

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITE MOHAMED BOUDIAF - M'SILA

FACULTE DE TECHNOLOGIE
DEPARTEMENT D'ELECTRONIQUE
N° :



DOMAINE : SCIENCES ET TECHNOLOGIE
FILIERE : GENIE ELECTRONIQUE
OPTION : SYSTEME EMBARQUE

**Mémoire présenté pour l'obtention
Du diplôme de Master Académique**

Par :

MAHDI Fatma Zohra

TABI Fattoum

Intitulé

**Caractérisation d'empreinte de l'articulation de
doigt pour l'authentification des personnes**

Soutenu devant le jury composé de :

Mr.	Université de M'sila	Président
Mr. ATTALLAH Bilal	Université de M'sila	Encadreur
Mr. BRIK Youcef	Université de M'sila	Co-Encadreur
Mr.	Université de M'sila	Examineur

Année universitaire : 2018 /2019

Dédicace

Je dédie ce mémoire:

À mes très chers parents pour leur soutien durant tout mon cursus scolaire et qui m'ont permis de réussir dans mes études.

Et mes frères et ma sœur

A tous la famille MAHDI et FAID

À tout mes amis

Et À toutes les professeurs et enseignants

A tout la promotion deuxième master Electronique

À toute personne ayant contribué à ce travail de près ou de loin.

Remerciements

Je remercie en premier lieu Dieu qui m'a donné ce bien là et pour que je vie ce jour et la force et la patience pour terminer ce travail.

Remercier les deux personne qui m'a aidé à réaliser ce travail dans les meilleures conditions mon encadreur Mr :ATTALLAH Bilal et le Co-encadreurMr : BRIK Youcef qui ont proposé et ont dirigé ce travail.

Je remercie monsieur le président de jury, ainsi que les membres de jury d'avoir accepté de juger ce travail.

Je tiens à remercier les responsables et tout le personnel du département d'Electronique de M'sila pour les facilités qu'ils m'ont accordés pour terminer ce travail.

Je tiens à remercier ma famille pour leur apport affectif et leurs sacrifices.

Le travail de mémoire que j'ai effectué doit beaucoup à certaines personnes que je tiens à les remercier sincèrement.

Enfin, je remercie tous ceux qui ont contribué de près ou de loin à ma formation et à l'élaboration de ce modeste mémoire.

Table des matières

Dédicace.....	I
Remerciements.....	II
Liste des abréviations.....	III
Liste des tableaux.....	IV
Liste des figures.....	V
Sommaire.....	VI
Introduction générale	I
Chapitre I: La biométrie	
I.1 Introduction.....	03
I.2 La biométrie	03
I.2.1 Définition	03
I.2.2 les caractéristiques biométriques.....	03
I.3 Modalités biométriques	04
I.3.1 Analyses biologiques	06
I.3.2 Analyses morphologiques.....	07
I.3.3 Analyse comportementale	10
I.4 Architecture et fonctionnement d'un système Biométrique	12
I.4.1 Mode Vérification	13
I.4.2 Mode identification	13
I.5 Principaux Modules	14
I.6 Évaluation d'une performance	14
I.7 Les applications de la biométrie	16
I.8 Avantages et Inconvénients des Techniques biométriques	17
I.9 choix d'une caractéristique biométrique	20
I.10 Le marché de la biométrie	21
I.11 Conclusion	21

Chapitre II: LE SYSTEME DE RECONNAISSANCE DES FKP PROPOSE

II.1 Introduction	23
II.2 Architecture globale du système	23
II.2.1 Le prétraitement de l’empreinte d’articulation	24
II.2.2 Génération des caractéristiques	24
II.3 Etat De L’art Sur Les Méthodes d’Extraction De Caractéristiques .	24
II.3.1 Approche statistique	25
II.3.2 Approche géométrique	25
II.4 Extraction Des Caractéristiques Avec La T.RADON	25
II.4.1 Définition	25
II.4.2 Résultats De L’implémentation	26
II.5 Extraction Des Caractéristiques Avec Les LBP	26
II.5.1 Définition	26
II.5.2 Résultats De L’implémentation	28
II.6 Extraction Des Caractéristiques Avec Les BSIF	28
II.6.1 Définition	28
II.6.2 Résultats De L’implémentation	30
II.7 Extraction Des Caractéristiques Avec La Fusion Entre le filtre de BSIF et Transforme de RADO	30
II.8 Normalisation des données	30
II.9 L’étape de classification	31
II.9.1 Machine à vecteurs de support(SVM)	31
II.9.1.1 Principe de SVM	32
II.9.1.2 Notions de base	32
II.9.2 SVM Multi-classes	39
II.9.3 Architecture du classifieur SVM proposée	40
II.10 Conclusion	41

Chapitre III: les résultats et la discussion

III.1 Introduction.....	43
III.2 La base de donnée.....	43
III.2.1 Description de la base.....	43
III.2.2Séparation des bases de données.....	43
III.3Expérimentations sur la FKP.....	44
III.4 Critères d'évaluation.....	44
III.5 Les Résultats.....	45
III.5.1 Les résultats obtenus dans la première expérimentation avec LBP.....	45
III.5.2 Les résultats obtenus dans la deuxième expérimentation avec BSIF.....	48
III.5.3 Les résultats obtenus dans la troisième expérimentation avec RADON.....	49
III.5.4 Les résultats obtenus dans la troisième expérimentation avec fusion.....	50
III.6 Etude comparative.....	52
III.7 Conclusion.....	57
Conclusion générale	58
Bibliographie.....	59
Résumé	

Liste des figures

Figure I.1: les techniques biométriques	5
Figure I.2: L'A.D.N.	خطأ! الإشارة المرجعية غير معرفة.
Figure I.3: la thermographie faciale.	خطأ! الإشارة المرجعية غير معرفة.
Figure I.4: Empreinte digitale.	خطأ! الإشارة المرجعية غير معرفة.
Figure I.5: La Géométrie de la main.	خطأ! الإشارة المرجعية غير معرفة.
Figure I.6: Image de la rétine.	خطأ! الإشارة المرجعية غير معرفة.
Figure I.7: Image de l'iris.	خطأ! الإشارة المرجعية غير معرفة.
Figure I.8: Empreintes des articulations des doigts (FKP).	خطأ! الإشارة المرجعية غير معرفة.
Figure I. 9: Visage.	خطأ! الإشارة المرجعية غير معرفة.
Figure I.10: la signature.	خطأ! الإشارة المرجعية غير معرفة.
Figure I.11: la voix.	خطأ! الإشارة المرجعية غير معرفة.
Figure I.12: Frappe dynamique sur le clavier.	خطأ! الإشارة المرجعية غير معرفة.
Figure I. 13: Démarche.	خطأ! الإشارة المرجعية غير معرفة.
Figure I.14: Architecture d'un système biométrique.	خطأ! الإشارة المرجعية غير معرفة.
Figure I.15: Architecture du mode vérification.	خطأ! الإشارة المرجعية غير معرفة.
Figure I.16: Architecture du mode identification.	خطأ! الإشارة المرجعية غير معرفة.
Figure I.17: courbe ROC.	خطأ! الإشارة المرجعية غير معرفة.
Figure I.18: Différentes courbes CMC.	خطأ! الإشارة المرجعية غير معرفة.
Figure I.19: Critères de choix des caractéristique biométriques.	خطأ! الإشارة المرجعية غير معرفة.
Figure I. 20: Les parts de marché par technologie.	خطأ! الإشارة المرجعية غير معرفة.
Figure I.21 : La croissance de la biométrie.	خطأ! الإشارة المرجعية غير معرفة.

Table des figures

Figure II. 1: Architecture globale du système FKP.....	24
Figure II. 2: le prétraitement des images de l’empreinte d’articulation.	24
Figure II.3: Définition de la transformée de RADON.....	26
Figure II. 4: (a) 4 images de l’empreinte d’articulation27	
Figure II.5: Une illustration de LBP basique.	27
Figure II.6: Quelques modalités et leurs images LBP.....	28
Figure II.7: Exemples de l’opérateur LBPP.R . Source. [25]	28
Figure II. 8: (a) 4 images de l’empreinte d’articulation (b) Résultats de l’étape d’extraction des caractéristiques par la méthode LBP.	28
Figure II.9: (a) Exemple d’image FKP. (b) Filtre BSIF de taille 11x11 et de longueur 12. (c) Les résultats de la convolution de l’image FKP avec un filtre BSIF. (d) Image finale FKP filtrée par BSIF filtre.....	30
Figure II.10: Résultats de l’étape d’extraction des caractéristiques pour 4 l’empreinte d’articulation d’une seule personne(BSIF30	
Figure II.11: Principe de la technique SVM.	33
Figure II. 12: L’hyperplan H qui sépare les deux ensembles de points.	33
Figure II.13: Les vecteurs de support.....	34
Figure II.14: Hyperplan optimal, vecteurs de support et marge maximale.....	34
Figure II.15: Meilleur hyperplan séparateur.	35
Figure II.16: Cas linéairement séparable.....	36
Figure II. 17: Cas linéairement séparable.....	36
Figure II.18: Exemple graphique des données linéairement séparables.	38
Figure II.19: Espace de projection des données non linéairement séparables.	40

Liste des tableaux

Tableau I.1: Avantages et inconvénients des différentes technologies biométriques.....	20
Tableau III.1: les résultats des apprentissages et Tests des algorithmes	52

Listes des abbreviations

FKP : Finger knuckle print.

LBP : Local Binary Pattern.

BSIF : binarized statistical image features.

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

NER : Nombre des empreintes reconnus.

TRC : Le taux de reconnaissance par classe.

TMBR : Le taux moyenne de bonne reconnaissance.

FAR : False Accepted Rate.

FRR : False Rejected Rate.

ERR : Error Rejected Rate.

Introduction Générale

La biométrie est un terme dont on entend de plus en plus parler dans la vie de tous les jours. Si de nombreuses applications utilisent aujourd'hui la biométrie, celle qui correspond au plus grand déploiement est la mise en place, prévue pour 2009 des passeports biométriques utilisant le visage et l'empreinte digitale pour la délivrance et le contrôle de l'identité. Cependant, la biométrie n'est pas vraiment récente. Son apparition remonte au 19ème siècle, avec les premières études alors appelées anthropométrie. Les empreintes digitales ont ensuite été utilisées pour l'identification des personnes par la police. Cette utilisation policière n'a d'ailleurs jamais été abandonnée, et les empreintes digitales sont toujours utilisées (aujourd'hui de manière automatique avec les traitements informatiques) pour l'identification criminelle. La biométrie souffre d'ailleurs un peu de cette image policière et a du mal à se faire accepter par le grand public pour d'autres types d'applications. Cela dit, aujourd'hui la biométrie n'est plus limitée aux empreintes digitales et à l'identification criminelle. De nombreuses modalités sont aujourd'hui utilisées pour des applications de contrôle d'accès à des locaux ou à des objets personnels. On peut citer le visage, la voix, la signature, l'iris ou la forme de la main, et d'autres encore sont à l'étude comme la démarche, la forme de l'oreille ou la dynamique de frappe au clavier et articulations des doigts.

Objectifs

Dans ce travail, l'un de ces systèmes a été choisi d'être étudié, c'est celui de la reconnaissance des personnes par leurs images de surfaces extérieures des doigts, ou plus exactement, un système qui utilise l'empreinte des articulations des doigts (Finger Knuckle Print (**FKP**)). Cette modalité a été choisie selon leur nombreux avantages remarquables, à savoir c'est une technique acceptable par les individus, simple et facile à utilisée. Finalement, la combinaison de tous les doigts (dix doigts dans les deux mains) peut être utilisé afin d'établir un système biométrique robuste et précis.

Dans le cadre de ce travail, dans la première série des expériences, nous avons concevoir un système mono-biométrique, c.-à-d. un système qu'utilise une seule modalité biométrique. Pour cela, trois algorithmes, BSIF et LBP,RADON , ont été utilisés pour la phase la plus importante, à savoir la phase d'extraction des caractéristiques. Ces deux algorithmes sont très utilisés pour l'analyse de texture. Dans la deuxième série des expériences, la fusion multimodale est examinée afin d'obtenir un système biométrique performant, c.-à-d. un système qui peut être fonctionné avec une très petite

erreur d'identification, cette erreur rend le système apte pour l'utiliser dans des applications de très hautes sécurisées.

L'organisation du manuscrit :

Notre mémoire est scindé en **trois chapitres** :

Dans le **premier** nous avons défini la biométrie ainsi que les différentes techniques biométriques utilisées. Ce chapitre est finalisé par un aperçu sur les principaux domaines d'application de la biométrie ainsi que leur contribution dans le marché mondial.

Le **deuxième chapitre** est consacré à l'étude des phases de prétraitement des empreintes d'articulation. Cette étape comprend aussi des processus de traitement d'image en général (Egalisation d'histogramme). On décrira aussi les différents outils utilisés pour la génération du vecteur caractéristique, en particulier les transformées BSIF et LBP,RADON.

Ensuite, le **troisième chapitre** est consacré pour les résultats expérimentaux. Dans la première section de ce chapitre, nous avons mis en œuvre la description de la base de données utilisé, ensuite les critères d'évaluation dans notre systèmes.. La deuxième section de ce chapitre discute les résultats expérimentaux obtenus pour les systèmes biométriques. Scénario de fusion, à savoir le système le système multi-algorithmique a été évalué. Afin de sélectionner le meilleur système, qui présente la plus faible erreur d'identification, une comparaison entre les différents systèmes est exécutée.

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

I.1 Introduction

Dans ces jours les méthodes de sécurité classique ou traditionnelle des systèmes d'informations ne sont pas acceptables tellement elles sont utilisées par quelqu'un, 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. La deuxième est basée sur ce que possède la personne comme un badge ou une carte à puce. Dans le premier cas, le mot de passe peut être oublié par son utilisateur ou bien deviné par une autre personne. Dans le second cas, le badge (ou la pièce d'identité ou la clef) peut être perdu ou volé. Pour contourner cette limitation ou cette faiblesse, un autre moyen de la sécurité a été développé qui permet d'utiliser, non pas l'information qu'un individu possède ou connaît, mais une information intrinsèque à cette personne. Cette nouvelle façon d'identification des individus est **la biométrie**. [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 Les caractéristiques biométriques

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

- ❖ **Universalité** : toutes les personnes à identifier doivent la posséder.
- ❖ **Unicité** : l'information doit être aussi dissimilaire que possible entre les différentes personnes.

- ❖ **Collectabilité** : l'information doit être collectable et mesurable afin d'être utilisée pour les comparaisons.
- ❖ **Permanence** : l'information collectée doit être présente pendant toute la vie d'un individu.
- ❖ **Acceptabilité** : le système doit respecter certains critères (facilité d'acquisition, rapidité...etc.) afin d'être employés.

I.3 Modalités biométriques

Aucune biométrie unique ne pouvant 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 ses conséquences, chaque biométrie est utilisé dans une application particulière.[2]

Les biométries dépendent en deux techniques :

- ✓ **Techniques intrusives** : Ces techniques requièrent un contact physique avec l'individu pour l'identifier tel que les empreintes digitales, la rétine, l'iris 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 direct avec l'utilisateur (visage, démarche,...).

On peut classer les techniques biométriques en trois catégories :

1. **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...
2. **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.
3. **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.









			
L'empreinte digitale	Le visage	L'iris	La rétine
			
La main	La signature	La frappe au clavier	La voix

Figure I.1 : les techniques biométriques

Les technologies les plus fréquemment utilisées sont les suivantes.

I.3.1 Analyses biologiques :

a. 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. [2]

b. 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 permanent durant toute la durée de vie.[3]

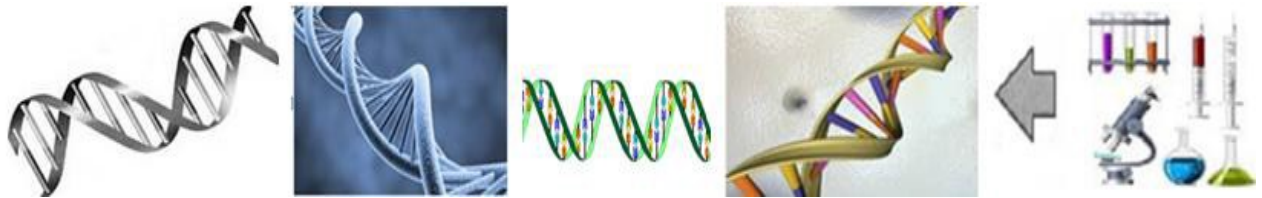


Figure I.2 : L'A.D.N.

c. La reconnaissance de la thermographie faciale

Une caméra infrarouge capte la chaleur émise par la peau. Contrairement à la reconnaissance faciale, on peut donc l'utiliser même dans l'obscurité ou de mauvaises conditions de visibilité. Mais les conditions de prise de vue peuvent conduire à des erreurs. [3]



Figure I.3: la thermographie faciale.

