République Algérienne Démocratique et Populaire
Ministre de l'enseignement Supérieur et de la Recherche Scientifique

Université A/Mira de Béjaia
Faculté des Sciences Exactes
Département d'Informatique

MÉMOIRE DE MASTER

En

Informatique

Option

INTELLIGENCE ARTIFICIELLE

Thème

Techniques de detection d'usurpations des Empreintes Digitales

Présenté par : Mlle. Oulmou Kenza

Mlle. Nacef Lynda

Soutenu le juillet 2022 devant le jury composé de :

Président	**Dr K. Bedjou**	**Maître de conf**	**U. A/Mira Béjaia.**
Examinateur	**Dr A. Akilal**	**Maître de conf**	**U. A/Mira Béjaia.**
Rapporteur	**Dr M.Moktefi**	**Maître de conf**	**U. A/Mira Béjaia.**
Co-rapporteur	**Dr M.Khammari**	**Maître de conf**	**U. A/Mira Béjaia.**

Béjaia, Juillet 2022.

⁂ *Remerciements* ⁂

Nous remercions Allah qui nous a aidés à réaliser ce travail Nous remercions également notre encadreur Moketfi Mohand et Mohammed Khammari pour leur aide et les conseils concernant ce travail Nous tenons aussi à remercier les membres du jury pour avoir accepté d'examiner et d'évaluer ce travail.

Nous adressons aussi nos plus sincères remerciement a tous nos proches et nos parents et amies spécialement Bennia anis et bouaghani, qui nous on toujours soutenues et encouragées au cours de la réalisation de ce mémoire.

Pour terminer, nous remercient tous personne ayant participé de prés ou de loin pour la réalisation de ce travail

⁂ *Dédicaces* ⁂

Je dédie ce modeste travail A mes très chers parents pour leur soutient et encouragement durant toutes mes années d'études et sans lesquels je n'aurais jamais réussi.
A tout les membres de ma famille m grande sœur fatima mon frère tarik et ma petite sœur narimane. A tous mes amis Bennia anis boughani imad hocine sylia widad massilia ainsi qu'à toutes les personnes que j'ai connues, qui m'ont aidées, soutenues et encouragées.
A tous mes enseignants durant mes années d'études avec lesquels j'ai beaucoup appris.

M. ***Oulmou kenza***

⁂ *Dédicaces* ⁂

A tout respect et amour je dédie ce travail a mon très cher père, A ma très chère mère pour tous leurs sacrifices, leur amour, leur tendresse, leur soutien tout au long de mes études.
Ainsi qu'a mes deux frère nordine et wassim et bien sur a tous mes amis boughani youssra taous mylda amel.
À tous les professeurs et enseignants qui m'ont suivi durant tout mon cursus scolaire et qui m'ont permis de réussir dans mes études. A toutes mes familles a mes cousines et cousins à tous mes amies en témoignage de mon affection.

M. ***Nacef lynda***

Table des matières

Table des figures

Liste des tableaux

Introduction générale

Savoir déterminer de manière à la fois efficace et exacte l'identité d'un individu est devenu un problème critique dans notre société, de nos jours on parle de plus de l'insécurité dans divers secteurs ainsi que des moyens informatiques à mettre en œuvre pour contrer cette tendance. La biométrie possède des applications très intéressantes dans le domaine de la sécurité, elle permet en effet de s'assurer de l'identité d'une personne et de contrôler ainsi les accès aux lieux et données sensibles et s'impose de plus en plus comme alternative afin de remédier aux problèmes des méthodes précédentes, cette dernière est basée sur des caractéristiques propres à l'individu, qui ne peuvent être ni perdues, ni volées. De plus, en pratique il n'est pas assez évident d'imiter une caractéristique biométrique. En effet, bien que nous ne nous en rendions pas toujours compte, notre identité est vérifiée quotidiennement par de multiples organisations, chaque personne s'efforce d'assurer la sécurité de ses appareils électroniques, en raison des informations personnelles et sensibles qu'ils contiennent, beaucoup de technique son représentée pour protéger les ressources personnelles telle que l'apparition des empreinte digitales. L'empreinte digitale est l'une des plus utilisées systèmes d'authentification puisqu'ils garantissent une haute précision d'identification, rentable et applicable à d'énormes ensembles de données d'images. Cependant, ces systèmes ne sont pas à l'abri des attaques malveillantes attaques, parmi les techniques d'usurpation proposées afin de remédier à ce problème, nous citons la vivacité qui est utilisée pour identifier les empreintes authentiques. En raison de l'importance et les progrès récents dans les systèmes de reconnaissance basés sur les empreintes digitales, il devient nécessaire de détecter la vivacité du trait présenté car les intrus peuvent facilement contrefaire le système d'authentification en utilisant divers instruments de présentation, l'amélioration et le développement de la sécurité des systèmes est devenu nécessaire contre les attaques par usurpation, afin d'apporter cette technologie en émergence rapide dans une utilisation pratique plusieurs travaux et études ont mis en évidence la nécessité de développer des méthodes de protection efficaces contre les attaques par usurpation d'identité.

