

**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 : ELECTRONIQUE**  
**OPTION : ELECTRONIQUE DES SYSTEMES**  
**EMARQUEES**

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

**Intitulé**

**IDENTIFICATION DES PERSONNES PAR**  
**LES EMPREINTES D'ARTICULATION**  
**DES DOIGTS ET LE DEEP LEARNING**

**Présenté Par :**  
BENABDI Mouad

**Soutenu devant le jury composé de:**

|                      |                   |              |
|----------------------|-------------------|--------------|
| Mr TABBAKH Mostafa   | Université M'SILA | Président    |
| Mr BRIK Youcef       | Université M'SILA | encadreur    |
| Mr ATTALAH Bilal     | Université M'SILA | Co-encadreur |
| Mme DERDOUR Khadidja | Université M'SILA | Examinatrice |

**Promotion : Juin 2019**

# *Remerciements*

Je remercie en premier lieu, Dieu tout puissant qui m'a donné la force, la volonté et surtout la patience pour accomplir ce travail

Je tiens essentiellement et particulièrement à exprimer ma sincère et profonde gratitude à l'égard de Monsieur **Dr. BRIK Youcef**, d'avoir eu l'aménité d'accepter de diriger ce travail, qui s'est montré d'une générosité sans bornes sur tous les plans, scientifique et humain ; voué d'une indulgence, et d'une patience inouïes ; je lui serais toujours reconnaissant pour le constant support intellectuel et ses directives, ce fut à la fois une chance et un grand honneur d'être votre étudiant, veuillez trouver dans ce travail mon respect et ma reconnaissance intarissable.

Je remercie également Monsieur Dr. ATTALAH Billel pour son soutien durant l'élaboration de mon mémoire ainsi que le président et les membres du jury qui nous font l'honneur d'accepter de juger mon travail. Sans oublier bien entendu tous les enseignants qui ont contribué par leur savoir et leurs encouragements le long de nos parcours.

Je tiens à remercier également les responsables et tout le personnel du département d'électronique de la faculté de technologie à l'université Mohamed Boudiaf – M'sila

Mes remerciements à tous mes amis ainsi qu'à toutes les personnes que j'ai connues, qui m'ont aidé, soutenu et encouragé.

Un grand merci à ma famille, qui m'aurez apporté la stabilité et les encouragements pour persévérer ; c'est grâce à votre présence que je sois toujours à la hauteur.

# *Dédicace*

**J**e dédie en premier lieu ce modeste travail à mes chers parents à ceux qui sont toujours présents et continuent de l'être pour faire mon bonheur.

**A** ma femme pour son soutien et encouragement

**A** mes frères, mes sœurs, mes neveux et mes nièces

**A** toute la famille Benabdi et Belhadj

**A** tous mes collègues de travail et tous les étudiants de la spécialité électronique des systèmes embarqués promotion (2019)

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

# Table des matières

|                                                               |     |
|---------------------------------------------------------------|-----|
| Table des matières.....                                       | I   |
| Liste des Figures.....                                        | IV  |
| Liste de Tableaux.....                                        | VII |
| Abréviation.....                                              | VII |
| Introduction générale.....                                    | .1  |
| <b>Chapitre 1 : la biométrie</b>                              |     |
| 1.1 Introduction.....                                         | 4   |
| 1.2 Biométrie .....                                           | 5   |
| 1.3 Caractéristiques de la biométrie .....                    | 5   |
| 1.4 Modalités de la biométrie.....                            | 5   |
| 1.4.1 Analyse des traces biologiques.....                     | 7   |
| 1.4.2 Analyse des traits physiques.....                       | 7   |
| 1.4.2.1Reconnaissance comportementale.....                    | 8   |
| 1.4.2.2 Reconnaissance physiologique.....                     | 9   |
| 1.5 Architecture d'un système biométrique.....                | 10  |
| 1.5.1 Systèmes biométriques monomodale.....                   | 10  |
| 1.5.1.1 Module de capture .....                               | 10  |
| 1.5.1.2 Module de traitement du signal.....                   | 10  |
| 1.5.1.3 Module du stockage.....                               | 10  |
| 1.5.1.4 Module de similarité.....                             | 10  |
| 1.5.1.5 Module de décision.....                               | 10  |
| 1.5.2 Systèmes biométriques multimodaux.....                  | 11  |
| 1.6 Principe de fonctionnement d'un système biométrique ..... | 12  |
| 1.6.1 Mode enrôlement.....                                    | 12  |
| 1.6.2 Mode authentification.....                              | 12  |
| ..... 1.6.3 Mode identification.....                          | 13  |
| 1.7 Performances des systèmes biométriques.....               | 14  |
| 1.8 L'évaluation d'authentification (vérification) .....      | 15  |
| 1.9 Evaluation d'identification.....                          | 17  |
| 1.10 Domaine d'application .....                              | 18  |
| 1.11 Marché biométrique.....                                  | 19  |

|                                               |    |
|-----------------------------------------------|----|
| 1.11.1 Présentation du marché .....           | 19 |
| 1.11.2 Marché mondial de la biométrie.....    | 19 |
| 1.11.3 Marché militaire de la biométrie ..... | 20 |
| 1.12 Conclusion.....                          | 21 |

## **Chapitre 2 : le système proposé**

|                                                               |    |
|---------------------------------------------------------------|----|
| 2.1 Introduction.....                                         | 22 |
| 2.2 Prétraitement de l’empreinte d’articulation de doigt..... | 22 |
| 2.3 Extraction Des Caractéristiques.....                      | 25 |
| 2.3.1 Extraction basé sur la texture .....                    | 26 |
| 2.3.2 Extraction basé sur le filtrage.....                    | 28 |
| 2.4 Classification .....                                      | 28 |
| 2.4.1 Méthodes supervisées .....                              | 29 |
| 2.4.2 Méthodes non supervisées .....                          | 30 |
| 2.5 Approches connexionnistes .....                           | 30 |
| 2.5.1 Apprentissage profond (deep learning).....              | 30 |
| 2.6 Approches statistiques.....                               | 31 |
| 2.6.1 Approches discriminantes.....                           | 31 |
| 2.6.2 Approches modélisantes .....                            | 32 |
| 2.6.2.1 Méthodes non paramétriques.....                       | 32 |
| 2.6.2.2 Méthodes paramétriques.....                           | 32 |
| 2.7 Auto-encodeur.....                                        | 33 |
| 2.8 Réseau de neurones à convolution.....                     | 34 |
| 2.9 Architecture du réseau de neurone convolutionnel .....    | 35 |
| 2.9.1 Couche de convolution(CONV).....                        | 35 |
| 2.9.2 Couches de pooling.....                                 | 35 |
| 2.9.3 Couches de correction (RELU) .....                      | 35 |
| 2.9.4 Couches totalement connectées .....                     | 36 |
| 2.9.5 Couche de perte.....                                    | 36 |
| 2.12 Conclusion.....                                          | 36 |

## **Chapitre 3 : résultats et discussion**

|                                             |    |
|---------------------------------------------|----|
| 3.1. Introduction .....                     | 37 |
| 3.2. Empreinte d’articulation.....          | 37 |
| 3.3. Système de reconnaissance de FKP ..... | 37 |

|                                                                   |    |
|-------------------------------------------------------------------|----|
| 3.4. Base de données FKP.....                                     | 39 |
| 3.4.1. Séparation de base de données.....                         | 40 |
| 3.5. Critère d'évaluation .....                                   | 41 |
| 3.5.1. Taux de bonne classification .....                         | 41 |
| 3.5.2. Taux d'erreur .....                                        | 41 |
| 3.5.2.1. Taux d'erreur fondamentale.....                          | 42 |
| 3.5.2.2. Taux d'erreur de systèmes d'authentification.....        | 42 |
| 3.5.2.3. Taux d'erreur de systèmes d'identification.....          | 42 |
| 3.5.3. Matrice de confusion .....                                 | 43 |
| 3.5.3.1. Calcul de la matrice Confusion .....                     | 43 |
| 3.5.3.2. Terminologies de la matrice Confusion.....               | 44 |
| 3.6. Résultats Expérimentales.....                                | 44 |
| 3.6.1. Stacked autoencoder.....                                   | 45 |
| 3.6.1.1. Résultats obtenus Avec un seul stacked auto-encoder..... | 45 |
| 3.6.1.2. Résultats obtenus Avec deux stacked auto-encoder.....    | 48 |
| 3.7. Conclusion .....                                             | 52 |
| Conclusion générale .....                                         | 53 |
| Bibliothèque.....                                                 | 54 |

# Liste des figures

|                                                                                                                  |    |
|------------------------------------------------------------------------------------------------------------------|----|
| <b>Figure 1.1</b> Catégories des méthodes d'identification biométriques .....                                    | 7  |
| <b>Figure 1.2</b> Architecture générique d'un système biométrique.....                                           | 11 |
| <b>Figure 1.3</b> Architecture de fusion en série .....                                                          | 11 |
| <b>Figure 1.4</b> Architecture de fusion en parallèle.....                                                       | 12 |
| <b>Figure 1.5</b> enrôlement d'une personne dans un système biométrique .....                                    | 12 |
| <b>Figure 1.6</b> Authentification d'un individu dans un système biométrique.....                                | 13 |
| <b>Figure 1.7</b> Identification d'un individu dans un système biométrique.....                                  | 14 |
| <b>Figure 1.8</b> Illustration du FFR et du FAR.....                                                             | 15 |
| <b>Figure 1.9.</b> Distribution des scores des personnes légitimes et des imposteurs.....                        | 16 |
| <b>Figure 1.10.</b> La courbe DET.....                                                                           | 16 |
| <b>Figure 1.11.</b> La courbe CMC.....                                                                           | 17 |
| <b>Figure 1.12 :</b> La croissance de la biométrie.....                                                          | 19 |
| <b>Figure 1.13</b> Les militaire inscrivent les empreintes digitales des citoyens de l'Afghanistan.              | 20 |
| <b>Figure 1.14 :</b> Croissance de la biométrie dans les secteurs civils et militaires.....                      | 21 |
| <b>Figure 2.1</b> filtrage et sous-échantillonnage de l'image de doigt .....                                     | 23 |
| <b>Figure 2.2</b> filtrage et sous-échantillonnage de l'image de doigt .....                                     | 23 |
| <b>Figure 2.3</b> sous-image extraite avant l'extraction de la ROI.....                                          | 23 |
| <b>Figure 2.4</b> image des contours obtenue.....                                                                | 23 |
| <b>Figure 2.5</b> courbes sur l'image de doigt.....                                                              | 24 |
| <b>Figure 2.6</b> image obtenue par l'application de codage de la direction convexe .....                        | 24 |
| <b>Figure 2.7</b> détermination de l'axe Y .....                                                                 | 25 |
| <b>Figure 2.8</b> localisation de la ROI dans l'image de doigt .....                                             | 25 |
| <b>Figure 2.9</b> Extraction de la ROI à partir de l'image de doigt.....                                         | 25 |
| <b>Figure 2.10</b> construction d'un motif binaire et calcul du code LBP.....                                    | 26 |
| <b>Figure 2.11</b> Organigramme de l'ensemble des étapes nécessaire à la construction du<br>descripteur LPQ..... | 28 |
| <b>Figure 2.12</b> méthode supervisée.....                                                                       | 29 |
| <b>Figure 2.13</b> méthode non supervisée.....                                                                   | 30 |
| <b>Figure 2.14</b> auto-encodeurs à une (a) ou plusieurs (b) couches cachées.....                                | 33 |
| <b>Figure 2.15</b> réseau de neurones à convolution.....                                                         | 34 |
| <b>Figure 2.16</b> architecture d'un réseau CNN.....                                                             | 35 |
| <b>Figure 2.17</b> pooling avec un filtre 2x2 .....                                                              | 35 |

|                                                                                                                           |    |
|---------------------------------------------------------------------------------------------------------------------------|----|
| <b>Figure 3.1</b> schéma de principe du système d'identification personnelle à base du FKP.....                           | 38 |
| <b>Figure 3.2</b> dispositif d'acquisition d'image FKP.....                                                               | 38 |
| <b>Figure 3.3</b> Collection des empreintes de l'articulation du doigt dans une base de données.....                      | 39 |
| <b>Figure 3.4</b> des échantillons de la base de données IITD .....                                                       | 40 |
| <b>Figure 3.5</b> Matrice de confusion à quatre mesures.....                                                              | 44 |
| <b>Figure 3.6</b> la structure de classification proposé basée sur un stacked autoencoder .....                           | 45 |
| <b>Figure 3.7</b> Les matrices de confusion produites.....                                                                | 46 |
| <b>Figure 3.8</b> Sorties de l'apprentissage et du test de l'autoencoder comparées avec les sorties désirées.....         | 46 |
| <b>Figure 3.9</b> performance du système en fonction de neurones de l'autoencoder.....                                    | 47 |
| <b>Figure 3.10</b> temps d'exécution de l'apprentissage .....                                                             | 47 |
| <b>Figure 3.11</b> la structure de classification proposé basée sur deux stacked autoencoder.....                         | 48 |
| <b>Figure 3.12</b> Configuration de deux stacked autoencoder .....                                                        | 49 |
| <b>Figure 3.13</b> Les matrices de confusion résultantes.....                                                             | 50 |
| <b>Figure 3.14</b> Sorties de l'apprentissage et du test de l'autoencoder empilé comparées avec les sorties désirées..... | 51 |

## Liste des tableaux

|                                                                                                                  |    |
|------------------------------------------------------------------------------------------------------------------|----|
| <b>Tableau 3.1</b> les taux de classification pour la base d'apprentissage en fonction de nombre de neurone..... | 49 |
| <b>Tableau 3.2</b> les taux de classification pour la base de test en fonction de nombre de neurone.....         | 50 |

# Abréviations

**ACP** : Analyse en Composante Principale

**ADN** : Acide d'Esoxyribo Nucléique

**CMC** : Cumulative Match Characteristics

**CNN** : Convolutional Neural Network

**DET** : Detection Error Trade-off

**FAR** ou **TFA** : False Acceptation Rate ou Taux de Fausse Acceptation

**FER** : False Equal Rate

**FKP** : Finger Knuckle Print

**FRR** ou **TFR** : False Rejet Rate ou Taux de Faux Rejet

**FTA** failure-to-acquire rate

**FTE** failure-to-enroll rate

**FNMR** false non-match rate

**FMR** false match rate

**FRR** false rejection rate

**FAR** false acceptance rate

**FNIR** false-negative identification-error rate

**FPIR** identification-error rate

**IDS** : Identity Dominance System

**IR** identification rate

**IITD** : Indian institute of technology Delhi

**K-PPV** : K Plus Proche Voisin

**LBP** : Local Binary Patterns

**LPQ** : Local Phase Quantization

**MCS** : Multiple Classifier Systems

**MIN-MAX** : minimum-maximum

**NN** : Neural Network

**PIN** : Personal Identification Number

**PR** penetration rate

**QLQ** : Quadratique-Linéaire-Quadratique

**ReLU** : Rectified Linear Unit

**ROI** : Region Of Interest

**SEEK** : Secure Electric Enrollment Kit

**SVM** : Support Vector Machine

**TANH** : tangente hyperbolique

**TCAC** : Taux de Croissance Annuel Composé

# Introduction générale

La sécurité des systèmes d'information est devenue un domaine de recherche d'une très grande importance. La conception d'un système d'identification fiable, efficace et robuste est une tâche prioritaire. L'identification de l'individu est essentielle pour assurer la sécurité des systèmes et des organisations. Elle correspond à la recherche de l'identité de la personne qui se présente dans une base de données et peut servir à autoriser l'utilisation des services. L'exemple de contrôle d'accès à une zone très sécurisée pour laquelle seul un nombre restreint de personnes (enregistrée dans une base de données) y ont accès. Elle peut être également utilisée par la police judiciaire.

Aujourd'hui, l'identification des personnes par la biométrie s'est imposée comme une approche fiable et robuste dans le monde, cette technologie compte sur le développement des différentes techniques par l'exploitation des caractéristiques humaines comportementales telles que la voix, la signature ou physiologiques comme le visage, l'empreinte digitale. Ces caractéristiques s'appellent modalités biométriques. Les modalités biométriques ne peuvent pas être facilement oubliées, perdues, échangées ou volées. Elles sont aussi permanentes ce qui signifie qu'elles ne varient pas ou peu au cours du temps.

Les systèmes de reconnaissance biométriques, utilisés de plus en plus tant dans le domaine privé que public, comportent de nombreux avantages pour les personnes qui les introduisent et les personnes concernées. Toutefois, l'utilisation de données biométriques pour l'identification ou la vérification d'une identité prétendue comporte également des risques quant au respect des droits et des libertés fondamentales. Ils se composent des quatre modules suivants:

- 1) Module d'acquisition des données : Les données sont obtenues à partir d'un dispositif d'acquisition (capteur ou caméra) où la qualité des images est très importante pour le module de prétraitement.
- 2) Module de prétraitement : Le but de ce module est l'amélioration de la qualité de l'image biométrique (modalité) par la réduction du bruit et la normalisation.
- 3) Module d'extraction de caractéristiques : Ce module basé sur des méthodes statistiques et stochastiques afin d'obtenir des caractéristiques possédant les propriétés stables et uniques.
- 4) Module de comparaison : Dans ce module le système biométrique fonctionne en deux modes: le mode de vérification et le mode d'identification. En mode de vérification (authentification), le système vérifie l'identité en comparant le trait biométrique inscrit dans la

base de données avec un trait biométrique de test (1: 1). Dans le mode d'identification le trait biométrique de test est comparé avec tous les N traits biométriques déjà inscrits dans la base de données (1: N).

Parmi les différents traits utilisés dans la biométrie est l'empreinte de l'articulation du doigt FKP qui a attiré beaucoup l'attention des auteurs à cause de divers facteurs avantageux comme la facilité d'acquisition, les images de ces modalités ayant une basse résolution (traitement plus rapide), une unicité très élevée (selon les estimations des chercheurs) et la stabilité qui est étendue durant la vie des individus, d'où une fiabilité extraordinaire.

Bien que les techniques biométriques montrent leur puissance, ils ne peuvent pas garantir actuellement un taux de reconnaissance de 100% avec les systèmes biométriques unimodaux basés sur une donnée biométrique ou signature unique. En outre, ces systèmes sont souvent affectés par les problèmes suivants: le bruit généré par le capteur, non universalité, le manque d'individualité, le manque de représentations invariantes, la sensibilité aux attaques. Pour remédier à ces inconvénients, la solution est l'utilisation de plusieurs modalités biométriques au sein du même système; qui est appelé système biométrique multimodal

C'était en 1995, lorsque le premier travail de fusion du visage et de la voix a été proposé; depuis lors, un grand nombre d'études ont été menées en combinant différentes modalités et compte tenu des différents niveaux de la fusion de données et plusieurs règles de fusion.

Le manuscrit est séparé en trois chapitres organisés comme suit :

Le premier chapitre est consacré à l'état de l'art de la biométrie. Sa définition, ses caractéristiques, la description de ses différentes modalités, et le détail sur l'architecture d'un système biométrique par ses différents importants modules qui mènent à la compréhension du principe de fonctionnement de ce dernier. 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 présente les étapes de prétraitement de FKP, ensuite plusieurs notions sur l'extraction des caractéristiques d'une modalité en détaillant ses bases et approches. La contribution à la classification est également présentée dans ce chapitre avec ses différentes méthodes et approches en encadrant l'auto-encodeur et le CNN.

Le troisième chapitre nous allons nous focaliser sur une étude en simulation d'un système d'identification par FKP comme modalité biométrique avec une présentation des résultats obtenus à l'issu des autoencoders avec différentes configurations.

# Chapitre 01

## La biométrie

### 1.1. Introduction

A notre époque, et avec l'évolution perpétuelle de la technologie, l'authentification automatique des individus devient une approche essentielle dans le domaine de la sécurité et de contrôle d'accès au sein des infrastructures et des systèmes informatiques. D'une part, la croissance internationale des communications, telle que Internet, tant en volume qu'en diversité (déplacement physique, transaction financière, accès aux services...), implique le besoin de s'assurer de l'identité des individus. D'autre part, l'importance des enjeux motive les fraudeurs à mettre en échec les systèmes de sécurité existants.

Il y a donc un intérêt grandissant pour les systèmes électroniques d'identification et d'authentification. Leur dénominateur commun est le besoin d'un moyen simple, pratique, fiable et peu onéreux, pour vérifier l'identité d'une personne, sans l'assistance d'une autre personne. Nous pouvons tirer deux rôles primordiaux de reconnaissance d'individus :

- ✓ L'identification d'une personne pour établir son identité.
- ✓ L'authentification qui vérifie la validité de l'identité d'un individu.[\[1\]](#)

La biométrie se réfère à l'identification automatique d'un individu à partir modalités biométriques physiologiques ou comportementales. Donc la biométrie représente ce que l'on est contrairement à ce que l'on possède (carte, badge, clé, etc.), ou ce que l'on sait (mot de passe, code PIN, etc.) permettant de surmonter les problèmes liés à ces deux derniers systèmes à savoir : la duplication, le vol, l'oubli, et la perte. Ainsi chaque caractéristique (physiologique et/ou comportementale) peut être qualifiée comme une modalité biométrique, si elle a les propriétés principales suivantes : [\[2\]](#) [\[3\]](#):

- ✓ l'universalité ;
- ✓ l'unicité ;
- ✓ la permanence ;
- ✓ la facilité ;
- ✓ l'acceptabilité ;
- ✓ la non-reproductibilité.

### 1.2. Biométrie

Qu'est-ce que la biométrie?