I.3.2 Analyses morphologiques :

a. Les empreintes digitales :

La reconnaissance des empreintes digitales est la plus utilisée. Les empreintes digitales sont composées de lignes localement parallèles présentant des points singuliers et constituent un motif unique, universel et permanent. Les lecteurs d'empreintes digitales scannent puis relèvent des éléments permettant de différencier les empreintes. Ces éléments sont appelés minuties. Il existe plusieurs types de minuties : lac, bifurcation, delta ou impasse...etc. 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.



Figure I.4: Empreinte digitale.

b. La Géométrie de la main :

La géométrie de la main est une technologie biométrique récente. Comme son nom l'indique, elle consiste à analyser et à mesurer la forme de la main, c'est-à-dire mesurer la longueur, la largeur et la hauteur de la main d'un utilisateur. Cette technologie offre un niveau raisonnable de précision est relativement facile à utiliser. Cependant elle peut être facilement trompée par des jumeaux ou par des personnes ayant des formes de la main proches.[4]



Figure I.5: La Géométrie de la main.

c. La reconnaissance de la rétine :

La rétine est la « pellicule photographique » de l'œil. Elle est constituée de 4 couches de cellules et est située au fond de l'œil.

Les éléments qui permettent de distinguer deux rétines sont les veines qui les tapissent. La disposition de ces veines est stable et unique.

La biométrie par la rétine procure également, un haut niveau en matière de reconnaissance. Cette technologie est bien adaptée pour des applications de haute sécurité (sites militaires et nucléaires, salles de coffres forts, etc.). La disposition des veines de la rétine assure une bonne fiabilité et une haute barrière contre la fraude.

L'utilisateur doit placer son œil à quelques centimètres d'un orifice de capture situé sur le lecteur de rétine. Il ne doit pas bouger et doit fixer un point vert lumineux qui effectue des rotations. A ce moment, un faisceau lumineux traverse l'œil jusqu' aux vaisseaux sanguins capillaires de la rétine. Le système localise et capture ainsi environ 400 points de référence. Après la capture d'une image de la rétine, le logiciel du dispositif de lecture découpe un anneau autour de la fovéa. Il repère l'emplacement des veines et leur orientation. Puis il les codifie dans un gabarit. Les algorithmes de l'opération restent relativement complexes.[2]



Figure I.6: Image de la rétine.

d. La reconnaissance de l'iris :

L'iris est la région, sous forme d'anneau, située entre la pupille et le blanc de l'œil, il est unique. L'iris a une structure extraordinaire et offre de nombreuses caractéristiques de texture qui sont uniques pour chaque individu. La reconnaissance de l'iris est développée dans les années 80 c'est pour cela elle est une technologie plus récente. L'image de l'iris est capturée par un appareil qui contient une caméra infrarouge, lorsque la personne se place à une courte distance de l'appareil.[6]



Figure I.7: Image de l'iris.

e. L'empreintes des articulations des doigts (FKP) :

C'est la technologie biométrique basée sur la surface arrière de doigt, elle contient des caractéristiques distinctives, telles que les lignes principales, les lignes secondaires et les crêtes, qui peuvent être **extraites** à partir des images à basse résolution. La main contient plusieurs doigts, pour cela, il faut conserver les informations à chaque doigt pour une reconnaissance précise dans le domaine d'identification.[3]



Figure I.8: Empreintes des articulations des doigts (FKP).

f. La reconnaissance de visage :

La reconnaissance de visages est la technique la plus commune et populaire. la reconnaissance de visages est une biométrie relativement peu sûre, sur le fait que le signal acquis est sujet à des variations beaucoup plus élevées que d'autres caractéristiques, comme la variation de l'éclairage, le changement de la position du visage, la présence ou l'absence de lunettes et autres; mais, au cours de ces dernières années plusieurs techniques de traitements d'images sont apparues, telle que la détection du visage, la normalisation de l'éclairage, etc. Sans oublier le développement considérable des technologies des caméras numériques, ce qui néglige l'effet de ces problèmes. [5]

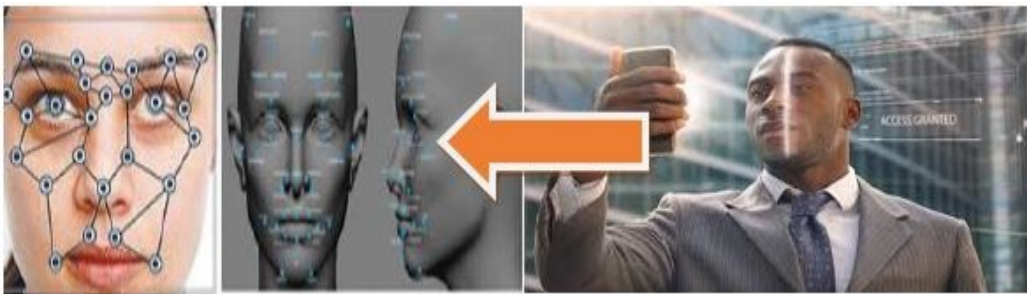


Figure I.9: Visage.

I.3.3 Analyse comportementale :

a. La reconnaissance de la signature :

C'est une écriture personnelle d'un individu, 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.[3]



Figure I.10: la signature.

b. La voix :

La voix humaine varie d'une personne à l'autre et peut se constituer de composantes physiologiques et comportementales. L'identification par la voix basée sur la forme et la taille des appendices (bouche, cavités nasales et les lèvres) utilisées dans la synthèse du son[6]. La reconnaissance des locuteurs est plus utilisé par les téléphones, les corps policiers, les hôpitaux...etc.



Figure I.11: la voix.

c. Frappe dynamique sur le clavier :

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 frappe, la suite des lettres, le temps de frappe et la pause entre chaque mot.[3]



Figure I.12: Frappe dynamique sur le clavier.

d. 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 .[3]



Figure I.13: Démarche.

I.4 Architecture et fonctionnement d'un système Biométrique

Un système biométrique est un système de reconnaissance des personnes qui 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.14**

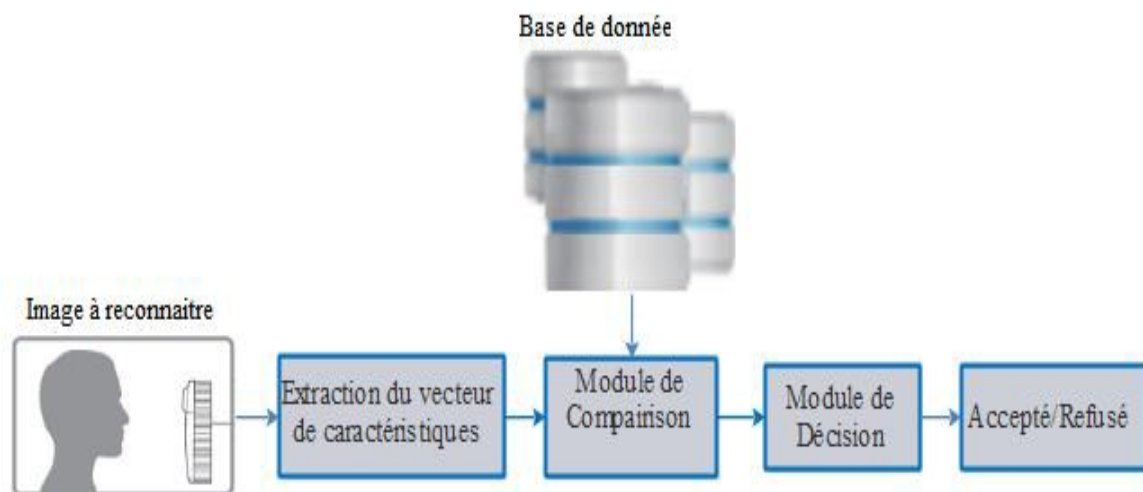


Figure I.14: Architecture d'un système biométrique.

En effet, il existe deux phases : la phase d'entraînement et la phase de test : Pendant **la phase d'entraînement** 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.4.1 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.15**).

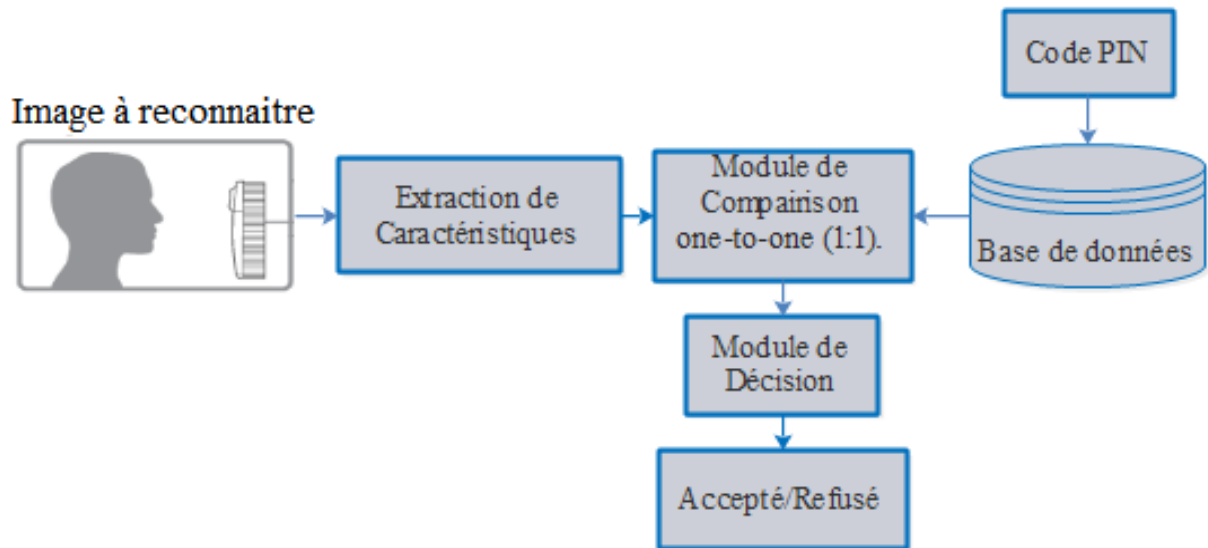


Figure I.15: Architecture du mode vérification.

I.4.2 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.16**), appelée aussi one-to-many (1:N)

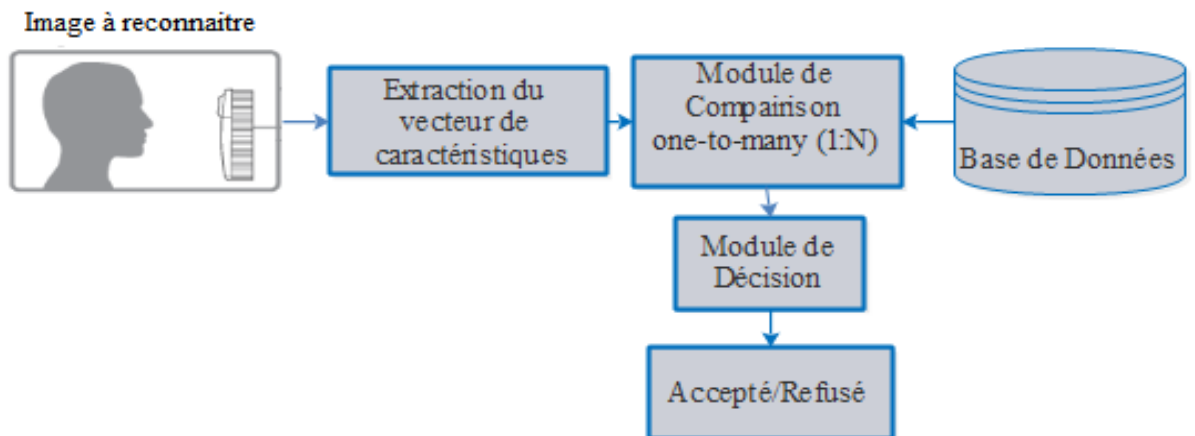


Figure I.16: Architecture du mode identification .

I.5 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.[3]

1. 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..)

2. 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

3. 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.

4. 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.6 Évaluation d'une performance

La performance d'un système d'identification biométrique peut se mesurer principalement à l'aide de trois critères : sa précision, son efficacité (vitesse d'exécution) et le volume de données qui doit être stocké pour chaque personne. Nous nous concentrerons dans cette section sur le premier aspect. Comme nous l'avons vu précédemment, l'identification et la vérification sont des modes opératoires différents. Elles nécessitent donc des mesures de précision différentes que nous étudierons dans les deux sous-sections suivantes.

❖ **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

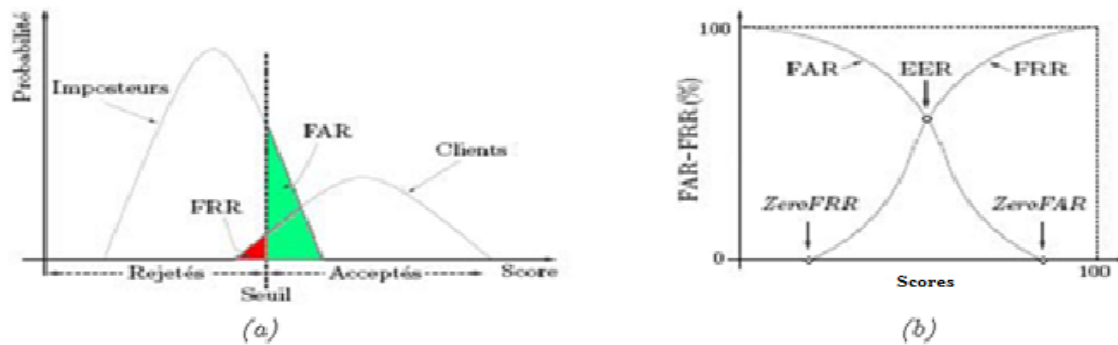


Figure I.17: Distribution des scores et les taux d'erreurs pour un seuil donné : (a) Distributions des Scores client et des scores imposteur ; (b) Variation des FRR et des FAR en fonction du seuil [7].

FRR) et la deuxième erreur mesure le taux d'acceptation des imposteurs, on parle alors à la fausse acceptation (False Acceptance Rate ou FAR). [7]

- ❖ **FAR** : C'est le pourcentage d'individus reconnus par le système biométrique, ce système classe alors deux caractéristiques provenant de deux personnes différentes

$$\text{FAR} = \frac{\text{nombre des imposteurs acceptés}}{\text{nombre totale d'accès imposteurs}}$$

- ❖ **FRR** : Ce taux représente le pourcentage d'individus censés être reconnus par le système mais qui sont rejetés, le système indique la probabilité qu'un utilisateur connu soit rejeté.

$$\text{FRR} = \frac{\text{nombre des clients rejetés}}{\text{nombre totale d'accès clients}}$$

Le taux le plus simple pour mesurer la performance d'un algorithme dans le contexte de la vérification est de calculer le point d'équivalence des erreurs (Equal Error Rate ou EER).

- ❖ **EER** : Ce taux est calculé à partir de FAR et FRR et constitue un point de mesure de performance courant, c.-à-d. **EER=FRR=FAR**.

$$\text{EER} = \frac{\text{nombre des fausses acceptations} + \text{nombre de faux rejets}}{\text{nombre totale d'accès}}$$

- ❖ **Courbe caractéristiques** :

Les performances d'un système biométrique peuvent être présentées graphiquement à l'aide de la courbe ROC (Receiver Operating Characteristic)[8]. Cette courbe représente les valeurs de FRR en termes de FAR. Ceci est obtenu en calculant le couple (FAR, FRR) ou

chaque valeur du seuil de décision. Celui-ci diffère de la plus petite valeur obtenue à une valeur supérieure. Cette courbe peut être décomposée en trois zones : zone de haute sécurité, zone de compromis et zone de basse sécurité.[6]

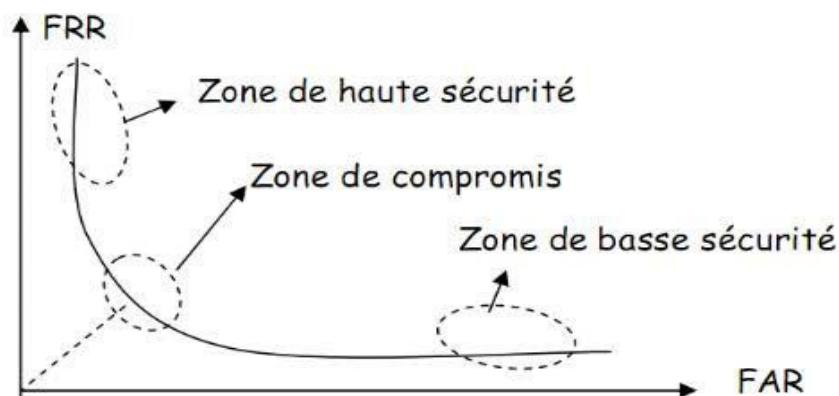


Figure I.18: courbe ROC.

