différentes c-à-dire différentes échelles) et la forme circulaire de rayon R (Voir Figure II.7).

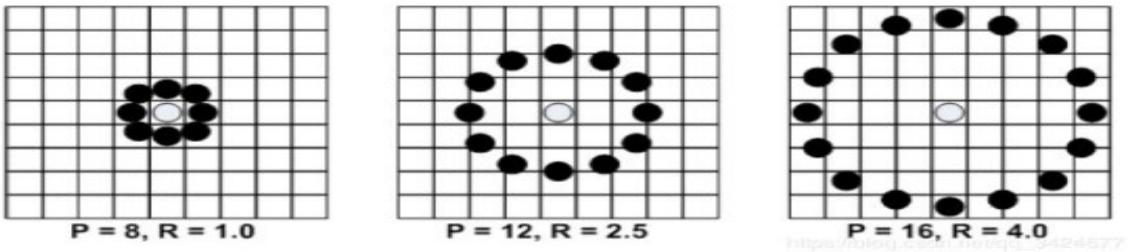


Figure II.6: Exemples de d'opérateur **LBPP**.**R**. Source.

II.5.2 Résultats De L'implémentation :

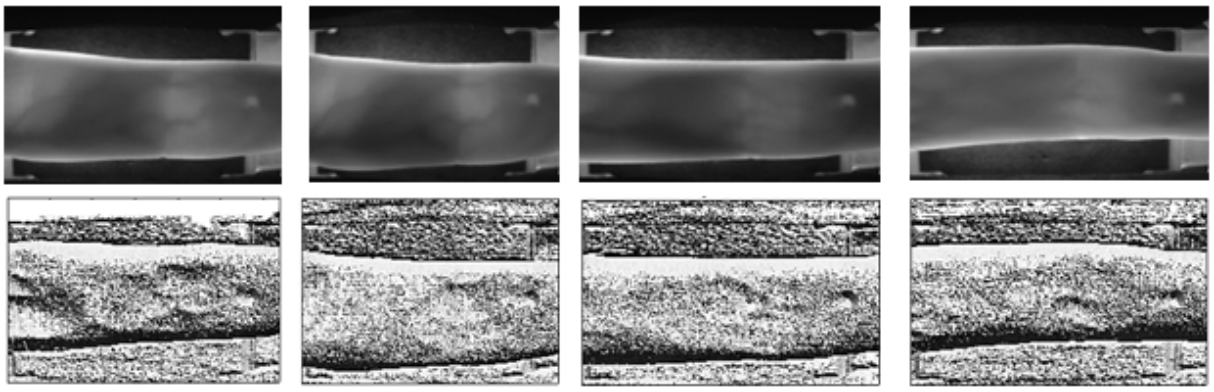


Figure II.7: (a) 4 images de FV (b) Résultats de l'étape d'extraction des caractéristiques par la méthode LBP.

II.6 Extraction Des Caractéristiques Avec Les BSIF :

II.6.1 Définition

BSIF est un descripteur local récent pour reconnaître des textures. BSIF descripteur a été mentionné pour la première fois par J. Kannala et E. Rahtu en 2012 [30]. Ce descripteur est basé sur un ensemble de filtres linéaires de taille fixe. BSIF filtre une image donnée I de taille NxN pixels avec un ensemble de filtres ${Q_I}^{N\times N}$alors les réponsesri sont binarisme. J. Kannala et E Rahtu utilisent un ensemble des images naturelles (ça-dire-appliqué les concepts introduites dans [31]) pour former un ensemble des filtres ${Q_I}^{N\times N}$, ces filtres sont estimés en maximisant l'indépendance statistique des répons ri par ICA. Également, nous avons utilisé les filtres open-source

$$ri = \sum x,y {Q_I}^{N\times N}(x, y)I(x, y).$$

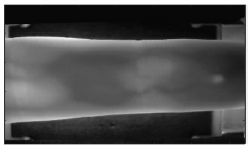
Où ${Q_I}^{N\times N}$est un filtre linéaire de taille N et i= {1, 2… n} indique le nombre de filtres statistiquement indépendants dont la réponse peut être calculée ensemble et binarisée pour obtenir la chaîne binaire comme suit :

$$b_i = \begin{cases} 1 si r_i > 0 \\ 0 si r_i \leq 0 \end{cases}$$

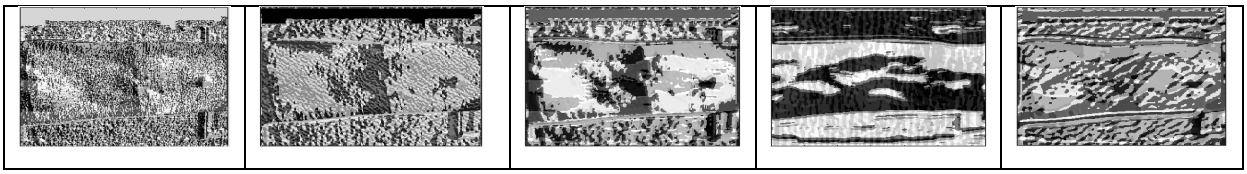
Enfin, les fonctions BSIF sont extraies comme l'histogramme des codes binaires de Chaque pixel. BSIF caractérise efficacement les composants de texture de l'image. Il existe deux facteurs importants dans le descripteur BSIF:

la taille du filtre N et n la longueur du filtre. L'image et l'image filtrée par BSIF correspondantes sont représentées sur la Figure II.9. La Figure II.9.a indiqué un exemple d'image FV. La Figure II.9 .b représente le filtre BSIF de taille 11x11 et de longueur 12. La Figure II.9.c montre les résultats de la convolution de l'image FV avec un filtre BSIF. La Figure II.9.de montre image filtrée par BSIF filtre .

(a)



(b)



(c)

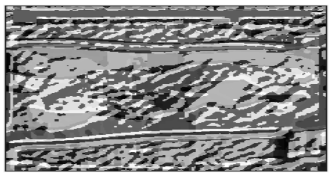


Figure II.8: (a) Exemple d'image FV. (b) Les résultats de la convolution de l'image FV avec des filtres BSIF. (c) Image finale FV filtrée par BSIF filtre.

II.6.2 Résultats De L'implémentation :

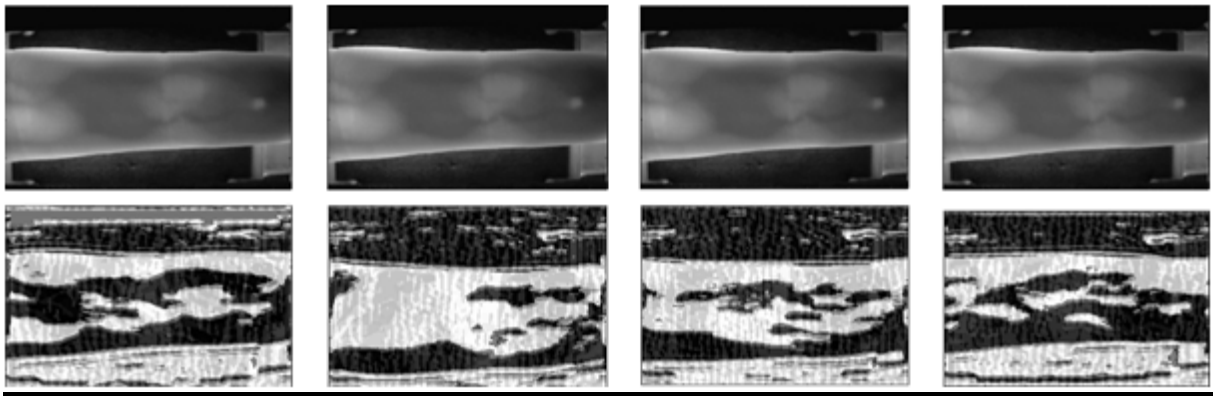


Figure II.9: Résultats de l'étape d'extraction des caractéristiques pour 4 FV d'une seule personne(BSIF).

II.7 Extraction Des Caractéristiques Avec La Fusion Entre le Filtre de BSIF et Transforme de RADON :

Afin d'améliorer les performances de notre système, nous proposons de fusionner les différentes caractéristiques (Radon et BSIF). Pour cela, et comme un exemple : Le vecteur caractéristique se compose de 384 composantes :

•256 composantes liées à la transformée de Radon.

•128 composantes liées à la transformée de BSIF

II.8 Normalisation des données :

Généralement, les composantes d'un vecteur caractéristique sont de nature hétérogène pouvant influer considérablement sur la qualité de la reconnaissance. Aussi, une solution à ce problème consiste à normaliser les caractéristiques de sorte que leurs valeurs se situent dans des gammes similaires. Une technique simple est la normalisation par les estimations de la moyenne et de la variance. Pour les données disponibles de la caractéristique , chaque composante du vecteur caractéristique via l'équation :

$\hat{X} = \frac{x_{ik} - \bar{x}_k}{\delta_k}$

Avec $\bar{x}_k = \frac{1}{N} = \sum_{i=1}^{N} x_{ik}$, $k = 1,2,\dots,l$

$$\delta_k^2 = \frac{1}{N-1}\sum_{i=1}^{N}(x_{ik} - \bar{x}_k)^2$$

l: désigne le nombre de vecteurs caractéristiques.

En d'autres termes, tous les composants du vecteur uniforme résultant sont uniformes Vous aurez maintenant une variation de zéro et d'unité. Évidemment c'est un moyen Le linéaire. D'autres techniques linéaires limitent les valeurs de caractéristique dans l'intervalle[0,1]Ou[1,1],par une mise à l'échelle appropriée. En plus des routes linéaires, des routes Les données non linéaires peuvent également être utilisées dans les cas où les données ne sont pas présentes . Également répartis autour de la Méditerranée. Dans ce cas, les transitions basées sur fonctions non linéaires (logarithmique ou sigmoïde) peuvent être utilisées, comme par exemple la fonction soft max dite qui se compose de deux étapes :

$$y = \frac{x_{ik} - \bar{x}_k}{r\delta_k} \,, \hat{x}_{ik} = \frac{1}{1 + \exp(-y)}$$

Il s'agit essentiellement d'une fonction d'écrasement des données en les limitant dans la gamme de [0, 1]. En effet, il n'est pas difficile de voir que pour les petites valeurs de yc'est une fonction approximativement linéaire par rapport à xki.