Le terme de biométrie est originaire d'une contraction des deux anciens termes grecs :

« *Bios* » qui signifie : la vie et « *metron* » qui se traduit par : mesure. [4]

La biométrie est un ensemble des technologies (appelées les technologies biométriques) qui exploitent des caractéristiques humaines physiques ou comportementales telles que l'empreinte digitale, la signature, l'iris, la voix, le visage, la démarche et la géométrie de la main pour différencier des personnes. Ces caractéristiques sont traitées par certain ordre des processus automatisés [5] [6] à l'aide des dispositifs comme des modules de balayage ou des appareils-photo. À la différence des mots de passe, ou des PINs (Numéros d'Identification Personnelle), qui sont facilement oubliés ou exposés à l'utilisation frauduleuse, ou des clefs ou des cartes magnétiques qui doivent être portées par l'individu et sont faciles à être volées, copiées ou perdues, les caractéristiques biométriques sont uniques à l'individu et il y a peu de possibilité que d'autres individus peuvent remplacer ces caractéristiques, donc les technologies biométriques sont considérées comme les plus puissantes en termes de sécurité[7]. La biométrie est également un outil puissant d'identification/authentification dans des scènes de crime dans le secteur juridique.

Un système biométrique peut fonctionner en deux modes distincts : en mode de vérification, le système confirme ou nie une identité réclamée, alors qu'en mode d'identification, il détermine l'identité d'un individu.

La biométrie offre une solution naturelle est fiable pour certains aspects de la gestion d'identité en utilisant des systèmes entièrement automatisés ou semi-automatisés de reconnaissance des individus. [8]

### 1.3. Caractéristiques de la biométrie

Les caractéristiques biométriques ne peuvent pas être facilement volées, falsifiées, ou partagées. Ainsi, elles sont plus fiables et sécurisées pour la reconnaissance de personne que les méthodes traditionnelles basées sur la connaissance ou la possession. Cependant ces caractéristiques physiques et comportementales doivent satisfaire plusieurs contraintes pour une grande fiabilité des systèmes biométriques. En effet, les objectifs de la reconnaissance biométrique sont la facilité d'utilisation par une reconnaissance sans carte ou code PIN, la sécurité accrue qui est traduite par la difficulté de contourner le contrôle d'accès ainsi que la plus grande performance quant à la précision et la rapidité des traitements. Ainsi, chaque

caractéristique physiologique et/ou comportementale peut être utilisée comme une biométrie pour reconnaître une personne dès lors qu'elle répond à ces exigences :

- ✓ universelles (exister chez tous les individus),
- ✓ uniques (permettre de différencier un individu par rapport à un autre),
- ✓ permanentes (autoriser l'évolution dans le temps),
- ✓ enregistrables (collecter les caractéristiques d'un individu avec son accord),
- ✓ mesurables (autoriser une comparaison future).

Cependant, dans un système biométrique pratique, il existe un certain nombre de paramètres qui doivent être examinés, notamment:

- L'acceptation par l'utilisateur qui reflète l'ampleur des inquiétudes et des objections que l'utilisation d'une technologie biométrique donnée tend à susciter. Dans certains pays, la reconnaissance faciale est mal acceptée ; dans d'autres pays, la reconnaissance des empreintes digitales a des connotations de criminalité. La mesure de l'acceptation reste très subjective et varie d'une personne à l'autre et d'un pays à l'autre, suivant le régime de protection des données en vigueur, le contexte culturel et les attentes personnelles des utilisateurs
- Le contournement, qui reflète combien il est facile de tromper le système par des méthodes frauduleuses.
- La permanence ou la stabilité qui est définie par la constance d'une caractéristique biométrique au cours du développement normal et du vieillissement d'une personne. En principe, plus une caractéristique est stable, moins il est nécessaire de mettre à jour les caractéristiques personnelles ou de réenregistrer la personne.

Un système biométrique pratique doit avoir une précision acceptable et une vitesse de reconnaissance raisonnable vis-à-vis des ressources requises, inoffensif pour les utilisateurs, accepté par la population, et suffisamment robuste à l'encontre des méthodes frauduleuses. De nombreuses modalités biométriques sont utilisées dans diverses applications. Chaque modalité biométrique a ses forces et ses faiblesses et le choix dépend généralement de l'application à traiter. Aucune modalité biométrique ne répond effectivement aux exigences de toutes les applications.

La comparaison entre les différentes biométries permet de choisir une technologie en fonction des contraintes liées à l'application. En effet, chaque caractéristique (ou modalité) biométrique a ses forces et ses faiblesses, et faire correspondre un système biométrique spécifique à une

application dépend du mode opérationnel de l'application et des caractéristiques biométriques choisies. [9]

### 1.4. Modalités biométriques

Il existe un très grand nombre de modalités biométriques, qui peuvent se diviser en deux catégories :

**1.4.1. Analyse des traces biologiques** : Elle est basée sur l'identification de traits biologiques particuliers qui, pour toutes personnes, sont uniques et permanents. Ce type de biométrie est très complexe à mettre en œuvre dans un système usuel de reconnaissance et n'est utilisé que dans un cas d'extrême nécessité (ex: Enquête criminelle, test de paternité) [10].

Cette catégorie regroupe la reconnaissance de l'ADN, le sang, la salive, l'urine, l'odeur, la thermographie.[11]

**1.4.2. Analyse des traits physiques** : facile à mettre en œuvre, elle se représente en deux grandes classes [1] (voire la figure 1.1):

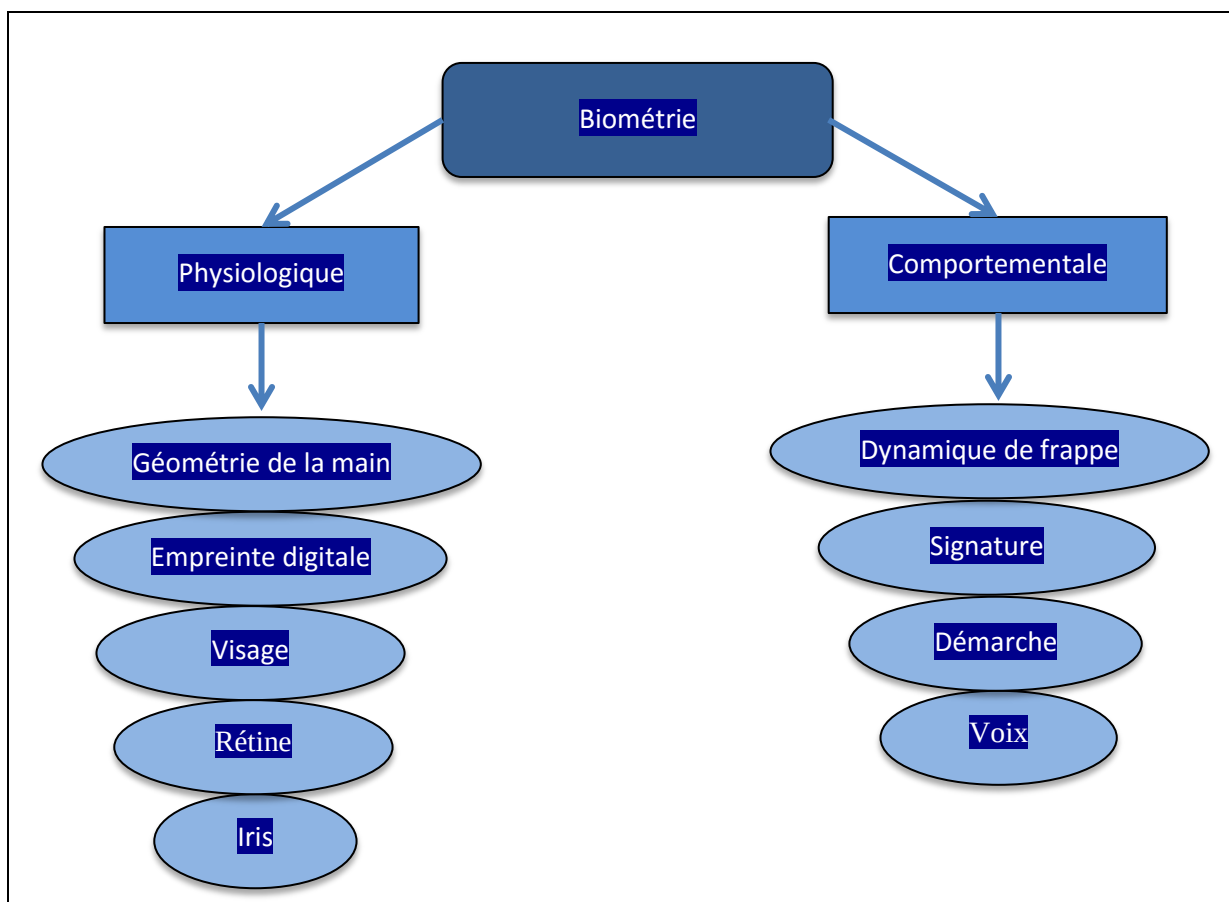


Figure 1.1 Catégories des méthodes d'identification biométriques

### 1.4.2.1. Reconnaissance comportementale

Dans ces techniques de reconnaissance, on s'intéresse aux caractéristiques physiques en activité des individus qui peuvent être typiques et permettent de distinguer une personne d'une autre. Plus explicitement, on étudie la manière de faire des individus, on cite quelques de ces modalité : [1]

**La voix** : la reconnaissance de la voix est une biométrie

comportementale n'exige aucun contact physique avec

le lecteur de système. En 1962 Lawrence Kersta [12]

a prouvé que la voix de chaque personne est unique

et qu'il est possible de la présenter graphiquement.

Il existe deux principales méthodes de traitements

de ce trait biométrique, la première dépend de texte

prononcé, et la deuxième (la plus difficile) est

indépendante de texte. Bien que cette modalité ne nécessite pas de matériel cher (microphone

par exemple), cependant le bruit ambiant et les propriétés acoustiques telles que la réflectivité

et l'absorption influence la vérification de la voix en réduisant ainsi son utilisation.



**La signature** : la vérification par la signature est

l'une des premières méthodes utilisées dans le domaine

de la biométrie. Les systèmes de reconnaissance de

l'écriture analysent soit la géométrie de la signature

(mode statique), soit ses caractéristiques spécifiques

comme la vitesse, la pression sur le crayon, ce mode

qui s'appelle le mode dynamique est le plus discriminant.



La capture se fait à l'aide d'une tablette graphique. bien que la signature soit bien acceptée par

les utilisateurs, sa variabilité (à cause de l'état de santé ou l'état émotionnel de l'individu)

pose un grand problème.

**La dynamique de frappe**

Selon [13], C'est une autre technique primitive dans

Laquelle un énorme apport en temps et en effort a été

investi, notamment par quelque grandes compagnies de

technologie de l'information. L'idée d'identifier

un individu par sa dynamique particulière de frappe

était clairement attrayante



### 1.4.2.2. Reconnaissance physiologique

Ces types de reconnaissance mesurent une caractéristique spécifique de la structure ou de la forme d'une partie du corps humain. Nous pouvons citer les exemples les plus connus : [1]

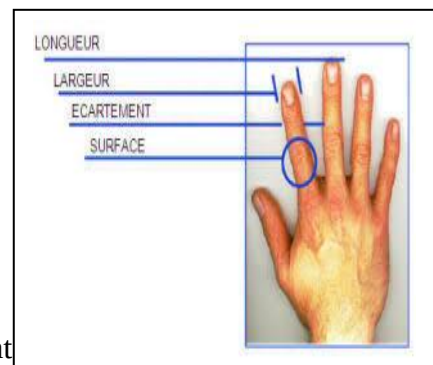
**L'empreinte digitale**: l'empreinte digitale est le modèle de relief cutané des doigts. L'identification par cette caractéristique est la technique la plus anciennement utilisée. En fait, c'était toujours le choix biométrique évident pour les services de police depuis plus de 100 ans, c'est pour cela qu'elle est généralement mal acceptée par les utilisateurs en raison de l'alignement fort avec la criminologie. Il existe plusieurs types de système de capture d'empreinte digitale : optique, thermique, électromagnétique et ultrasons. [14]



**Le visage** : le visage est le moyen le plus naturel Pour Identifier les personnes, ce qui explique pourquoi cette caractéristique est bien acceptée par les utilisateurs. L'image de visage peut être captée par une caméra numérique, ou un appareil photo. Plusieurs recherches sont effectuées, pendant 25 ans [15], [16] pour améliorer la performance de ce système cependant de nombreux problèmes se posent.



**La géométrie de la main** : cette modalité consiste à analyser la forme de la main sa longueur, sa largeur, son hauteur, la courbure des doigts etc. Cette technique est récente, simple et bien acceptée par les utilisateurs qui suivent des guides des capteurs (LEDs infrarouge, des appareils photos numériques) pour qu'ils bien positionner leurs doigts, ce qui rende ainsi la détection / la segmentation plus aisée, cependant



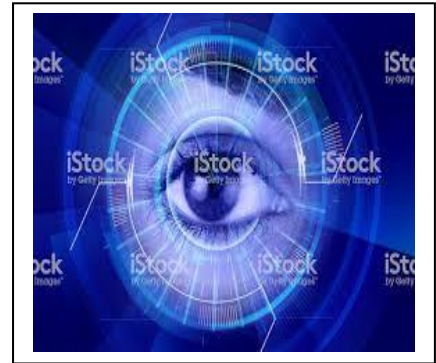
ce genre de système peut être trompé par de vrais jumeau ou même par des personnes ayant des formes de la main proches.

**L'iris** : l'iris est la région annulaire située entre la pupille et le blanc de l'œil. La biométrie par ce trait est la plus récente, et la plus fiable, selon les estimations de Daugmann. La probabilité de trouver 2 iris suffisamment identiques est 1 sur  $10^{72}$  environ. L'image de l'iris est capturée par



une caméra standard contraignante (exemple la distance entre la camera et l'iris ne dépasse pas un mètre), ce qui limite l'utilisation de cette modalité.

**La rétine** : la rétine est la couche sensorielle de l'œil qui permet la vision, cette zone est parcouru par des vaisseaux sanguins dont leurs positions est inchangeable durant toute la vie de la personne. L'identification de la rétine n'est pas récente, elle remonte aux années 30. Cette technologie est la plus fiable toutefois elle est mal acceptée par les utilisateurs à cause des contraintes de l'acquisition.



## 1.5. Architecture d'un système biométrique

### 1.5.1. Systèmes biométriques monomodale

L'architecture d'un système biométrique contient cinq modules comme le montre la figure 1.2

**1.5.1.1. Module de capture** : qui consiste à acquérir les données biométriques afin d'extraire une représentation numérique. Cette représentation est ensuite utilisée pour l'enrôlement, la vérification ou l'identification. Il s'agit d'un capteur biométrique qui peut être de type sans ou avec contact.

**1.5.1.2. Module de traitement du signal** : qui permet de réduire la représentation numérique extraite afin d'optimiser la quantité de données à stocker lors de la phase d'enrôlement, ou pour faciliter le temps de traitement pendant la phase de vérification et l'identification. Ce module peut avoir un test de qualité pour contrôler les données biométriques acquises.

**1.5.1.3. Module du stockage** : qui contient les modèles biométriques des utilisateurs enrôlés du système.

**1.5.1.4. Module de similarité** : qui compare les données biométriques extraites par le module d'extraction de caractéristiques à un ou plusieurs modèles préalablement enregistrés. Ce module détermine ainsi le degré de similarité (ou de divergence) entre deux vecteurs biométriques.

**1.5.1.5. Module de décision** qui détermine si l'indice de similarité retourné est suffisant pour déterminer l'identité d'un individu. [17]

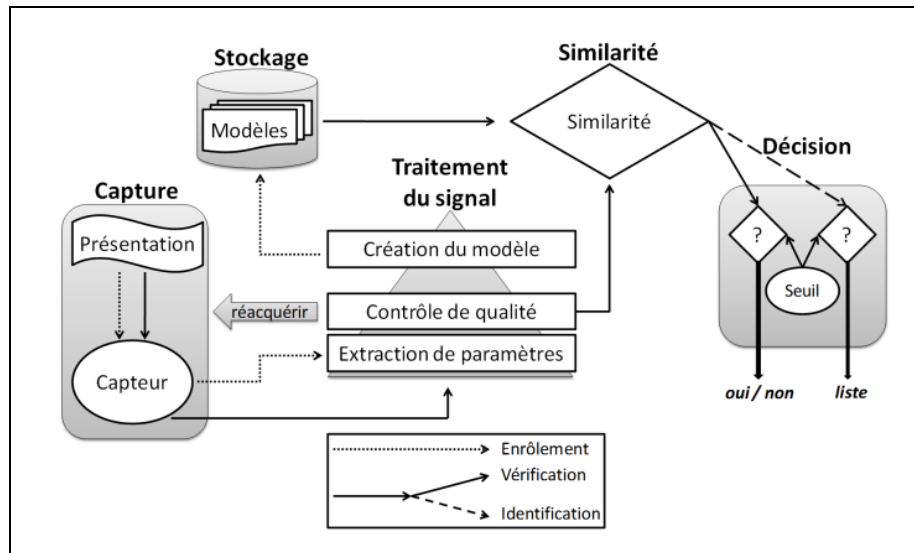


Figure 1.2 Architecture générique d'un système biométrique

### 1.5.2. Systèmes biométriques multimodaux

Les systèmes multimodaux associent plusieurs systèmes biométriques et nécessitent donc l'acquisition et le traitement de plusieurs données. L'acquisition et le traitement peuvent se faire successivement, on parle alors d'architecture en série, ou simultanément, on parle alors d'architecture en parallèle.

L'architecture est donc en général liée au traitement et en particulier à la décision. En effet la différence entre un système multimodal en série et un système multimodal en parallèle réside dans le fait d'obtenir un score de similarité à l'issue de chaque acquisition (fusion en série) (voir figure 1.3) ou de procéder à l'ensemble des acquisitions avant de prendre une décision (fusion en parallèle) (voir figure I.4)

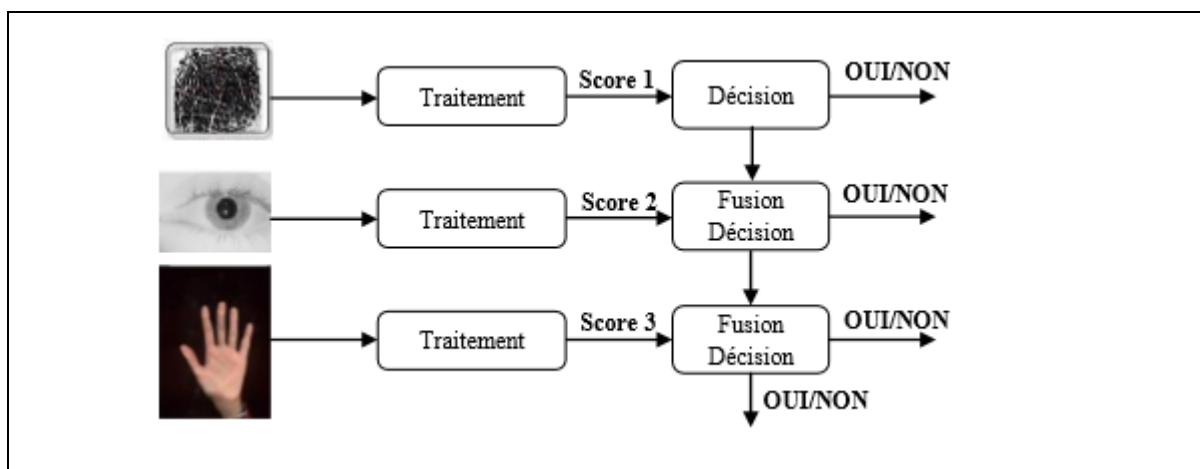


Figure 1.3 Architecture de fusion en série

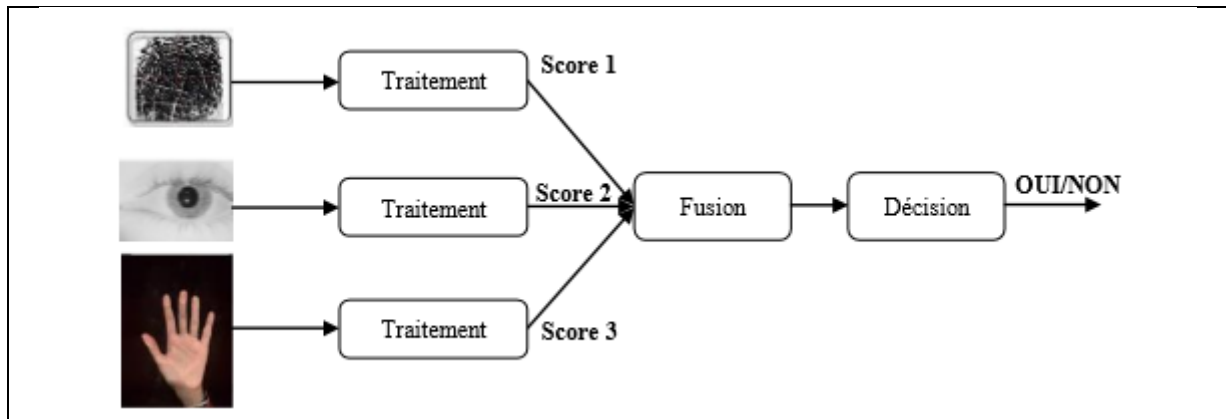


Figure 1.4 Architecture de fusion en parallèle

## 1.6. Principe de fonctionnement d'un système biométrique

Les systèmes biométriques peuvent fournir trois modes de fonctionnement, à savoir, l'enrôlement, l'authentification (ou vérification) et l'identification. Dans ce qui suit, les figures illustreront l'exemple d'un système biométrique utilisant l'empreinte digitale comme modalité.

**1.6.1. Mode enrôlement** C'est la première phase de tout système biométrique (voir figure I.5), il s'agit de l'étape pendant laquelle un utilisateur est enregistré dans le système pour la première fois et où une ou plusieurs modalités biométriques sont capturées et enregistrées dans une base de données. Cet enregistrement peut s'accompagner par l'ajout d'information biographique dans la base de données.