I.7 Les applications de la biométrie :

Aujourd'hui, les principales applications sont la production de titres d'identité, le contrôle d'accès à des sites sécurisés, le contrôle des frontières, l'accès aux réseaux, systèmes d'information et stations de travail, le paiement électronique, la signature électronique et même le chiffrement de données. Cette liste n'est pas exhaustive, et de nouvelles applications vont très certainement voir rapidement le jour.

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

- **Application commerciales** : telles que l'accès au réseau informatique, la sécurité de données électroniques, le commerce électronique, l'accès d'internet, l'ATM, la carte de crédit, le contrôle d'accès physique, le téléphone portable, le PDA, la gestion des registres médicales, l'étude de distances, etc.... [2]
- **Applications de gouvernement** : telles que la carte nationale d'identifications, le permis de conduite, la sécurité sociale, le contrôle de passeport, etc....

- **Applications juridiques** : telles que l'identification de cadavre, la recherche criminelle, l'identification de terroriste, les enfants disparus, etc.

I.7.1 Les applications de la biométrie :

a. Contrôle d'accès aux locaux :

- Salles informatiques, Sites sensibles (service de recherche, site nucléaire).

b. Equipements de communication :

- Terminaux d'accès, Téléphones portables.

c. Systèmes d'informations :

- Lancement du système d'exploitation, Accès au réseau, Transaction (financière pour les banques, données entre entreprises).

d. Machines & Equipements divers :

- Distributeur automatique de billets, Lieu sensible (club de tir, police), Contrôle des adhérents dans les clubs privés, Contrôle des temps de présence.

e. Etat/Administration :

- Fichier judiciaire, Services sociaux (sécurisation des règlements), Système de vote électronique.

I.8 Avantages et Inconvénients des Techniques biométriques

Modalité	Avantages	Inconvénients
L'A.D.N	<ul style="list-style-type: none"> - Une Très grande précision. - Il impossible que le système a fait des erreurs. - Il est standardisé 	<ul style="list-style-type: none"> - Très cher

<p>L'iris</p>	<ul style="list-style-type: none"> - L'iris n'est pas modifiable même par intervention chirurgicale. - Grande quantité d'information contenue dans l'iris - L'iris ne varie presque pas au cours d'une vie. 	<ul style="list-style-type: none"> - Aspect psychologiquement invasif de la méthode - Des problèmes peuvent survenir lors de la mesure (reflet, variation de la taille de la pupille, etc.). Une photo ou une lentille de contact reproduisant l'image de l'iris peut affecter la fiabilité
<p>La rétine</p>	<ul style="list-style-type: none"> -La rétine est différente chez les vrais jumeaux, - La rétine est stable durant la vie d'un Individu - très efficace. Carte vasculaire propre à chaque individu et différente, même entre jumeaux. - Haute sécurité. 	<ul style="list-style-type: none"> -Mauvaise acceptation du public (l'œil est un organe sensible), - Coût plus important que d'autres technologies, - L'aspect des vaisseaux sanguins peut être modifié par la maladie ou l'âge
<p>Le visage</p>	<ul style="list-style-type: none"> - Le facial-scan fait par caméra photo est réputé pour être la technique la plus simple et la moins contraignante. Son principal avantage est son côté peu intrusif. - Comparable à se faire prendre en photo, il est relativement mieux accepté Socialement. 	<ul style="list-style-type: none"> - La reconnaissance des visages ne fonctionne pas bien incluent l'éclairage pauvre, les lunettes de soleil, les longs cheveux, ou d'autres objets couvrant partiellement le visage du sujet et des images à basse résolution. - la distance pour la capture de l'image du visage n'est pas inconfortable.

- La technologie la plus éprouvée techniquement et la plus connue du grand public.
 - Petite taille du lecteur facilitant son intégration dans la majorité des applications (téléphones portables, PC).
 - Traitement rapide
 - Bon compromis entre le taux de faux rejet et le taux de fausse acceptation.
- Les empreintes digitales
- Difficulté de lecture : sensibilité aux altérations pouvant survenir au cours de la vie (égratignure, cicatrice, vieillissement ou autres) et à certaines variations (température, humidité, saleté)

<p>Forme de la main</p>	<ul style="list-style-type: none"> - Bonne acceptation des usagés, - Très simple à utiliser, - Fichier "gabarit" de petite taille. - Le résultat est indépendant de l'humidité et de l'état de propreté des doigts, 	<ul style="list-style-type: none"> - La forme de la main ou des doigts se modifie avec le vieillissement, ce qui nuit à la mesure à long terme. - Risque de fausse acceptation pour des jumeaux ou des membres d'une même famille
<p>La voix</p>	<ul style="list-style-type: none"> - Technologie biométrique facile à mettre en œuvre - Permet de sécuriser une conversation téléphonique. 	<ul style="list-style-type: none"> - La voix n'est pas un attribut permanent (elle change bien entendu avec l'âge). - Sensible aux bruits ambiants.
<p>signature</p>	<ul style="list-style-type: none"> - La signature écrite sur un document peut être conservée des certains documents, - Action qui implique (responsabilité)le demandeur 	<ul style="list-style-type: none"> - Besoin d'une tablette graphique, - Sensible aux émotions de l'individu.

Empreintes des articulations des doigts (FKP)	<ul style="list-style-type: none"> - Technique acceptable. - Utilisation simple. - En combinant tous les doigts de la main, il est possible d'établir un système biométrique robuste et précise. 	<ul style="list-style-type: none"> - Très similaire pour les jumeaux. - Problème dans le cas de couper un doigt. - Pose incorrecte de doigt sur le lecteur provoque une grande erreur.
---	---	---

Tableau I.1: Avantages et inconvénients des différentes technologies biométriques.

I.9 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 (certaines modalités présentent des contraintes d'ergonomie, de coût d'acceptabilité) ainsi que l'environnement de leur usages (facilité d'emploi, d'analyse, de stockage, et de vérification).

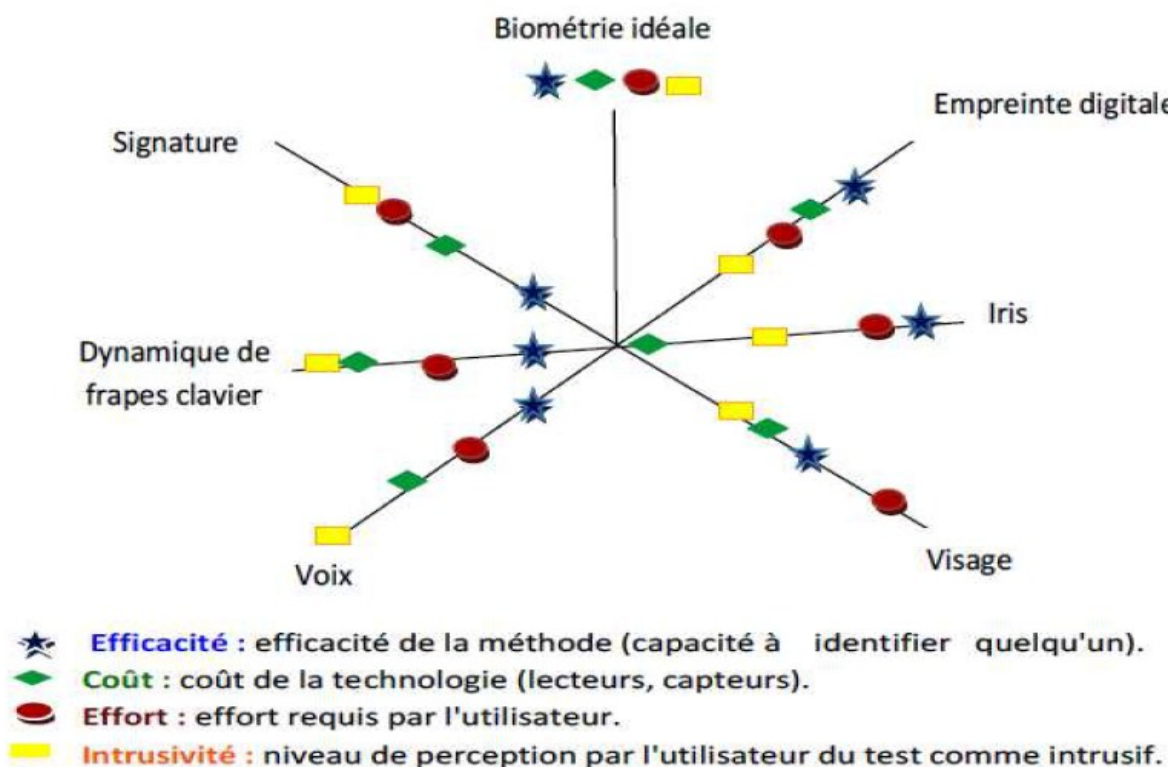


Figure I.2: Critères de choix des caractéristiques biométriques.

Nous remarquons dans la figure I.19 que l’empreinte digitale est proche d’être une modalité idéale par rapport aux autres caractéristiques biométriques, de par son efficacité, son coût minimal de mise en œuvre avec un moindre effort requis par l’utilisateur, ce qui rend intrusive la méthode surtout que c’est la plus ancienne et la plus naturelle.

I.10 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.

Dans son rapport intitulé « Sensors for Biometry 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.

Selon Yole, 525 millions d’unités de capteurs auraient été vendues en 2015 et ce chiffre devrait atteindre 1.500 millions d’unités d’ici à 2021. À côté de la détection des empreintes digitales pour le déverrouillage et le paiement mobile, il faut compter avec les technologies de reconnaissance visuelle pour la sécurité basées sur les images combinées de l’œil et du visage. En outre, les assistants vocaux développés par Amazon et Google mettent en jeu des modules de reconnaissance vocale enregistrée.

Les performances des futurs capteurs disposant d’un SNR (rapport signal sur bruit) élevé et de mémoires de comportement vont modifier le marché. Des applications émergentes potentielles émergent dans le bâtiment ou le secteur automobile, assurant la détection et

l'identification des personnes grâce à des capteurs d'empreintes digitales flexibles disposés sur la poignée de porte ou sur le volant.

En ce qui concerne le marché de la sécurité, la Chine, l'Afrique, l'Inde et l'Amérique du Sud sont les nouveaux filons du marché des lecteurs biométriques.[9]

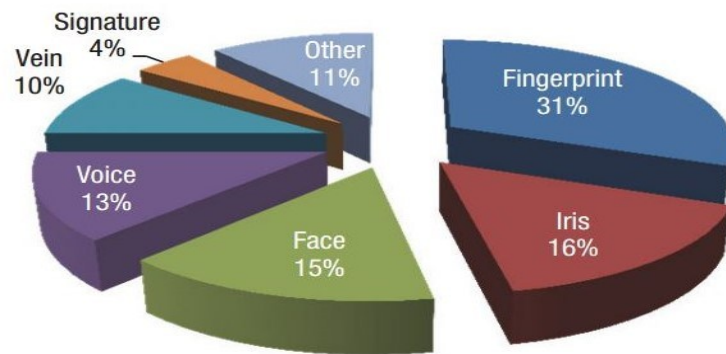


Figure I.3: Les parts de marché par technologie [9].



Figure I.4: La croissance de la biométrie [9].

I.11 Conclusion

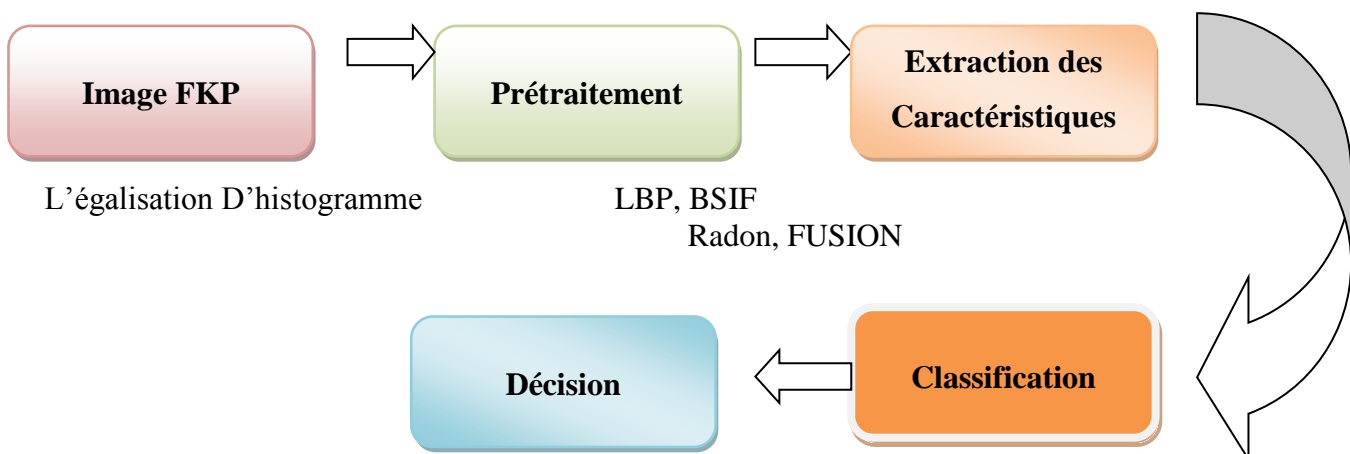
Dans ce chapitre nous avons décrit les technologies utilisées dans les systèmes biométriques pour l'identification des personnes, leurs architectures et leurs différentes applications, ainsi nous avons donné un aperçu sur les techniques de mesure des performances des systèmes biométriques et montré les différentes modalités biométriques tout en soulignant les avantages et les inconvénients de chacune. Nous avons constaté aussi que les performances des systèmes biométriques dépendent de plusieurs facteurs et qu'elles varient d'un système à un autre.

I.1 Introduction

Les caractéristiques biométriques sont une solution alternative aux anciens moyens de vérification d'identité. L'avantage de ces caractéristiques biométriques est d'être universelles, c'est-à-dire présentes chez toutes les personnes à identifier. Ces caractéristiques sont utilisées afin de décrire et ainsi différencier les objets. D'autre part, elles sont mesurables et uniques : deux personnes ne peuvent pas posséder exactement la même caractéristique. Elles sont aussi permanentes ce qui signifie qu'elles ne varient pas ou peu au cours du temps. Les systèmes biométriques éprouvent des contraintes à l'enregistrement et à l'utilisation des informations acquises. Parce que leurs tailles sont très larges, et la différence de ses sources. Pour résoudre cette problème et améliorer les performances de ces systèmes, les chercheurs additionnent une étape avant l'extraction des caractéristiques qu'ils La prétraitement des image FKP (les empreintes d'articulation du doigt, et La classification). A travers ce chapitre, nous allons présenter la méthode de prétraitement utilisé pour les FKP, ainsi que les méthodes d'extraction des caractéristiques. En particulier et leur classification, A la fin, nous terminons par une conclusion.

I.2 Architecture globale du système

Pour déterminer l'identité de la personne avec la reconnaissance de FKP, il faut nécessairement référencer les images FKP, sous la forme d'une base de données de FKP 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 FKP à reconnaître avec celui de chacun des FKP de la base de données.



Oui ou no

SVM

Figure II.1: Architecture globale du système FKP.**I.2.1 Le prétraitement d'une image:**

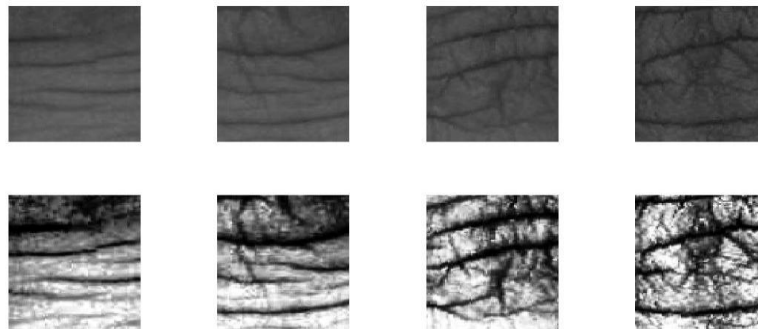
Le traitement d'images est une discipline de l'informatique et des mathématiques appliquées qui étudie les images numériques et leurs transformations, dans le but d'améliorer leur qualité ou d'en extraire de l'information.