La gamme des valeurs dexki qui correspondent à la partie linéaire dépend de l'écart-type et le facteur, qui est définie par l'utilisateur. Les valeurs plus lointaines de la moyenne sont écrasées de façon exponentielle.

II.9 L'étape de classification :

Cette étape consiste à modéliser les paramètres extraits d'une modalité d'un individu en se basant sur leurs caractéristiques communes. Un modèle est un ensemble d'informations utiles, discriminantes et non redondantes qui caractérise un ou plusieurs individus ayant des similarités, ces derniers seront regroupés dans la même classe, et ces classes varient selon le type de décision .[33]

II.9.1 Machine à vecteurs de support(SVM) :

SVM (Support Vector Machine ou Machine à vecteurs de support) : Les SVMs sont une famille d'algorithmes d'apprentissage automatique qui permettent de résoudre des problèmes tant de classification que de régression ou de détection d'anomalie. Ils sont connus pour leurs solides garanties théoriques, leur grande flexibilité ainsi que leur simplicité d'utilisation même sans grande connaissance de l'exploration de données. Il peut résoudre des problèmes linéaires et non linéaires et fonctionne bien pour de nombreux problèmes pratiques. L'idée de SVM est simple: l'algorithme crée une ligne ou un hyperplan qui sépare les données en classes.

Les classifieurs SVM utilisent l'idée de l'hyperplan Optimal pour calculer une frontière entre des nuages de points. Elles projettent les données dans l'espace de caractéristiques en utilisant des fonctions non-linéaires. Dans cet espace on construit l'hyperplan optimal qui sépare les données transformées. [32]

L'idée principale est de construire une surface de séparation linéaire dans l'espace des caractéristiques qui correspond à une surface non-linéaire dans l'espace d'entrée.

II.9.1.1 La façon dont SVM trouve la meilleure ligne :

Selon l'algorithme SVM, nous trouvons les points les plus proches de la ligne des deux classes. Ces points sont appelés vecteurs de support. Maintenant, nous calculons la distance entre la ligne et les vecteurs de support. Cette distance s'appelle la marge. Notre objectif est de maximiser la marge. L'hyperplan pour lequel la marge est maximale est

l'hyperplan optimal. Ainsi SVM essaie de faire une frontière de décision de telle manière que la séparation entre les deux classes (cette rue) soit aussi large que possible.

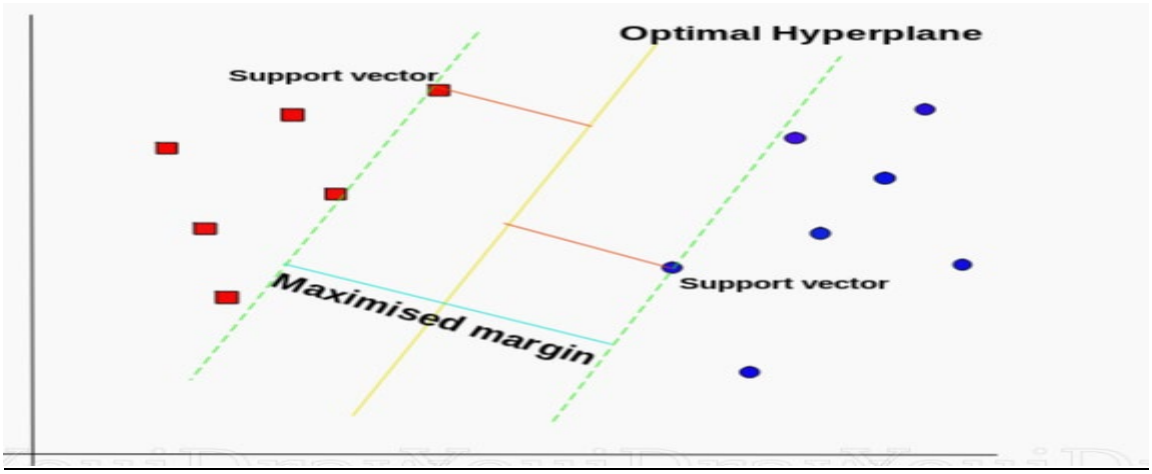


Figure II.10 : La façon dont SVM trouve la meilleure ligne .

II.9.1.2 Principe de SVM :

Les classifieurs SVM utilisent l'idée de l'hyperplan Optimal pour calculer une frontière entre des nuages de points. Elles projettent les données dans l'espace de caractéristiques en utilisant des fonctions non-linéaires. Dans cet espace on construit l'hyperplan optimal qui sépare les données transformées. L'idée principale est de construire une surface de séparation linéaire dans l'espace des caractéristiques qui correspond à une surface non-linéaire dans l'espace d'entrée.

Le problème principal à relever ici est comment bien manipuler la transformation de tous les vecteurs d'entrée dans l'espace des caractéristiques de façon à éviter une augmentation du coût en nombre de paramètres libres

L'approche SVM passe par deux étapes :

Etape d'apprentissage : la recherche d'un hyperplan optimal de séparation en maximisant la marge, avec la résolution d'un programme quadratique et détermination des multiplicateurs de Lagrange .

Etape de test : après la détermination des multiplicateurs de Lagrange, on applique la fonction de décision sur l'échantillon de test pour déterminer sa classe .

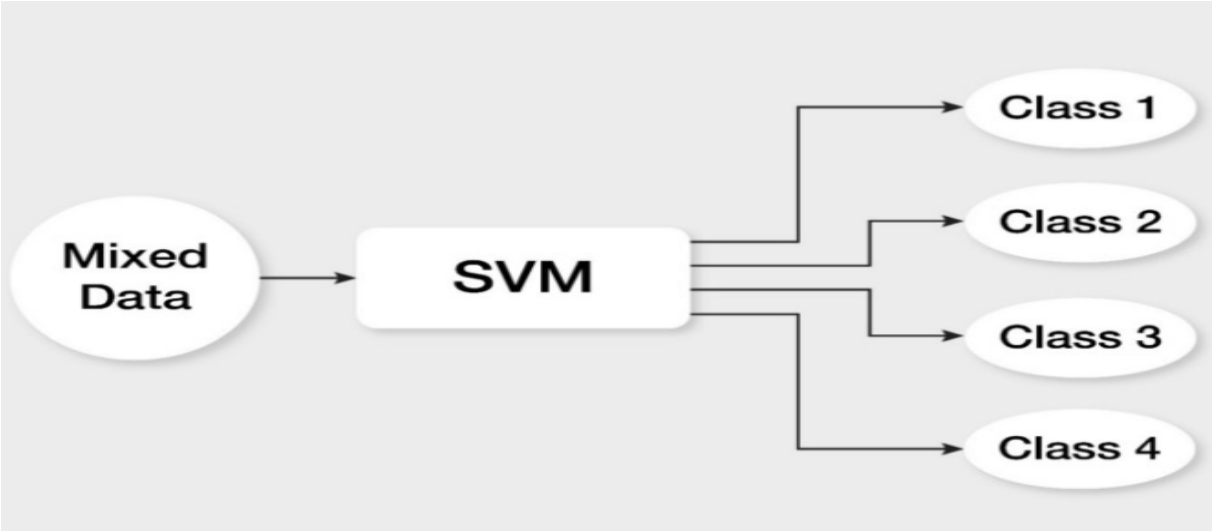


Figure II.11: Principe de la technique SVM**.**

II.9.2 Architecture du classifieur SVM proposée :

Comme nous l'avons vu dans la section 3.4 de ce chapitre, les SVM sont proposées initialement pour traiter des problèmes de classification linéaires binaires. Leur extension aux problèmes non linéaires multi-classes, qui représentent le cas de la majorité des applications réelles est actuellement un domaine de recherches très actif. Plusieurs approches ont été proposées dans ce sens tel que : un contre un, un contre tous, méthodes directes,… ; Cependant, des études [27] comparatives récentes ont prouvé que la méthode « un contre tous » est meilleure du point de vu généralisation et temps d'exécution, par rapport aux autres approches, nous avons utilisé SVMs binaire puisque chaque classifieur binaire n'a à discriminer qu'entre deux classes. Aussi, nous avons choisi d'implémenter ce classifieur pour traiter notre problématique figure II.13.

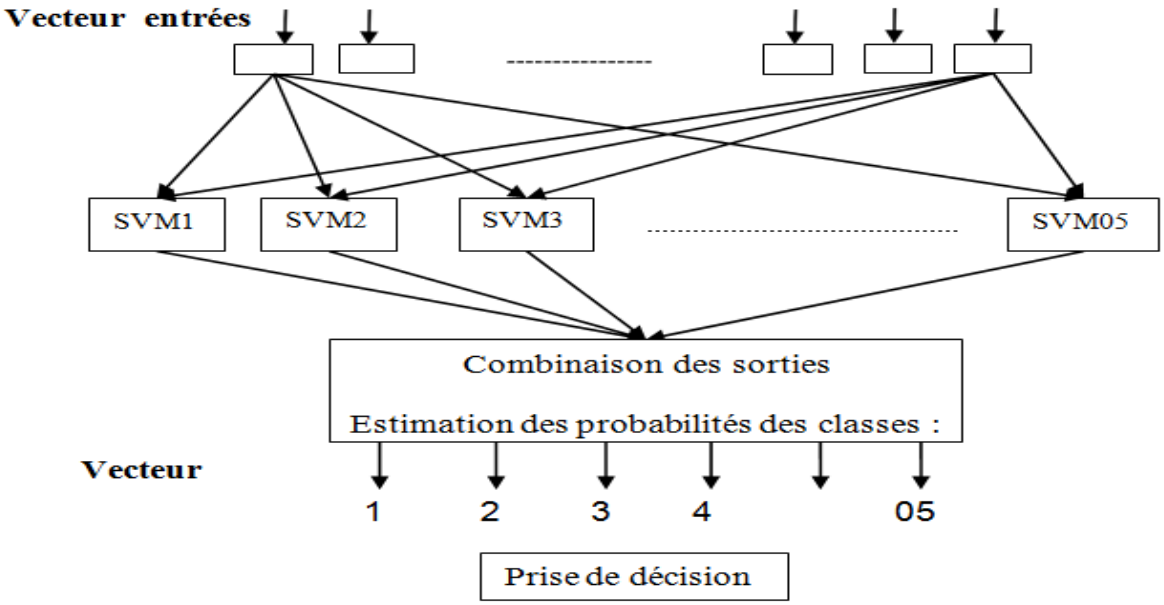


Figure II.12 : Architecture détaillée du classifieur SVM implémenté.