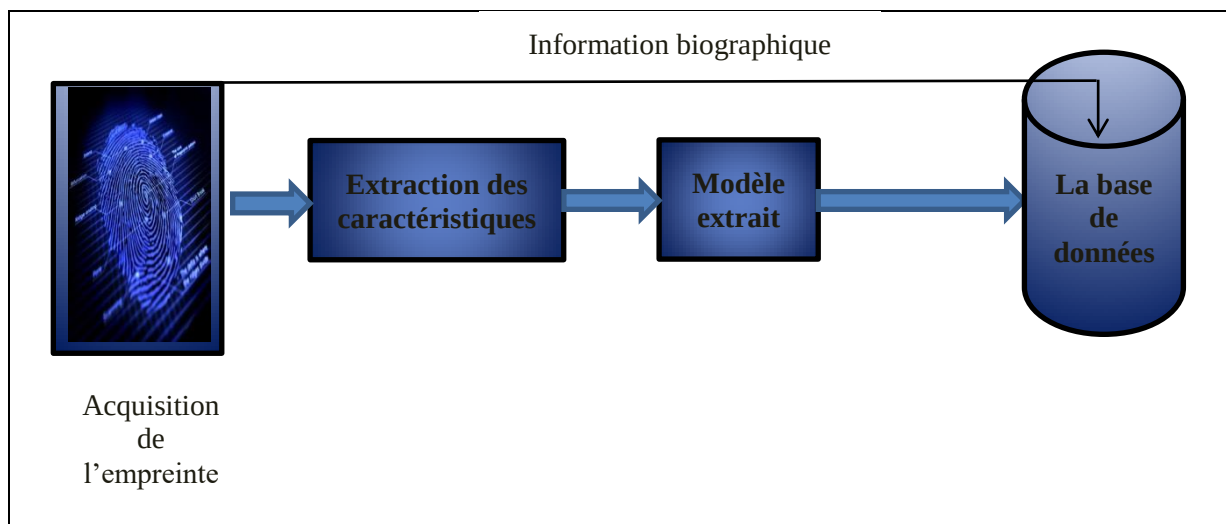


Figure 1.5 enrôlement d'une personne dans un système biométrique

**1.6.2. Mode authentification** L'utilisateur affirme son identité et le système vérifie si cette affirmation est valide ou non (voir figure I.6).

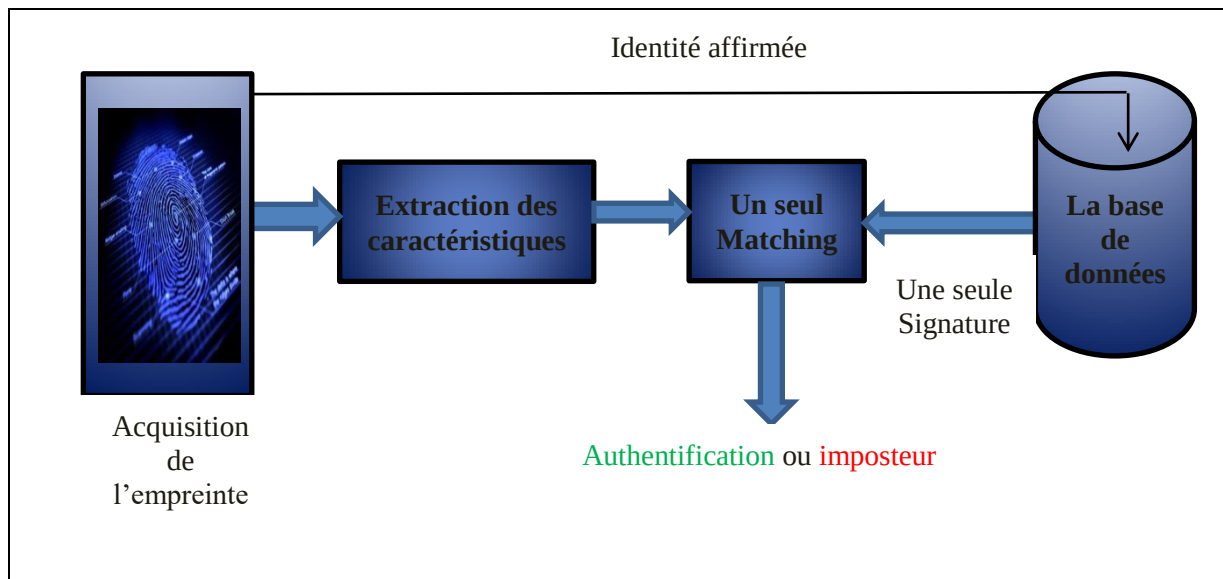


Figure 1.6 Authentification d'un individu dans un système biométrique

Pour illustrer ce principe, prenons la situation où un utilisateur (M. X) souhaite retirer de l'argent à un distributeur de billets en entrant son code personnel d'identification (code PIN) et en présentant une modalité biométrique. Le système acquiert alors les données biométriques et va les comparer uniquement avec le modèle enregistré correspondant à M. X. On parle alors de correspondance 1:1. Ainsi, si l'entrée biométrique de l'utilisateur et le modèle enregistré dans la base de données correspondant à l'identité affirmée possèdent un degré de similitude élevé, l'affirmation est validée et l'utilisateur est considéré comme étant un authentique. Dans le cas contraire, l'affirmation est rejetée et l'utilisateur est considéré comme étant un imposteur. En résumé, un système biométrique opérant en mode vérification répond à la question "Suis-je bien M. X?".

**1.6.3. Mode identification** L'utilisateur ne dévoile pas explicitement son identité (voir figure I.7). Cependant, l'affirmation implicite faite par l'utilisateur est qu'elle est une des personnes déjà enrôlées par le système. Ainsi, l'échantillon biométrique de l'individu est comparé avec les modèles de toutes les personnes de la base de données. On parle alors de correspondance 1:N. La sortie du système biométrique est constituée par l'identité de la personne dont le modèle possède le degré de similitude le plus élevé avec l'échantillon biométrique présenté en entrée. Typiquement, si la plus grande similarité entre l'échantillon et tous les modèles est inférieure à un seuil de sécurité minimum fixé, la personne est rejetée, ce qui implique que l'utilisateur n'était pas une des personnes enrôlées par le système. Dans le cas contraire, la personne est acceptée.

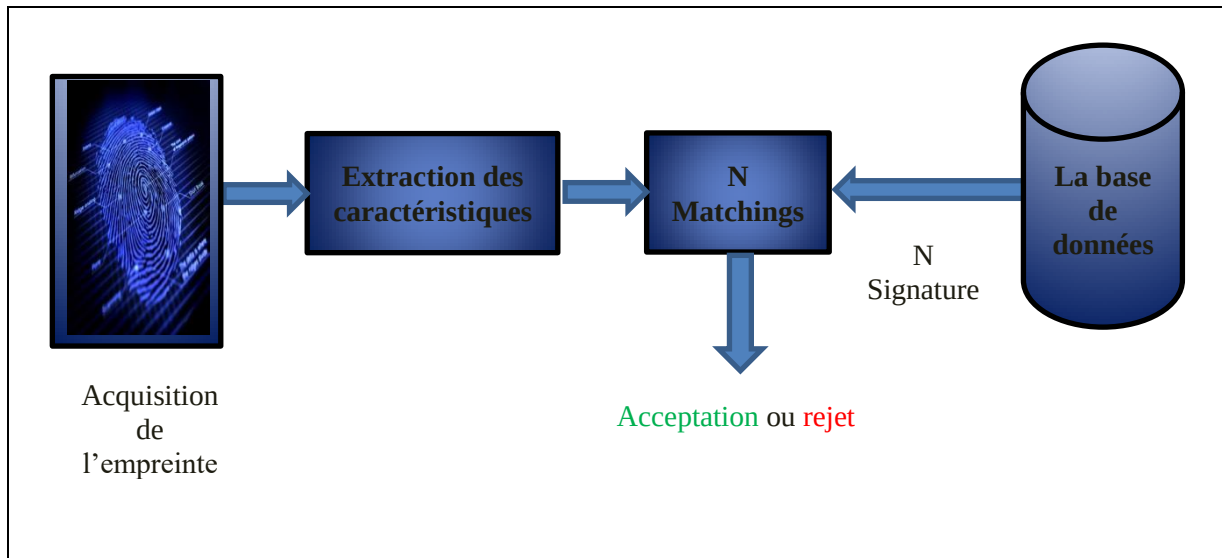


Figure 1.7 Identification d'un individu dans un système biométrique

Un exemple de système opérant en mode identification serait l'accès à un bâtiment sécurisé : tous les utilisateurs qui sont autorisés à entrer dans le bâtiment sont enrôlés par le système, lorsqu'un individu essaye de pénétrer dans le bâtiment, il doit d'abord présenter ses données biométriques au système et, selon la détermination de l'identité de l'utilisateur, le système lui accorde le droit d'entrée ou non. En résumé, un système biométrique opérant en mode identification répond à la question "Suis-je bien connu du système ?". [9]

### 1.7. Performances des systèmes biométriques

Les performances d'un système biométrique sont données par la mesure de deux taux d'erreurs : le **FRR** (False Rejet Rate ou Taux de Faux Rejet) et le **FAR** (False Acceptation Rate ou Taux de Fausse Acceptation). Le **FRR** ou le **TFR** (Taux de Faux Rejets) : estime le pourcentage d'utilisateurs valides qui ne seront pas reconnus par le système. Le **FAR** ou le **TFA** (taux de fausse acceptation) : estime le pourcentage d'utilisateurs non connus qui seront faussement reconnus par le système. Le paramétrage d'un système consiste à trouver le bon équilibre entre ces deux taux, le **FAR** augmentant lorsque le **FRR** diminue, et inversement. Un contrôle d'accès très sécurisé aura un **FAR** très bas, pour garantir qu'aucune personne non autorisée n'accède au site, mais, en contrepartie le **FRR** sera élevé, ce qui signifie que des utilisateurs valides se verront refuser l'accès. Les autres mesures de performance sont les temps d'encodage de l'empreinte et de mise en correspondance. Là encore, ces valeurs peuvent varier considérablement d'une application à une autre. Un troisième paramètre **FER** (False Equal Rate) mesure le taux d'échec à l'enrôlement. Il traduit la probabilité d'absence d'une caractéristique biométrique pour un individu dans une population, donne un point sur

lequel le **TFA** est égal au **TFR**. La figure 1.8 illustre le **FRR** et le **FAR** à partir de distributions des scores authentiques et imposteurs [18]

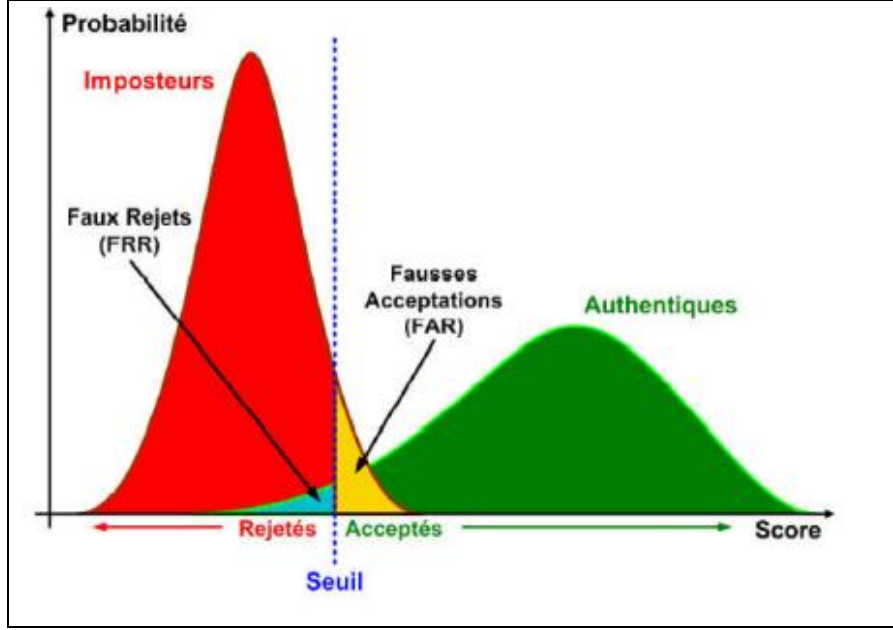


Figure 1.8 Illustration du FRR et du FAR

## 1.8. Evaluation d'authentification (vérification)

L'authentification consiste à appairer le modèle biométrique stocké d'une personne (I) et les données acquises par le système biométrique, plus formellement :

Soient  $X_Q$  le vecteur de caractéristique (Feature vector), de la personne proclamée I, et  $X_I$  celui de la personne I stockée dans la base de données, le test de vérification est défini ainsi :

[19]

$$(I, X_Q) = \begin{cases} W_1, & \text{si } S(X_Q, X_I) \geq t \\ W_2, & \text{sinon} \end{cases} \quad (1.1)$$

Où  $S$  est la fonction de similarité entre le vecteur  $X_Q$  et  $X_I$ ,  $w_1$  indique que la personne proclamée est un client et  $w_2$  désigne qu'elle est imposteur, et  $t$  c'est le seuil. La figure 1.9 illustre l'estimation des taux FAR et FRR suivant les distributions des imposteurs et des personnes légitimes données par les équations (2) et (3) ci-dessous [2]

$$FAR = \int_0^t p(S(X_Q, X_I) | H_0) ds \quad (1.2)$$

$$FRR = \int_t^1 p(S(X_Q, X_I) | H_1) ds \quad (1.3)$$

*Légende :*

$H_0$  : Hypothèse indique que la signature  $X_Q$  et  $X_I$ , ne proviennent pas de la même personne.

$H_1$  : Hypothèse indique que la signature  $X_Q$  et  $X_I$ , proviennent de la même personne.

$D_0$  : la décision associée à  $H_0$  qui indique que la personne n'est pas celle qu'elle prétend être.

$D_1$  : la décision associée à  $H_1$  qui indique que la personne est celle qu'elle prétend être.

$P(s|H_0)$  : la distribution des scores des personnes imposteurs.

$P(s|H_1)$  : la distribution des scores des personnes légitimes.

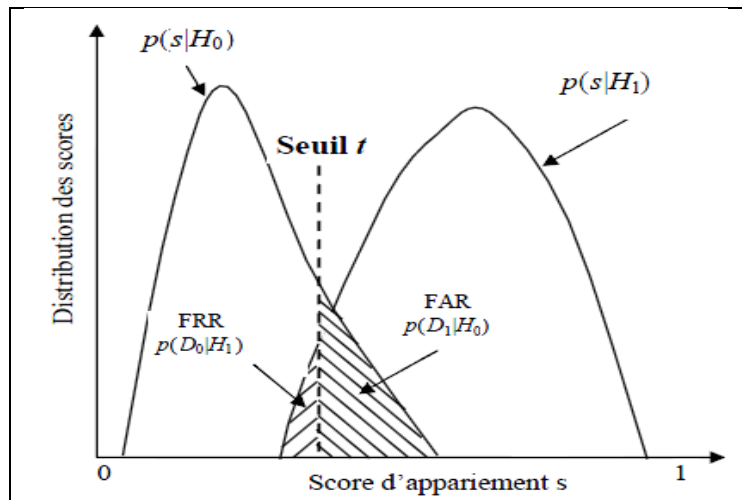


Figure 1.9. Distribution des scores des personnes légitimes et des imposteurs

FAR et FRR sont influencés par un seuil de décision. Donc le choix de ce point de fonctionnement est important, il dépend essentiellement du type d'application et des performances souhaitées. En effet plus le seuil de décision est bas, plus le système acceptera de client, mais plus il acceptera aussi d'imposteur, par contre, plus ce seuil est grand plus le système rejettera d'imposteur mais plus il rejettera aussi de client.

L'utilisation de la courbe **DET** (Detection Error trade-off) est très fréquente pour l'évaluation de tels systèmes d'authentification, elle représente la variation de taux **FRR** en fonction du taux de **FAR**. L'allure de cette courbe est illustrée par la figure 1.10

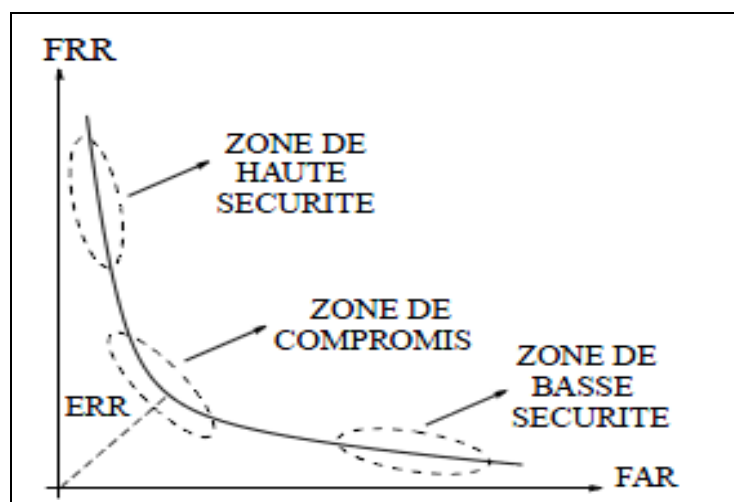


Figure 1.10. La courbe DET

## 1.9. Evaluation d'identification

L'identification peut se formuler par:

Soit  $X_Q$  le vecteur de caractéristique d'entrée, l'identification revient à déterminer l'identité  $I_k$ ,  $k \in \{1, 2, \dots, N, N+1\}$ , où  $I_1, I_2, \dots, I_N$  sont les identités des personnes préalablement enrôlées dans le système, et  $I_{N+1}$  indique une identité rejetée. La fonction d'identification est définie ainsi: [19]

$$(I, X_Q) = \begin{cases} I_K, & \text{si } \max\{S(X_Q, X_{I_k})\} \geq t, K = 1, \dots, N \\ I_{N+1}, & \text{sinon} \end{cases} \quad (1.4)$$

Où  $X_{I_k}$  est le vecteur de caractéristique correspond à l'identité  $I_k$ , et le  $t$  est le seuil fixé.

Le teste d'identification se fait souvent en utilisant la courbe **CMC** (Cumulative Match Characteristics) qui représente le taux d'identification de système en fonction d'une variable que l'on appelle le rang, c'est-à-dire le taux d'erreur est mesuré sur  $k$  décision avec  $k$  variant de 1 à  $N$ , où  $N$  est le nombre d'identités enregistré dans la base de référence. On dit qu'un système reconnaît au rang 1 lorsqu'il choisit le plus proche individu (selon le module de similarité) correspond à l'identité proclamée. On dit qu'un système reconnaît au rang 2 lorsqu'il choisit parmi deux images celle qui correspond le mieux à l'image d'entrée, et ainsi de suite. La courbe **CMC** est une courbe croissante autrement dit, plus le degré du rang augmente, plus le taux de reconnaissance correspondant est lié à un niveau de sécurité faible.

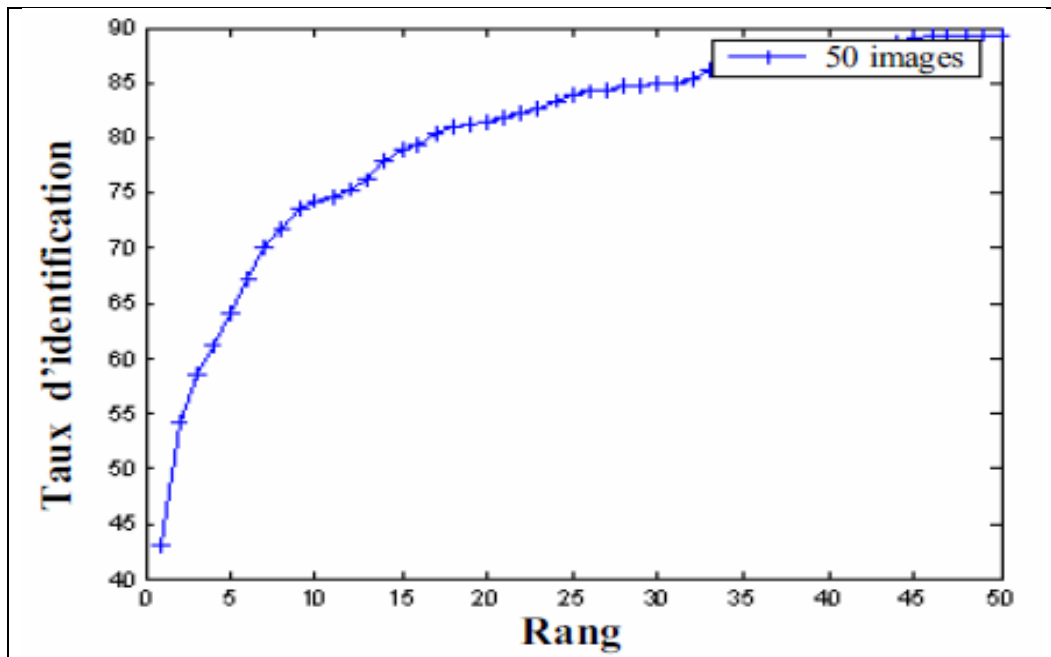


Figure 1.11. La courbe CMC

### 1.10. Domaine d'application

Le champ d'application de la biométrie est très vaste. En effet, tous les domaines qui nécessitent de vérifier ou déterminer l'identité de personnes sont concernés [17]. 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.

**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.

On cite quelques exemples des applications de la biométrie :

- ✓ Contrôle d'accès aux locaux: salles informatiques, Sites sensibles (service de recherche, site nucléaire) ;
- ✓ Equipements de communication: terminaux d'accès, téléphones portables.
- ✓ Systèmes d'informations: lancement du système d'exploitation, accès au réseau, transaction (financière pour les banques, données entre entreprises).
- ✓ 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.
- ✓ Etat administration : fichier judiciaire, services sociaux (sécurisation des règlements), système de vote électronique

### 1.11. Marché biométrique

#### 1.11.1. Présentation du marché

Le marché de la biométrie est actuellement en pleine explosion. On note une recrudescence des sites équipés par cette technologie, qui a pour but d'assurer à la fois le contrôle, la gestion, et la sécurité au sein de différents établissements. On peut donc affirmer qu'aujourd'hui, la biométrie connaît un engouement exponentiel. S'il existe des secteurs déjà équipés, tels d'identification criminelle ou celle des citoyens, d'autres marchés sont en pleine émergence comme le contrôle d'accès physique, la téléphonie, la surveillance etc....