Pour améliorer le contraste, nous avons appliqué légalisation d'histogramme :

- 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:** le prétraitement des images de l'empreinte d'articulation.

I.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.

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

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

- Approche statistique.
- Approche géométrique

I.3.1 Approche statistique

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

$$\text{fenêtre. } \bar{x} = \frac{1}{N} \sum_{i=1}^N x_i \quad (\text{II.1})$$

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

$$\delta^2 = \frac{1}{N-1} \sum_{i=1}^N (x - \bar{x})^2 \quad (\text{II.2})$$

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

$$E = \sum_i P_i \cdot \log(P_i) \quad (\text{II.3})$$

Où 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.

I.3.2 Approche géométrique

Plusieurs méthodes ont été proposées pour générer un vecteur caractéristique en tenant Compte de la géométrie de la forme [11]. Nous pouvons citer : les concavités, moments géométriques [12]. 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.

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

I.4.1 Définition :

En 1917, le mathématicien J .Radon a pu démontrer la disponibilité de reconstruire une fonction d'un espace à partir de la connaissance de ses intégrations le long d'hyperplans de ce

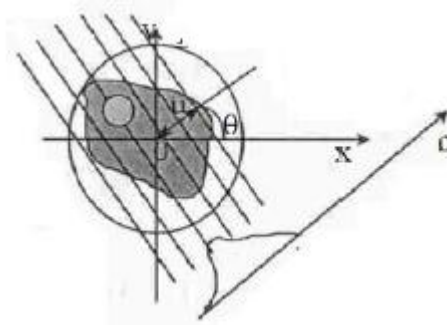
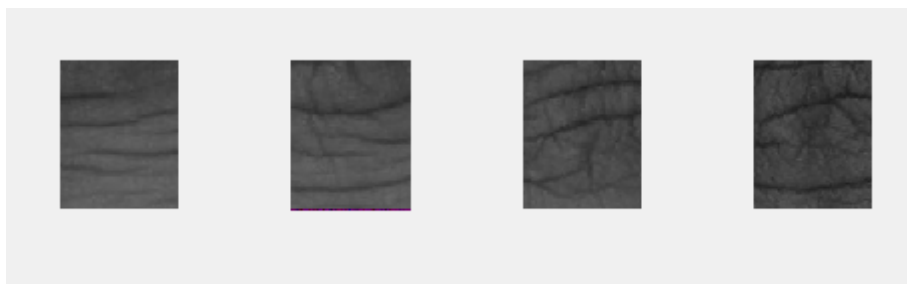


Figure II.3: Définition de la transformée de Radon. même espace. Cette famille d'intégration est appelée la transformée de Radon. La transformée de Radon représente l'image à l'aide d'une collection de projections suivant des directions différentes. Elle est largement utilisée dans des domaines allant de la sismologie à la vision par ordinateur. La transformée de Radon d'une image $f(x, y)$, notée $g(x, y)$, est définie comme étant sa gamme intégrale le long d'une ligne inclinée à un angle de l'axe des y et à une distance de l'origine [13] comme le montre la (Figure III.3)

I.4.2 Résultats De L'implémentation :

(a)



(b)

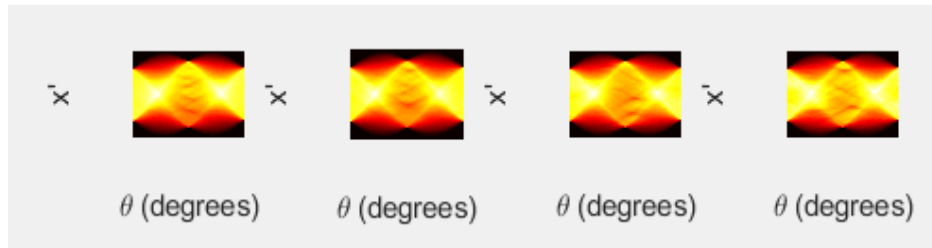


Figure II.4: (a) 4 images de l'empreinte d'articulation (b) Résultats de l'étape d'extraction des caractéristiques pour 4 l'empreinte d'articulation d'une Personnes désignées(BSIF).

I.5 Extraction Des Caractéristiques Avec Les LBP:

I.5.1 Définition :

L'opérateur d'analyse de la texture LBP, introduite par Ojala et al [14]. D'où le principe général est de comparer le niveau de gris d'un pixel avec les niveaux de ses voisins. Tous les voisins prendront une valeur 1 si leur valeur est supérieure ou égale au pixel courant et 0 si leur valeur est inférieure (Voir Figure II.5). Les pixels de ce motif binaire sont alors multipliés par des poids et sommés afin d'obtenir un code LBP du pixel courant.LBP est un moyen puissant de description de texture et parmi ses propriétés dans des applications réelles sont ses discriminatives puissances, simplicité de calcul[14]

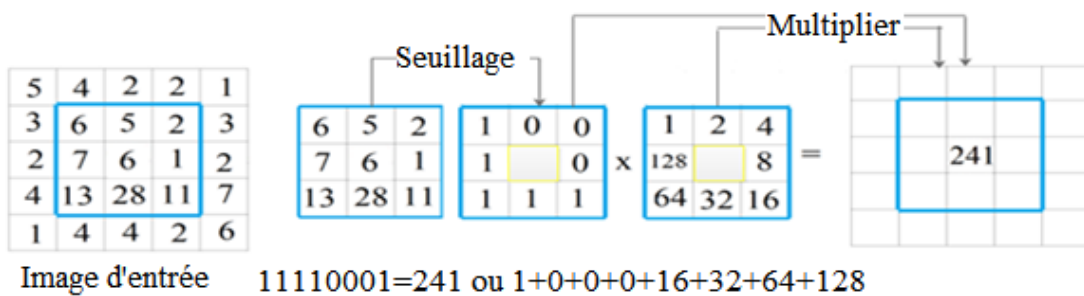


Figure II.5: Une illustration de LBP basique.

Soit g_c un pixel dans l'image d'entrée, ses p pixels voisins sont $(g_0, g_1, \dots, g_{p-1})$. La réponse LBP du pixel g_c est calculée comme suit :

$$LBP(x_c, y_c) = \sum_{i=0}^{p-1} f(x)(g_i - g_c) \cdot 2^i \tag{II.4}$$

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

$$f(x) = \begin{cases} 1 & \text{si } x \geq 0 \\ 0 & \text{si } x < 0 \end{cases} \tag{II.5}$$

La Figure II.6 Montre un exemple de quelques modalités biométriques avec leurs images LBP en utilisant l'opérateur LBP basique.

(a)

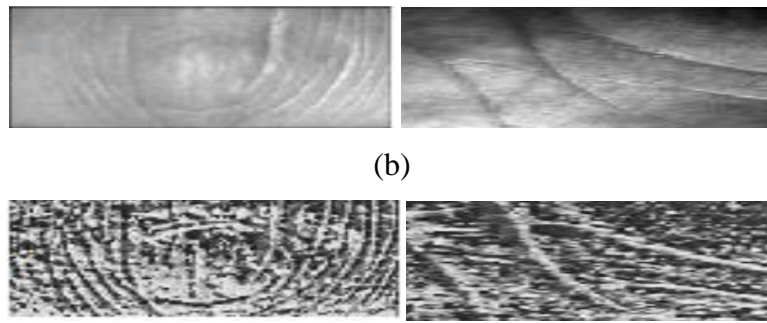


Figure II.6 : Quelques modalités et leurs images LBP.

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 [15] (Voir Figure II.7).

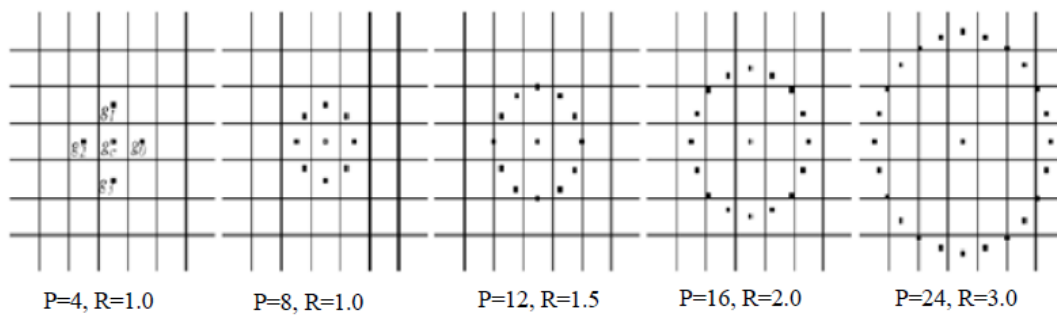


Figure II.7: Exemples de d'opérateur LBPP.R. Source. [15]

I.5.2 Résultats De L'implémentation

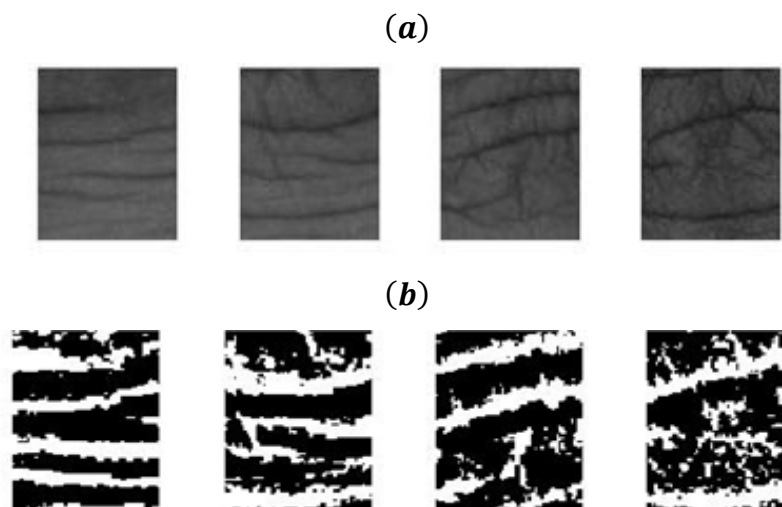


Figure II.8 : (a) 4 images de l'empreinte d'articulation (b) Résultats de l'étape d'extraction des caractéristiques par la méthode LBP.

I.6 Extraction Des Caractéristiques Avec Les BSIF :

I.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[16]. Ce descripteur est basé sur un ensemble de filtres linéaires de taille fixe. BSIF filtre une image donnée I de taille $N \times N$ pixels avec un ensemble de filtres φ_i de taille $N \times N$ alors les réponses r_i sont binaires. J. Kannala et E. Rahtu utilisent un ensemble des images naturelles (ça-dire-appliqué les concepts introduites dans [17]) pour former un ensemble des filtres φ_i de taille $N \times N$, ces filtres sont estimés en maximisant l'indépendance statistique des réponses r_i par ICA. Également, nous avons utilisé les filtres open-source[16]

$$r_i = \sum_{x,y} \varphi_i^{N \times N}(x,y) I(x,y) \quad (\text{II.6})$$

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

$$b_i = \begin{cases} 1 & \text{si } r_i > 0 \\ 0 & \text{si } r_i \leq 0 \end{cases} \quad (\text{II.7})$$

Enfin, les fonctions BSIF sont extraites 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 indique un exemple d'image FKP. La **Figure II.9 .b** représente le filtre BSIF de taille 11×11 et de longueur 12. La Figure II.9.c montre les résultats de la convolution de l'image FKP avec un filtre BSIF. La Figure II.9.d.e montre image filtrée par BSIF filtre.

(a)



(b)

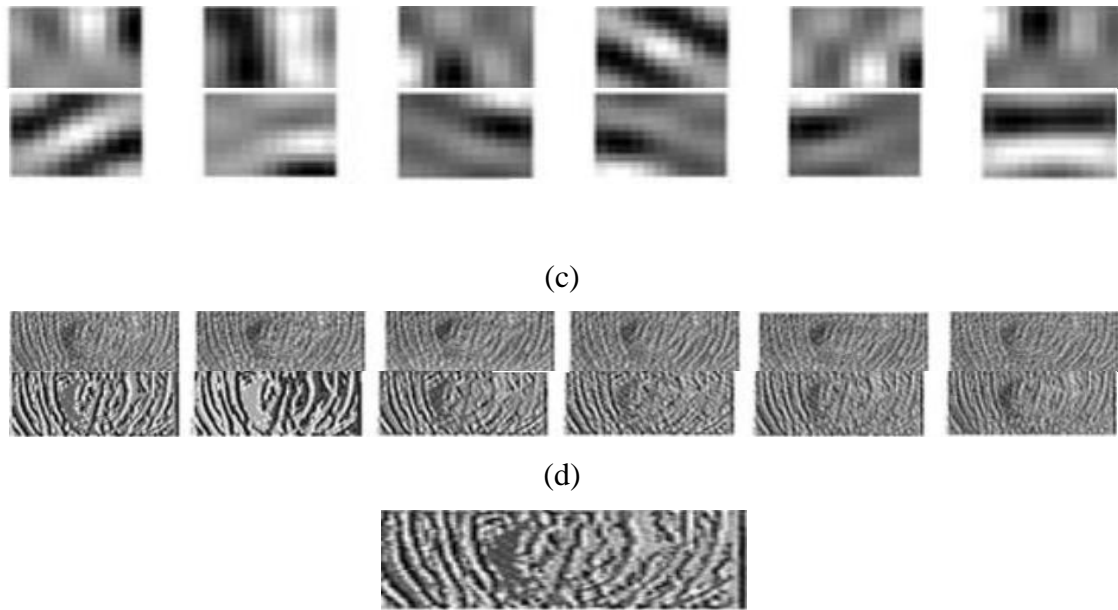


Figure II.9: (a) Exemple d'image FKP. (b) Filtre BSIF de taille 11×11 et de longueur 12. (c) Les résultats de la convolution de l'image FKP avec un filtre BSIF. (d) Image finale FKP filtrée par BSIF filtre.

I.6.2 Résultats De L'implémentation :

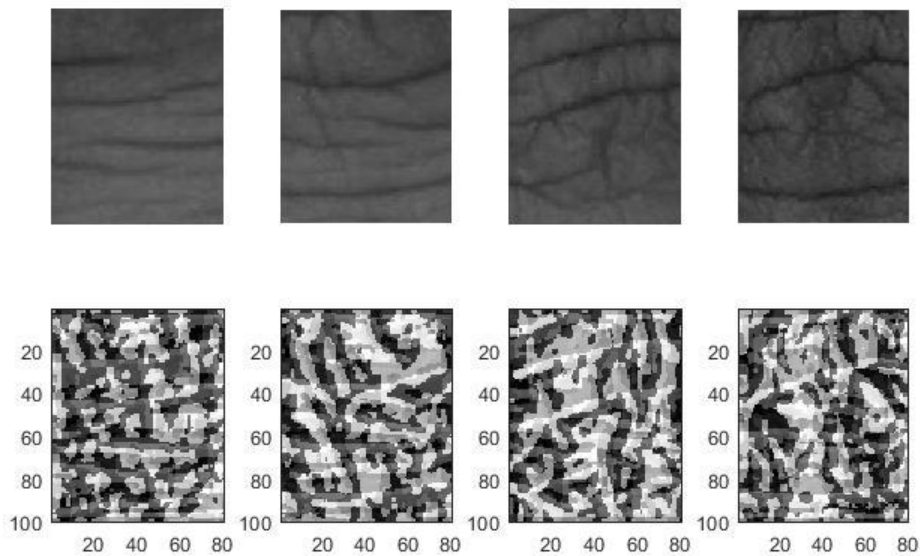


Figure II.10: Résultats de l'étape d'extraction des caractéristiques pour 4 l'empreinte d'articulation d'une seule personne(BSIF).

I.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

I.8 Normalisation des données

Généralement, les composantes d'un vecteur caractéristique sont de nature hétérogène pouvant influencer 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 N moyenne et de la variance. Pour les données Disponibles de la caractéristique, chaque composante du vecteur caractéristique via l'équation :

$$\hat{x}_{ik} = \frac{x_{ik} - \bar{x}_k}{\delta_k} \quad (\text{II.8})$$

$$\text{Avec : } \bar{x}_k = \frac{1}{N} \sum_{i=1}^N x_{ik}, k = 1, 2, \dots, l \quad (\text{II.9})$$

$$\delta_k^2 = \frac{1}{N-1} \sum_{i=1}^N (x_{ik} - \bar{x}_k)^2 \quad (\text{II.10})$$

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 :

$$y = \frac{x_{ik} - \bar{x}_k}{r\sigma_k}, \hat{x}_{ik} = \frac{1}{1 + \exp(-y)} \quad (\text{II.11})$$

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 y c'est une fonction approximativement linéaire par rapport à x_{ki} .