II.10 Conclusion

Au module d'extraction des caractéristiques, les systèmes de reconnaissances faits des étapes plus importantes avant le stockage des informations dans ces bases de données. Ces étapes sont basées sur des algorithmes spécifiques comme suit :

Le prétraitement des images FV , ensuite l'extraction de caractéristiques : pour obtenir les caractéristiques pertinentes de chaque image acquise, en forme de vecteur ; il-y-a plusieurs méthodes pour faire cette opération comme BSIF, LBP et Radon.

Classification des données : dernière étape fait classer les caractéristiques semblables d'un ou plusieurs individus à la même classe, cette étape est appliquée par des algorithmes comme SVM. Dans ce chapitre, nous avons décrit les différents prétraitements couramment utilisés dans les systèmes de reconnaissance desFV.

Le module de prétraitement englobe principalement une étapes pour l'amélioration de la qualité de l'image : égalisation d'histogramme. Enfin, nous avons présenté les méthodes d'extraction des caractéristiques, en insistant sur les transformée LBP et BSIF.

Dans notre travail, la recherche de méthodes d'extraction des caractéristiques a nécessité une attention particulière pour pouvoir générer des vecteurs caractéristiques qui permettent de discriminer au mieux des images FV provenant de personnes différentes.
Et faciliter ainsi la tache de classification.

Chapitre III

Résultats et Discussions

1

2

III.1 Introduction :

Dans ce chapitre, nous présenterons les résultats que nous avons obtenus pour nous assurer de la validité de notre système. D'abord nous commençons par la description de la base de données utilisée. Ensuite, nous faisons plusieurs expériences sur cette base pour étudier l'effet de notre système sur elle. Ensuite nous présentons les résultats que nous avons obtenus avec des caractéristiques différentes (LBP et BISIF et RADON). Grâce à ces résultats, nous assurons la performance de notre système.

III.2 La base de données :

III.2.1 Description de la base :

La base de données des ***veines des doigts (FV)*** se compose de 3816 images des expressions de FV de 106 personnes distinctes (Figure III.1).

La reconnaissance des veines des doigts est un hot spot de recherche récemment développé. Nous incluons dans SDUMLA-HMT une base de données de veines de doigt qui, à notre connaissance, est la première base de données de veine de doigt ouverte. L'appareil utilisé pour capturer les images des veines des doigts est conçu par Joint Lab for Intelligent Computing and Intelligent Systems de l'Université de Wuhan. Dans le processus de capture, il a été demandé à chaque sujet de fournir des images de son index, de son majeur et de son annulaire des deux mains, et la collecte pour chacun des 6 doigts est répétée 6 fois pour obtenir des images de veine à 6 doigts. Par conséquent, notre base de données sur les veines des doigts est composée de 3816 images. Chaque image est stockée au format «bmp» avec une taille de 320 × 240 pixels, et ainsi, la base de données des veines du doigt occupe environ 0,85 Go au total.

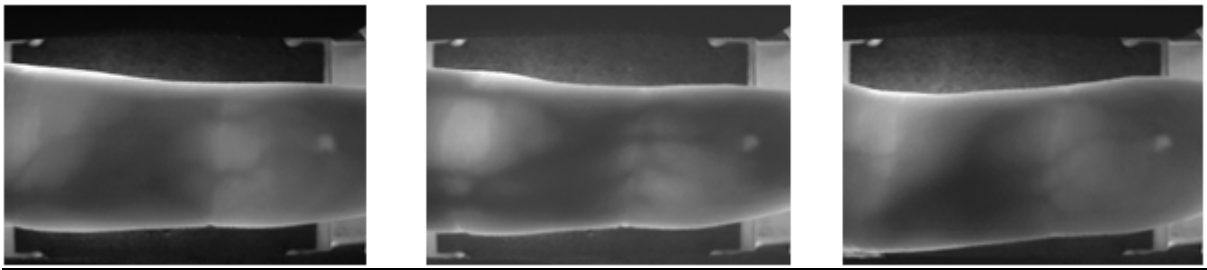


Figure III.1: Exemples des images de la base de données veines des doigts FV.

III.2.2 Séparation des bases de données :

Pour que notre système fonctionne et reconnaisse le FV, nous devons avoir deux bases de données : l'une pour l'apprentissage et l'autre pour tester le système et confirmer son fonctionnement déterminer leurs performances, mais nous n'avons pas deux bases de données. Dans ces tests, nous avons divisé la base comme suit :

- **Images apprentissages :**

La première, la cinquième et la neuvième image de chaque personne servent pour la phase d'apprentissage.

- **Images Tests :**

Les deux images restantes de chaque individu nous ont servi pour la réalisation des différents tests. Le but est d'évaluer le taux de reconnaissance de différents descripteurs présenté.

III.3 Expérimentations sur la FV :

Nous avons implémenté le système de reconnaissance basé sur les algorithmes LBP, BISIF et Radon avec FV. Dans ces expériences, Nous utilisons plusieurs bases de données qui sont: 636 (106 x 6) 6 photos pour chaque personne[446 photos pour l'apprentissage et le reste pour les tests (190)], 1272 (106 x 12) 12 photos pour chaque personne[891 photos pour l'apprentissage et le reste pour les tests (381)], et 1908 (106 x 18) 18 photos pour chaque personne[1336 photos pour l'apprentissage et le reste pour les tests (572)]. Pour obtenir les résultats du test, chaque vecteur de l'image de test a été comparé à tous les vecteurs de la base de référence et les résultats sont évalués selon certains critères: taux de classification, taux d'erreur et matrice de confusion, si les deux vecteurs sont de la même personne (même classe), l'appariement entre eux est compté comme utilisateur; Sinon, il n'est pas considéré comme utilisateur.

III.4 Critères d'évaluation :

Dans ce passage, nous décrivons les normes (les critères) les plus utilisés pour évaluer l'efficacité de système de reconnaissance. Le but est d'obtenir l'estimation la plus précise possible du comportement du système dans des conditions réelles d'utilisation. Pour cela, des normes classiques tels que le taux de reconnaissance sont utilisés presque systématiquement.

Le taux de reconnaissance est le nombre d'images de veine de doigt Reconnus pour une classe divisé par le nombre total d'images de veine de doigt.

Le taux de reconnaissance est utilisé pour évaluer la performance des systèmes de reconnaissance en phase de généralisation. Ce taux est évalué à l'aide d'une basa de données de test dont les formes sont décrites dans le même espace de représentation que celles utilisées pour l'apprentissage. Ils sont également classés en fonction de leur classe réelle afin qu'ils puissent vérifier les réponses du classeur. Pour que l'estimation du taux de reconnaissance soit aussi fiable que possible, il est essentiel que le classificateur n'utilise pas d'échantillons de cette base de données pour l'apprentissage (la base de données de test ne doit avoir aucun individu impliqué dans la base de données d'apprentissage et fondements possibles pour la vérification). De plus, cette base de test doit être suffisamment représentative du problème de classification .

Le taux de reconnaissance par classe (TRC) est défini par :

$$TRC(\%) = \frac{\text{nombre des veines de doigts reconnus pour une classe}}{\text{nombre totale des veines de doigts de cette classe}}$$

Le taux moyenne de bonne reconnaissance (TMBR) est défini par :

$$TMBR(\%) = \frac{\text{nombre des veines de doigts reconnues}}{\text{nombre totale des veines de doigts}}$$

III.5 Les Résultats :

Pour expliquer les performances de notre système, nous avons réalisé trois expériences. Dans chaque essai, nous avons évalué et comparé les performances des méthodes d'extraction de caractéristiques de la base de données FV .

III.5.1 Les résultats obtenus dans la première expérimentation avec LBP :

Pour exécuter l'algorithme LBP, nous avons effectué plusieurs expériences avec la valeur préférentielle de R jusqu'à ce que nous obtenions des résultats concernant les temps de calcul, l'apprentissage et le taux de test.

- **Pour base des donnée de 636 images :** 1

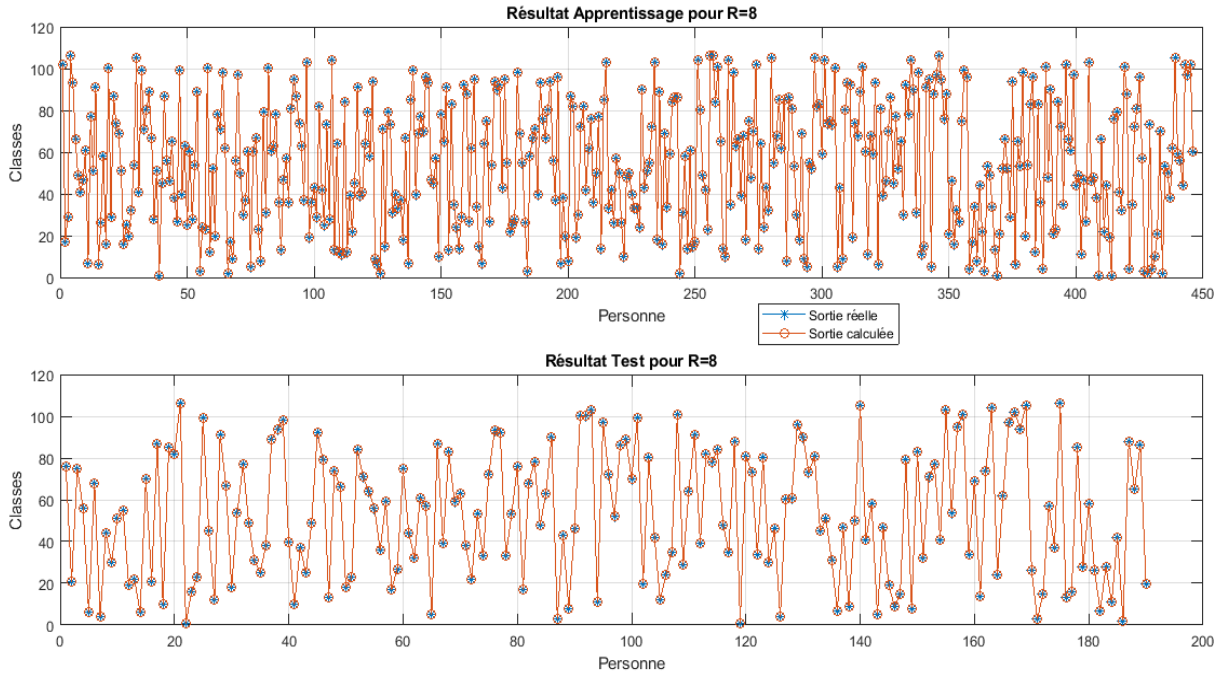


Figure III.2: le résultat d'apprentissage et test en utilisant LBP pour R=8.

nous avons obtenu de meilleurs résultats en utilisant R =[8], car il n'y a pas de différence entre la sortie réelle et la sortie calculée.