Sur le marché une tendance se vérifie :

La biométrie commence à remplacer le mot de passe à l'ouverture d'un logiciel ou d'un poste d'informatique et surtout, se démocratise dans le contrôle d'accès aux locaux. [20]

#### 1.11.2. Marché mondial de la biométrie

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 smartphone 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. A 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 [21]. En outre, les assistants vocaux développés par Amazon et Google mettent en jeu des modules de reconnaissance vocale enregistrée.

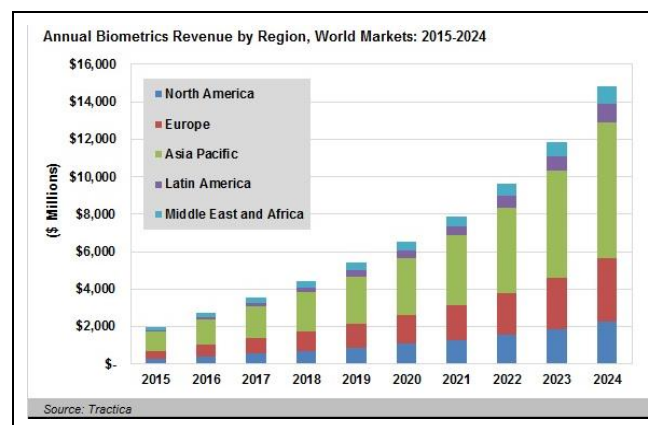


Figure 1.12 : La croissance de la biométrie

### 1.11.3. Marché militaire de la biométrie

Technavio a publié une nouvelle étude intitulée (global military biometrics Market 2016-2020), qui prévoit que le marché mondial de la biométrie militaire devrait croître à un TCAC de plus de 7% pendant la période de prévision.

Le rapport d'étude de marché comprend également une analyse de marché et des prévisions à jour pour les différents segments et toutes les régions géographique.

« Le marché mondial de la biométrie devrait connaître un rythme soutenu en raison des préoccupations croissantes en matière de sécurité et de l'augmentation de la migration illégale de personnes dans le monde », a déclaré Moutushi Saha, analyse principal de technavio pour la recherche sur la défense « de nombreux pays ont mis en place des infrastructures biométrique pour contrôler les flux illicites de personnes ».

L'analyse des études de marché catégorise le marché de la biométrie militaire en quatre grands segments de produits, y compris l'identification des empreintes digitale, la reconnaissance faciale, la reconnaissance de l'iris, et d'autres.

Le marché mondial de l'identification biométrique des empreintes digitales dans le secteur militaire devrait croître à un TCAC de 7% pendant la période de prévision, ce qui en fait le plus largement adopté parmi les technologies biométrique en raison de son faible cout des systèmes matériels et la mise en œuvre facile.

L'armée américaine envisage de moderniser sa biométrie tactique avec identity dominance system 2 (IDS 2) (système multimodal de collecte de donnée biométrique : empreinte digitale, iris, visage) [22]



Figure 1.13 Les militaire inscrivent les empreintes digitales des citoyens de l'Afghanistan dans le système Secure Electric Enrollment Kit (SEEK-II) de CrossMatch

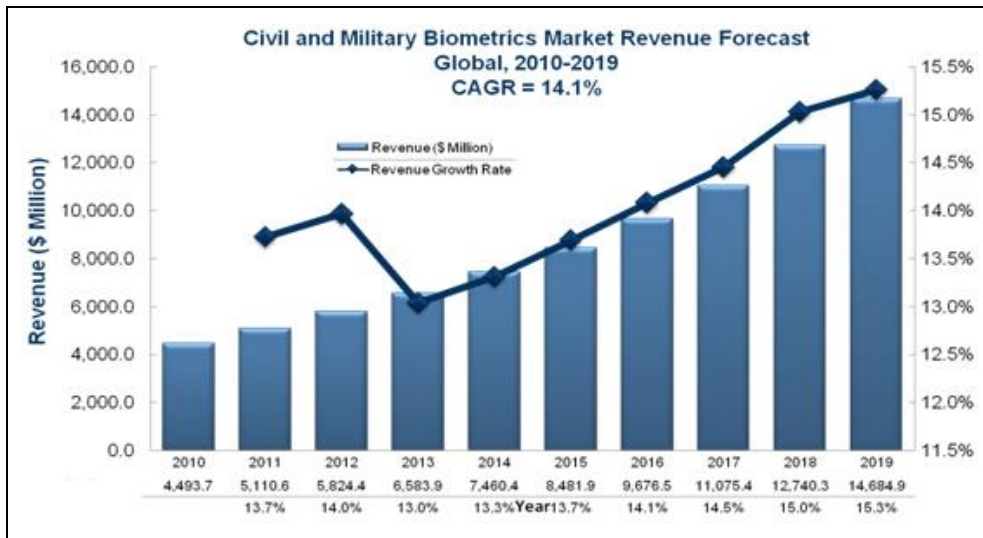


Figure 1.14 : Croissance de la biométrie dans les secteurs civils et militaires

### 1.12. conclusion

Dans ce premier chapitre, nous avons abordé des généralités sur la biométrie: et sa caractéristique ainsi que ses différentes modalités, ensuite nous avons présenté l'architecture d'un système biométrique avec son principe de fonctionnement et les critères d'évaluation de ses performances, enfin nous avons clôturé le chapitre par quelques applications de la biométrie et la description de son marché.

## Chapitre 02

### Le système proposé

#### 2.1. Introduction

Sans aucun doute, le domaine contemporaine de la reconnaissance automatique suit une évolution continue, par conséquent il a motivé le développement du domaine de la biométrie par ces différentes modalités de reconnaissance, lesquelles sont citées dans le chapitre 01, parmi ces dernières on trouve la reconnaissance par l’empreinte de l’articulation des doigts. Cette modalité peut être utilisée dans nombreuses applications telles que l’identification de personnes pour des raisons de sécurité.

Pour améliorer les systèmes biométriques, le domaine a su une méthode efficace et importante dans la réduction des certaines limitation de ces systèmes, on parle de la biométrie multimodale, elle sert à fusionner et à combiner plusieurs systèmes biométriques. Dans ce chapitre on va expliquer l’une des niveaux de fusion, c’est la fusion des classifieurs.

#### 2.2. Prétraitement de l’empreinte d’articulation de doigt

La phase de prétraitement vient après la phase de détection. Elle permet de préparer l’image de l’articulation de doigt de telle sorte qu’elle soit exploitable dans la phase d’enrôlement. On l’appelle aussi phase de normalisation puisqu’elle ramène à un format prédéfini toutes les images extraites de l’image brute [23]. Afin d’extraire la région d’intérêt (Region Of Interest ROI) qui contient les textures autour de l’articulation. Cette opération a pour but d’éliminer le fond (réduction de la taille d’image) et d’avoir des résultats plus précis [24]

**Etape 1 Filtrage et sous-échantillonnage** : La taille de chaque image de la base des données est d’un nombre de pixels important avec une résolution importante. Il n’est pas nécessaire d’utiliser cette résolution pour l’extraction des caractéristiques (une faible résolution peut représenter bien les lignes principales et secondaires autour de l’articulation). Par conséquent, l’image du doigt subit une opération de filtrage suivi par une opération de sous-échantillonnage. L’objectif de l’opération de filtrage est de réduire le bruit dans l’image. Un filtre passe-bas (filtre gaussien), peut être appliqué pour réduire ce bruit et améliorer la qualité de l’image originale. L’opération de sous-échantillonnage permet de réduire la résolution de l’image. L’avantage de cette opération est de réduire considérablement le coût de

calcul en réduisant la quantité de données. Nous notons ID l'image résultante. Le résultat de cette étape est illustré dans la figure (2.1)



Figure 2.1 filtrage et sous-échantillonnage de l'image de doigt

**Etape 2 Détermination de l'axe :** Une fois que l'image de l'empreinte a été filtrée et sous-échantillonnée, l'algorithme détermine l'axe horizontal X. La limite inférieure du doigt peut être facilement extraite par un détecteur de contour de type Canny. Le filtre de Canny est utilisé en raison de ses avantages (bonne détection, bonne localisation). En fait, cette limite inférieure est presque conforme à toutes les images parce que tous les doigts sont mis sur le bloc de base dans l'acquisition de l'image. En adaptant cette frontière comme une ligne droite, l'axe X est déterminé. La figure (2.2) montre l'axe X dans la frontière basse du doigt.

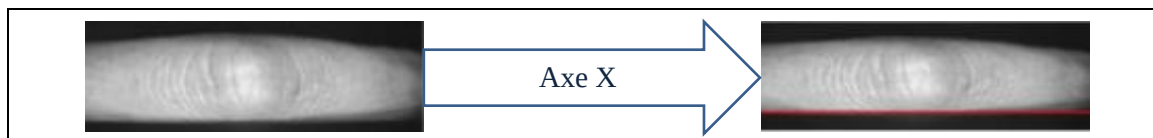


Figure 2.2 filtrage et sous-échantillonnage de l'image de doigt

**Etape 3 Extraction d'une sous-image :** Les informations utiles qui peuvent être utilisées pour une identification biométrique ne résident que dans une partie de l'image du doigt. Donc ça nécessite une coupure d'une sous-image IS, à partir de l'image originale

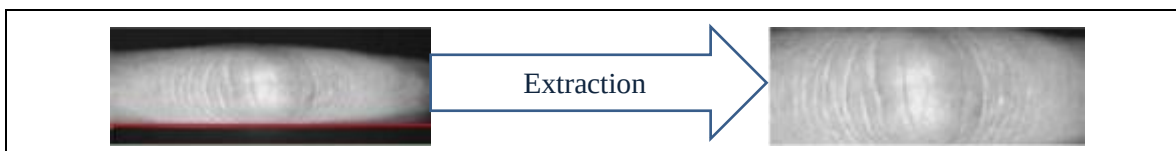


Figure 2.3 sous-image extraite avant l'extraction de la ROI

Les limites gauche et droite d'IS sont deux valeurs axées empiriquement. Les limites hautes et basses sont estimées selon la limite de vrais doigts. La figure (2.3) montre un exemple d'une sous-image. Cette sous-image est utilisée pour calculer l'axe Y.

**Etape 4 Détection de contour :** A l'application du détecteur de contour de type Canny à l'image IS, l'image des contours IE peut être obtenue. Voir la figure (2.4) pour un exemple

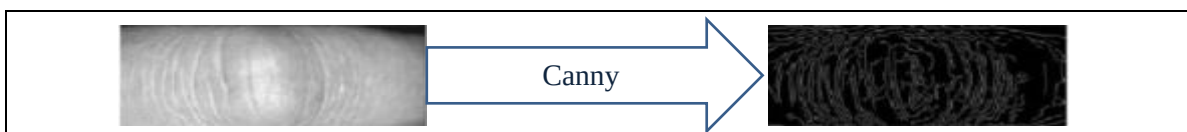


Figure 2.4 image des contours obtenue

**Etape 5 Codage des directions convexe :** Cette étape basée sur les caractéristiques des courbes des contours dans l'image, IE, nous pouvons coder IE pour obtenir une image codée, ICD, qui représente les directions convexes des courbes. Dans cette étape, chaque pixel dans IE sera donc désigné par un code afin de représenter la direction (convexe) locale de ce pixel. Basé sur l'observation des images de doigt, la figure (2.5) illustre un modèle idéal des courbes dans l'image de doigt comme Dans ce modèle, une courbe dans l'image est soit convexe vers la gauche Ou convexe vers la droite

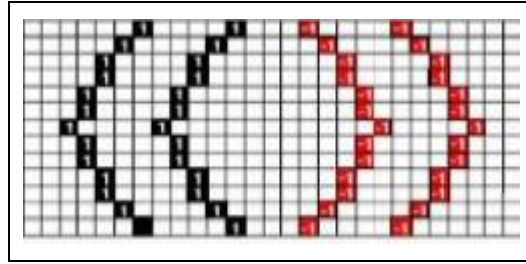


Figure 2.5 courbes sur l'image de doigt

Nous pouvons coder les pixels sur les courbes convexes (vers la gauche) par « 1 », les pixels sur les courbes convexes (vers la droite) par « 1 » et les autres pixels (n'appartiennent pas à ces deux courbes) par « 0 ». La figure (2.6) montre les directions convexes ICD.

**Etape 6 Détermination de l'axe Y :** Pour une image de doigt, la plupart des courbes sur la partie gauche de l'image sont dirigées vers la gauche et ceux sur la partie droite sont dirigés vers la droite. Cependant, il n'y a pas Des directions convexes évidentes dans une petite zone autour de l'articulation.

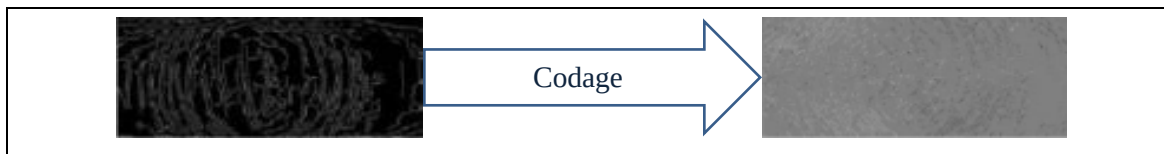


Figure 2.6 image obtenue par l'application de codage de la direction convexe

A partir de cette observation, nous pouvons définir une grandeur de convexité  $q$  comme suit :

$$q(x) = \text{abs}(\sum_w I_{CD}) \quad (2.1)$$

Où  $x$  est la position horizontale (représente une colonne) de la fenêtre.  $W$  est une fenêtre symétrique par rapport à l'axe  $X = x$ . La fenêtre  $W$  est de taille  $d \times h$ , avec  $h$  égale à la hauteur de l'image  $IS$  et  $d$  est choisi, La grandeur  $(x)$  peut atteindre sa minimale autour du centre de l'articulation. La fenêtre doit réaliser un trajet qui part de la gauche et qui va balayer les différents  $x$ . L'axe  $Y$  est définit comme suit :

$$Y = \operatorname{argmin}_{\infty} [q(x)] \quad (2.2)$$

Cette position peut être utilisée pour définir l'axe Y. La figure (2.7) montre la position de l'axe Y dans l'image du doigt

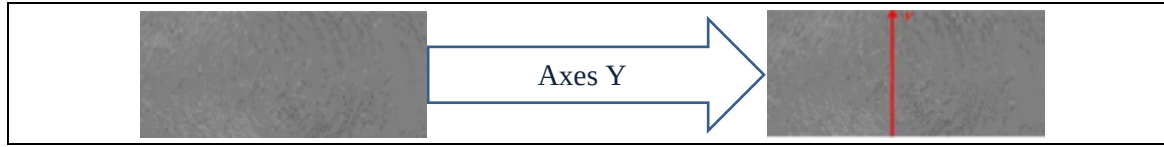


Figure 2.7 détermination de l'axe Y

**Etape 7 Localisation de la ROI :** Après avoir localisé les axes X et Y, nous pouvons déterminer une zone dans l'image ID, nommée IROI, qui représente la région d'intérêt. D'après la figure (2.8), la ROI, avec une taille fixe, peut être extraite à partir de l'image ID



Figure 2.8 localisation de la ROI dans l'image de doigt

**Etape 8 Extraction de ROI :** Une région d'intérêt de l'empreinte est définie et découpée autour de l'axe Y (comme le montre la figure (2.9).) Une région rectangulaire, qui correspond au ROI, avec une dimension fixe et contenant la majorité de l'empreinte, est ensuite extraite.

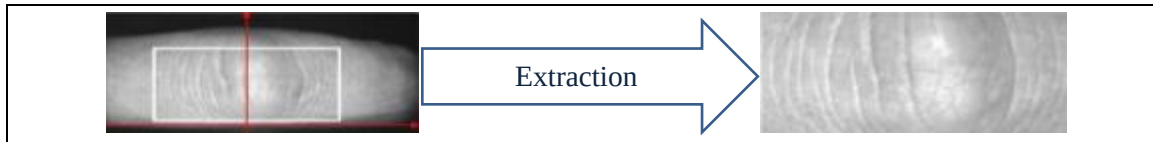


Figure 2.9 Extraction de la ROI à partir de l'image de doigt

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

### 2.3. Extraction Des Caractéristiques

L'extraction des caractéristiques à partir de l'image de modalité (dans notre cas c'est FKP) représente une phase très importante pour concevoir un système d'identification efficace. Cependant, le choix de la méthode d'extraction des caractéristiques est basé sur trois

informations essentielles à savoir la texture, les lignes et l'apparence de l'empreinte [24]. Donc cette étape représente le cœur du système de reconnaissance, on extrait de l'image les informations qui seront sauvegardées en mémoire pour être utilisées plus tard dans la phase de décision. On distingue deux approches pour l'extraction des caractéristiques :

### 2.3.1. Extraction basé sur la texture

#### ➤ Motifs binaires locaux

Les motifs binaires locaux ont initialement été proposés par Ojala en 1996 afin de caractériser les textures présentes dans des images en niveaux de gris. Ils consistent à attribuer à chaque pixel P de l'image à analyser, une valeur caractérisant le motif local autour de ce pixel. Ces valeurs sont calculées en comparant le niveau de gris du pixel central P aux valeurs des niveaux de gris des pixels voisins. Le concept du LBP est simple, il propose d'assigner un code binaire à un pixel en fonction de son voisinage. Ce code décrivant la texture locale d'une région est calculé par seuillage d'un voisinage avec le niveau de gris du pixel central. Afin de générer un motif binaire, tous les voisins prendront alors une valeur "1" si leur valeur est supérieure ou égale au pixel courant et "0" autrement (Figure 2.10). Les pixels de ce motif binaire sont alors multipliés par des poids et sommés afin d'obtenir un code LBP du pixel courant. On obtient donc pour toute l'image, des pixels dont l'intensité se situe entre 0 et 255 comme dans une image à 8 bits ordinaire. Plutôt que de décrire l'image par la séquence des motifs LBP, on peut choisir comme descripteur de texture un histogramme de dimension 255 [25]

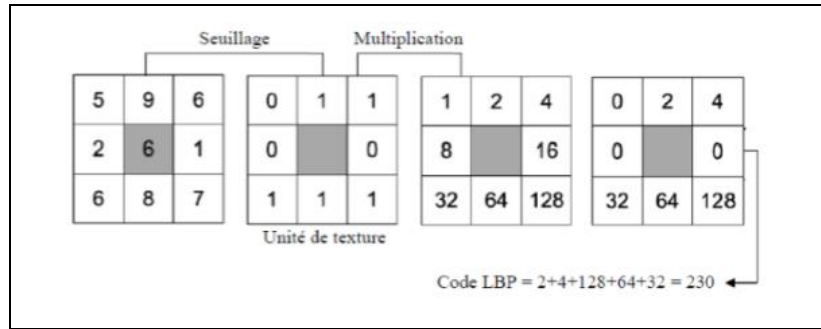


Figure 2.10 construction d'un motif binaire et calcul du code LBP

Pour calculer un code LBP dans un voisinage de P pixels, dans un rayon R, on compte simplement les occurrences de niveaux de gris  $g_p$  plus grands ou égaux la valeur centrale.

$$LBP(X_c, Y_c) = \sum_{n=0}^{p-1} U(g_i - g_c) * 2^n \quad (2.3)$$

Où  $x_c$  et  $y_c$  les coordonnées du pixel central,  $u()$  est la fonction signe et où  $g_i$  et  $g_c$  sont respectivement les niveaux de gris d'un pixel voisin et du pixel central

$$U(x) = \begin{cases} 1, & \text{si } x \geq 0 \\ 0, & \text{autrement} \end{cases} \quad (2.4)$$

➤ Descripteur de base LPQ (Local phase quantization) :

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

$$F_U(x) = \sum_{m \in N_x} h(m-x) f(m) e^{-j2\pi u^T m} = E_U^T f_x \quad (2.5)$$

Où  $E_u$ , de taille  $1 \times M^2$ , est un vecteur de base de 2DWFT avec la fréquence  $u$ , et  $F_x$ , taille  $M^2 \times N$ , est un vecteur contenant les valeurs des pixels d'image dans  $N_x$  à chaque position  $x$ . La fonction fenêtre,  $h(x)$  est une fonction rectangulaire.