La gamme des valeurs de x_{ki} 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.

I.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 [19].

I.9.1 Machine à vecteurs de support(SVM)

Une machine à vecteurs de support ou Support Vector Machine (SVM) est une technique de discrimination, c'est une méthode d'apprentissage supervisé utilisée pour la classification et la régression. Elle consiste à séparer deux ou plusieurs ensembles de points par un hyper plan. Selon les cas et la configuration des points [20].

I.9.1.1 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 [21].

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 [22].

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 [21]

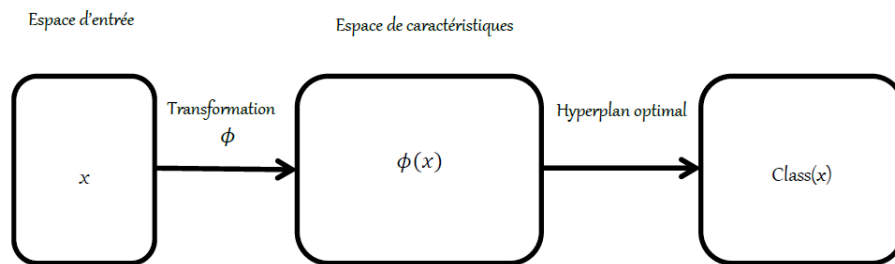


Figure II.11: Principe de la technique SVM[21].

I.9.1.2 Notions de base :

❖ Hyperplan :

Plaçons-nous dans le cas d'une classification binaire (i.e. les exemples à classer réparties en classes). On appelle hyperplan séparateur un hyperplan qui sépare les deux classes (Figure II.12), en particulier il sépare leurs points d'apprentissage. De cette notion nous pouvons dire qu'il est évident de trouver une multitude d'hyperplans, mais la propriété délicate des SVM est d'avoir l'hyperplan dont la distance minimale aux exemples d'apprentissage est maximale, cet hyperplan est appelé L'hyperplan optimal, et ce dernier va maximiser la marge. [24, 25,21].

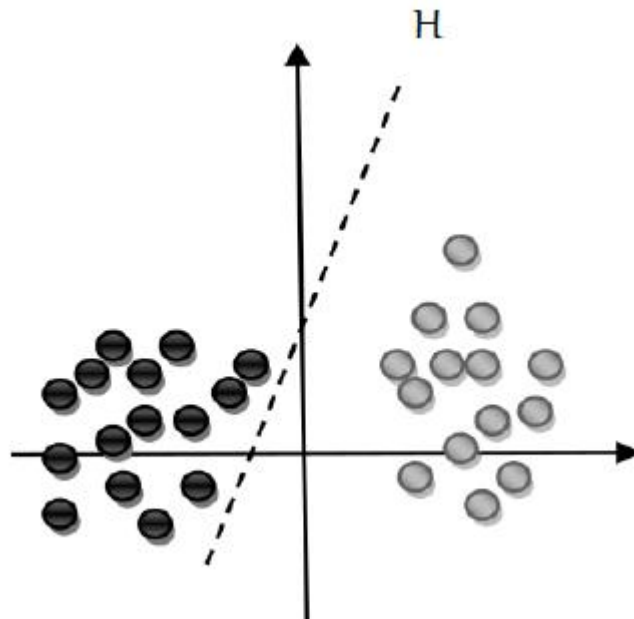


Figure II.12: L'hyperplan H qui sépare les deux ensembles de points.

❖ **Vecteurs de support :**

Pour une tâche de détermination de l'hyperplan séparable des SVM est d'utiliser seulement les points les plus proches (i.e. les points de la frontière entre les deux classes des données) parmi l'ensemble total d'apprentissage, ces points sont appelés vecteurs de support Figure II.13 [24,25].

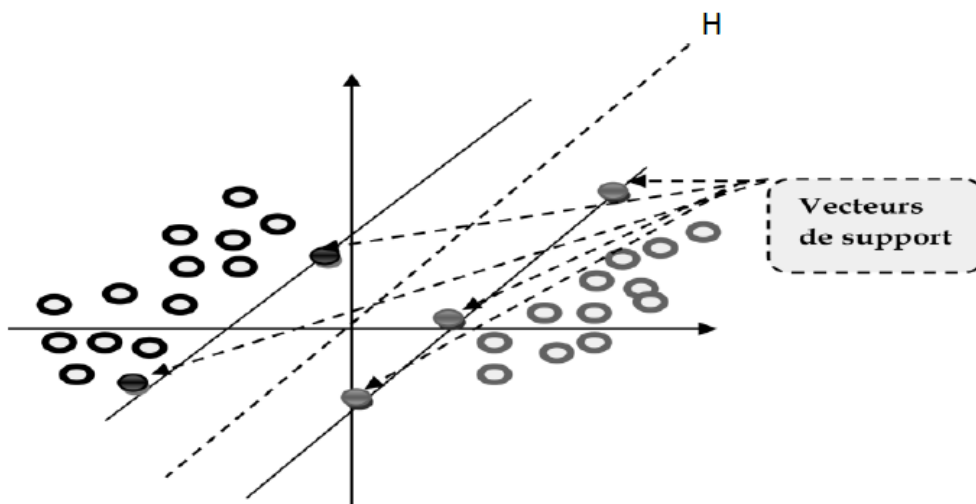


Figure II.13: Les vecteurs de support.

❖ **Marge :**

Il existe une infinité d'hyperplans capables de séparer parfaitement les deux classes d'exemples. Le principe des SVM est de choisir celui qui va maximiser la distance minimale entre l'hyperplan et les exemples d'apprentissage (i.e. la distance entre l'hyperplan et les vecteurs de support), cette distance est appelée la marge (**Figure II.13**) [24,25].

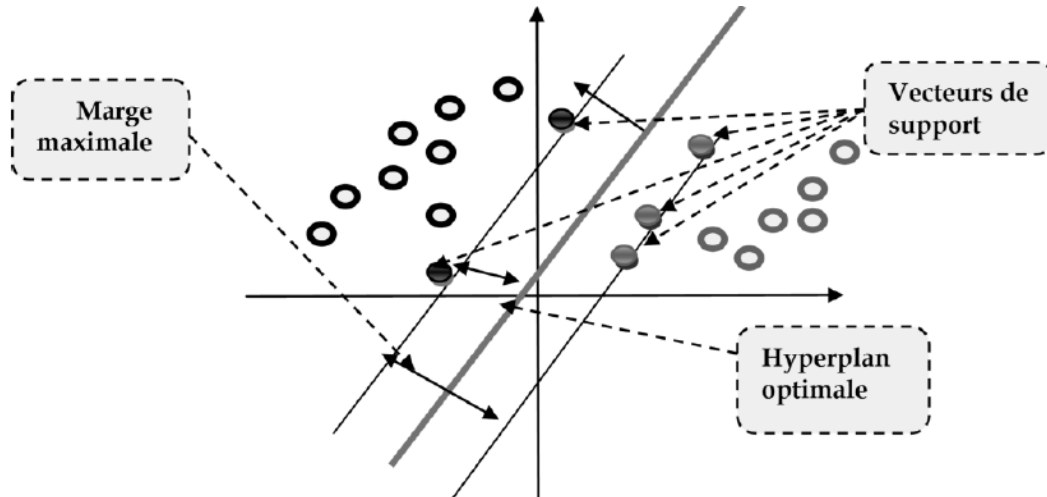


Figure II.14: Hyperplan optimal, vecteurs de support et marge maximale.

Propriétés fondamentales :

❖ Pourquoi maximiser la marge ?

Intuitivement, le fait d'avoir une marge plus large procure plus de sécurité lorsque l'on classe un nouvel exemple. De plus, si l'on trouve le classificateur qui se comporte le mieux vis-à-vis des données d'apprentissage, il est clair qu'il sera aussi celui qui permettra au mieux de classer les nouveaux exemples. Dans le schéma Figure II.15, la partie droite nous montre qu'avec

Un hyperplan optimal, un nouvel exemple reste bien classé alors qu'il tombe dans la marge. On constate sur la partie gauche qu'avec une plus petite marge, l'exemple se voit mal classé [24,25].

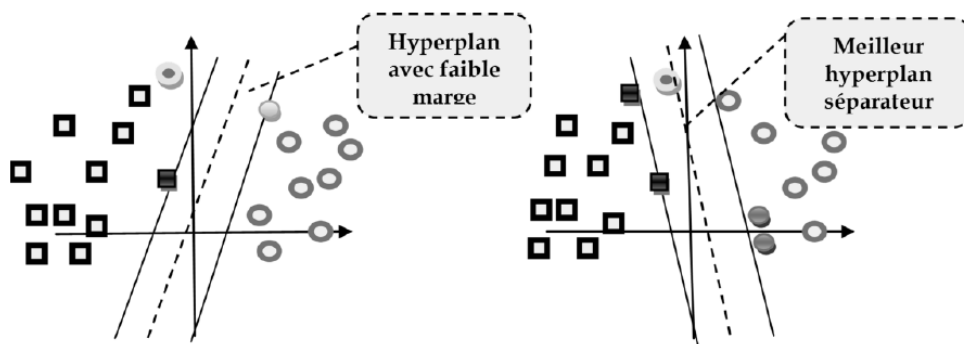


Figure II.15: Meilleur hyperplan séparateur.

❖ Linéarité dans les SVM :

Parmi les modèles des SVM, on constate les cas linéairement séparables et les cas non linéairement séparables (Figure II.16, Figure II.17).

Les premiers sont les plus simples des SVM car ils permettent de trouver au moins une fonction linéaire qui classe correctement tous les objets de la base d'apprentissage. Dans la plupart des problèmes réels il n'y a pas de séparation linéaire possible entre les données, le classificateur de marge maximale ne peut pas être utilisé car il fonctionne seulement si les classes de données d'apprentissage sont linéairement séparables [24,25].

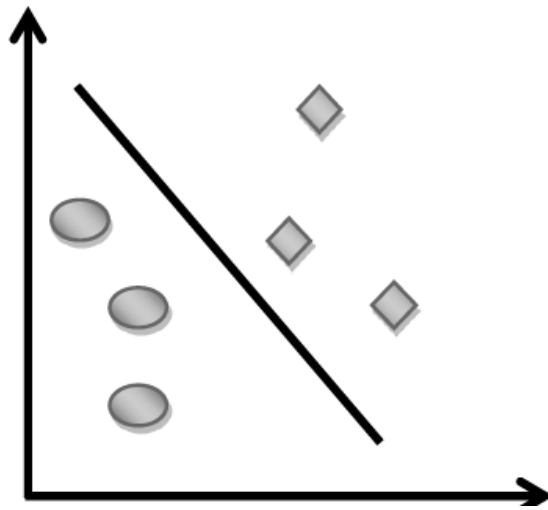


Figure II.16: Cas linéairement séparable

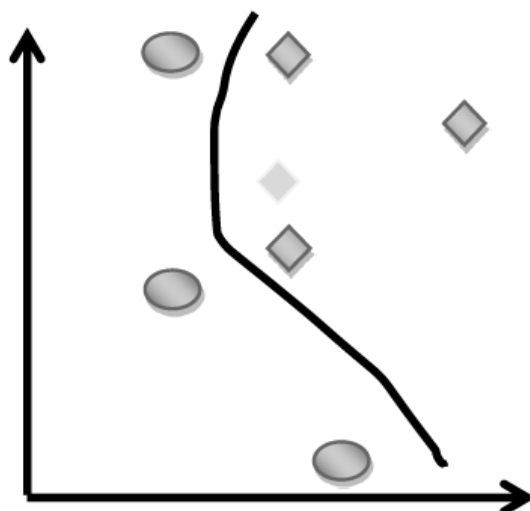
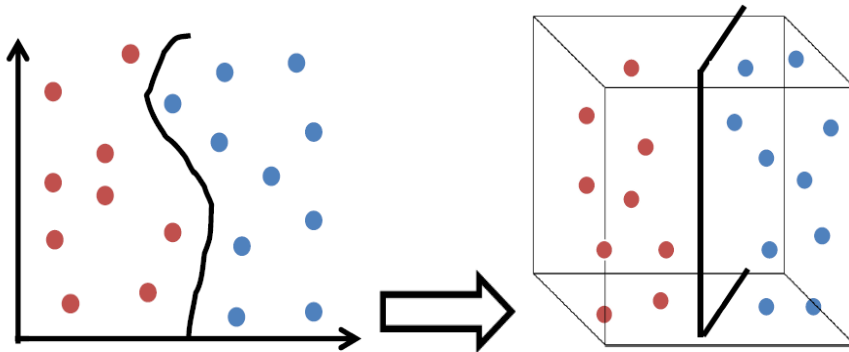


Figure II.17: Cas linéairement séparable.

❖ Le non linéaire dans les SVM :

Pour surmonter les inconvénients des cas non linéairement séparable, l'idée des SVM est de changer l'espace des données. La transformation non linéaire des données peut permettre une séparation linéaire des exemples dans un nouvel espace. On va donc avoir un changement de dimension. Ce nouvel espace est appelée « espace de re-description » [21]. En effet, intuitivement, plus la dimension de l'espace de re-description n'est grande, plus la probabilité de pouvoir trouver un hyperplan séparateur entre les exemples est élevée. Ceci est illustré par le schéma suivant :



On a donc une transformation d'un problème de séparation non linéaire dans l'espace de représentation en un problème de séparation linéaire dans un espace de re-description de plus grande dimension. Cette transformation non linéaire est réalisée *via* une fonction noyau. En pratique, quelques familles de fonctions noyau paramétrables sont connues et il revient à l'utilisateur de SVM d'effectuer des tests pour déterminer celles qui conviennent le mieux pour son application. On peut citer les exemples de noyaux suivants : polynomiale, gaussien, sigmoïde et Laplacien [24,25].

Fondement mathématiques :

Le cas linéairement séparable :

Si les données sont linéairement séparables, alors [26] il existe un hyperplan d'équation $\langle W, \cdot \rangle + b = 0$ tel que :

$$\begin{cases} W \cdot X + b \geq 1 & \text{si } y_i = +1 \\ W \cdot X + b \leq -1 & \text{si } y_i = -1 \end{cases} \quad (\text{II.12})$$

On peut combiner ces deux inéquations en une seule :

$$y_i(W \cdot X + b) \geq +1 \quad (\text{II.13})$$

La distance perpendiculaire de l'origine a l'hyperplan :

$$H_1 : W \cdot X + b = 1 \quad \text{est} \quad \frac{|1-b|}{\|W\|} \tag{II.14}$$

De même pour :

$$H_2 : W \cdot X + b = -1 \quad \text{est} \quad \frac{|1+b|}{\|W\|} \tag{II.15}$$

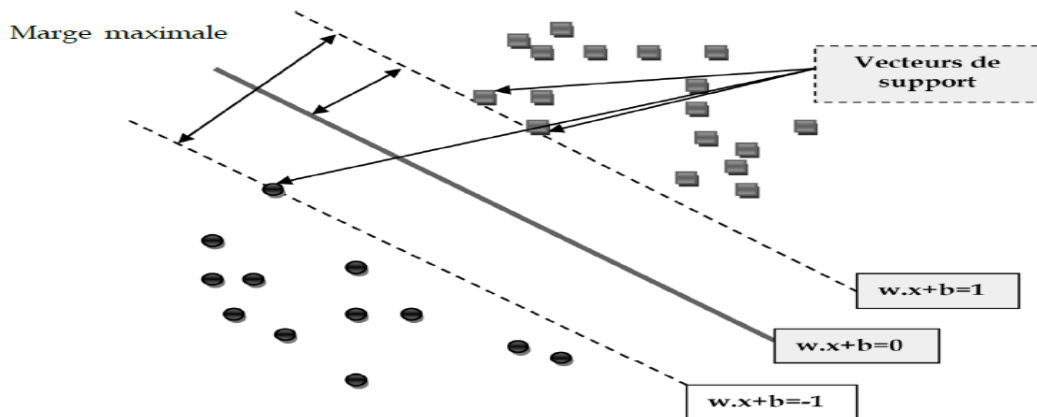


Figure II.18: Exemple graphique des données linéairement séparables.