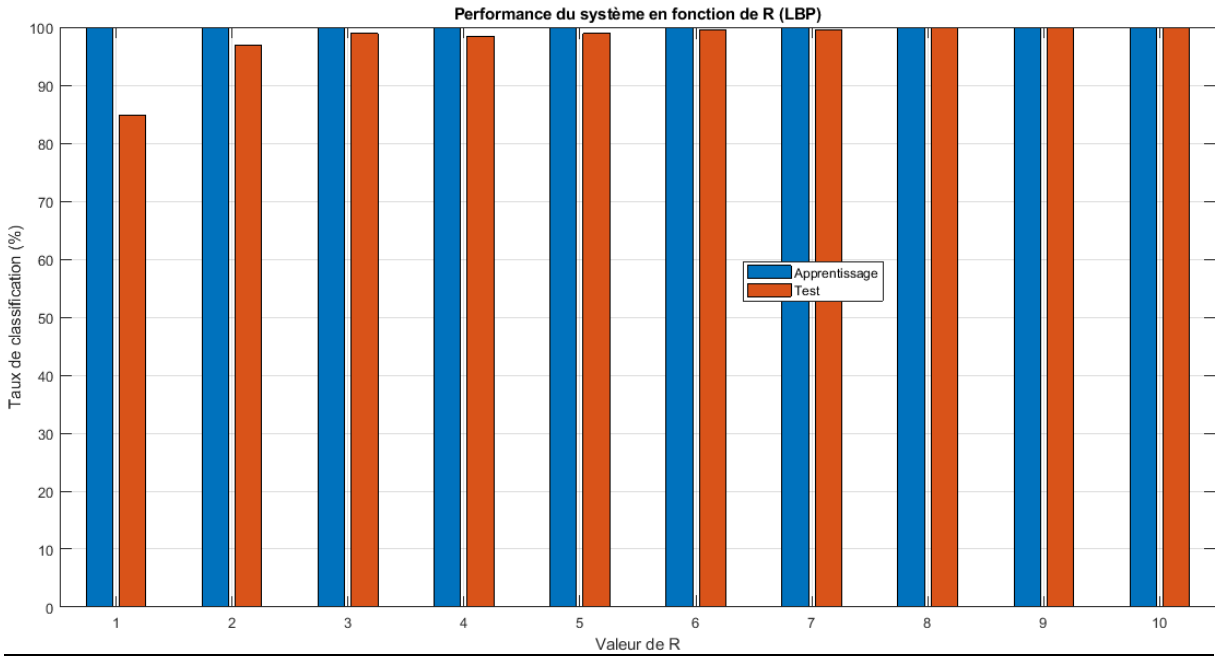


Figure III.3:la performance du système en fonction de R avec LBP.

Le taux d'apprentissage est 100% pour toutes les valeurs de R . Mais , le taux de test varie d'une valeur à l'autre de R, atteignant le maximum avec R =[8 9 10].

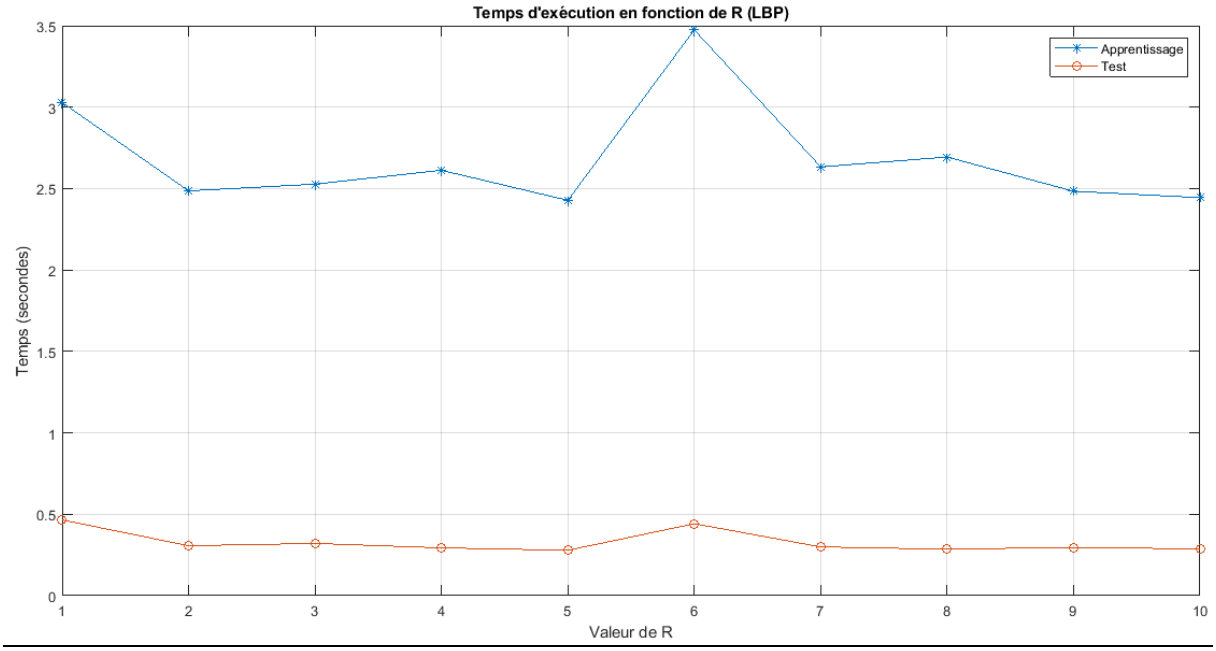


Figure III.4: les temps d'exécution en fonction de R avec LBP.

- **Pour base des donnée de 1272 images :** 1

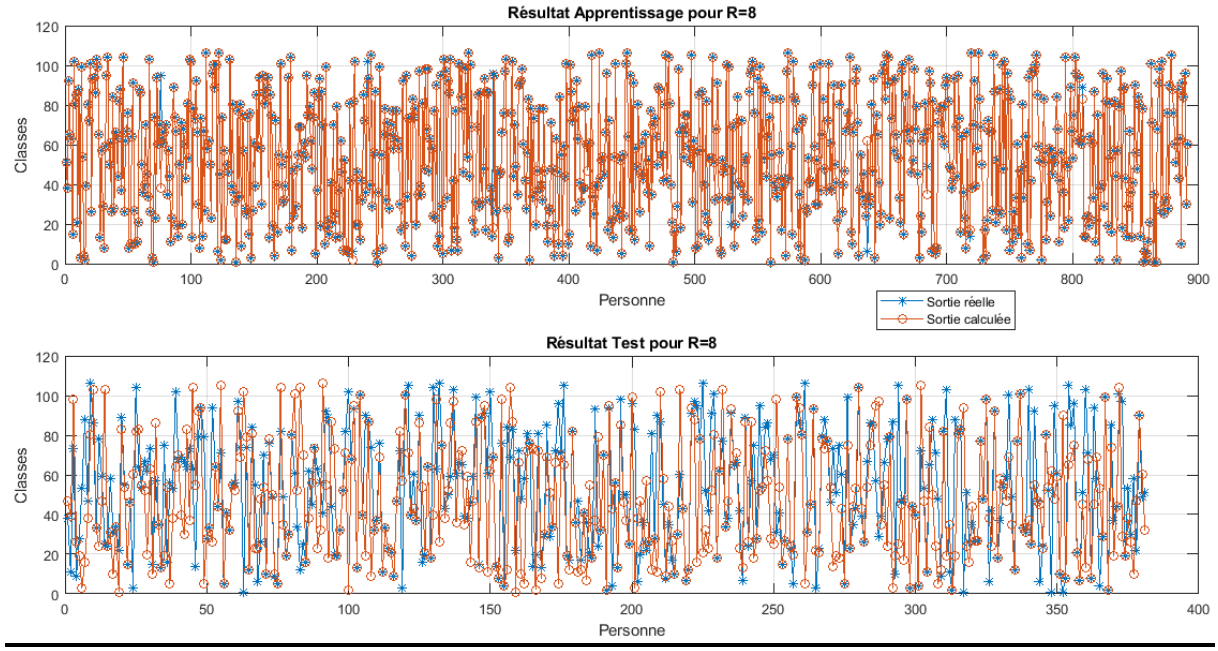


Figure III.5: le résultat d'apprentissage et test en utilisant LBP pour R=8.

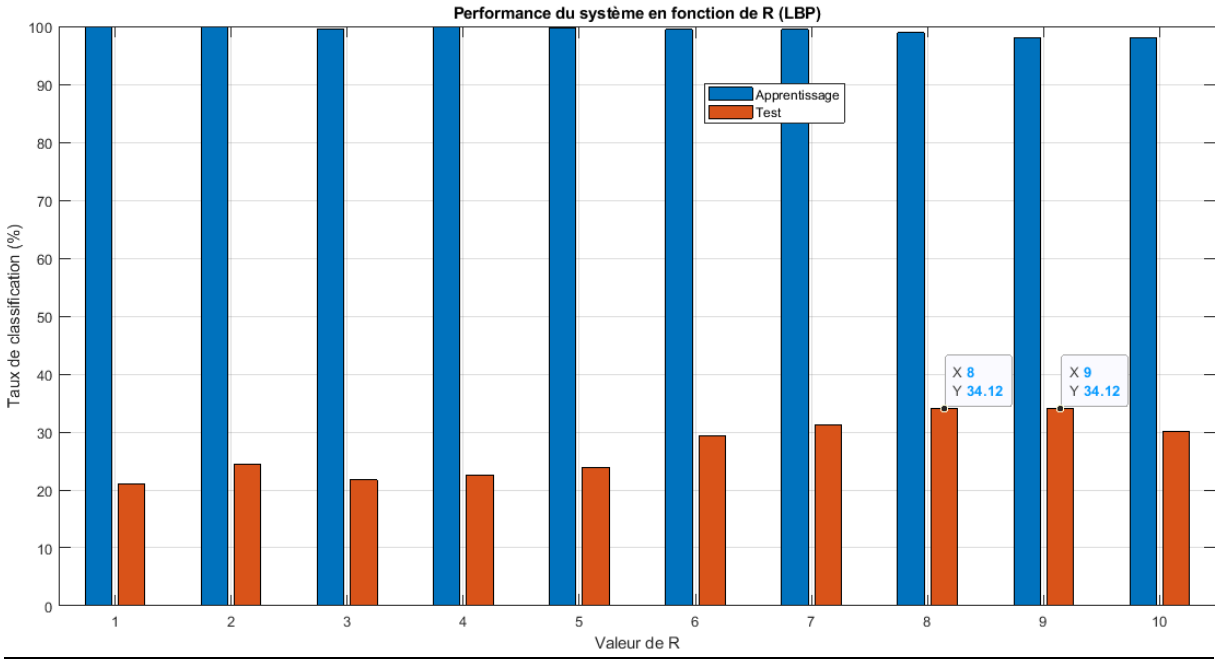


Figure III.6:la performance du système en fonction de R avec LBP.