La transformation est calculée à quatre valeurs de la fréquence,  $u = [u_0, u_1, u_2, u_3]$  où  $u_0 = [\mathbf{a}, ]$ ,  $u_1 = [0, ]$ ,  $u_2 = [\mathbf{a}, ]$  et  $u_3 = [\mathbf{a}, -\mathbf{a}]^T$ . La valeur  $\mathbf{a}$  est la plus haute fréquence scalaire pour laquelle  $H_{ui} > 0$ . Ainsi, seuls quatre fonctions complexes comme un banc de filtres sont nécessaires pour produire huit images résultantes, composées de 4 images de la partie réelle et 4 images de la partie imaginaire de la transformée. Chaque pixel de l'image complexe résultant peut être codé en une valeur binaire représentée dans l'équation (2.6) en appliquant (the quadrant bit coding) [26]

$$B_{Ui}^{Re}(x) = \begin{cases} 1 & \text{si } F_{Ui}^{Re}(x) > 0 \\ 0 & \text{si } F_{Ui}^{Re}(x) \leq 0 \end{cases} \quad B_{Ui}^{Im}(x) = \begin{cases} 1 & \text{si } F_{Ui}^{Im}(x) > 0 \\ 0 & \text{si } F_{Ui}^{Im}(x) \leq 0 \end{cases} \quad (2.6)$$

Ce procédé de codage attribue deux bits pour chaque pixel pour représenter le quadrant dans lequel se trouve l'angle de phase. En fait, il fournit également la quantification de la fonction de phase de Fourier. En général, LPQ est une chaîne binaire, présentée dans l'expression (2.7), obtenue pour chaque pixel par la concaténation des codes quadrant bits réelles et imaginaires des huit coefficients de Fourier de  $u_i$

$$LPQ(x) = [B_{U0}^{Re}(x), B_{U0}^{Im}(x), \dots, B_{U3}^{Re}(x), B_{U3}^{Im}(x)] \quad (2.7)$$

La chaîne binaire est convertie en nombre décimal par l'expression (2.8) pour produire une étiquette de LPQ. (La figure 2.11) résume l'ensemble de ces étapes.

$$LPQ(x) = B_{U0}^{Re}(x) + B_{U0}^{Im}(x) \times 2^1 + \dots + B_{U3}^{Re}(x) \times 2^{k-1} + B_{U3}^{Im}(x) \times 2^K \quad (2.8)$$

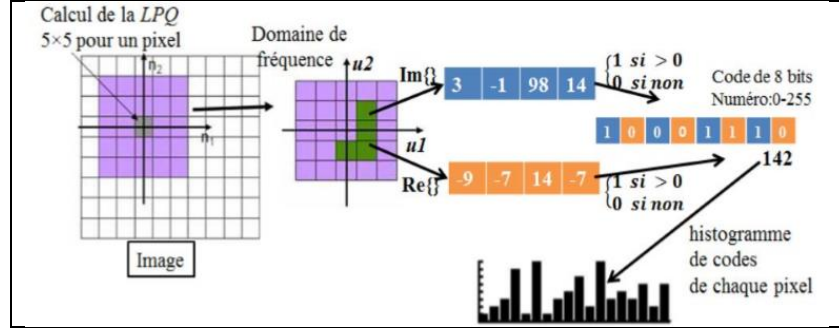


Figure 2.11 Organigramme de l'ensemble des étapes nécessaires à la construction du descripteur LPQ

### 2.3.2. Extraction basé sur le filtrage

#### ➤ Filtre de Gabor

Pour les applications nécessitant une analyse par orientations, les fonctions de Gabor qui produisent une décomposition en ondelettes est très utilisée. De nombreuses applications en traitement d'images font appel à l'utilisation ces types des fonctions, comme par exemple l'analyse de textures ou objets par attributs fréquentiels. En effet, les lignes de l'empreinte sont caractérisées par leur fréquence locale et leur orientation. En utilisant des filtres de Log Gabor, bien choisis, il est possible d'en extraire les caractéristiques biométriques. Cependant, lorsque ceux-ci sont correctement paramétrés, ils permettent de préserver les lignes et fournissent des informations sur l'orientation locale de la texture. Dans le domaine fréquentiel, la réponse ( $f_{Gb}$ ) de filtre log-Gabor 1D se définit comme:

$$f_{Gb} = \exp \left[ \frac{- \left( \log \left( \frac{f}{f_0} \right) \right)^2}{2 \left( \log \left( \frac{\sigma}{f_0} \right) \right)^2} \right] \quad (2.9)$$

Où  $f_0$  est la fréquence centrale et dénote la variance.

Pour l'application du filtre de Log-Gabor, il faut un choix empirique de paramètres de filtre ( $f_0$  et  $\sigma$ ). Ces paramètres empiriques sont très difficiles à déterminer et c'est l'un des inconvénients des approches basées sur ce filtre [27]

### 2.4. Classification

La classification des images consiste à répartir systématiquement des images selon des classes établies au préalable, classer une image lui fait correspondre une classe, marquant ainsi sa parenté avec d'autres images.

En général reconnaître une image est une tâche aisée pour un humain au fil de son existence, il a acquis des connaissances qui lui permettent de s'adapter aux variations qui résultent de

conditions différents d'acquisition. il lui est par exemple relativement simple de reconnaître un objet dans plusieurs orientations partiellement caché par un autre de près ou de loin et selon diverses illuminations.

Toutefois les progrès technologiques en terme d'acquisition d'images (microscopes, caméras, capteurs) et de stockage engendrent des bases de données riche en information et multiplient les domaines d'applications, il devient alors difficile pour l'humain d'analyser le nombre important d'images, le temps requis le caractère répétitif de la tâche et la concentration nécessaire sont problématiques. Toutefois celle-ci n'est pas forcément aisée pour un programme informatique pour lequel une image est un ensemble de valeur numérique

L'objectif de la classification d'images est d'élaborer un système capable d'affecter une classe automatiquement à une image. Ainsi, ce système permet d'effectuer une tâche d'expertise qui peut s'avérer coûteuse à acquérir pour un être humain en raison notamment de contraintes physiques comme la concentration, la fatigue ou le temps nécessité par un volume important de données images.

### 2.4.1. Méthodes supervisées

L'objectif de la classification supervisée est principalement de définir des règles permettant de classer des objets dans des classes à partir de variables qualitatives ou quantitatives caractérisant ces objets. On dispose au départ d'un échantillon dit d'apprentissage dont le classement est connu. Cet échantillon est utilisé pour l'apprentissage des règles de classement. Il est nécessaire d'étudier la fiabilité de ces règles pour les comparer et les appliquer, évaluer les cas de sous apprentissage ou de sur apprentissage (complexité du modèle). On utilise souvent un deuxième échantillon indépendant, dit de validation ou de test.

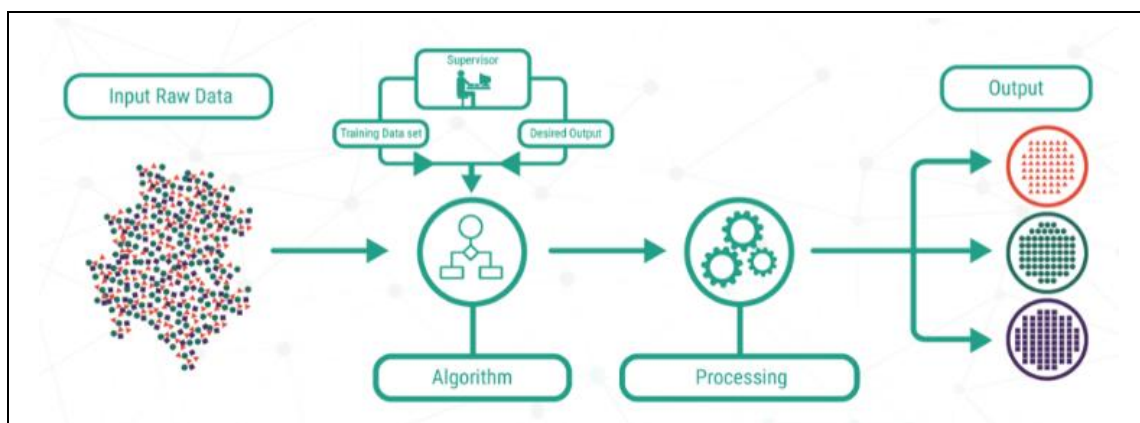


Figure 2.12 méthode supervisée

### 2.4.2. Méthodes non supervisées

Procède de la façon contraire. C'est à dire ne nécessitent aucun apprentissage et aucune tâche préalable d'étiquetage manuel. Elle consiste à représenter un nuage des points d'un espace quelconque en un ensemble de groupes appelé Cluster. Il lié généralement au domaine de l'analyse des données comme l'ACP. Un «Cluster» est une collection d'objets qui sont «similaires» entre eux et qui sont «dissemblables » par rapport aux objets appartenant à d'autres groupes. [28]

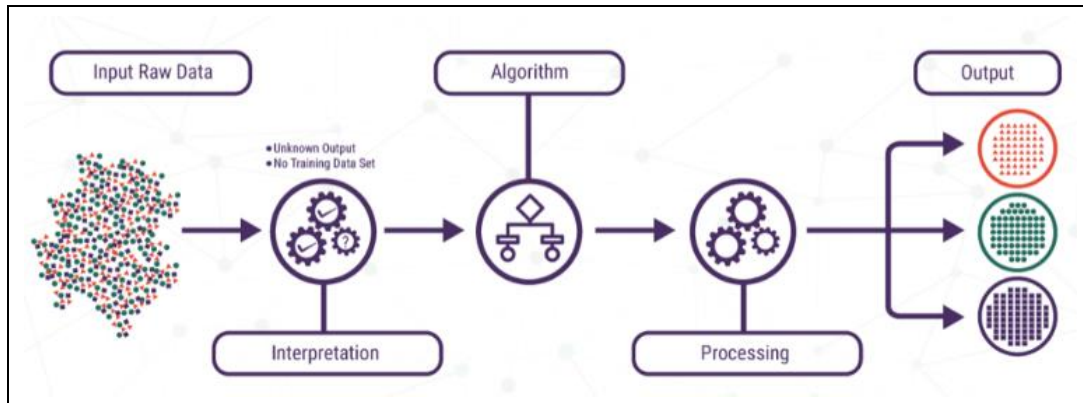


Figure 2.13 méthode non supervisée

### 2.5. Approches connexionnistes

Le problème de reconnaissance de formes peut être résolu en trouvant une fonction, qui associe un ensemble de formes de départ à un ensemble de classes d'arrivée, donc le réseau connexionniste jouera le rôle d'une fonction de transfert de telle sorte que si on représente une valeur en entrée et on applique cette fonction elle nous fournit la valeur de sortie, alors on espère que cette dernière corresponde à la sortie d'appartenance de la valeur d'entrée.

Les réseaux connexionnistes modélisent les surfaces de séparation entre les classes, ce qui va diminuer l'erreur de classification, pour cela il prend en compte la structure interclasse des données. Les techniques connexionnistes sont très efficaces pour des tâches très difficiles de reconnaissance de formes. Cette approche est très coûteuse en temps pendant l'apprentissage et difficile de donner exactement l'architecture du réseau. Les réseaux de neurones (Neural Network : NN) ont connu un grand succès à partir des années 90, notamment grâce à la mise au point d'un algorithme d'apprentissage efficace et facile à mettre en œuvre : la rétro-propagation du gradient.

#### 2.5.1. Apprentissage profond (deep learning)

L'apprentissage profond (« deep learning ») est un ensemble de techniques d'apprentissage automatique qui a permis des avancées importantes en intelligence artificielle dans les

dernières années. Dans l'apprentissage automatique, un programme analyse un ensemble de données afin de tirer des règles qui permettront de tirer des conclusions sur de nouvelles données. L'apprentissage profond est basé sur ce qui a été appelé, par analogie, des « réseaux de neurones artificiels », composés de milliers d'unités (les « neurones ») qui effectuent chacune de petites opérations simples. Les résultats d'une première couche de « neurones » servent d'entrée aux calculs d'une deuxième couche et ainsi de suite. Par exemple, pour la reconnaissance visuelle, des premières couches d'unités identifient des lignes, des courbes, des angles... des couches supérieures identifient des formes, des combinaisons de formes, des objets, des contextes... Les progrès de l'apprentissage profond ont été possibles notamment grâce à l'augmentation de la puissance des ordinateurs et au développement de grandes bases de données (« big data »).

### **2.6. Approches statistiques**

La reconnaissance est fondée sur l'étude statistique des mesures que l'on effectue sur les formes à reconnaître. Elle a besoin d'un nombre élevé d'exemples afin de réaliser un apprentissage correct des lois de probabilité des différentes classes. L'étude de leur répartition dans un espace métrique et la caractérisation statistique des classes permet de prendre une décision du type : plus forte probabilité d'appartenance à une classe. La phase d'apprentissage supervisé consiste à déterminer les règles de décision à partir des exemples de la base d'apprentissage. Pour un ensemble d'apprentissage donné, on peut construire les frontières de décision de deux manières différentes. La première solution consiste à générer les frontières implicitement à partir des distributions de probabilité de chaque classe (approches modélisantes : mixture de gaussiennes, Modèle de Markov caché, K plus proches voisins). Le deuxième type d'approche consiste à estimer explicitement les frontières de décision entre les classes (approches discriminantes).

#### **2.6.1. Approches discriminantes**

Elles visent à construire directement des frontières de décision par la minimisation d'un critère d'erreur entre les sorties réelles et escomptées du classifieur. Le critère d'erreur choisi est souvent le taux de classification ou l'erreur quadratique. Il existe plusieurs classifieurs discriminants, et le plus récemment, les machines à vecteurs de support. Les machines à vecteurs de support (ils sont aussi appelées : Classifieurs à Marge Optimale ou encore Séparateur à Vaste Marge) ont connu de nombreuses applications en reconnaissance de caractères ces dernières années. Considérées comme les classifieurs possédant les meilleures capacités de généralisation.

### 2.6.2. Approches modélisantes

Elles construisent les frontières de décision à partir des distributions de probabilités de chaque classe. Ces approches bénéficient des méthodes d'apprentissage automatique qui s'appuient sur des bases théoriques connues telles que :

#### 2.6.2.1. Méthodes non paramétriques

Elles sont mises en œuvre dans le cas où l'on ne dispose pas de connaissances a priori sur la distribution de probabilité des classes. L'approche non paramétrique la plus connue est le k plus proche voisin (K-PPV ou K-NN).

**Méthode par k plus proches voisins** est une méthode simple qui ne nécessite pas d'apprentissage. La modélisation utilisée pour la classification est la base d'apprentissage qui constitue l'ensemble des connaissances du système de reconnaissances. Le principe est d'attribuer à la donnée en entrée du reconnaisseur la classe la plus représentée dans son plus proche voisinage. Il faut donc déterminer le nombre k d'individus considérés et la métrique utilisée qui peut être une distance élastique pour comparer les individus et sélectionner les plus proches voisins. L'efficacité de cette méthode dépend de la qualité de sa base d'apprentissage et de la capacité de stockage de celle-ci. Elle est donc limitée à une reconnaissance globale avec un vocabulaire restreint pour ne pas alourdir les temps de traitement et les coûts de stockage. Elle est donc particulièrement adaptée à une reconnaissance mono-scripteur, l'utilisateur devra alors, avant d'utiliser le système, procéder à la saisie de la base d'apprentissage.

**2.6.2.2. Méthodes paramétriques** : dans les méthodes paramétriques, on considère que la forme des distributions de probabilité est connue, des gaussiennes dans le cas classique. Lors de l'apprentissage, on cherche donc à estimer les paramètres inconnus des gaussiennes pour chaque classe : moyennes et variances, ou éventuellement matrices de covariances pour chaque classe. Une fois ces paramètres estimés, la décision se fait naturellement par la règle de Bayes. L'approche paramétrique la plus connue est les Modèles de Markov Cachés.

**Modèles de Markov Cachés** : Un modèle de Markov représente le caractère par un double processus stochastique: la séquence de primitives (symboles) appelée observations , et la séquence d'états. Dans la modélisation Markovienne, une suite d'observations est modélisée par une suite d'états avec des probabilités d'émission. La suite d'états est conditionnée par des probabilités de transitions. A chaque état est associé une probabilité d'émission de symboles observables. Ces états ne sont pas directement observables, c'est pourquoi, ils sont dits cachés, d'où le terme de Modèles de Markov Cachés. La comparaison consiste à chercher

dans ce graphe d'état, le chemin de probabilité maximale correspondant à une suite d'éléments observés dans la chaîne d'entrée [29]

## 2.7. Auto-encodeur

Un auto-encodeur peut simplement être défini comme un réseau de neurones artificiels qui apprend une représentation cachée dans le but de reconstruire ses entrées. Il s'agit donc d'une architecture non-supervisée où les entrées du modèle sont similaires aux sorties, et où le modèle optimise ses paramètres selon l'erreur quadratique moyenne. Un auto-encodeur peut être utilisé à des fins de pré-entraînement ou à des fins de réduction de dimensionnalité lorsque l'architecture prend la forme d'un goulot d'étranglement. À des fins de simplicité, considérons un auto-encodeur à une couche cachée; l'auto-encodeur pourra par la suite apprendre plusieurs niveaux de représentations en empilant des couches cachées. Dans un premier temps le vecteur d'entrée  $x$  de dimension  $D$  est transformé par

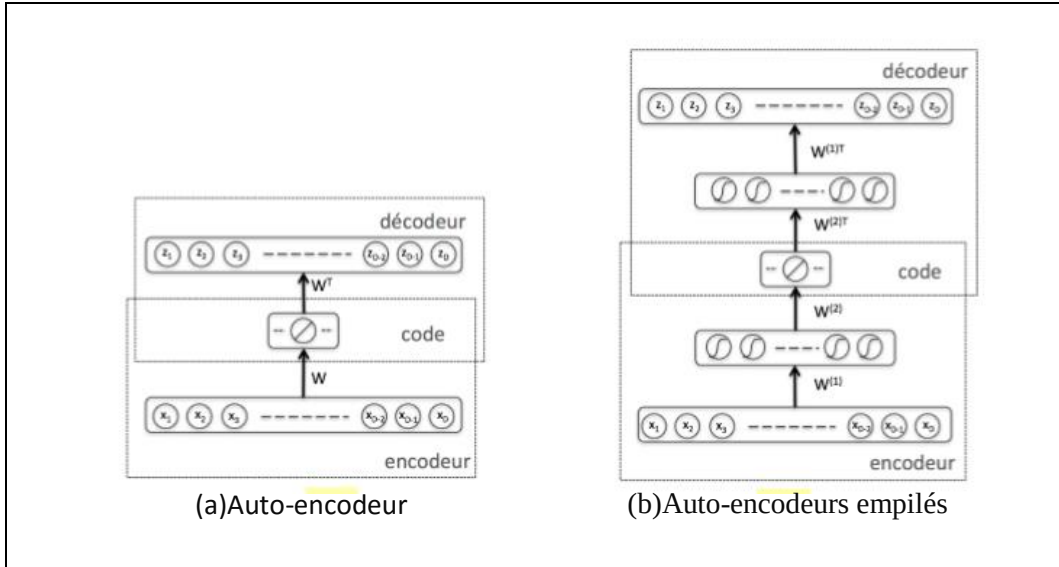


Figure 2.14 auto-encodeurs à une (a) ou plusieurs (b) couches cachées

une fonction d'encodage  $f$  vers la couche cachée  $h$  (souvent appelée code dans le cas des auto-encodeurs) :

$$h=f(x)=s(W^{(1)}x+b^{(1)}) \quad (2.10)$$

où  $W^{(1)}$  est la matrice des paramètres de la fonction d'encodage,  $b^{(1)}$  le vecteur de biais et  $s(\cdot)$  la fonction d'activation. Il est à noter qu'un auto-encodeur à une couche cachée correspond à une analyse en composantes principales si la fonction d'activation est linéaire. Une fois le code produit, une fonction de décodage  $g$  est appliquée pour revenir à la dimension du vecteur d'entrée  $x$  ce qui résulte en un vecteur de reconstruction  $z$  :

$$h=g(f(x))=s(W^{(2)}h+b^{(2)}) \quad (2.11)$$

où  $W^{(2)}$  est la matrice des paramètres de la fonction de décodage. Contraindre la transposée de  $W^{(1)}$  à être égale à  $W^{(2)}$  –c'est-à-dire  $W^{(2)} = W^{(1)T}$ – offre de nombreux avantages. Cela joue un rôle de régulariser : en évitant des mises à jour des poids par de faibles valeurs, et en réduisant le nombre de paramètres à optimiser. Dans le cas de la réduction de dimensionnalité, le code  $h$  possède nécessairement une plus faible dimensionnalité que le vecteur d'entrée  $x$ . [30]

### 2.8. Réseau de neurones à convolution

Les réseaux de neurones convolutionnels sont à ce jour les modèles les plus performants pour classer des images. Désignés par l'acronyme CNN, de l'anglais Convolutional Neural Network, ils comportent deux parties bien distinctes. En entrée, une image est fournie sous la forme d'une matrice de pixels. Elle a 2 dimensions pour une image en niveaux de gris. La couleur est représentée par une troisième dimension, de profondeur 3 pour représenter les couleurs fondamentales [Rouge, Vert, Bleu].

La première partie d'un CNN est la partie convolutive à proprement parler. Elle fonctionne comme un extracteur de caractéristiques des images. Une image est passée à travers une succession de filtres, ou noyaux de convolution, créant de nouvelles images appelées cartes de convolutions. Certains filtres intermédiaires réduisent la résolution de l'image par une opération de maximum local. Au final, les cartes de convolutions sont mises à plat et concaténées en un vecteur de caractéristiques, appelé code CNN [31]

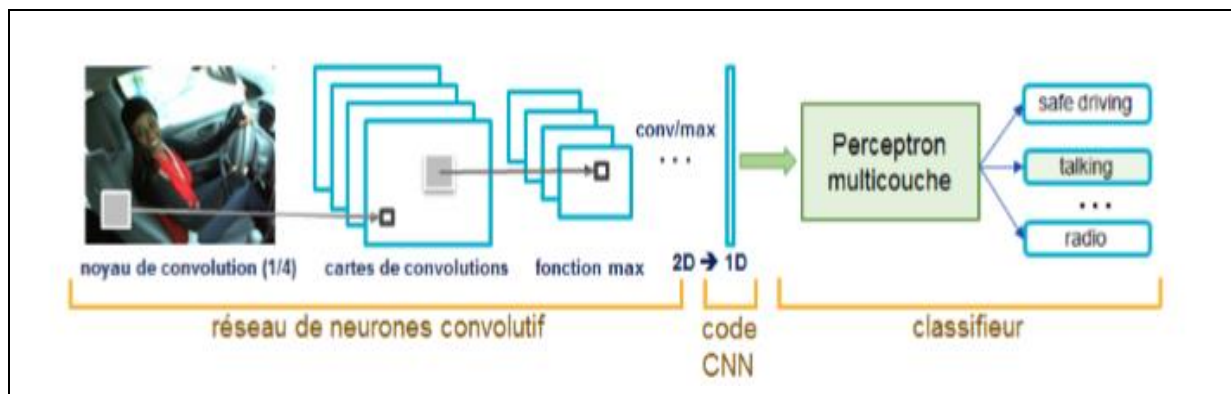


Figure 2.15 réseau de neurones à convolution

Ce code CNN en sortie de la partie convolutive est ensuite branché en entrée d'une deuxième partie, constituée de couches entièrement connectées (perceptron multicouche). Le rôle de cette partie est de combiner les caractéristiques du code CNN pour classer l'image.

La sortie est une dernière couche comportant un neurone par catégorie. Les valeurs numériques obtenues sont généralement normalisées entre 0 et 1, de somme 1, pour produire une distribution de probabilité sur les catégories.