Calcul de la marge :

Rappelons que (en deux dimensions) la distance entre un point (x_0, y_0) et une droite $Ax + By + c = 0$ est donnée par la relation suivante :

$$\frac{|Ax_0 + By_0 + c|}{\sqrt{A^2 + B^2}} \tag{II.16}$$

De façon similaire, la distance entre un point situé sur H_1 et l'hyperplan H_0 est donnée par

$$\frac{|w \cdot x + b|}{\|w\|} = \frac{1}{\|w\|} \tag{II.17}$$

Donc la marge (la distance entre les deux hyperplans H_1 et H_2) est : $\frac{2}{\|w\|}$

La maximisation de cette quantité revient à minimiser l'inverse $\frac{\|w\|}{2}$, Donc finalement notre problème peut être formulé comme suit : $\min \frac{1}{2} w^T w$ en restant dans le cadre de la condition initiale qui est :

$$y_i(w \cdot x + b) \geq +1 \tag{II.18}$$

On a :

$$\left\{ \begin{array}{l} \min \left(\frac{1}{2} w^T w \right) \\ \text{sous la contrainte} \\ y_i(w \cdot x + b) \geq +1 \end{array} \right. \tag{II.19}$$

Ce genre de problème d'optimisation peut être résolu en associant un multiplicateur de Lagrange α_i à chaque contrainte ($\alpha_i \geq 0$) [37]. Le lagrangien est donné par :

$$L(w, s, a) = \frac{1}{2} w^t w - \sum_{i=1}^N \alpha_i y_i (w \cdot x_i + b) + \sum_{i=1}^N \alpha_i \quad (\text{II.20})$$

En passant à la formulation duale, le problème devient : maximiser le Lagrangien, cela revient à dire, de trouver les α_i et w qui annulent ses dérivées partielles:

$$\frac{\partial L(w,b,a)}{\partial w} = 0, \frac{\partial L(w,b,a)}{\partial b} = 0 \text{ et } \alpha_i \geq 0 \quad (\text{II.21})$$

On trouve :

$$W = \sum_{i=1}^N \alpha_i y_i x_i \text{ et } \sum_{i=1}^N \alpha_i y_i = 0 \quad (\text{II.22})$$

Et en les réinjectant dans le Lagrangien on obtient le Lagrangien dual :

$$L(w, b, a) = \sum_{i=1}^N \alpha_i - \frac{1}{2} \sum_{i=1}^N \sum_{j=1}^N \alpha_i \alpha_j y_i y_j x_i x_j \quad (\text{II.23})$$

La résolution des α_i donne la valeur du vecteur $w = \sum_{i=1}^N \alpha_i y_i x_i$ et peut classer une nouvelle cible suivant son vecteur de caractéristique x selon la fonction:

$$f(x) \text{ signe}(w \cdot x + b) = \text{signe}(\sum_{i=1}^N \alpha_i y_i x_i \cdot x + b) \quad (\text{II.24})$$

Dans le cas non linéairement séparable, on introduit des variables d'écart $\xi_i (i=1..N)$ avec $\xi_i > 0$ dans les contraintes, qui deviennent

$$\begin{cases} w \cdot x + b \geq 1 - \xi_i \text{ si } y_i = +1 \\ \text{et} \\ w \cdot x + b \leq -1 + \xi_i \text{ si } y_i = -1 \end{cases} \quad (\text{II.25})$$

Un moyen naturel de donner un coût aux erreurs est de remplacer la fonction à minimiser précédente par :

$$\frac{\|w\|^2}{2} + C(\sum \xi_i)^K \quad (\text{II.26})$$

Dans le cas où les données sont non linéairement séparables, c'est-à-dire la surface séparatrice est non linéaire, on transpose le problème dans un autre espace F de dimension plus élevée pour rendre les nuages de points des deux classes linéairement séparables au moyen d'une transformation Φ tel que :

$$\Phi : X \rightarrow \Phi \in F \quad (\text{II.27})$$

Le calcul de la surface de séparation revient alors à chercher l'hyperplan optimal dans ce nouvel espace F .

La fonction de décision peut être représentée par le produit scalaire :

$$\Phi^T(x_i) * \Phi(x_j) \quad (\text{II.28})$$

Cette dernière quantité peut être remplacée par une fonction de la forme $K(x_i, y_i)$ (Les fonctions scalaires symétriques et définies positives, que l'on désigne souvent simplement par "noyaux", sont plus précisément des "noyaux de Mercer"), c'est ce qu'on appelle le noyau [27].

$$\text{Donc : } k(x_i, y_i) = \Phi^T(x_i) * \Phi(x_j) \quad (\text{II.29})$$

Le lagrangien devient alors :

$$L(W, b, a) = \sum_{i=1}^N a_i - \frac{1}{2} \sum_{i=1}^N \sum_{j=1}^N a_i a_j y_i y_j K(x_i, y_j) \quad (\text{II.30})$$

A ce stade, le problème se situe dans le choix de la transformation Φ ou plus généralement à la fonction noyau K . Ils existent peu de noyaux régulièrement utilisés avec les SVM.

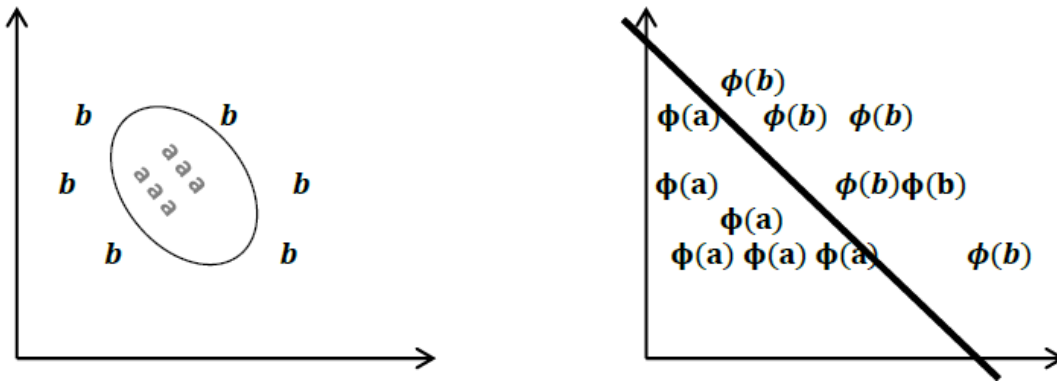


Figure II.19: Espace de projection des données non linéairement séparables.

❖ Les fonctions noyaux (Kernel) :

Un noyau caractérise le degré de similarité ou la corrélation entre deux éléments. Il a une valeur élevée pour deux vecteurs qui se ressemblent et faible pour deux vecteurs plus différents [27][24].

Les noyaux les plus classiques sont :

- Noyau linéaire : $K(x, z) = x \cdot z$
- Noyau polynomial : $k(x, y) = (a * \langle x, z \rangle + b)^d$
- Noyau Gaussien : $K(x, z) = e^{-\left(\frac{\|x-z\|^2}{2\sigma^2}\right)}$

I.9.2 SVM Multi-classes

A l'origine, les SVM ont été conçus essentiellement pour les problèmes à 2 classes, cependant plusieurs approches permettant d'étendre cet algorithme aux cas à N classes ont été proposées. La généralisation dans le cas multi-classes peut se faire de trois façons différentes.

Les deux premières méthodes sont basées sur une multiplication des classifieur bi-classes tandis que la dernière propose une résolution globale [18].

- ❖ **Un-contre-tous** : l'approche la plus naturelle est d'utiliser cette méthode de discrimination binaire et d'apprendre N fonctions de décision $\{f_m\}_{m=1\dots N}$ permettant de faire la discrimination entre chaque classe de toutes les autres (chaque classe est opposée à toutes les autres).il faut donc poser N problèmes Binaires. L'affectation d'un nouveau point x à une classe C_i se fait par la relation :

$$i = \operatorname{argmax}_{m=1\dots N} F_m(x)$$

- ❖ **Un-contre-un** : la deuxième méthode est une méthode dite de un contre un. Au lieu d'apprendre N fonctions de décisions, ici chaque classe est discriminée d'une autre. Ainsi, $N(N-1)/2$ fonctions de décisions sont apprises et chacune d'entre elles effectue un vote pour l'affectation d'un nouveau point x . La classe de ce point x devient ensuite la classe majoritaire après le vote.
- ❖ **Méthode globale** : la dernière méthode est une approche étendant la notion de marge aux cas multi-classes. Le problème fait intervenir N fonctions de décision et il est très gourmand en temps de calcul et en espace mémoire ce qui fait qu'il reste peu utilisé dans les cas réels.

I.9.3 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 vue 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 3.10.

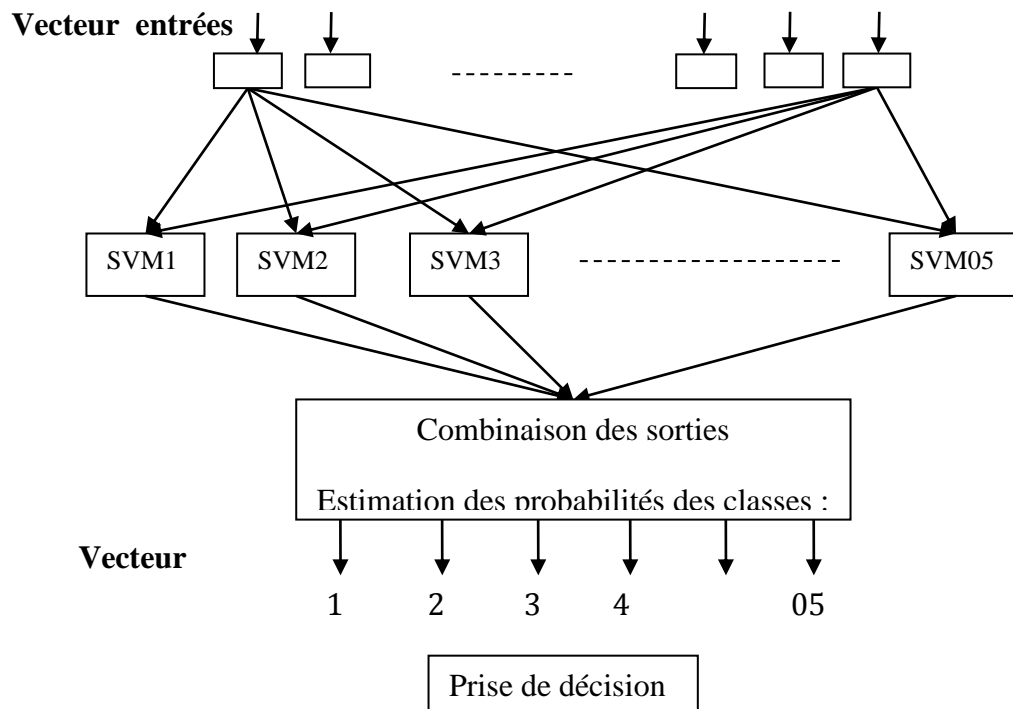


Figure II.20 : Architecture détaillée du classifieur SVM implémenté.

I.10 Conclusion

Au module d'extraction des caractéristiques, les systèmes de reconnaissances font 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 FKP, 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.

I.1 Introduction

Ce chapitre est dédié à la présentation des résultats obtenus pour la validation de notre système. La description de la base de données utilisée est tout d'abord présentée. Puis plusieurs expériences sont menées pour l'étude de l'influence des paramètres initiaux sur les performances du système. Les résultats obtenus sont présentés avec la combinaison des différentes catégories de caractéristiques (LBP et BISIF et RADON). Ces résultats permettent de mesurer les performances de notre approche.

I.2 La base de données

I.2.1 Description de la base

La base de données ITT delhi finger knuckle se compose de 790 images des expressions de FKP de 158 personnes distinctes (Figure III.3).

Pour cette base de données, chaque personne est représentée par 5 images de doigt. Cette base de donnée a été acquise en IIT Delhi en aout 2006-juin 2007 en utilisant une caméra numérique et les images sont présentées dans le groupe d'Age 16-55 ans cette base de données de 790 image ont été numériquement séquentiellement pour chaque utilisateur avec un identifié / identification. La résolution de ces Images est de 80*100 pixels et tous ces images sont disponibles en format bitmap.[30]

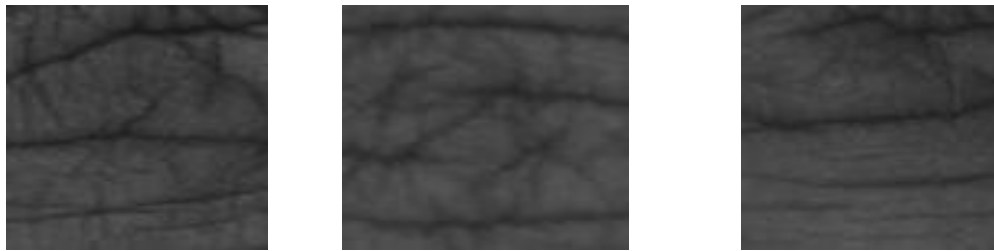


Figure III.1: Exemples des images de la base de données ITT Delhi finger knuckle.

I.2.2 Séparation des bases de données

Afin de développer une application de reconnaissance de FKP, il est nécessaire de disposer de deux bases de données : une base pour effectuer l'apprentissage et une autre pour tester les techniques et déterminer leurs performances, mais Il n'y a pas de règles pour déterminer ce partage de manière quantitative. Il résulte souvent d'un compromis tenant compte du nombre de données dont on dispose et du temps pour effectuer l'apprentissage. Dans les séries de test que nous avons effectué la base a été scindée de la façon suivante :

- **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.

I.3 Expérimentations sur la FKP

Nous avons mis en œuvre un système de reconnaissance à base des algorithmes LBP, BISIF et radon avec la modalité FKP. Dans cette expérimentation, n'utiliserons pas tous les classes de La base de données ITT delhi finger knuckle nous utilisons 150(30×5) classe seulement pour 30 personnes à chaque personne prenons 5 images, 105 images pour l'apprentissage et le reste pour le test. Pour obtenir les résultats des tests, chaque vecteur de l'image de test a été comparé avec tous les vecteurs dans la base des références et les résultats sont évalués selon certains critères: taux de classification, taux d'erreur et la matrice de confusion, Si les deux vecteurs sont de la même classe (même personne), la mise en correspondance entre eux a été compté comme un client ; sinon il a été considéré comme un imposteur.

I.4 Critères d'évaluation

Nous décrivons dans ce paragraphe les critères les plus souvent employés pour évaluer la performance des systèmes de reconnaissance en phase de généralisation. L'objectif est d'obtenir une estimation la plus fidèle possible du comportement du système dans des conditions réelles d'utilisation. Pour cela, des critères classiques comme par exemple le taux de reconnaissance est presque systématiquement utilisé.

Le taux de reconnaissance permet d'évaluer la qualité du classifieur par rapport au problème pour lequel il a été conçu. Ce taux est évalué grâce à une base de test qui contient des formes décrites dans le même espace de représentation que celles utilisées pour l'apprentissage. Elles sont aussi étiquetées par leur classe réelle d'appartenance afin de pouvoir vérifier les réponses du classifieur. Pour que l'estimation du taux de reconnaissance soit la plus fiable possible, il est primordial que le classifieur n'ait jamais utilisé les échantillons de cette base pour faire son apprentissage (la base de test ne doit avoir aucun individu en commun avec la base d'apprentissage et les éventuelles bases de validation). De plus cette base de test doit être suffisamment représentative du problème de classification, Dans (Guyon et al., 1998) les auteurs donnent une méthode pour déterminer la taille d'une base de test statistiquement significative dans le contexte de la reconnaissance de formes.

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

$$TRC(\%) = \frac{\text{nombre d'empreintes reconnus pour une classe}}{\text{nombre totale d'empreintes de cette classe}}$$

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

$$TMBR(\%) = \frac{\text{nombre d'empreintes reconnues}}{\text{nombre totale des empreintes}}$$

I.5 Les Résultats

Afin de montrer et expliquer la performance du système proposé clairement, Quatre expérimentations ont été menées. Dans chaque expérimentation, nous avons évalué et comparé les performances codage des méthodes d'extraction de caractéristiques sur la base de données FKP

I.5.1 Les résultats obtenus dans la première expérimentation avec LBP

A fin d'exécuter l'algorithme LBP nous avons fait plusieurs expériences avec différent valeur de R afin que d'obtenir des résultats liée aux temps du calcul ,taux l'apprentissage et le test.