Le taux d'apprentissage est 100% pour toutes les valeurs de R. Cependant, le taux de test est faible, atteignant son maximum avec R = [8 9], qui est de 34,12%.

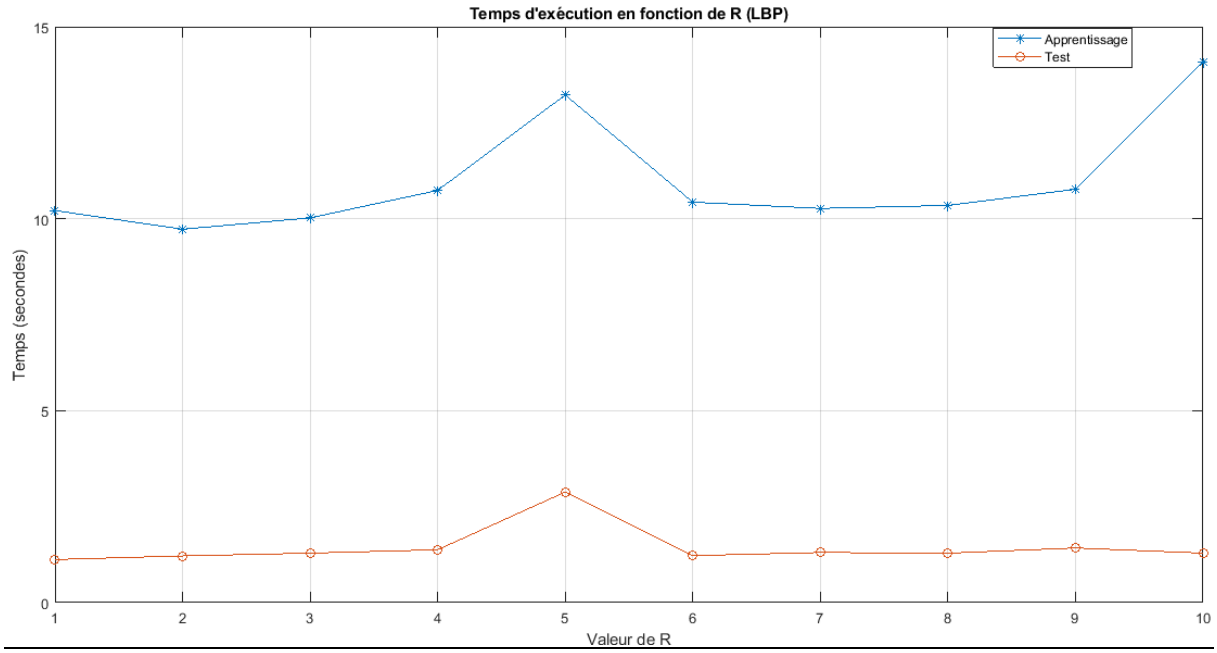


Figure III.7: les temps d'exécution en fonction de R avec LBP.

- **Pour base des donnée de 1908 images :** 1

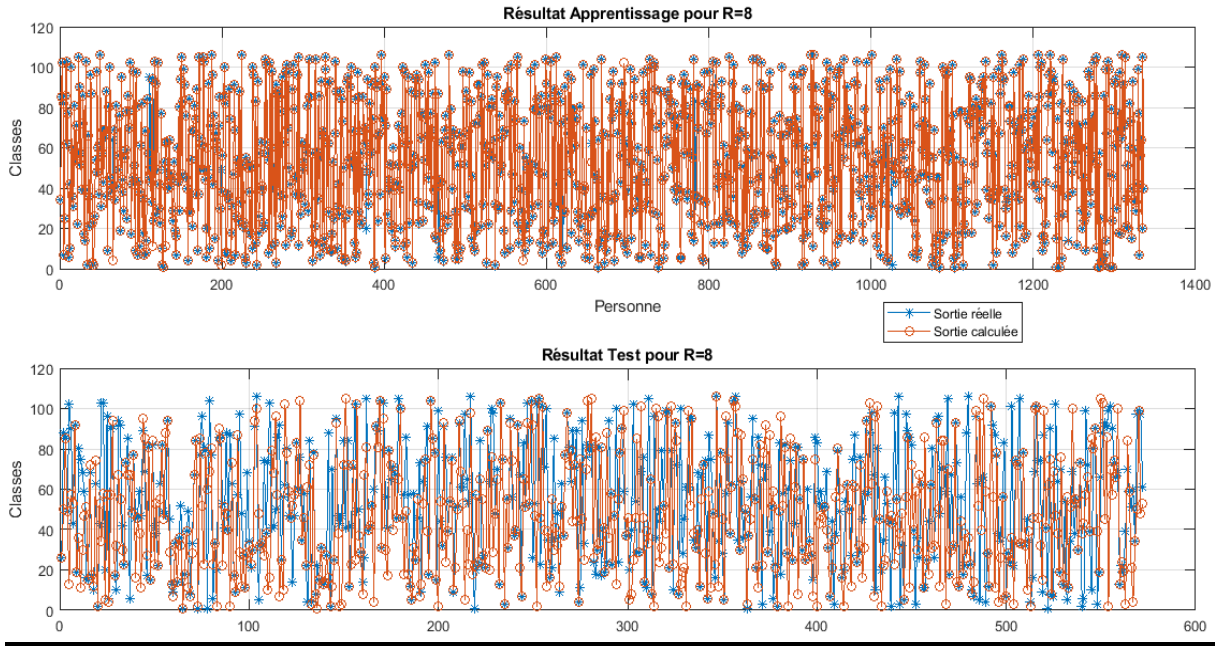


Figure III.8: le résultat d'apprentissage et test en utilisant LBP pour R=8.

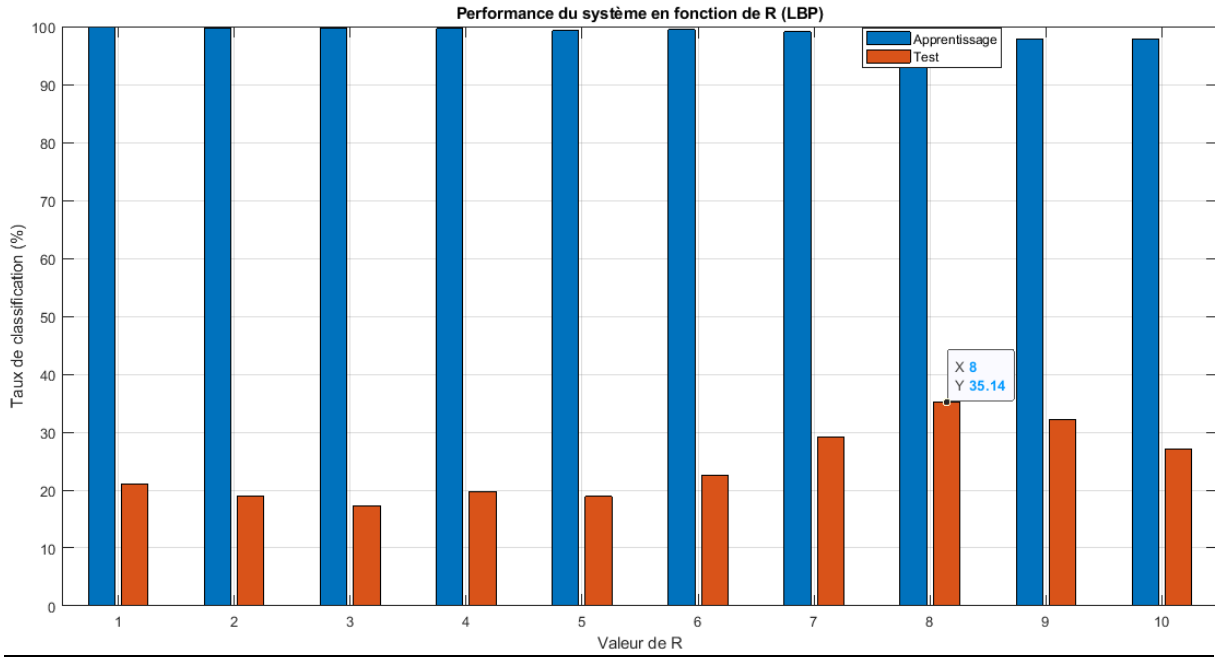


Figure III.9:la performance du système en fonction de R avec LBP.

Le taux d'apprentissage atteint 100% pour presque toutes les valeurs R. Cependant, le taux de test diffère d'une valeur à l'autre de R, Où le maximum est pris avec R = 8, Où il a atteint 35,14%.