## 2.9. Architecture du réseau de neurone convolutionnel

Une architecture CNN est formée par un empilement de couches de traitement indépendantes

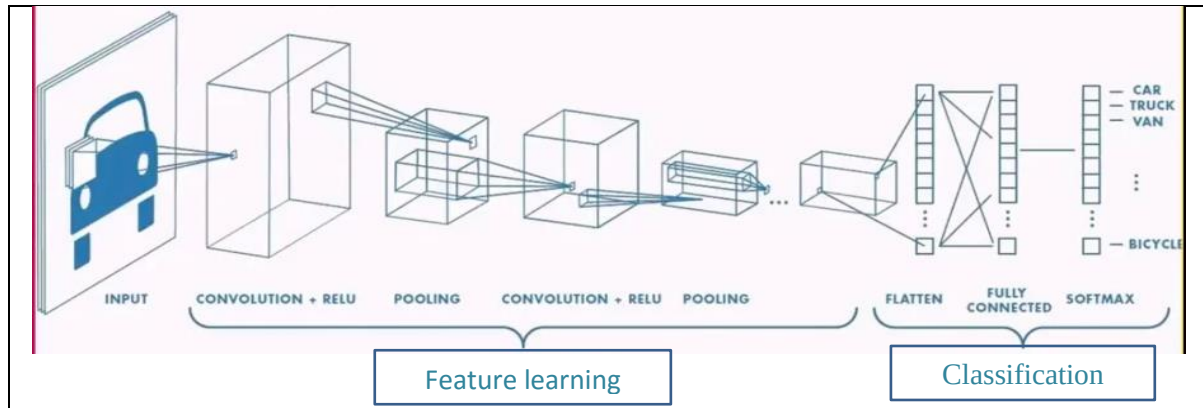


Figure 2.16 architecture d'un réseau CNN

### 2.9.1. Couche de convolution(CONV)

Les couches convolutives constituent le noyau du réseau convolutif. Ces couches se composent d'une grille rectangulaire de neurones qui ont un petit champ réceptif étendu à travers toute la profondeur du volume d'entrée. Ainsi, la couche convolutionnelle est juste une convolution d'image de la couche précédente, où les poids spécifient le filtre de convolution.

### 2.9.2. Couches de pooling

Après chaque couche convolutive, il peut y avoir une couche de pooling. La couche de pooling sous-échantillonne leur entrée. Il y a plusieurs façons de faire cette mise en commun, comme prendre la moyenne ou le maximum, ou une combinaison linéaire apprise des neurones dans le bloc. Par exemple, ( la Figure2.17). montre max pooling sur une fenêtre 2×2.

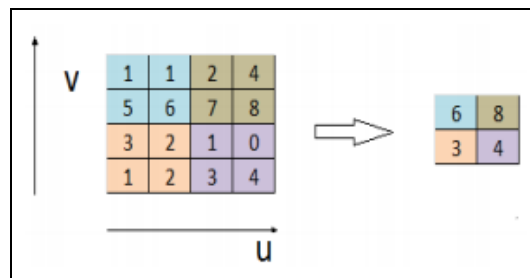


Figure 2.17 pooling avec un filtre 2x2

### 2.9.3. Couches de correction (ReLU)

Il est possible d'améliorer l'efficacité du traitement en intercalant entre les couches de traitement une couche qui va opérer une fonction mathématique (fonction d'activation) sur les signaux de sortie.

La fonction ReLU (abréviation de Unités Rectifié linéaires) :  $F(x)=\max(0,x)$  Cette fonction force les neurones à retourner des valeurs positives.

### 2.9.4. Couches totalement connectées

Enfin, après plusieurs couches de convolution et pooling, le raisonnement de haut niveau dans le réseau neuronal se fait via des couches totalement connectées. Dans les réseaux de neurones convolutifs, chaque couche agit comme un filtre de détection pour la présence de caractéristiques spécifiques ou de motifs présents dans les données d'origine. Les premières couches d'un convolutif détectent des caractéristiques qui peuvent être reconnues et interprétées relativement facilement. Les couches ultérieures détectent de plus en plus des caractéristiques plus abstraites. La dernière couche du réseau convolutif est capable de faire une classification ultra-spécifique en combinant toutes les caractéristiques spécifiques détectées par les couches précédentes dans les données d'entrée.

### 2.9.5. Couche de perte

La couche de perte spécifie comment l'entraînement du réseau pénalise l'écart entre le signal prévu et réel. Elle est normalement la dernière couche dans le réseau. Diverses fonctions de perte adaptées à différentes tâches peuvent y être utilisées. La fonction « Softmax » permet de calculer la distribution de probabilités sur les classes de sortie. [32]

## 2.10. Conclusion

la reconnaissance automatique de l'empreinte de l'articulation des doigts est considérée comme un processus de reconnaissance de forme, pour ce sens nous avons présenté les techniques de prétraitement de la modalité concernée et l'extraction de ses caractéristiques, ensuite on a abordé l'explication de la classification avec ses différents classifieurs après on a présenté les leaders de la classification automatique ,l'auto-encoder et les réseaux à convolutions qui ont un rôle important dans la conception des systèmes moderne de la biométrie.

## Chapitre 03

### Résultats et discussion

#### 3.1.Introduction

Pour but d'évaluer les performances d'un système de reconnaissance de FKP, un nombre de règles communes ont été établies par les scientifiques, permettant de disposer les mêmes critères d'évaluation. Ces critères s'appliquent sur des bases de données également communes et partagées par l'ensemble de la communauté scientifique. Une base de données regroupe plusieurs images de plusieurs personnes.

Ce chapitre représente les résultats de tests effectués avec l'utilisation d'un seul autoencoder et un autoencoder empilé sur une base de données indienne IITD de delhi campus. Rappelons que notre travail consiste à concevoir un système d'identification biométrique de personnes par reconnaissance FKP basant sur l'apprentissage profond (deep learning) Nous évaluerons dans ce chapitre les résultats obtenus sur notre base de données.

#### 3.2. Empreinte d'articulation

Récemment, on constate que l'empreinte d'articulation ou l'empreinte dorsale du doigt, qui se réfère aux formes inhérentes de la surface externe autour du doigt et spécialement la partie haute du doigt, est fortement unique et peut servir à une modalité biométrique distinctive. L'articulation du doigt est encore à la phase de développement et peut être considérée comme nouvelle tendance dans la biométrie. L'articulation du doigt peut ajouter de nouvelles informations à la texture du doigt. Ce trait biométrique a le mérite d'une grande acceptation de la partie utilisateur.

#### 3.3. Système de reconnaissance de FKP

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 [24]. A chaque image est associé un vecteur de 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.

Ceci permet de retrouver la personne ayant le FKP le plus ressemblant, qui est celui dont le vecteur est le plus similaire

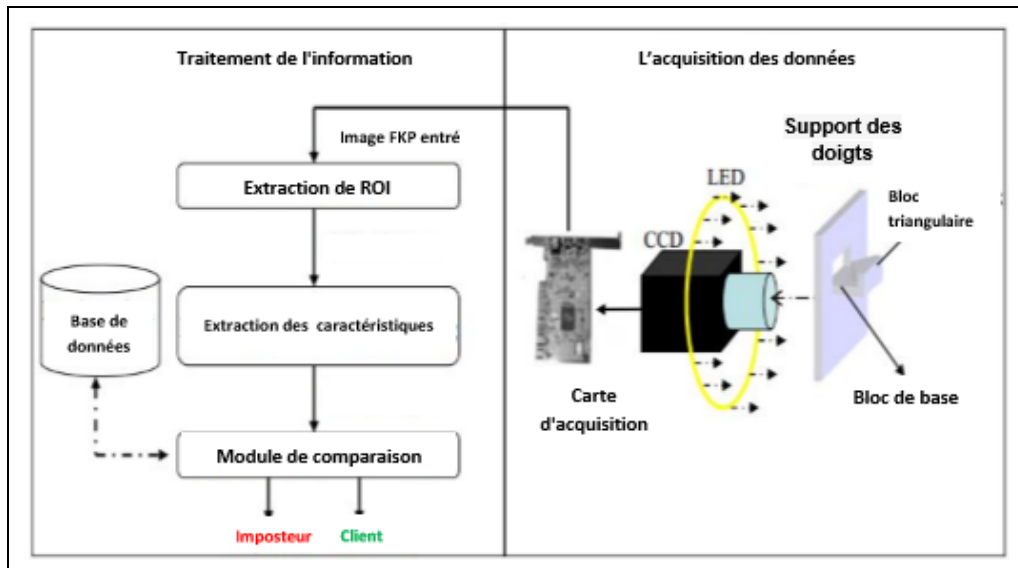


Figure 3.1 schéma de principe du système d'identification personnelle à base du FKP [36]

Le schéma de principe du système d'identification à base du FKP est montré dans la Figure 1.1. Le système est composé d'un module d'acquisition de données et un module de traitement de données. Le module d'acquisition de données est composé d'un support de doigt, un anneau LED source de lumière, une lentille, une caméra CCD et une carte d'acquisition. L'image FKP capturée est entrée dans le module de traitement de données qui comprend trois étapes de base: ROI, extraction des caractéristiques, et l'appariement "matching". Figure 3.2 montre le dispositif d'acquisition d'image FKP dont la taille globale est 160mm × 125mm × 100mm.



Figure 3.2 dispositif d'acquisition d'image FKP

### 3.4. Base de données FKP

La reconnaissance par l'articulation de doigts est en train de devenir une méthode biométrique extrêmement pratique et très acceptée par les utilisateurs. Cependant, cette modalité biométrique a attiré très peu d'attention des chercheurs. Au meilleur de notre connaissance, il n'existe pas à ce jour de base de données d'images disponibles pour les doigts dans le domaine public. Le Laboratoire de recherche en biométrie de l'IIT Delhi développe la base de données d'images de doigts articulés depuis août 2006. L'objectif est d'établir une base de données d'images à grande échelle pour les doigts et de la rendre accessible au domaine public.

La base de données d'images IITD à Delhi comprend les images acquises auprès des étudiants et du personnel de l'IIT Delhi, à New Delhi, en Inde. Cette base de données a été acquise sur le campus de l'IIT à Delhi entre août 2006 et juin 2007 à l'aide d'un appareil photo numérique. La base de données actuellement disponible contient 158 utilisateurs, chaque individu a 5 captures de l'index. Toutes les images sont au format bitmap (\* .bmp). Tous les sujets de la base de données appartiennent au groupe d'âge des 16 à 55 ans. Cette base de données de 790 images a été numérotée de manière séquentielle pour chaque utilisateur avec une identification / un nombre entier. La résolution de ces images est de  $80 \times 100$  pixels et toutes ces images sont disponibles au format bitmap. [39]

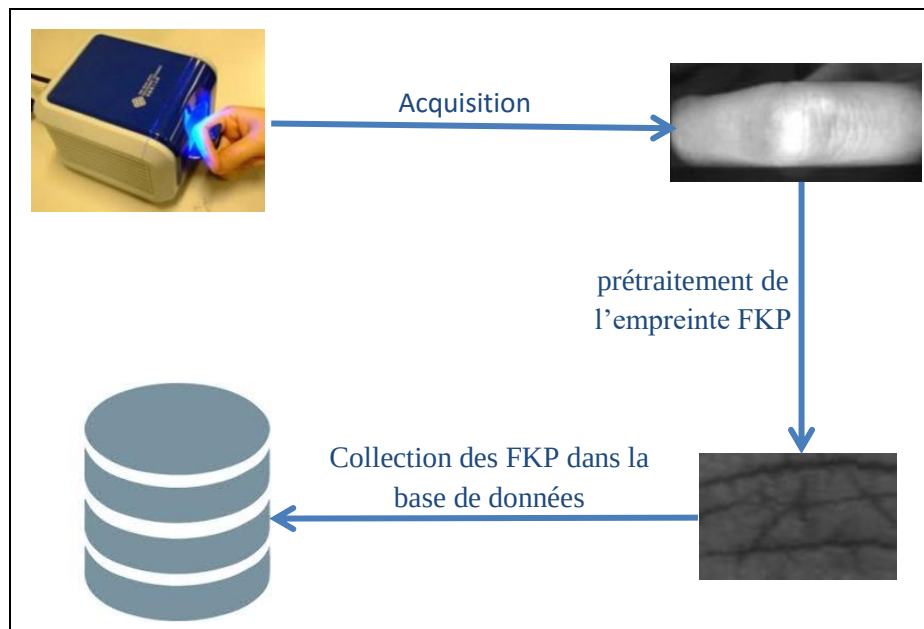


Figure 3.3 Collection des empreintes de l'articulation du doigt dans une base de données

La base de données complète décrite ci-dessus est disponible pour la recherche. Les exemples d'images de cette base de données sont reproduits dans les quatre jeux d'images suivants.

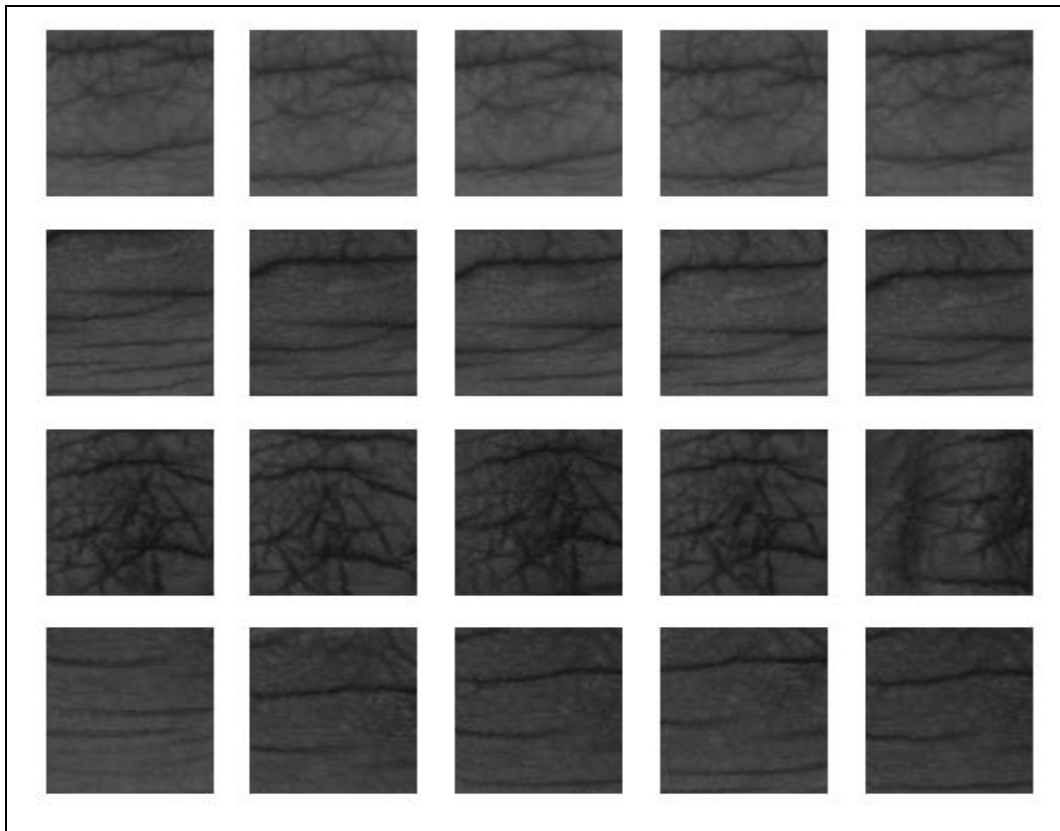


Figure 3.4 des échantillons de la base de données IITD

### 3.4.1. Séparation de base de données

Pour développer une application de reconnaissance de l'empreinte de l'articulation de doigt, 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, cependant qu'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 nous n'avons pris que 50 images de 10 personnes de la base de données qui a été scindée de la façon suivante:

- Images apprentissages (enrôlement) : les trois premières images de chaque personne ( $3 \times 10 = 30$  images) servent pour la phase d'apprentissage.
- Images Tests Les deux images restantes de chaque individu ( $2 \times 10 = 20$  images) nous ont servi pour la réalisation des différents tests. Le but est d'évaluer le taux de reconnaissance, en suivant un protocole de test basé sur la mesure de taux d'identification.

### 3.5. Critère 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

#### 3.5.1. Taux de bonne classification

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.

En général, quand les échantillons étiquetés à disposition sont suffisamment nombreux, ils sont séparés en deux parties disjointes et en respectant les proportions par classes de la base initiale. Une partie sert pour former la base d'apprentissage et l'autre pour former la base de test. Le découpage le plus courant est de 1/2 pour l'apprentissage et le 1/2 restant pour la base de test. Les performances en termes de taux de reconnaissance sont alors déterminées en présentant au classifieur chacun des exemples de la base de test et en comparant la classe donnée en résultat à la vraie classe. Le taux de reconnaissance par classe (TRC) est simplement défini par : [40]

$$\text{TRC}(\%) = \frac{\text{Nombre d'empreinte reconnus pour une classe}}{\text{Nombre total d'empreinte de cette classe}} \quad (3.1)$$

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

$$\text{TMBR}(\%) = \frac{\text{Nombre d'empreinte reconnus}}{\text{Nombre total des empreintes classe}} \quad (3.2)$$

#### 3.5.2. Taux d'erreur

Selon l'Organisation Internationale de Normalisation ISO/IEC 19795-1 [41], les mesures des taux d'erreur sont divisées en trois classes que sont les taux d'erreur fondamentale, taux d'erreur de systèmes d'authentification et taux d'erreur de systèmes d'identification.

### 3.5.2.1. Taux d'erreur fondamentale

Taux d'échec à l'acquisition (failure-to-acquire rate, FTA) : proportion des tentatives de vérification ou d'identification pour lesquels le système biométrique n'a pas pu acquérir l'information biométrique requise;

Taux d'échec à l'enrôlement (failure-to-enroll rate, FTE) : proportion des individus pour lesquels le système n'a pas pu générer le modèle biométrique durant la phase d'enrôlement. Prenons par exemple le cas des empreintes, il existe certaines personnes qui n'ont pas d'empreintes pour des raisons génétiques, ou des empreintes quasi-inexistantes pour des raisons médicales;

Taux de fausse non-correspondance (false non-match rate, FNMR) : proportion de fausse non-correspondance, par l'algorithme de comparaison, entre la donnée biométrique acquise et le modèle correspondant;

Taux de fausse correspondance (false match rate, FMR) : proportion de fausse correspondance, par l'algorithme de comparaison, entre la donnée biométrique acquise et le modèle correspondant à un autre individu.

### 3.5.2.2. Taux d'erreur de systèmes d'authentification

Taux de faux rejets (false rejection rate, FRR) : proportion des transactions des utilisateurs légitimes rejetées par erreur. Ces transactions sont rejetées, par l'algorithme de correspondance, en raison de non-correspondance à tort ainsi que ceux rejetées en raison d'un échec à l'acquisition.

Taux de fausses acceptations (false acceptance rate, FAR) : proportion des transactions des imposteurs acceptées par erreur.

### 3.5.2.3. Taux d'erreur de systèmes d'identification

Taux d'identification (identification rate, IR) : le taux d'identification au rang  $r$  est la proportion de transactions d'identification, par des utilisateurs enrôlés dans le système, pour lesquels l'identifiant de l'utilisateur est dans les  $r$  identifiants retournés;

Taux de faux-négatif d'identification (false-negative identification-error rate, FNIR) : proportion de transactions d'identification, par des utilisateurs enrôlés dans le système, pour lesquels l'identifiant de l'utilisateur ne figure pas dans la liste des identifiants retournée.

Taux de faux-positif d'identification (false-positive identification-error rate, abrégé par FPIR) : proportion de transactions d'identification, par des utilisateurs non enrôlés dans le système, pour lesquels la liste des identifiants retournée est non vide.

Erreur de l'algorithme de présélection (pre-selection error) : l'algorithme de présélection

permet de réduire le nombre de modèles biométriques à comparer avec l'image acquise pendant la phase d'identification. L'erreur de l'algorithme de présélection est l'erreur qui se produit quand le modèle correspondant à la donnée biométrique acquise ne figure pas dans la liste des modèles retournée.

Taux de pénétration (penetration rate, PR) : mesure, en moyenne, le nombre de modèles biométriques présélectionnés par rapport au nombre total de modèles.

### **3.5.3. Matrice de confusion**

Une Confusion Matrix (matrice de confusion) ou tableau de contingence est un outil permettant de mesurer les performances d'un système de classification en vérifiant notamment à quelle fréquence ses prédictions sont exactes par rapport à la réalité dans des problèmes de classification.

Une Confusion Matrix est un résumé des résultats de prédictions sur un problème de classification. Les prédictions correctes et incorrectes sont mises en lumière et réparties par classe. Les résultats sont ainsi comparés avec les valeurs réelles.

Cette matrice permet de comprendre de quelle façon le modèle de classification est confus lorsqu'il effectue des prédictions. Ceci permet non seulement de savoir quelles sont les erreurs commises, mais surtout le type d'erreurs commises. Les utilisateurs peuvent les analyser pour déterminer quels résultats indiquent comment les erreurs sont commises.

#### **3.5.3.1. Calcul de la matrice de confusion**

Pour calculer une matrice de confusion, il est nécessaire de disposer d'un ensemble de données de test (test dataset) ou d'un ensemble de données de validation (validation dataset) avec les valeurs de résultat attendues. On fait ensuite une prédiction pour chaque ligne du « test dataset ».

A partir des résultats escomptés et des prédictions, la matrice indique le nombre de prédictions correctes pour chaque classe et le nombre de prédictions incorrectes pour chaque classe organisées en fonction de la classe prédite. Chaque ligne du tableau correspond à une classe prédite, et chaque colonne correspond à une classe réelle.

Dans les lignes sous les classes réelles, les prédictions ou les résultats sont inscrits. Ces résultats peuvent être l'indication correcte d'une prédiction positive comme « vraie positive » (true positive) et d'une prédiction négative comme « vraie négative » (true negative), ou une prédiction positive incorrecte comme « fausse positive » (false positive) et une prédiction négative incorrecte comme « fausse négative » (false negative).

|                        |   | Réponse de l'expert |              |
|------------------------|---|---------------------|--------------|
|                        |   | p                   | n            |
| Réponse du classifieur | Y | Vrai Positif        | Faux Positif |
|                        | N | Faux Négatif        | Vrai Négatif |

Figure 3.5 Matrice de confusion à quatre mesures

L'avantage de ces matrices est qu'elles sont très simples à lire et à comprendre. Elles permettent de visualiser très rapidement les données et les statistiques afin d'analyser les performances d'un modèle et d'identifier les tendances qui peuvent aider à modifier les paramètres. Pour les problèmes de classification avec trois classes ou plus, il est aussi possible d'utiliser une Confusion Matrix en ajoutant des lignes et des colonnes.