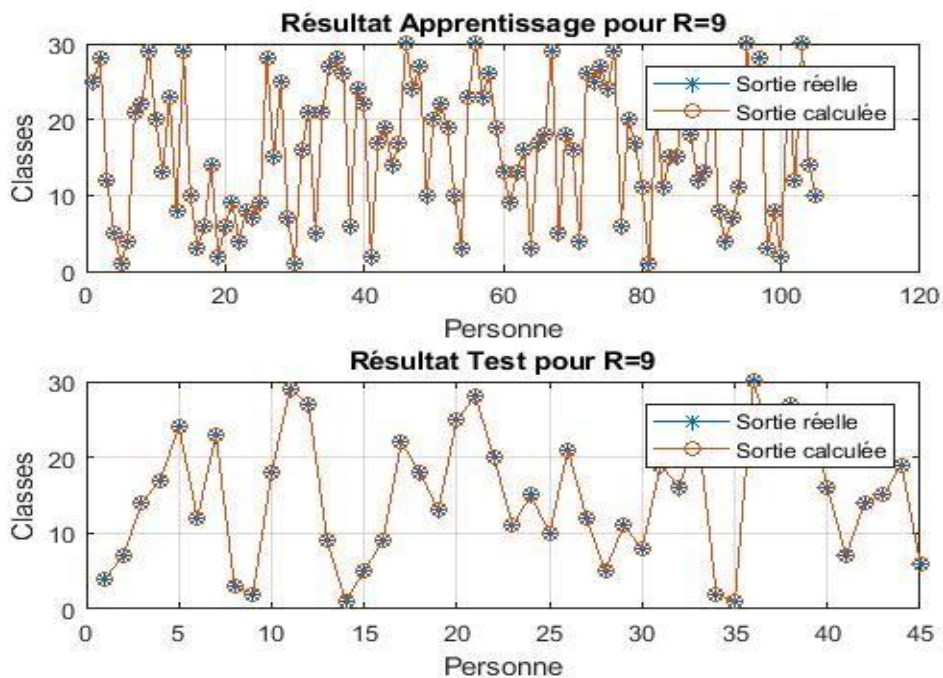


Figure III.2: le résultat d'apprentissage et test en utilisant LBP pour R=9.

Pour les taux d'apprentissage et le test, nous avons obtenu des meilleurs résultats avec R=9, puisque il n'y a pas un déférence entre la sortie réelle et la sortie calculée.

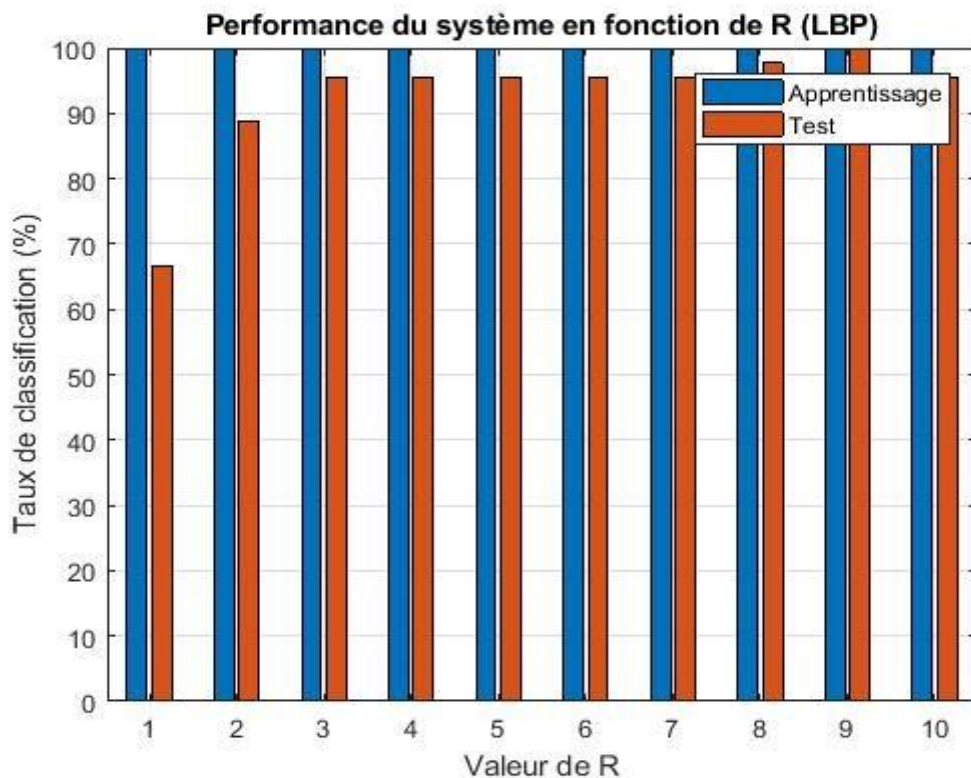


Figure III.3: la performance du système en fonction de R avec LBP.

Le taux d'apprentissage atteint 100% pour toutes les valeurs de R. Cependant, le taux de test se diffère d'une valeur à une autre de R, où il a pris le maximum avec R=9.

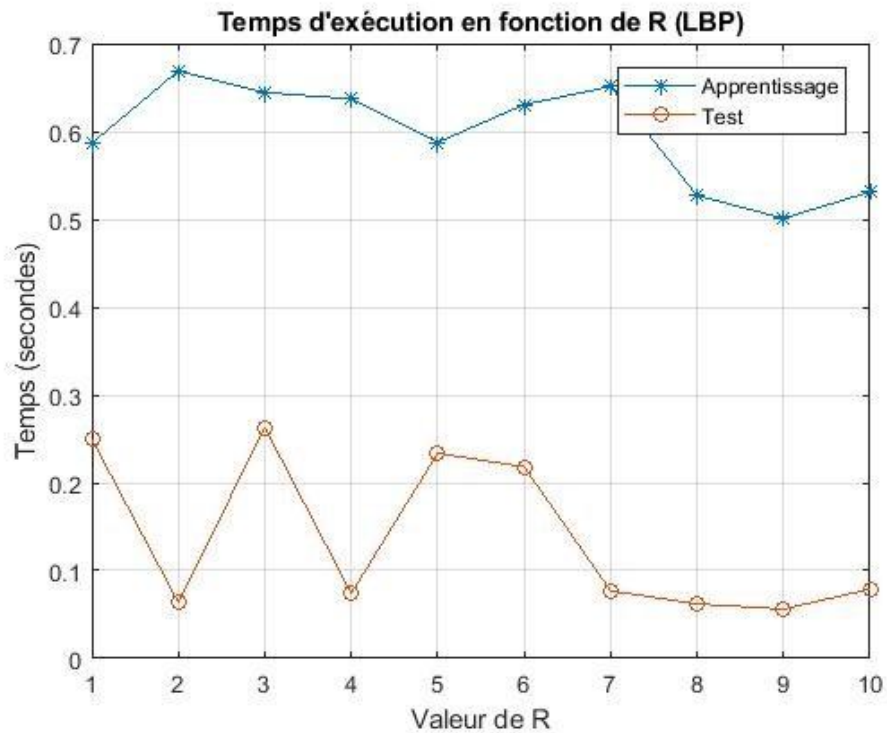


Figure III.4: les temps d'exécution en fonction de R avec LBP.

C'est évident que le temps d'exécution dans la phase d'apprentissage est plus grand que le temps de test. Aussi, le temps d'apprentissage varie en fonction de R, nous avons remarqué qu'il diminue lorsque R augmente. Ceci est justifié par l'impact que le masque avec une valeur de R importante se balaye rapidement sur l'image.

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

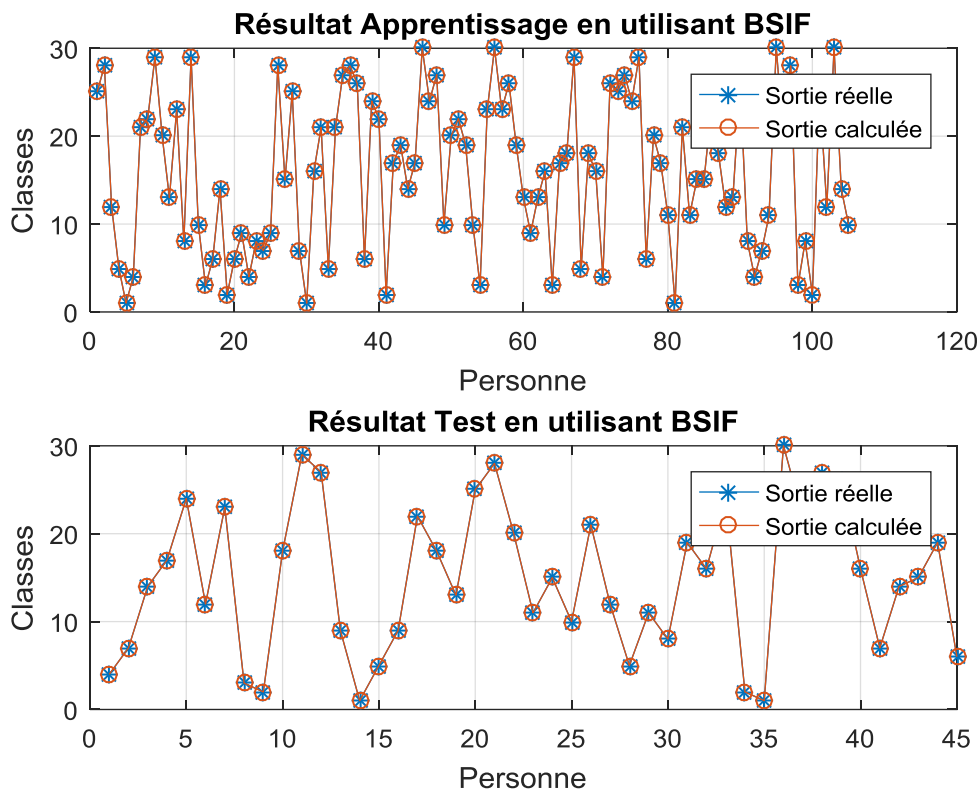


Figure III.5: les résultats d'apprentissage et test en utilisant BSIF.

Pour les résultats liés au descripteur BSIF, plusieurs tests avec différentes tailles de filtre et différent nombre de bits ont été faits. Les meilleurs résultats obtenus est ceux avec le filtre 17*17 et 11 bits.

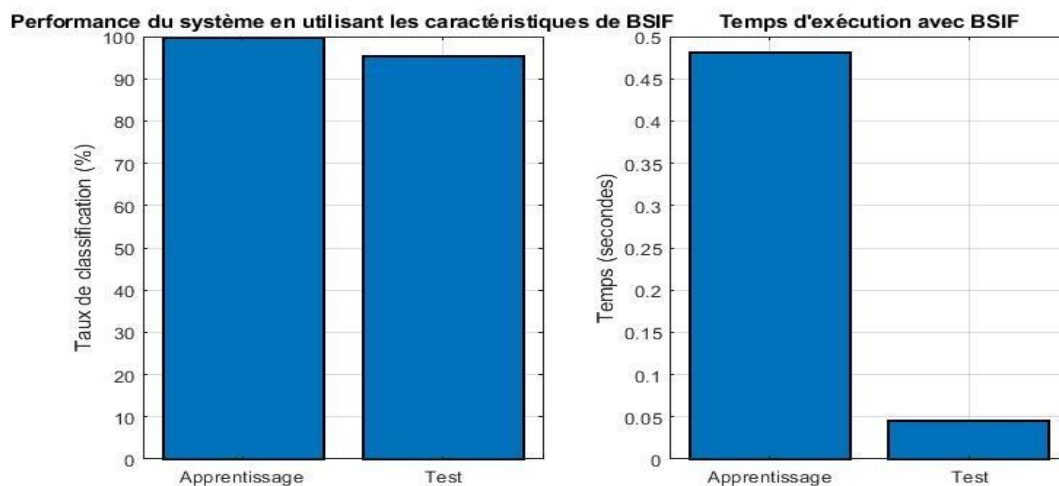


Figure III.6: la performance du système et le temps d'exécution avec BSIF.

Avec ce descripteur, nous avons atteint 100% et 93.33% en terme de taux d'apprentissage et de test, respectivement. Concernant le temps d'exécution, toujours l'apprentissage consomme beaucoup de temps comparativement au temps de test.

I.5.3 Les résultats obtenus dans la troisième expérimentation avec Radon

Afin de bien évaluer le descripteur de Radon, plusieurs tests avec différentes valeurs de R et Θ ont été faits pour trouver ses paramètres optimaux.

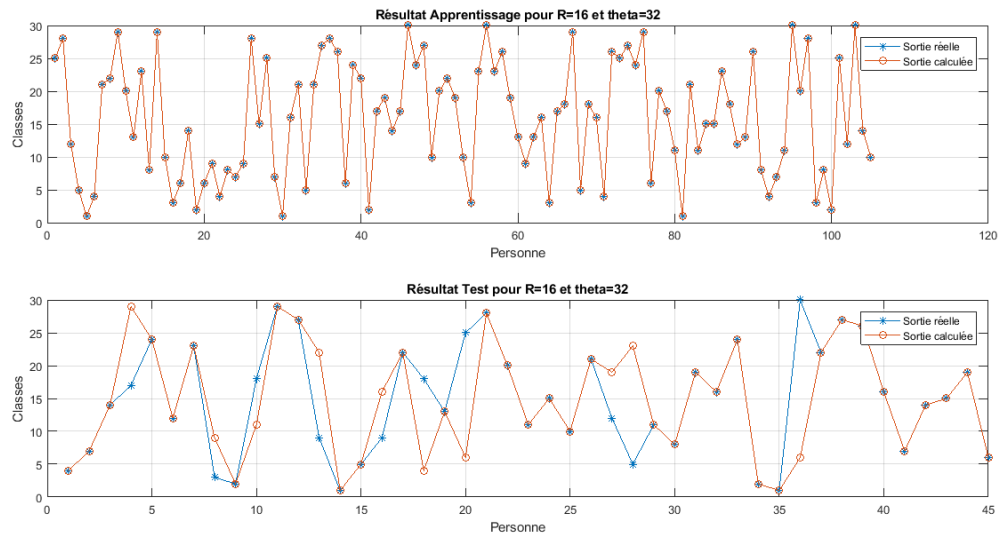


Figure. III.7: les résultats d'apprentissage et test en utilisant Radon.

Les bons résultats trouvés pour le taux d'apprentissage est 100% par contre pour le taux de test est égale 77.77 % avec $R=16$ et $\Theta =32$.

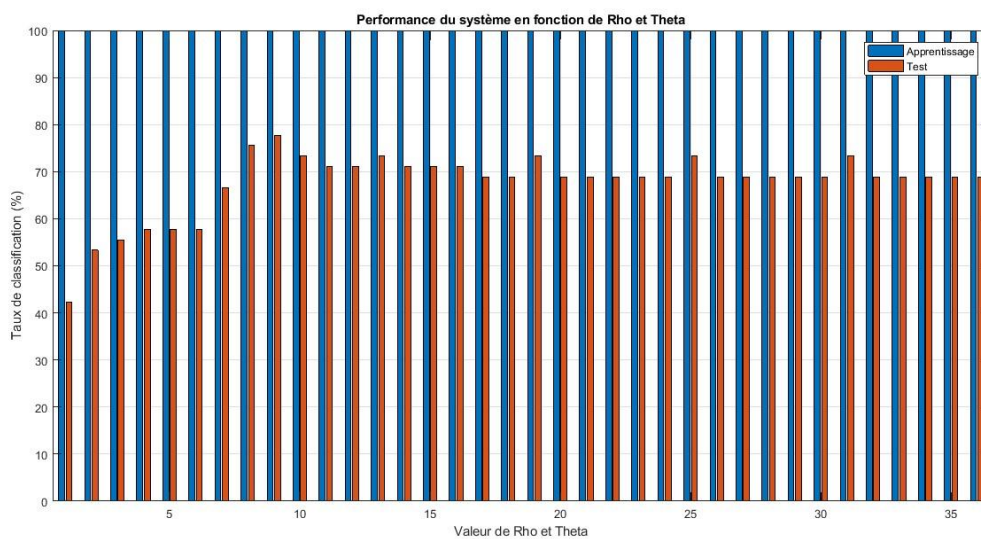


Figure III.8: la performance du système en fonction de ρ , θ avec Radon.