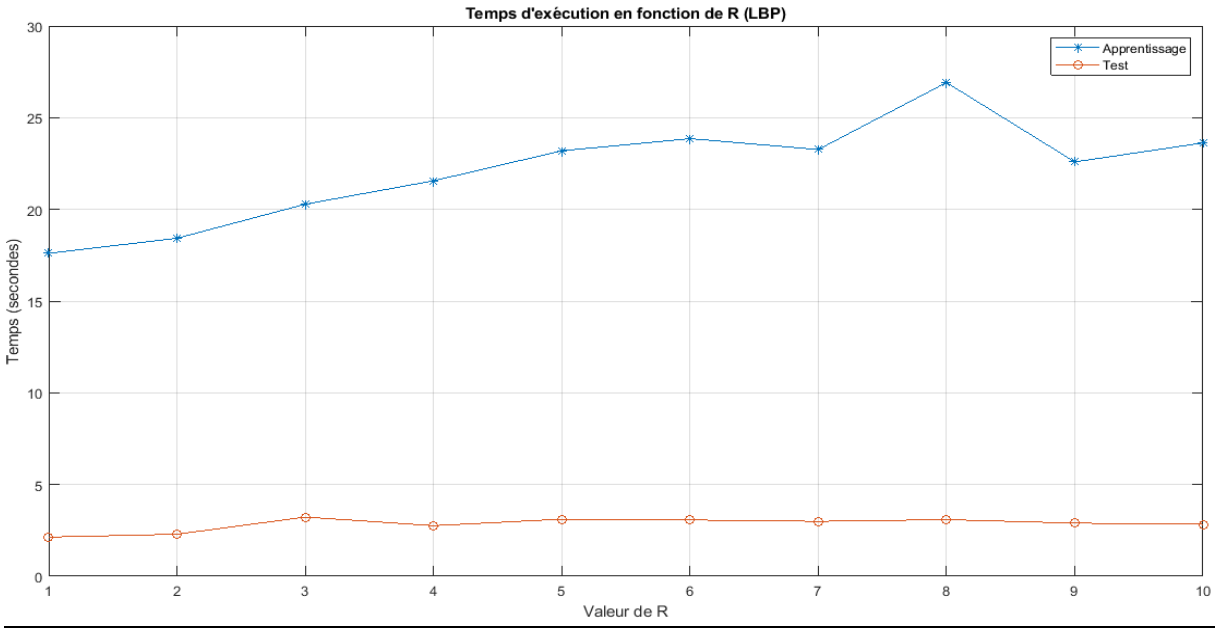


Figure III.10: les temps d'exécution en fonction de R avec LBP.

Il est clair que le temps d'exécution dans la phase d'apprentissage (dans les trois cas) est supérieur au temps de test. Aussi, le temps d'apprentissage varie en fonction de R, nous avons observé qu'il diminue quand il augmente R. Ceci est justifié par l'effet que le masque à grande valeur R balaye l'image rapidement.

III.5.2 Les résultats obtenus dans la deuxième expérimentation avec BSIF

- **Pour base des données de 636 images :** 1

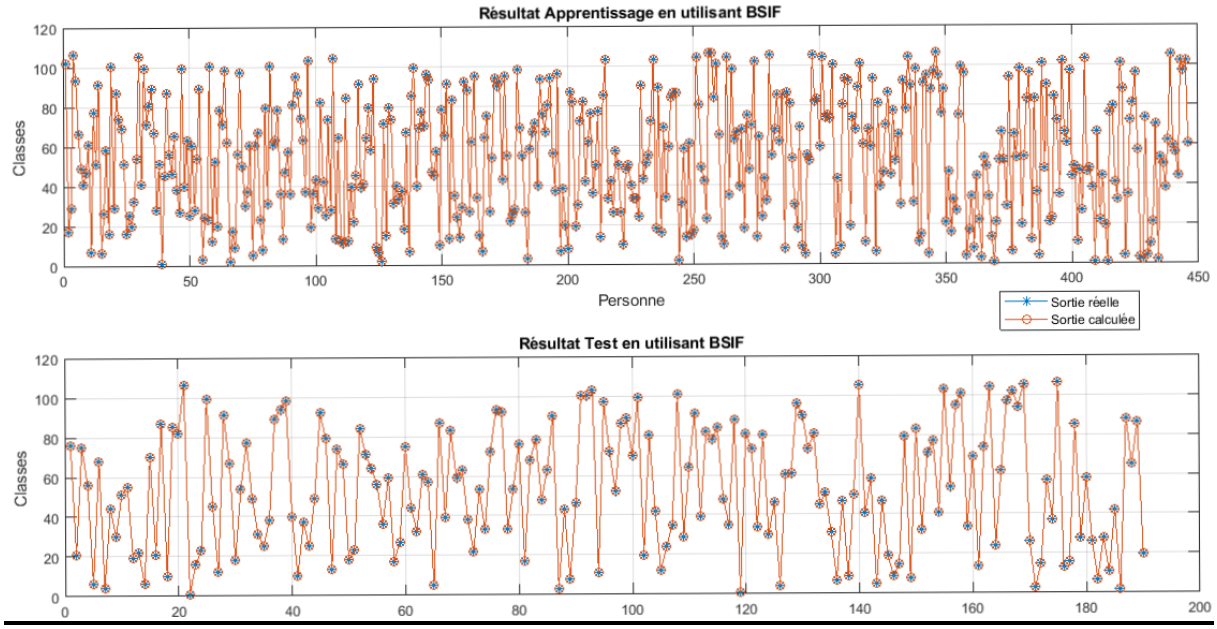


Figure III.11:les résultats d'apprentissage et test en utilisant BSIF .

De nombreux tests ont été réalisés avec différentes tailles de filtres et avec différents nombres de bits. Les meilleurs résultats obtenus sont ceux avec un filtre 17 * 17 et 11 bits.

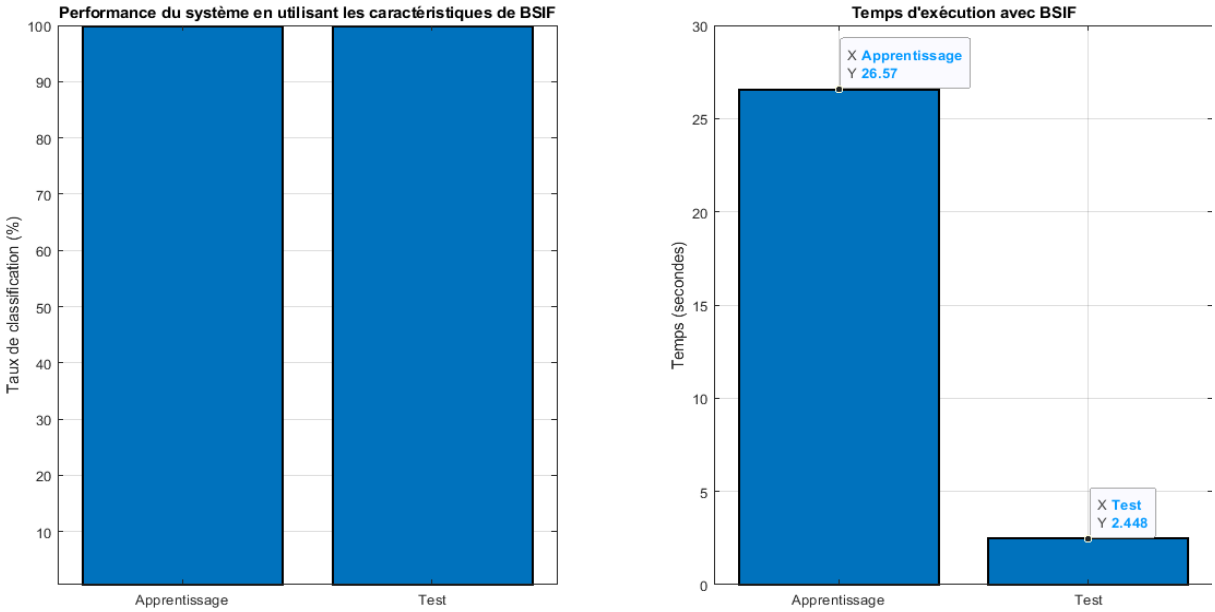


Figure III.12: la performance du système et le temps d'exécution avec BSIF .

Pour les résultats du descripteur du BSIF, nous avons atteint respectivement 100% et 100% en termes de taux d'apprentissage et de test.

En termes de temps d'exécution, l'apprentissage prend encore beaucoup de temps par rapport au temps de test.

- **Pour base des données de 1272 images :** 1

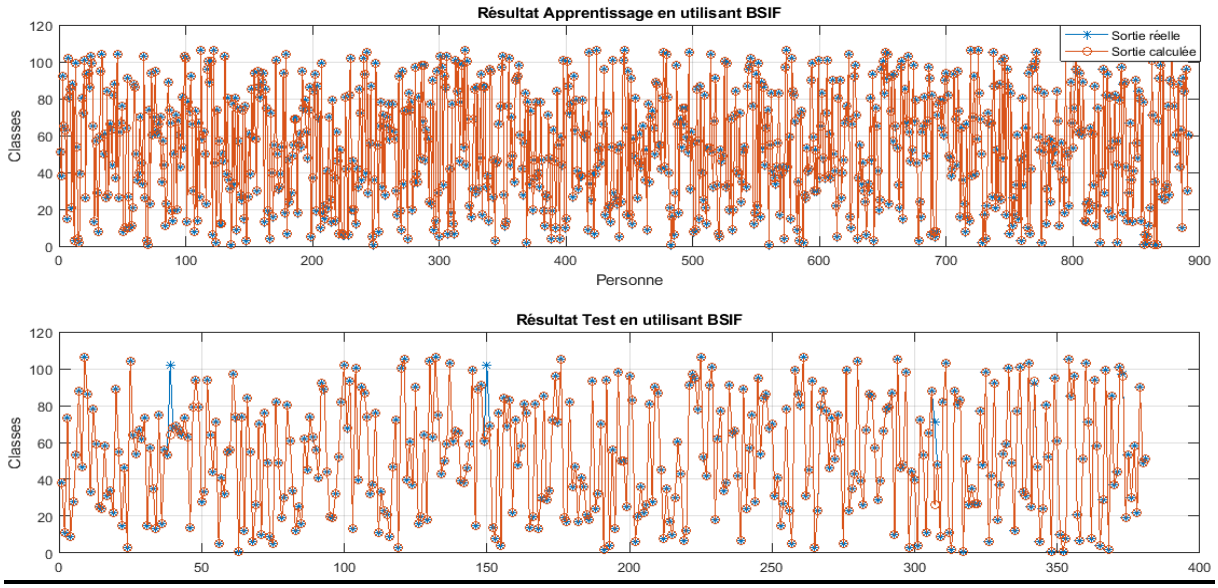


Figure III.13:les résultats d'apprentissage et test en utilisant BSIF.