### 3.5.3.2. Terminologies de la matrice confusion

Pour bien comprendre le fonctionnement d'une matrice de confusion, il convient de bien comprendre les quatre terminologies principales : TP, TN, FP et FN. Voici la définition précise de chacun de ces termes :

- TP (True Positives) : les cas où la prédiction est positive, et où la valeur réelle est effectivement positive.
- TN (True Negatives) : les cas où la prédiction est négative, et où la valeur réelle est effectivement négative.
- FP (False Positive) : les cas où la prédiction est positive, mais où la valeur réelle est négative.
- FN (False Negative) : les cas où la prédiction est négative, mais où la valeur réelle est positive. [42]

## 3.6. Résultats Expérimentales

Dans cette partie on a utilisé deux expériences de classification appliquées sur la modalité FKP (les empreintes d'articulation de doigt) le premier test avec un seul autoencoder et le deuxième test avec un autoencoder empilé (stacked autoencoder) dans un premier temps, nous avons étudié les résultats obtenues issues par l'utilisation d'un autoencoder empilé avec un seul autoencoder ensuite on a réutilisé la même base de données et la procédure avec un autoencoder empilé avec deux autoencoder.

## 3.6.1. Stacked autoencoder

### 3.6.1.1. Résultats obtenus Avec un seul stacked auto-encoder

Comme nous l'avons supra cité dans les sections précédentes, les autoencoders sont des réseaux de neurones à trois couches, une couche de sortie, une couche d'entrée, et une seule couche cachée. Ils sont basés sur l'apprentissage non supervisé où l'algorithme d'apprentissage utilise la fonction d'erreur quadratique. La figure suivante montre la structure proposée dont l'objectif de classifier les images FKP.

La couche d'entrée comporte les données expérimentales présente dans la base de données sous forme des pixels renfermée dans les images de cette dernière, et chaque pixel représente une entrée, donc dans notre travail on a des images de taille de  $80 \times 100 = 8000$  pixels ce qui implique qu'on ait 8000 entrée dans notre réseau proposé.

Nous allons proposer la structure suivante :

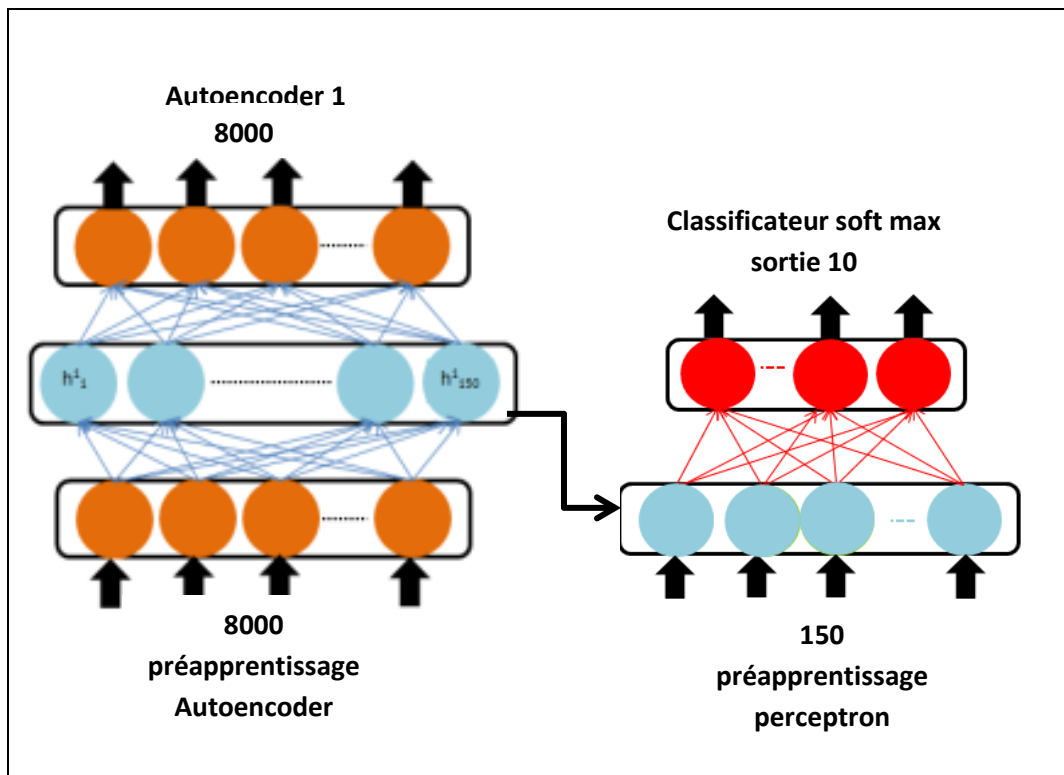


Figure 3.6 la structure de classification proposé basée sur un stacked autoencoder

**Autoencodeur:** comporte une entrée et une sortie de 8000 avec une couche cachée de 150 neurones. Les fonctions d'activation de couche cachée (Encodeur) est 'logsig' et pour la sortie 'purelin'.

**Classificateur softmax :** comporte une entrée de 150 et une sortie de 10 neurones. La fonction d'activation de couche de la sortie est softmax.

## Résultats et discussion

Après l'exécution de notre programme avec la configuration mentionnée dans la structure proposée on a obtenu les résultats suivants :

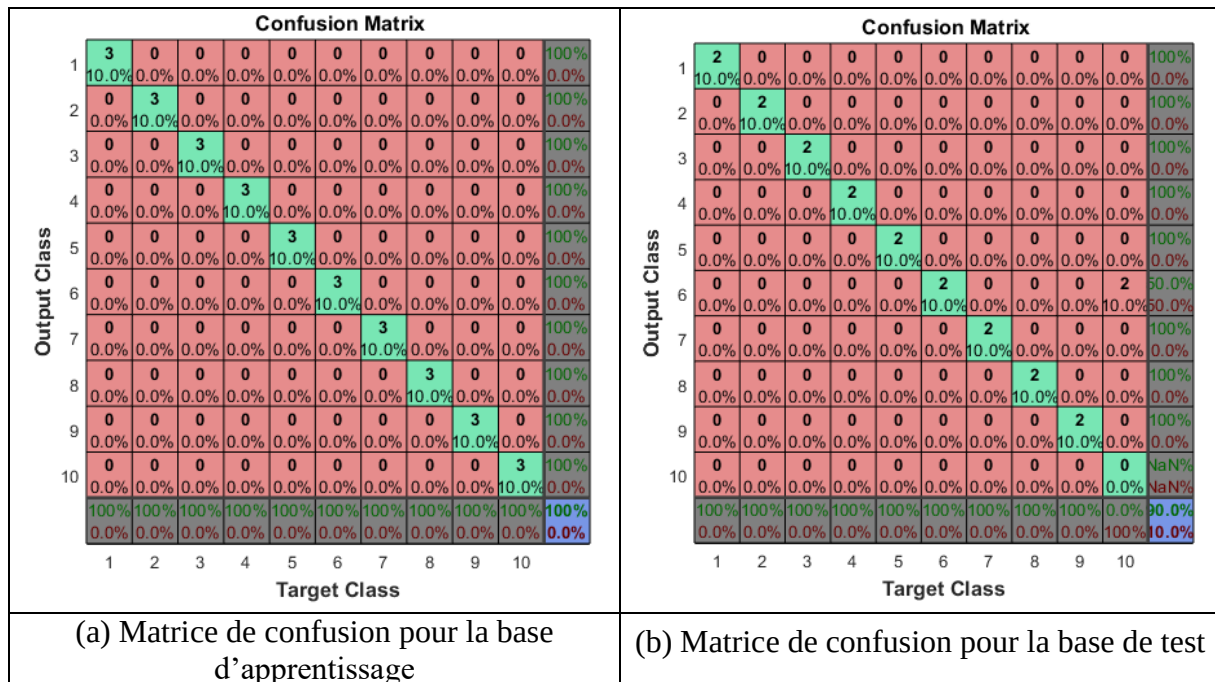


Figure 3.7 Les matrices de confusion produites

La figure 3.7 présente la matrice de confusion pour la base d'apprentissage et la base de test, on remarque une classification de taux de 100% dans la base d'apprentissage; ce qui montre que l'apprentissage soit efficace. D'autre part, la matrice de confusion de la base de test présente un taux de 90% de classification.

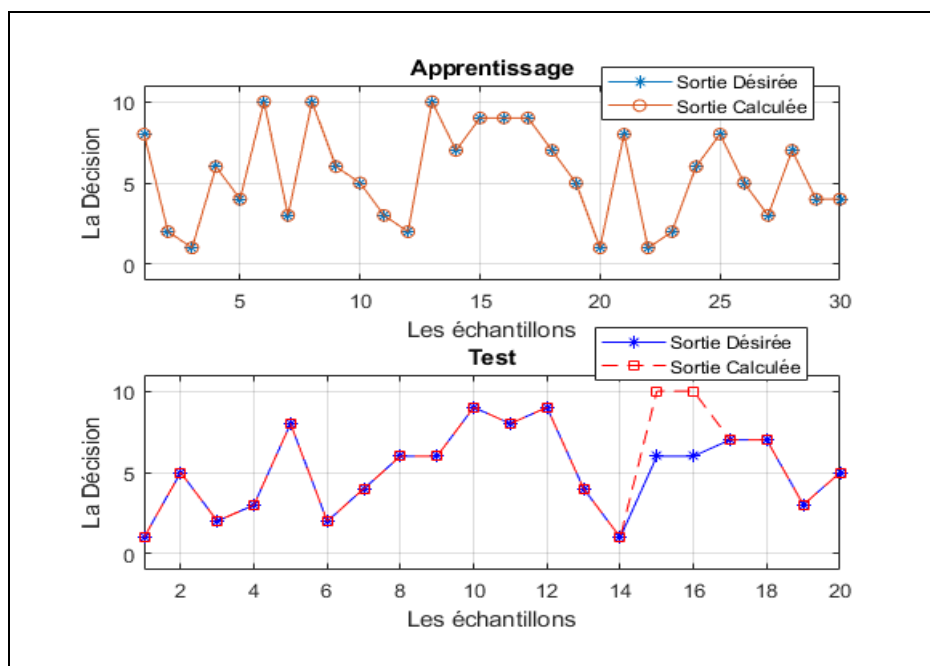


Figure 3.8 Sorties de l'apprentissage et du test de l'autoencodeur comparées avec les sorties désirées.

## Résultats et discussion

La figure 3.8 représente une précision remarquable pour les sorties désirés de l'apprentissage avec les sorties de l'autoencodeur (les sorties sont entièrement identiques), et une précision considérable pour les sorties désirés de test avec la sortie de l'autoencodeur, en remarquant que le test était échouée à l'échantillon N°15 et N°16.

Dans la figure ci-dessous on y récapitule les performances de notre système

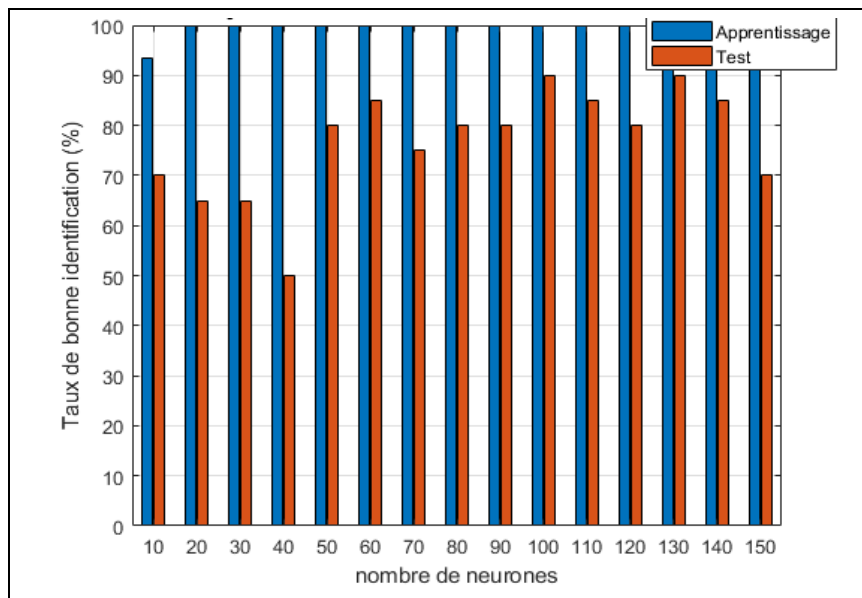


Figure 3.9 performance du système en fonction de neurones de l'autoencodeur

A l'aide du bilan dont on a posé dans la figure 3.9, on tire les performances explicites du système en disant que le système a atteint 90% de taux de bonne identification aux neurones 100 et 130. donc dans ce cas on prend le nombre de neurone 100 puisque l'autoencodeur à ce stade a atteint le taux maximal et pour but de diminuer le temps d'exécution.

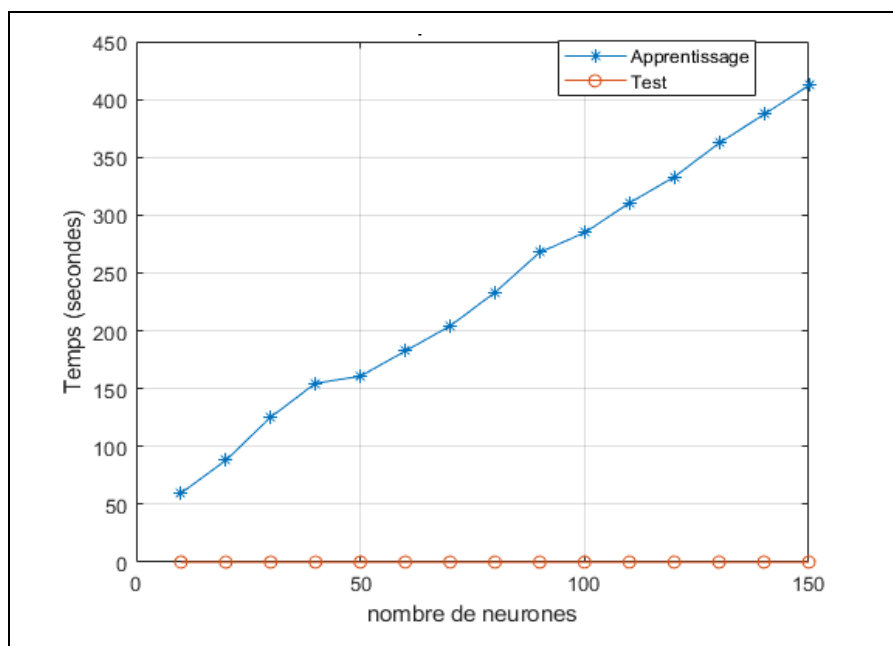


Figure 3.10 temps d'exécution de l'apprentissage

On remarque dans la figure 3.10 que le temps d'exécution est en relation de corrélation directe avec le nombre de neurones. Le temps d'exécution de notre algorithme est environ 410 secondes.

### 3.6.1.2. Résultats obtenus Avec deux stacked auto-encoder

Pour atteindre notre objectif nous allons proposer la structure suivante :

**Réseau 1 (Autoencodeur 1) :** comporte une entrée et une sortie de **8000** avec une couche cachée de **100** neurones. Les fonctions d'activation de couche cachée (Encodeur) est 'logsig' et pour la sortie 'purelin'.

**Réseau 2 (Autoencodeur 2) :** comporte une entrée et une sortie de **100** avec une couche cachée de **10** neurones. Les fonctions d'activation de couche cachée (Encodeur) est 'logsig' et pour la sortie 'purelin'.

**Réseau 3 (softmax) :** comporte une entrée de **10** et une sortie de **10** neurones. La fonction d'activation de couche de la sortie est softmax

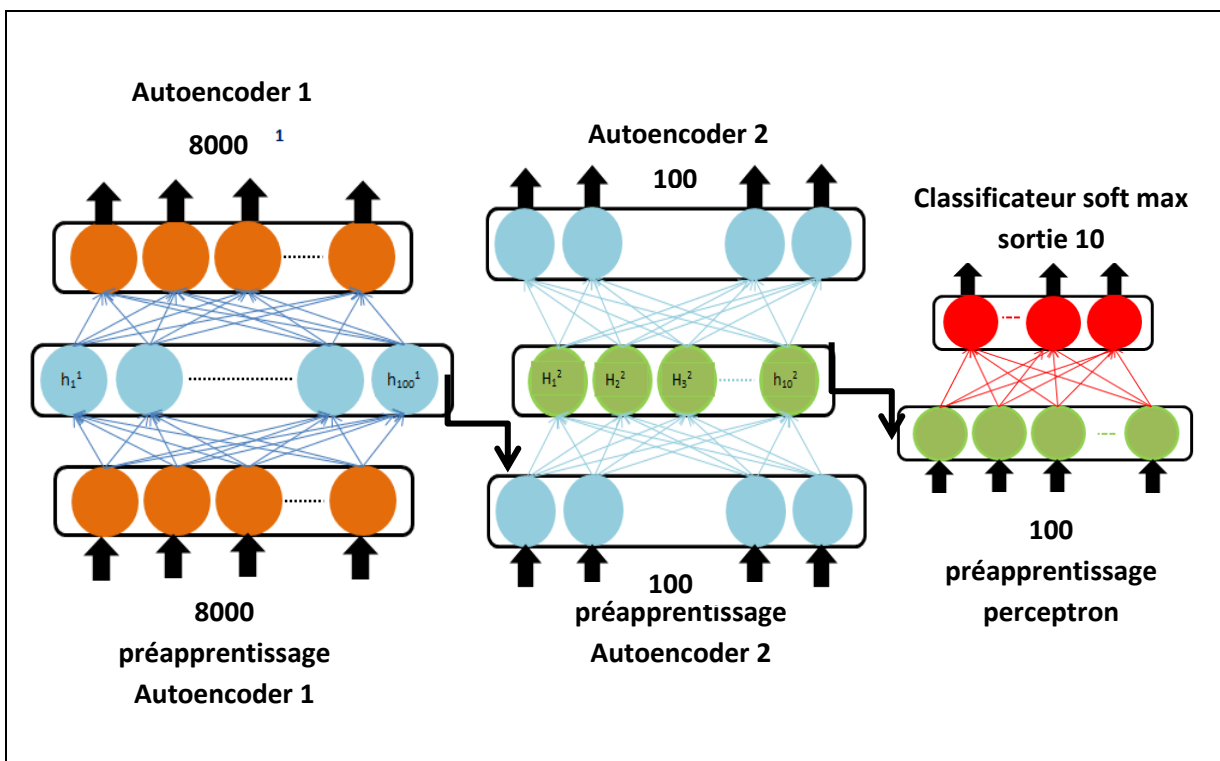


Figure 3.11 la structure de classification proposé basée sur deux stacked autoencoder

On constate que le premier autoencodeur contient 8000 entrées et sorties avec 100 neurones pour la couche cachée ensuite cette dernière sera l'entrée du deuxième autoencodeur et qui a une couche cachée contient 10 neurones laquelle sera l'entrée du perceptron, la figure 3.12 démontre cette configuration

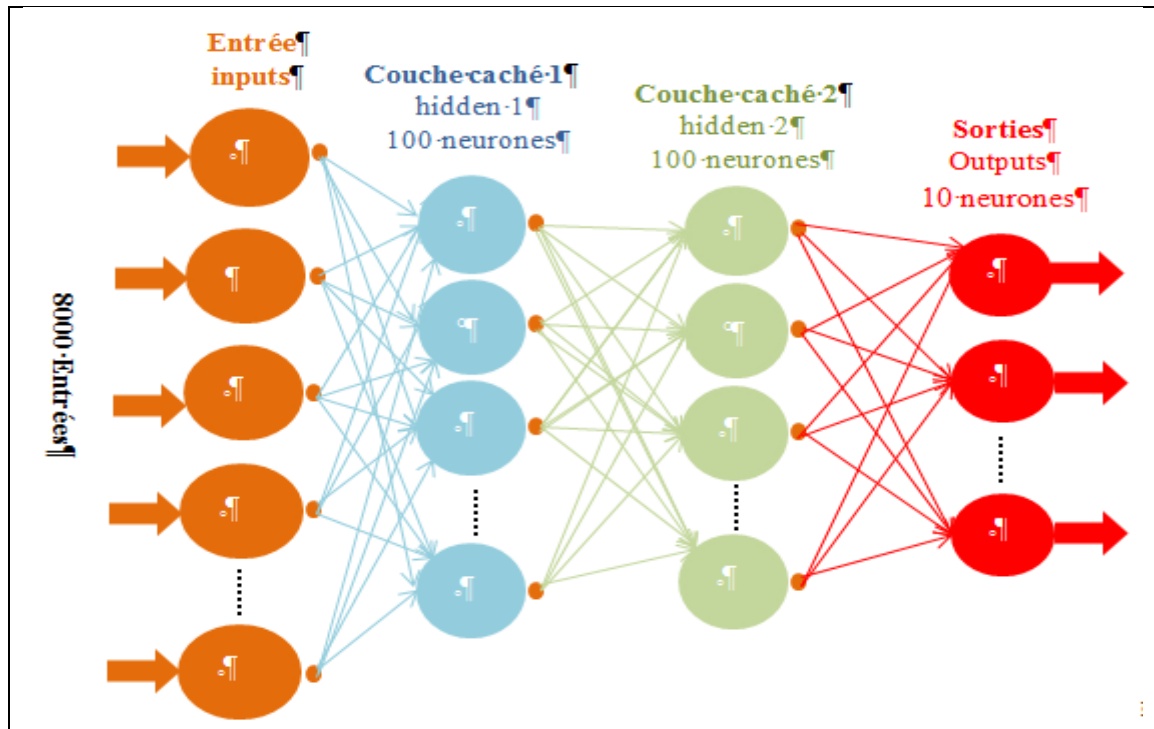


Figure 3.12 Configuration de deux stacked autoencoder

Le choix sera fait par une boucle de calcul afin de choisir les nombres de neurones convenable pour chaque couche pour obtenir une meilleure classification. La boucle est incrémentée par 10 neurones pour chaque étape et dans chaque cas, nous allons calculer et comparer les taux des classifications obtenus. Nous allons effectuer un test dont l'objectif est de déterminer le nombre de neurones qu'il faut utiliser dans le premier et le deuxième autoencodeur. A la fin de l'exécution de l'algorithme d'évaluation d'un autoencodeur empilé (avec deux autoencodeurs), on a réalisé les tableaux ci-dessous qui contiennent les résultats obtenus

|                                        |     | nombre de neurone de l'auto encodeur 1 |       |     |       |     |     |     |     |     |     |
|----------------------------------------|-----|----------------------------------------|-------|-----|-------|-----|-----|-----|-----|-----|-----|
|                                        |     | 10                                     | 20    | 30  | 40    | 50  | 60  | 70  | 80  | 90  | 100 |
| nombre de neurone de l'auto encodeur 2 | 10  | 90                                     | 86,66 | 90  | 93,33 | 100 | 100 | 90  | 90  | 90  | 90  |
|                                        | 20  | 96,66                                  | 100   | 90  | 93,33 | 100 | 100 | 90  | 90  | 90  | 90  |
|                                        | 30  | 100                                    | 100   | 90  | 96,66 | 100 | 100 | 100 | 90  | 100 | 100 |
|                                        | 40  | 100                                    | 100   | 90  | 93,33 | 90  | 100 | 100 | 90  | 100 | 100 |
|                                        | 50  | 100                                    | 100   | 100 | 100   | 100 | 100 | 100 | 90  | 100 | 100 |
|                                        | 60  | 100                                    | 100   | 100 | 96,66 | 100 | 100 | 100 | 90  | 100 | 100 |
|                                        | 70  | 100                                    | 100   | 100 | 100   | 90  | 90  | 100 | 90  | 100 | 100 |
|                                        | 80  | 100                                    | 100   | 90  | 96,66 | 100 | 100 | 100 | 90  | 100 | 100 |
|                                        | 90  | 100                                    | 100   | 90  | 96,66 | 100 | 100 | 100 | 100 | 100 | 100 |
|                                        | 100 | 100                                    | 100   | 100 | 96,66 | 100 | 100 | 100 | 90  | 100 | 100 |