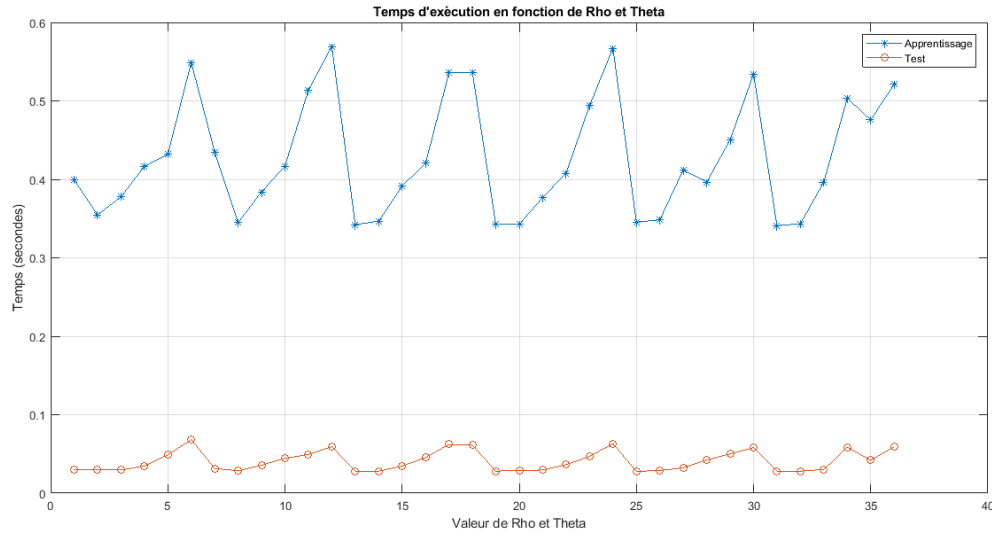


Figure III.9: les temps d'exécution avec Radon.

Dans la figure III.9, l'axe horizontal représente les variations des valeurs (R, θ) allant de (8.8) jusqu'au (128.128) en passant par 16, 32 et 56.

Toujours pour Le temps d'exécution, la phase d'apprentissage consomme plus que celui de la phase de test.

I.5.4 Les résultats obtenus avec la fusion de RADON et BSIF

Après avoir testé les trois descripteurs, nous avons remarqué que les résultats obtenus avec les deux descripteurs RADON et BSIF sont assez faibles. Pour ce fait, nous avons pensé à fusionner les deux afin d'augmenter ces performances. Cette méthode s'articule sur la multi-modalité biométrique. L'ensemble des tests effectués a permis de conclure, qu'avec l'utilisation de plusieurs modalités biométriques comme entrées du système d'identification apporte une amélioration considérable au taux d'identification.

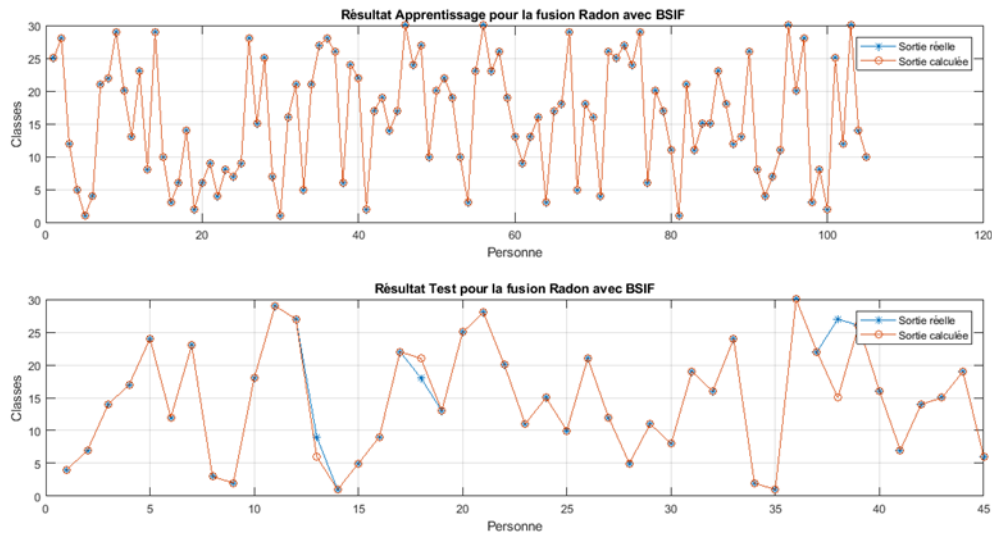


Figure III.10: les résultats d'apprentissage et test en utilisant la fusion.

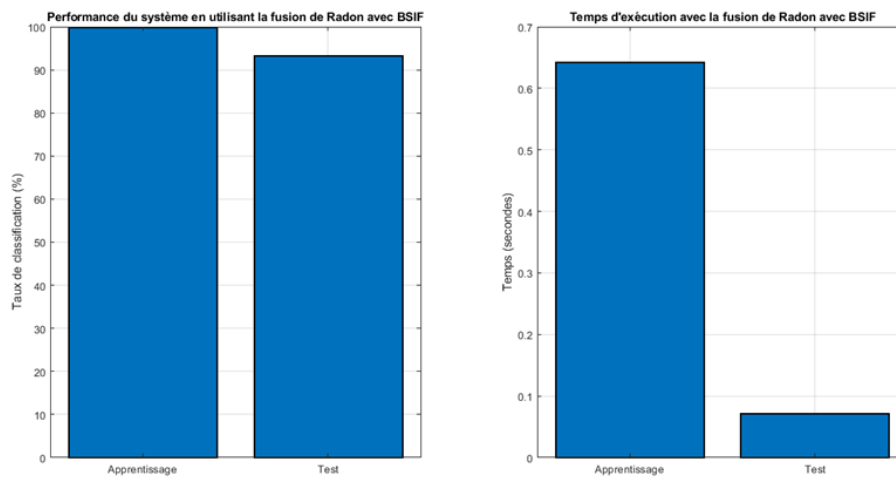


Figure III.11: la performance du système et le temps d'exécution de fusion.

D'après les résultats illustrés dans les figures III.11 et III.12, on a remarqué que la performance globale de la fusion est presque la même que celle de BSIF. Donc, on constate que la fusion des descripteurs n'a pas vraiment apporté une amélioration sur le système.

I.6 Etude comparative

Dans cette section, nous avons effectué une étude comparative concernant les différentes méthodes. Les critères de comparaison sont le taux d'identification et le temps de calcul.

Le but est de sélectionner la meilleure méthode pour réaliser un système d'identification biométrique. Nous avons noté que tous les tests de ce mémoire ont été effectués sous MATLAB et avec une machine d'un processeur i52.67 Ghz avec 6Go de RAM. Les résultats de la comparaison sont rapportés dans le Tableau(III. 2).

caractéristique	indicateurs	taille	apprentissage		Tests	
			Taux (%)	Temps (s)	Taux (%)	Temps (s)
LBP	R=9	256	100	0,5258	100	0,0543
BISIF	Filtre=17 :17 11bite	150	100	0,6424	93,33	0,0701
RADON	g=16 θ=32	256	100	0,5201	77,77	0,0446
Fusion BISIF + RADON	R=9 Filtre=17 :17 11bite	406	100	0,6424	93,33	0,0701

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

D'après ce tableau, on remarque que le meilleur résultat obtenu est lorsque on utilise la caractérisation de LBP où on a atteint 100% de bonne identification. Le temps de calcul du système basé sur la méthode BSIF est plus grand que les systèmes basés sur le descripteur de LBP et de Radon. Finalement, d'après ces résultats, on peut dire qu'un système d'identification par FKP et LBP est considéré comme un système fiable et sécurisé. Il permet une bonne séparabilité des classes clients et imposteurs. Nous considérons les résultats obtenus comme satisfaisant.

I.7 Conclusion

Dans ce chapitre, les travaux biométriques présentés ont conduit à l'élaboration d'un système d'identification des personnes par reconnaissance d'empreintes des articulations des doigts. Pour ce faire, nous avons proposé plusieurs systèmes biométriques. Nous avons exploré quelques systèmes multimodaux. Ces différents systèmes sont testés dans le but d'améliorer le taux d'identification dans les modes d'identification. Nous avons généré trois types de descripteurs notamment : Radon, BSIF et LBP. Egalement, la fusion des descripteurs a été évaluée pour assurer une éventuelle amélioration. En validant ces systèmes sur une base de données réelle de 150 images de 30 personnes, nous avons dégagé une amélioration considérable du taux d'identification (100%) avec les descripteurs de LBP.

Conclusion Générale

Le travail présenté dans ce mémoire s'inscrit dans le contexte de l'identification automatique des personnes basée sur leurs caractéristique biométriques. Nous avons utilisé une nouvelle modalité biométrique, à savoir les empreintes des articulations des doigts, pour réaliser nos systèmes biométriques proposés. Après avoir introduit les concepts généraux de la biométrie, nous avons présenté un état de l'art des modalités biométriques. Nous avons également présenté quelques méthodes d'extraction des caractéristiques.

Nos tests sur la base des données d'empreinte de FKP ont montré que notre méthode pouvait fournir d'excellents résultats en termes de taux d'apprentissage, de taux de reconnaissance et temps d'exécution.

A l'issu des conclusions retenues de nos travaux réalisés, nous nous envisageons dans les futures travaux d'utiliser d'autres méthodes pour l'extraction des caractéristiques des modalités biométriques. Ainsi, nous viserons à utiliser d'autre niveau de fusion (niveau des classifieurs, et niveau décision).

Références

- [1] F. Perronnin, J. Dugelay, “An Introduction to Biometrics Audio and Video-Based Person Authentication ”, Volume 19 – n4,2002 .
- [2] 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 .
- [3] A. Meraoumia, “Modèle de Markov caché applique à la multi biométrie”, USTHB, 2014.
- [4] S. Boudjellal, “ Détection et identification des personnes par méthode biométrique”, Mémoire de Magister, Université Mouloud Mammari, Tizi-Ouzou.
- [5] Belkacem, mébarka, “ Authentification et Identification en biométre en biométre”, thèse doctora , université Mohamed Kider biskra 2013.
- [6] B , Abderahmane , T, Lina “ Reconnaissance des personnes basée sur l’empreinte de l’articulation de doigt”, Memoire Master academique , Universite Kasdi merbah Ouargla, 2015 /2016 .
- [7] M ,Moulay,M,Arbaoui,“ authentification des personnes par l’articulation du doigt”,Universite Kasdi Merbah Ouargla,2015 .
- [8] A. Murhula, ,“ Conception et mise en place d'une plateforme de sécurisation par synthese et reconnaissance biométrique de documents de trafic”, Polytechnique-Initelematique-Burundi - Ingénieur Civil en Informatique et télécommunications,2015.
- [9] Le marché biométrie,“ biométrie – online . net”.
- [10] [https:// www.bimétrie_online.net](https://www.bimétrie_online.net).
- [11] H. O. Nyongesa, S. Al-Khayatt, S. M. Mohamed ,M. Mahmoud,“ Fast Robust”.[11] E. Liu, H.Zhao,“Fingerprint segmentation based on an AdaBoost classifier ”,Higher Education Press and Springer-Verlag Berlin Heidelberg ,2010.
- [12] 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.
- [13] O.D.Trier, A.K.Jain ,“Feature extraction methods for character recognition: ASurvey, Pattern Recognition”, Vol. 29, No. 4, pp. 641-662, 1996.

- [14] 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.
- [15] Ojala, T. Pietikäinen, M. Mäenpää, T. Multiresolution gray-scale and rotation invariant texture classification with local binary patterns, *IEEE Trans. Pattern Anal. Mach. Intell.* 24(7), 971–987 (2002).
- [16] J. Kannala, E. Rahtu, Bsic: Binarized statistical image features. In *Pattern Recognition (ICPR), 2012 21st International Conference on* (pp. 1363-1366), IEEE. (2012, November).
- [17] K. W. Bowyer, K. Chang, P. Flynn, A survey of approaches and challenges in 3D and multi-modal 3D+ 2D face recognition. *Computer vision and image understanding*, 101(1), 1-15,(2006).
- [18] S. Tabbone, L. Wendling ,“Binary shape normalization using the Radon transform”, *Discrete Geometry for Computer Imagery, Lecture Notes in Computer Science*, Springer Verlag, Vol. 2886, pp. 184-193. 2003.
- [19] M.R . Alismail, N .E. Ourchani ,“Fusion multimodale des scores pour la reconnaissance des personnes”, *Université Mohamed Khider Biskra*, 2011.
- [20] A. Nait-Ali, R. Fournier,“Traitement du signal et de l'image pour la biométrie”, *L'OUASIR*, 2012.
- [21] A .N. Eddine,“Modèle automatique des machines a vecteurs de support : application a la reconnaissance d'images de chiffres manuscrits”, *Thèse de doctorat, Ecole de Technologie Supérieure, Québec*, 2004.
- [22] W. Boukhari,“Identification biométrique des individus par leurs empreintes palmaires”, *Mémoire de magister, Université des Sciences et de la Technologie d'Oran USTO-MB*,2007.
- [23] [23] Ch. Bentaouza,“ Classification des images médicales par les séparateurs a vaste marge”, *Mémoire de magister, Université des Sciences et de la Technologie d'Oran USTO-MB*, 2007.
- [24] A. Benishak,“ Sélection de variables par les machines a vecteurs supports pour la discrimination binaire et multi classe en grande dimension”, *Thèse doctorat, Université de Tunis*, 2007.
- [25] M . Senoussaoui ,“ Application des modèles de Markov caches les machines a vecteurs de support pour la reconnaissance des caractères isoles d'écriture en ligne”, *Mémoire de magister, Université des Sciences et de la Technologie d'Oran USTO-MB, SIMPA*, 2007.

- [26] R . Belghechi ,“ Contribution a la reconnaissance d’empreintes digitales par une approche hybride”,Mémoire de magister, Institut National de formation en Informatique (I.N.I), 2006.
- [27] K . Khellat ,“ La reconnaissance automatique de la maladie de parkinson” , Mémoire de magister, Universite des Sciences et de la Technologie d'Oran USTO-MB, LAMOSI, 2012.
- [28] V .Vapnik, The Nature of Statistical Learning Theory, Springer Verlag, New York , 1995 .
- [28] C. Migniot, “ Segmentation de personnes dans les images et les vidéos” , Thèse de Doctorat, Université de Grenoble, Français, 2012.
- [29] Kumar,A.,&Zhou,Y.(2009,September).Humanidentificationusingknucklecodes.In2009IEEE E3rdInternationalConferenceonBiometrics:Theory,Applications,andSystems(pp.1-6).IEEE.

RESUME

Au cours des dernières années, l'identification personnelle automatique devient une exigence importante variété d'applications telles que le contrôle d'accès, les systèmes de surveillance et des bâtiments physiques. Biométrie, qui traite de l'identification des individus en fonction de leurs caractéristiques physiques ou comportementales, est apparue comme une technologie d'identification automatique efficace, qui offre plus de propriétés et plusieurs avantages par rapport à la sécurité traditionnelle. L'empreinte de l'articulation de doigts (FKP) est une caractéristique biométrique importante. Qui fournit l'unicité, la stabilité et la haute distinction capacité. Dans notre travail, un multi-bloc Quantification de la Phase locale (LBP, BISIV, RADON) sont des techniques utilisées afin d'en extraire les caractéristiques discriminantes de la modalité FKP. Nos résultats expérimentaux, en utilisant la base de données FKP (ITTD) démontrent la meilleure performance du système d'identification sur la base FKP proposée.

Mots clés : Biométrie, Empreintes d'articulation de doigt , Reconnaissance, Classification, SVM, , fusion.

ABSTRACT

In recent years, automatic personal identification is becoming an important requirement in variety applications such as access control, surveillance systems and physical buildings. Biometrics, which deals with identification of individuals based on their physical or behavioral features, has been emerging as an effective automatic identification technology, which offers more properties and several advantages over the traditional security. Finger-Knuckle-Print (FKP) is one important biometric feature. Which provides uniqueness, stability and high distinguish ability. In our work, a (LBP, BISIF,RADON) techniques are used in order to extract the discriminant characteristics of the FKP modality. Our experimental results, using FKP database (ITTD), demonstrate the higher performance of the proposed FKP based identification system.

Keywords: Biometrics, fingerprints, recognition, classification, SVM, fusion..

ملخص

خلال السنوات الأخيرة , أصبحت الهوية الشخصية مطلب هام وأساسي في عدة تطبيقات مثل الأمن, أنظمة المراقبة والعمارات...الخ.تعالج الأنظمة البيومترية هويات الأشخاص بدلالة مميزاتهم الفيزيائية أو المعنوية. وقد تبين أنها تقنية فعالة للتعرف التلقائي على الأشخاص , وتتميز بكثير من المميزات على الأنظمة التقليدية.تحتوي بصمة مفصل الإصبع FKP على ميزات بيومترية هامة , والتي تتوفر فيها الوحدانية, الثبات, وقدرة تمييز عالي. ولقد قمنا بتطبيق خوارزمي BSIF , Radon , LBP, كما أننا استعملنا في هذه التجربة قاعدة المطيات ITTD الكلمات المفتاحية : البيومتري, بصمة مفصل الإصبع, المصنف SVM, التعرف