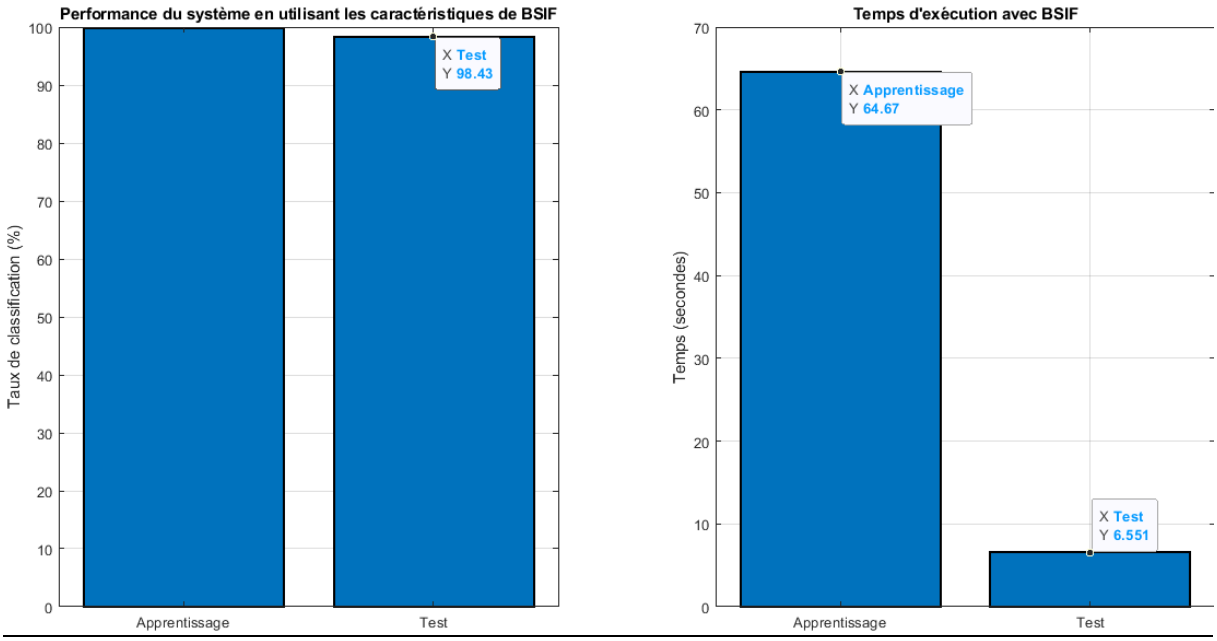


Figure III.14: la performance du système et le temps d'exécution avec BSIF.

Les meilleurs résultats obtenus sont ceux avec un filtre 17 * 17 et 11 bits , nous avons atteint 100% et 98.43% en terme de taux d'apprentissage et de test, respectivement. Concernant le temps d'exécution, l'apprentissage prend encore beaucoup de temps par rapport au temps de test.

- **Pour base des donnée de 1908 images :** 1

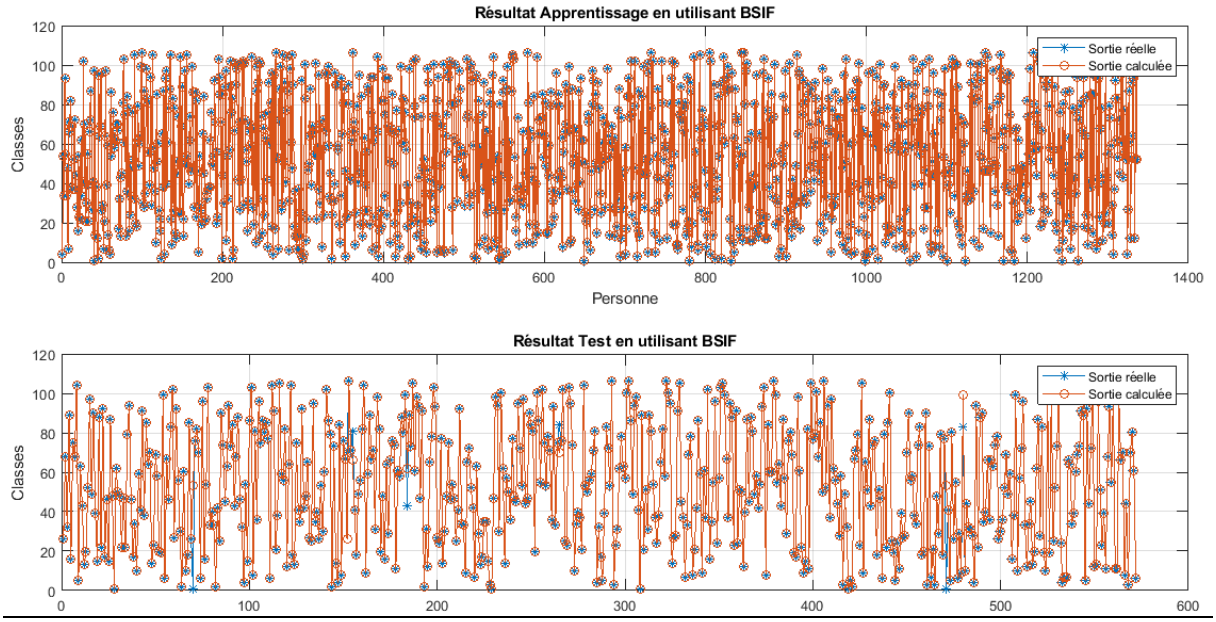


Figure III.15:les résultats d'apprentissage et test en utilisant BSIF.

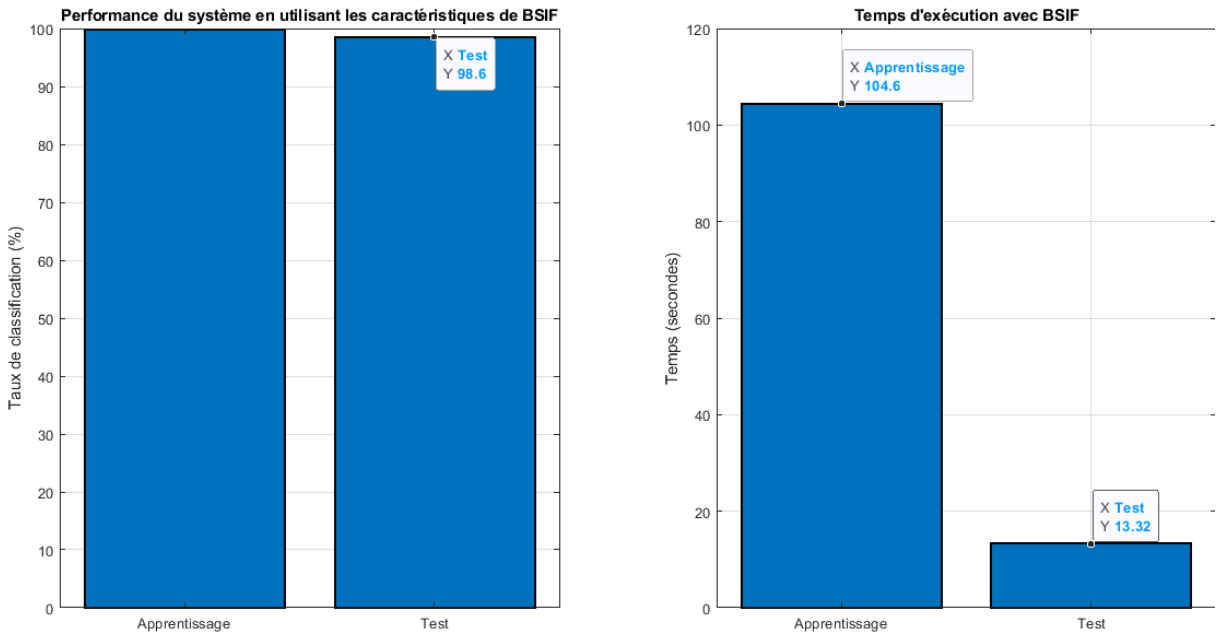


Figure III.16: la performance du système et le temps d'exécution avec BSIF.

nous avons atteint respectivement 100% et 98,6% en termes de taux d'apprentissage et de test. En termes de temps d'exécution, toujours l'apprentissage consomme beaucoup de temps comparativement au temps de test.

III.6 Etude comparative :

Dans ce paragraphe, nous avons mené une étude comparative des différentes approches. Les critères de comparaison sont le taux d'identification et le temps de calcul.

Le but est de choisir la meilleure méthode pour créer un système d'identification. Nous avons remarqué que tous les tests de cette mémoire ont été réalisés avec MATLAB et avec un appareil doté d'un processeur i5 à 2,50 GHz avec 4 Go de RAM. Les résultats de la comparaison sont présentés dans le tableau (III. 1).

Caractéristique	indicateurs	Base Des données	Taille	Apprentissages		Tests	
				Taux(%)	Temps(s)	Taux(%)	Temps(s)
LBP	R=8	636	257	100	2,694	100	0,2851
		1272		100	13,74	34,12	1,628
		1908		100	27,8	35,14	3,72
BSIF	Filtre=17 :17 11 bit	636	2049	100	26,57	100	2,448
		1272		100	64,67	98,43	6,551
		1908		100	104,6	98,6	13,32

TableauIII.1:les résultats des apprentissages et Tests des algorithmes.

D'après ce tableau, nous notons que le meilleur résultat obtenu est lorsque nous utilisons la caractérisation BSIF dans les trois cas où nous avons atteint une bonne spécification comprise entre (98,43 et 100)%. Le temps de calcul du système basé sur la méthode BSIF est plus long que pour les systèmes basés sur LBP. Enfin, d'après ces résultats, On peut dire que le système d'identification par FV et BSIF est considéré comme un système fiable sécurisé. Il permet une bonne séparation entre les catégories de clients et de fraudeurs.

III.7 Conclusion

Dans ce chapitre, l'introduction du travail biométrique a conduit au développement d'un système de reconnaissance des personnes grâce à la reconnaissance des veines des doigts. Pour ce faire, nous avons proposé plusieurs systèmes biométriques. Nous avons exploré certains systèmes multimédias. Ces différents systèmes sont testés afin d'optimiser le taux d'identification dans les modes d'identification. Nous avons créé trois types de descripteurs : BSIF et LBP. En validant ces systèmes par rapport à différentes bases de données réelles constituées de [636, 1272 et 1908] images de 106 sujets, nous avons trouvé une amélioration significative du taux d'identification (100%) à l'aide des descripteurs BSIF.

Conclusion Générale

La biométrie est un domaine passionnant et très complexe. Parce qu'il tente, avec des outils mathématiques très complexes, de distinguer les individus, ce qui nous oblige à travailler dans un contexte large riche en diversité en présentant une analyse des différentes technologies de reconnaissance qui se sont développées ces dernières années, pour mettre en évidence les caractéristiques de chacun d'eux ainsi que les avantages et inconvénients de chacun.