Tableau 3.1 les taux de classification pour la base d'apprentissage en fonction de nombre de neurone

## Résultats et discussion

D'après le tableau ci-dessus, le meilleur taux de classification est de 100% ce qui implique que la phase d'apprentissage à atteindre le taux de classification maximal.

|                                       |     | nombre de neurone de l'auto encoder 1 |    |    |    |    |    |    |    |    |     |
|---------------------------------------|-----|---------------------------------------|----|----|----|----|----|----|----|----|-----|
|                                       |     | 10                                    | 20 | 30 | 40 | 50 | 60 | 70 | 80 | 90 | 100 |
| nombre de neurone de l'auto encoder 2 | 10  | 60                                    | 50 | 45 | 45 | 70 | 60 | 50 | 65 | 70 | 60  |
|                                       | 20  | 55                                    | 35 | 45 | 35 | 80 | 70 | 60 | 55 | 70 | 70  |
|                                       | 30  | 40                                    | 40 | 55 | 50 | 70 | 65 | 85 | 50 | 75 | 80  |
|                                       | 40  | 40                                    | 55 | 65 | 30 | 55 | 65 | 70 | 40 | 75 | 80  |
|                                       | 50  | 60                                    | 50 | 55 | 55 | 70 | 65 | 90 | 50 | 85 | 80  |
|                                       | 60  | 55                                    | 60 | 65 | 50 | 75 | 65 | 90 | 55 | 75 | 80  |
|                                       | 70  | 40                                    | 50 | 75 | 35 | 60 | 45 | 90 | 50 | 85 | 85  |
|                                       | 80  | 80                                    | 50 | 40 | 55 | 70 | 65 | 80 | 50 | 85 | 80  |
|                                       | 90  | 80                                    | 50 | 45 | 60 | 70 | 55 | 80 | 75 | 80 | 80  |
|                                       | 100 | 55                                    | 60 | 45 | 55 | 60 | 55 | 75 | 45 | 90 | 80  |

Tableau. Les taux de classification pour la base de test en fonction de nombre de neurone

D'après le tableau ci-dessus, le meilleur taux de classification est de 90% au nombre de neurone 70 et 90 pour le premier autoencodeur, et au nombre 50,60 et 70 pour le deuxième autoencodeur. alors on va opter 70 neurone de la couche cachée pour le 1<sup>er</sup> autoencodeur et on choisit 50 pour le 2<sup>ème</sup> autoencodeur. pour atteindre les meilleurs résultats en temps d'exécution réduit.

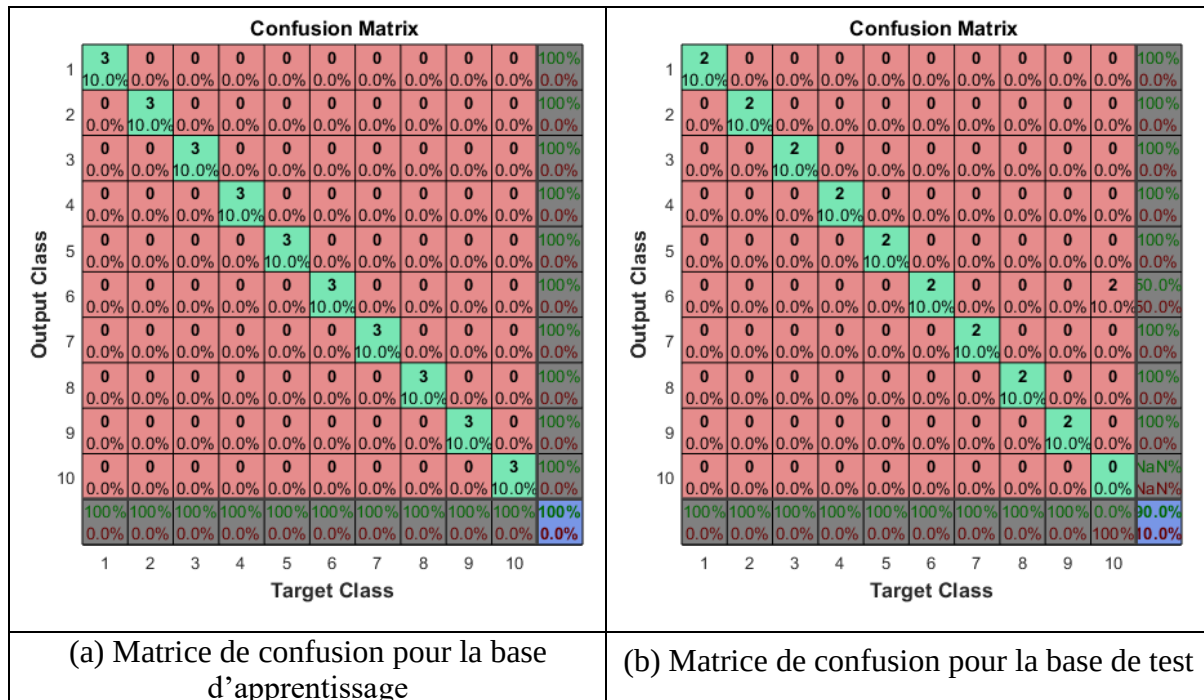


Figure 3.13 Les matrices de confusion résultantes

La figure 3.13 présente la matrice de confusion pour la base d'apprentissage et la base de test, on remarque une classification de taux de 100% dans la base d'apprentissage; ce qui montre que l'apprentissage soit efficace. D'autre part, la matrice de confusion de la base de test

présente un taux de 90% de classification coïncidée avec le résultat dans le test passé quand on a utilisé un seul autoencoder.

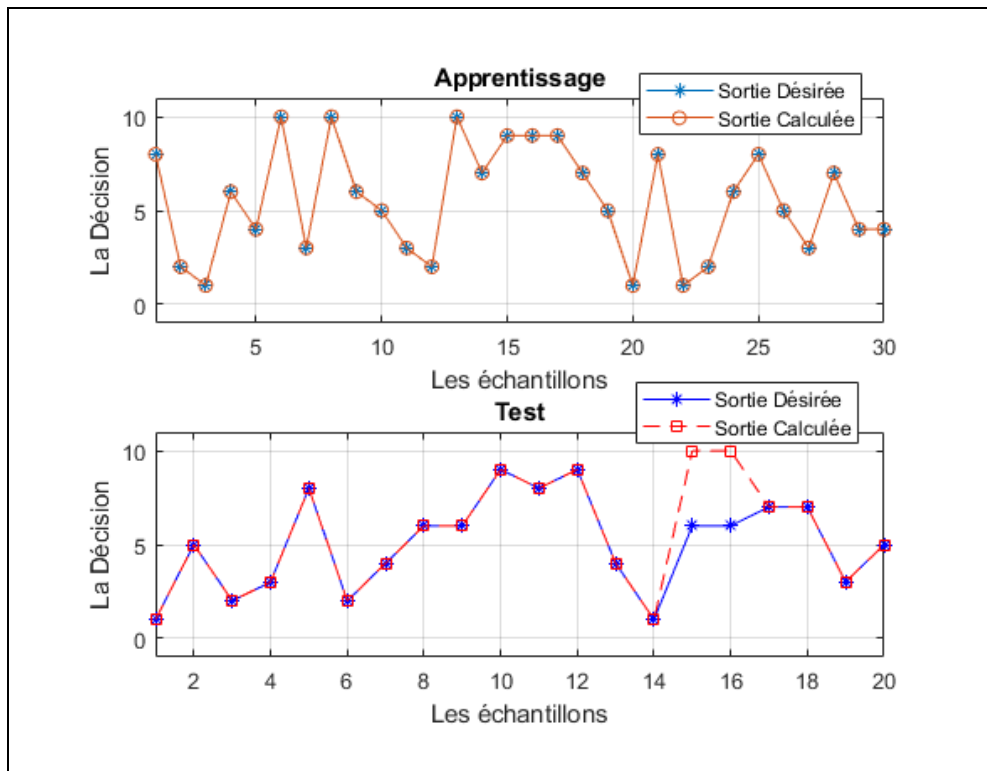


Figure 3.14 Sorties de l'apprentissage et du test de l'autoencoder empilé comparées avec les sorties désirées.

La figure 3.14 représente une précision importante pour les sorties désirés de l'apprentissage avec les sorties de l'autoencoder empilé (les sorties sont entièrement identiques), et une précision considérable pour les sorties désirés de test avec la sortie de l'autoencoder empilé(les sorties sont partiellement identiques)

Comparant avec les résultats obtenus par les deux tests ; on préfère d'utiliser le stacked autoencoder avec deux autoencoders (deux couches cachées) puisqu'il nous a donné de meilleur résultats en terme de performance et du temps d'exécution car notre objectif toujours c'est d'augmenter les performances et de diminuer le temps d'exécution.

Finalement, d'après ces résultats, le système d'identification par la modalité FKP est un système fiable. Il permet une bonne séparabilité des classes clients et imposteurs. Nous considérons les résultats obtenus comme satisfaisants. L'ensemble des tests effectués a permis de conclure, qu'avec l'utilisation du stacked autoencoder on peut réaliser un système biométrique robuste, efficace et avec une haute performance.

### 3.7. Conclusion

Dans ce chapitre, nous avons présenté et étudié en simulation l'une des apprentissages machine c'est l'auto-encodeur. Ce modèle d'apprentissage est appliqué dans le domaine de la biométrie qui est efficace dans l'aspect sécuritaire et la reconnaissance automatique des personnes à l'aide de la modalité FKP concerné dans notre travail. Cette étude a permis la validation et l'évaluation des performances de la technique présentée.

## Conclusion générale

Dans le domaine de la biométrie, et l'apprentissage automatique, la classification d'images de ces dernières est une tâche importante, de bien que les capacités des activités réalisées dans le domaine de classification des images soient nombreuses, aucune méthode n'est jugée faible à 100%, mais au fur et à mesure les nouveaux travaux essayent d'améliorer les. C'est dans ce cadre que s'inscrit notre travail, qui a pour objectif de proposer une technique qui réalise l'identification de personnes par leurs empreintes de l'articulation de doigt FKP. Dans cette thèse nous avons introduit les concepts généraux de la biométrie en détaillant son architecture ainsi que son principe de fonctionnement et nous avons présenté quelques modalités biométrique ensuite Nous avons également abordé les méthodes d'extraction des caractéristiques basées sur la texture. Nos tests sur la base des données d'empreinte de FKP de IITD à Delhi ont montré que notre méthode pouvait fournir d'excellents résultats en termes de taux de reconnaissance et de séparation globale des distributions des imposteurs et clients. Pour réaliser notre travail de classification on a utilisé le deep learning, la méthode d'apprentissage qui a boosté ses performances ces dernières années et nous avons choisi la technique d'apprentissage avec l'autoencodeur comme méthode de classification, ce choix est justifié par la simplicité et l'efficacité de ce système. Le résultat obtenu lors de la phase de test confirme l'efficacité de notre approche.

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

Le travail présenté dans ce mémoire s'inscrit dans le contexte de l'identification automatique des personnes basée sur leurs descripteurs biométriques. Nous avons utilisé une nouvelle modalité biométrique, à savoir l'empreinte des articulations des doigts,

# Bibliographie

- [1] BETAOUAF Talib Hichem « Caractérisation de la rétine pour la reconnaissance biométrique des personnes » mémoire de master Université Aboubakr Belkaïd Tlemcen 2011
- [2] D. Maltoni, D. Maio, A.K. Jain, S. Prabhakar, « Handbook of Fingerprint Recognition », Springer, p. 340, 2005.
- [3] F. Perronnin, J.-L. Dugelay, « Introduction à la Biométrie - Authentification des Individus par Traitement Audio-Vidéo », Revue Traitement du Signal, vol. 19, no. 4, 2002.
- [4] GREGORY Peter And SIMON Michael A., « Biometrics For Dummies », Cisa, Cissp, 2008.
- [5] A.K. Jain, L. Hong and S. Pankanti, « Biometrics: Promising Frontiers for Emerging Identification Market », Comm. ACM, pp. 91-98, February. 2000.
- [6] J.-L. Dugelay et al., « Recent Advances in Biometric Person Authentication » , IEEE Int. Conf. on Acoustics Speech and Signal Processing (ICASSP), Orlando, Florida, May 2002.
- [7] International Biometric Group, home page: [www.biometricgroup.com](http://www.biometricgroup.com)
- [8] Aiello L, Gardner T, King G, Blankenship G, Cavallerano J, Ferris F, Klein R. « *Diabetic Retinopathy* »Diabetes Care 1(21):143–156, 1998.
- [9] HADJAR Ahmed « Identification des individus par la biométrie multimodale » mémoire de magister université des sciences et de la technologie d'Oran Mohamed Boudiaf, 2014
- [10] DIB Soumeia. « Identification des individus par les techniques multimodales : application sur les images du visage ». Mémoire de magistère en informatique, Juin 2015
- [11] KHELLAT-KIHEL Badra. « Sécurisation des réseaux WIFI par authentification biométrique par empreinte digitale ». Mémoire d'ingéniorat en informatique, Juin 2009.
- [12] Bruce E. KOENIG "Spectrographic voice identification: A forensic survey", FBI, Engineering section, Technical Service Division, 1986
- [13] ASHBOURN Julian , « Guide To Biometrics For Large-Scale Systems », Springer 2011.
- [14] P. Meenen, R. Adhami, « Fingerprinting for Security », IEEE potentials, vol. 20, n°3, p. 33-38, 2001.
- [15] R. Chellappa, C. Wilson, S. Sirohey, « Human and Machine Recognition of Faces: A Survey », Proceedings of IEEE, vol. 83, p.705-740, 1995.
- [16] W. Zhao, R. Chellappa, A. Rosenfeld, P. Phillips, « Face Recognition: A Literature Survey », UMD CAR-TR, 2000.
- [17] EL-ABED Mohamad. « Evaluation de système biométrique Cryptographie et sécurité » thèse de doctorat Université de Caen, 2011. Français.
- [18] BENCHENNANE Ibtiham « Etude et mise au point d'un procédé biométrique multimodale pour la reconnaissance des individus » thèse de doctorat Université des Sciences et de la Technologie d'Oran Mohamed Boudiaf (2016).

- [19] A.K.Jain,R.Arun, P.Salil, « An Introduction to Biometric Recognition », IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics, vol. 14, p. 1, 2004.
- [20] Hightech concept « la technologie a porté de main ».
- [21] <https://www.biometrie-online.net/biometrie/le-marche>.
- [22]<https://iatranshumanisme.com/2016/12/19/le-marche-de-la-biometrie-militaire-augmentera-de-plus-de-7-du-taux-croissance-annuel-cagr-jusquen-2020/>.
- [23] BOUDJELLAL Sofiane « Détection et identification de personne par méthode biométrique » mémoire de magister Université Mouloud Mammeri de TIZI-OUZOU UMMTO.
- [24] BENAGGA Abderahmane , TELIB Lina « Reconnaissance des personnes basée sur l’empreinte de l’articulation de doigt » mémoire de master université KASDI MERBAH OUARGLA 2016.
- [25] BENOUAER Soumia, TAHRINE Aichouche. « Système biométrique basé sur les motifs locaux binaires orientés (LBP<sup>0</sup>) ».université Kasdi merbah Ouargla, 2016.
- [26] OUAMANE Abdelmalik « Reconnaissance Biométrique par Fusion Multimodale du Visage 2D et 3D » Thèse de doctorat.Université Mohamed Khider, biskra 2015.
- [27] GHACHOUA Abdelatif, KAHLAOUI Ibrahim. « Reconnaissance de personnes en utilisant L’empreintes Palmaires multi spectral basés sur L’apprentissage approfondi. Ouargla » : Mémoire master académique.université Kasdi Merbah , 2016.
- [28] <https://www.math.univ-toulouse.fr/~besse/Wikistat/pdf/st-m-Intro-ApprentStat.pdf>.
- [29] BRIK Youcef « Reconnaissance des chiffres Manuscrits par les Modèles de Markov Cachés Continus » mémoire de magister université des sciences et de la technologie Houari Boumediene 2010.
- [30] THONG William « apprentissage de représentations pour la classification d’images biomédicales » université de Montréal (2015.).
- [31] MOKRI Mohammed Zakaria « Classification des images avec les réseaux de neurones convolutionnels » mémoire de master Université Abou Bakr Belkaid Tlemcen 2017
- [32] <https://hal.archives-ouvertes.fr/hal-01561518/document>.
- [33] Z. Yu, M. Y. Nam, S. Sedai, and P. K. Rhee. « Evolutionary Fusion of a Multi-Classifier System for Efficient Face Recognition ». International Journal of Control, Automation, and Systems, vol. 7, no. 1, pp. 33-40. 2009.
- [34] X. Zhang, D. Liu, and J. Chen. « An Illumination Independent Face Verification Based on Gabor Wavelet and Supported Vector Machine ». Communications in Computer and Information Science, vol. 15, pp. 153-160, 2008.
- [35] Z. S. Zhao, J. Z. Wang, Q. J. Tian, J. M. Zhou. « Classifier Fusion of Improved Laplacianfaces ». IEEE Proceedings of the Ninth International Conference on Machine Learning and Cybernetics, Qingdao, pp. 11-14 July 2010.

- [36] MOULAY Brahim Oussama , ARBAOUI Mohamed Ibrahim « Identification des personnes par les articulations des doigts » mémoire de master université Kasdi Merbah Ouargla 2015.
- [37] L. Allano, « La Biométrie multimodale : stratégies de fusion de scores et mesures de dépendance appliquées aux bases de personnes virtuelles », Thèse de doctorat, Université d'Evry Val d'Essonne, 2009.
- [38] P. Verlinde. « A contribution to multi-modal identity verification using decision fusion. PhD thesis », Ecole Nationale des Télécommunications France, 1999.
- [39] [http://www4.comp.polyu.edu.hk/~csajaykr/IITD/iitd\\_knuckle.htm](http://www4.comp.polyu.edu.hk/~csajaykr/IITD/iitd_knuckle.htm).
- [40] ATTALLAH Bilal « Conception d'un système de Reconnaissance des empreintes digitales par apprentissage » mémoire magister université des sciences et de la technologie d'Oran Mohammed Boudiaf.2012
- [41] ISO/IEC 19795-1. Information technology – biometric performance testing and reporting part 1 : Principles and framework, 2006.
- [42] <https://www.lebigdata.fr/confusion-matrix-definition>.

# Abstract

In recent years, automatic personal identification is becoming an important requirement for variety of applications such as access control, surveillance systems and physical buildings. Biometrics, which deals with the identification of individuals based on their physical or behavioral characteristics, has emerged as an effective automatic identification technology, which offers more properties and several advantages over traditional security. The finger knuckle print (FKP) is an important biometric feature. Which provides uniqueness, stability and high distinction ability. In our work we have used deep learning exploiting the autoencoder as being the image classification tool that is efficient in the sense of solving classification problems with complex data.

Our experimental results, using the FKP database (IITD DELHI) demonstrate the effectiveness of autoencoders for the realization of the high-performance identification system based on FKP.

**Key words:** biometrics, finger knuckle print FKP, deep learning, classification, autoencoder.

# Résumé

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 on a utilisé l'apprentissage profond (le deep learning) exploitant l'autoencoder comme étant l'outil de classification des images qui est efficace dans le sens de résolution des problèmes de classification avec des données complexes.

Nos résultats expérimentaux, en utilisant la base de données FKP (IITD DELHI) démontrent l'efficacité des autoencoders pour la réalisation du système performant d'identification sur la base FKP.

**Mots clés :** biométrie, l'empreinte de l'articulation de doigt FKP, apprentissage profond , classification ,autoencoder.