Le travail présenté dans cette lettre s'inscrit dans le cadre de l'identification automatique des personnes à travers leurs descripteurs biométriques. Nous avons utilisé une nouvelle méthode biométrique, les veines des doigts, pour réaliser notre système biométrique. Cette technologie biométrique est extrêmement robuste en termes de sécurité, en raison de ses propriétés biométriques uniques d'un individu, sans la possibilité que d'autres individus aient les mêmes caractéristiques. Même chez des jumeaux identiques.

Nous pensons avoir atteint un système qui répond à l'objectif que nous nous étions fixé au départ, qui est de mettre en œuvre un système permettant l'identification individuelle et le contrôle d'accès. Une extension de ce travail peut également être réalisée en intégrant un système d'acquisition d'images pour éviter que ces processus d'identification et de vérification ne soient une simulation. De plus, il sera également intéressant d'appliquer à l'avenir la méthode développée dans cette thèse au système de sécurité biométrique.

Références

[1] B.soufiane,"Détection et identification de personne par méthodebiométrique ", Mémoire de Magister, Université Mouloud MAMMERI , TIZI-OUZOU.

[2] David-Zhang-Guangming-Lu-Lei-Zhang-Advanced-Biometrics-Springer-2018.

[3] B.Fatima,"Caractéristiques Biométrique pour l'identification", Mémoire de Magister, Université Ahmed ben Bella,Oran,2015.

[4] L.ALLANO, 'La Biométrie multimodale : stratégies de fusion de scores et mesures de dépendance appliquées aux bases de personnes virtuelles', thèse de doctorat, Université D'Every Val D'Essonne, 2009.

[5] S.GUERFI ABABSA, "Authentification d'individus par reconnaissance de caractéristiques biométriques liées aux visages 2D/3D", thèse de doctorat, Université D'Every Val D'Essonne ,2008.

[6] T.AMELLAL, K. BENAKLI, "Système de reconnaissance de visage basé sur les GMM ", mémoire fin d'étude d'ingéniera en informatique, Institut National de formation en Informatique (I.N.I) Oued-Smar Alger, 2007.

[7] F.LOUIBA et R. HADJ, " Système de contrôle d'accès physique basé sur le visage et la Java Card", mémoire fin d'étude d'ingéniera en informatique, Institut National de formation en Informatique (I.N.I), 2010.

[8] L.MENSSOURA, 'identification des visages humains par réseaux de nuerons', mémoire de magister, université de Batna, 2013.

[9] A.BENAGGA et L. TELIB, " Reconnaissance des personnes basée sur l'empreinte de l'articulation de doigt", Mémoire de master académique, université Kasdi Mer bah Ouargla, 2016.

[10] F. DAVOINE, B. ABBOUD et V. MO DANG,' Face and facial expression analysisbased on an active apparence model ', Traitement du signal, Vol.21, No.3, 2004.

[11] M ,Moulay,M,Arbaoui," authentification des personnes par l'articulation du doigt",Université Kasdi Mer bah Ouargla,2015 .

[12] A. Murhula, ,“ Conception et mise en place d'une plateforme de sécurisation par synthèse et reconnaissance biométrique de documents de trafic”, Polytechnique-Initelematique- Burundi - Ingénieur Civil en Informatique et télécommunications,2015.

[13] B,Abderrahmane , T, Lina “ Reconnaissance des personnes basée sur l’empreinte de l’articulation de doigt”, Mémoire Master académique , Université Kasdi mer bah Ouargla, 2015 /2016

[14] B.Ibtisam“ Etude et mise au point d’un procédé biométrique multimodale pour la reconnaissance des individus”, Diplôme de Doctorat en Sciences Université des Sciences et de la Technologie d’Oran Mohamed Boudiaf à 2015 / 2016 .

[15] Le marché biométrie,“ biométrie – online . net”.

[16] une article ,www.thalesgroup.com , Mise à jour le 10 mai 2020 .

[17] un rapport sur le marché de la biométrie,IBG (International Biometric Group) édite régulièrement , http://www.biometricgroup.com .

[18] S.AKROUF, ”Une Approche Multimodale pour l’Identification du Locuteur”, thèse de doctorat, Université Ferhat Abbas- Sétif , 2011.

[19] F. LOUIBA et R. HADJ, ” Système de contrôle d’accès physique basé sur le visage et la Java Card”, mémoire fin d’étude d’ingéniera en informatique, Institut National de formation en Informatique (I.N.I), 2010.

[20] T.AMELLAL, K. BENAKLI, ”Système de reconnaissance de visage basé sur les GMM ”, mémoire fin d’étude d’ingéniera en informatique, Institut National de formation en Informatique (I.N.I) Oued-Smar Alger, 2007.

[21] Julie de Meslon ,un article,’’ La société Easydentic ‘’,07/10/2008.

[22] M.Fatma Zohra, T. Fattoum,’’Caractérisation d’empreinte de l’articulation de doigt pour l’authentification des personnes’’,mémoire fin d’étude,université de Mohamed Boudiaf - M’sila.

[23] O.ASSAS, ” Classification floue des images”, thèse de doctorat, université de Batna, 2013.

[24] H.O. Nyongesa, S. Al-Khayatt, S. M. Mohamed and M. Mahmoud, " Fast RobustFingerprint Feature Extraction and Classification ", Journal of Intelligent & Robotic Systems Volume 40, Number 1, 103-112,2010,2004

[25] E. Liu, H.Zhao, "Fingerprint segmentation based on an AdaBoost classifier ",Higher Education Press and Springer-Verlag Berlin Heidelberg ,2010.

[26] P.Dargenton, "Contribution à la segmentation et la reconnaissance de l'écriture manuscrite", Thèse de Doctorat, Institut national des sciences appliquées de Lyon, France, p 227, 1994.

[27] O.D.Trier, A.K.Jain and T. "Feature extraction methods for character recognition: A Survey, Pattern Recognition", Vol. 29, No. 4, pp. 641-662, 1996.

[28] P. Milanfar, "A Model of the Effect of Image Motion in the Radon Transform Domain", IEEE Transactions on Image processing, vol. 8, no. 9, September 1999.

[29] Ojala, T., Pietikäinen, M., & Harwood, D. (1996). A comparative study of texture measures with classification based on featured distributions. Pattern recognition, 29(1), 51-59.

[30] Kannala, J., &Rahtu, E. (2012, November). Bsif: Binarized statistical image features. In Pattern Recognition (ICPR), 2012 21st International Conference on (pp. 1363-1366). IEEE.

[31] Bowyer, K. W., Chang, K., & Flynn, P. (2006). A survey of approaches and challenges in 3D and multi-modal 3D+ 2D face recognition. Computer vision and image understanding, 101(1), 1-15.

[32] "Support vector machine".

Document available at http://en.wikipedia.org/wiki/Support_vector_machine.

[33] Zhang, L., Zhang, L., Zhang, D., & Guo, Z. (2012). Phase congruency induced local features for finger-knuckle-print recognition. Pattern Recognition, 45(7), 2522-2531.

[34] Hsieh, C. T., & Hu, C. S. (2014). Fingerprint Recognition by Multi-objective Optimization PSO Hybrid with SVM. Journal of applied research and technology, 12(6), 1014-1024.

[35] Li, W., Zhang, D., Zhang, L., Lu, G., & Yan, J. (2011). 3-D palmprint recognition with joint line and orientation features. IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 41(2), 274-279.

[36] Jain, A., Flynn, P., & Ross, A. A. (Eds.). (2007). Handbook of biometrics. Springer Science & Business Media.

RESUME

À la lumière des progrès scientifiques continus, l'identification automatique est devenue une exigence importante dans une variété d'applications telles que le contrôle d'accès, les systèmes de surveillance et les bâtiments physiques. La biométrie, qui traite de l'identification des individus en fonction de leurs caractéristiques physiques ou comportementales, est devenue une technologie d'identification automatique efficace, qui offre plus de caractéristiques et de nombreux avantages par rapport à la sécurité traditionnelle. L'empreinte digitale du réseau veineux (F) est une propriété biométrique importante. Cela offre unicité, une stabilité et une grande capacité à exceller. Dans nos travaux, les techniques d'identification de phase multi-blocs locales (LBP, BISIV, RADON) sont des techniques utilisées pour extraire les traits caractéristiques de la méthode FV. Nos résultats expérimentaux, utilisant la base de données FV (ITTD) montrent les meilleures performances du système d'identification basé sur le FV proposé.

Mots clés : Biométrie, Empreintes veines de doigte, Reconnaissance, Classification, SVM, fusion.

ABSTRACT

In light of continuous scientific advancements, automatic identification has become an important requirement in a variety of applications such as access control, surveillance systems and physical buildings. Biometrics, which deals with the identification of individuals based on their physical or behavioral characteristics, has become an effective automatic identification technology, which offers more characteristics and many advantages over traditional security. The fingerprint of the venous network (F) is an important biometric property. This provides uniqueness, stability and a great ability to excel. In our work, local multi-block phase identification techniques (LBP, BISIV, RADON) are techniques used to extract the characteristic features of the FV method. Our experimental results, using the FV database (ITTD) show the best performance of the proposed FV-based identification system.

Keywords: Biometrics, Finger vein imprints, Recognition, Classification, SVM,, fusion.

ملخص

في ضوء التطورات العلمية المستمرة ، أصبح التعرف التلقائي مطلبًا مهمًا في مجموعة متنوعة من التطبيقات مثل التحكم في الوصول وأنظمة المراقبة والمباني المادية. أصبحت القياسات الحيوية ، التي تتعامل مع تحديد الأفراد بناءً على خصائصهم الجسدية أو السلوكية ، تقنية تحديد تلقائي فعالة ، والتي توفر المزيد من الخصائص والعديد من المزايا على الأمان التقليدي. تعد بصمة الشبكة الوريدية (F) خاصية بيومترية مهمة. وهذا يوفر التفرد والاستقرار والقدرة الكبيرة على التفوق. في عملنا ، تقنيات تحديد الطور المحلي متعدد الكتل (LBP ، BISIF، RADON) هي تقنيات مستخدمة لاستخراج السمات المميزة لطريقة FV. تظهر نتائجنا التجريبية ، باستخدام قاعدة بيانات FV (ITTD) أفضل أداء لنظام التعريف المقترح القائم على FV .

الكلمات المفتاحية : القياسات الحيوية ، بصمات وريد الأصابع ، الاعتراف ، التصنيف ، SVM.