Dans la littérature, selon le type de caractéristiques extraites, les systèmes de reconnaissance d'empreintes digitales peuvent être divisés en deux approches principales : les systèmes basés sur les matérielles et les systèmes basés sur les logicielles. Dans la première catégorie, l'image d'empreinte digitale doit passer par plusieurs étapes de prétraitement pour extraire les minuties. Ces étapes sont : l'amélioration de la qualité de l'image de l'empreinte digitale, l'estimation locale de l'orientation de la crête, la binarisation, la squelettisation et la détection des minuties. Pour la deuxième catégorie, les caractéristiques globales ou locales sont extraites directement de l'image d'empreinte digitale sans aucun processus de prétraitement. Ce type de système de reconnaissance d'em-

preinte digitale est préféré dans le cas d'images de mauvaise qualité, car il est difficile d'extraire des ensembles de minuties fiables dans ce cas. Plusieurs descripteurs basés sur l'image pour la reconnaissance de l'empreinte digitale sont proposés dans la littérature. Ces descripteurs peuvent être regroupés en deux catégories principales. Les descripteurs de la première catégorie transforment l'image de l'empreinte digitale en un histogramme de taille fixe comme : Local Binary Pattern (LBP), filtre de Gabor avec le descripteur LBP (GLBP), Local Phase Quantization (LPQ). Dans la deuxième catégorie, l'image d'empreinte digitale est transformée en un vecteur de différentes caractéristiques

Dans l'étape de la classification, l'utilisation d'un ensemble réduit de caractéristiques par transformation nécessite une grande capacité de mémoire et plus de temps de calcul par rapport aux caractéristiques obtenues par les algorithmes de sélection. Ainsi, dans ce travail, nous avons considéré les algorithmes de sélection des caractéristiques pour sélectionner les bins d'histogrammes qui représentent les caractéristiques BSIF SWLD. Dans ce travail, nous avons appliqué la stratégie de sélection de code pour sélectionner les bins d'histogramme en utilisant plusieurs méthodes basées sur l'information mutuelle pour la reconnaissance d'empreintes digitales et avec plusieurs types de caractéristiques BSIF et SWLD. Notre objectif principal est donc de chercher une combinaison (type de caractéristiques/ méthode de sélection de caractéristiques) optimale pour la tâche d'identification des personnes par empreintes digitales.

Notre travail est organisé en quatre chapitres qui nous permettront de présenter les différents aspects de notre travail. Dans le premier chapitre, nous donnons des généralités sur la biométrie et les empreintes digitales et quelque méthode d'usurpation des empreintes digitales. Le deuxième chapitre quelque revue littérature sur les méthodes de caractérisation des empreintes digitale. Le troisième chapitre sera dédié à la présentation des étapes de prétraitement et celles d'extraction des caractéristiques de l'image de l'empreinte digitale en donnant une description des méthodes d'extraction des caractéristiques utilisées dans le présent travail Binarized Statistical Image Features (BSIF) et Simplified weber local descriptor (SWLD). Le quatrième chapitre dédie à décrire notre système de reconnaissance d'empreintes digitales développé et ces différentes étapes. Nous présentons aussi les résultats obtenus et la discussion. Premièrement, nous avons fait des expériences sur la base de données utilisée avec toutes les caractéristiques extraites sans sélection. Puis, nous avons appliqué les techniques de sélection des caractéristiques pour améliorer les performances du système en termes de taux de reconnaissance, Enfin, une conclusion générale résume les différents travaux effectués.

Chapitre 1

Généralités sur les techniques d'usurpation des empreintes digitales

1.1 Résume

Les empreintes digitales sont composées de lignes localement parallèles présentant des points singuliers (minuties) et constituent un motif unique, universel et permanent. Pour obtenir une image de l'empreinte d'un doigt, les avancées technologiques ont permis d'automatiser la tâche au moyen de capteurs intégrés, remplaçant ainsi l'utilisation classique de l'encre et du papier. Notre travail consiste à réaliser un système de détection d'usurpation des empreinte digitales. Précisément, deux composantes forment l'essence de notre travail. D'une part, nous avons utilisé les caractéristiques locales afin de bien décrire l'empreinte. D'autre part, nous exploitons les méthodes d'extraction des caractéristiques et on a choisie BSIF et SWLD d'un ensemble d'entraînement donné et l'avons encore adapté à notre effort de classification d'où on a utilisé le CNN pour chaque méthode afin d'augmenter nous donne et puis faire la classification avec le SVM.

mot clé : Biométrie, Empreintes digitales, Reconnaissance d'empreintes digitales, réseau de neurones, BSIF, SWLD, FCV Classification SVM.

1.2 Introduction

Au cours de la dernière décennie, il a été prouvé à maintes reprises qu'un système de vérification des empreintes digitales peut être trompé par de fausses empreintes digitales. Les empreintes digitales ne peuvent pas mentir, mais les menteurs peuvent faire des empreintes digitales », cette citation est attribuée à "Mark Twain", qui a raison dans de nombreuses occasions. La technologie se développe années après années et les gens deviennent également conviviaux avec la mise à niveau de la technologie. La détection de fausses empreintes digitales est une tâche difficile dans le secteur de la cybercriminalité dans n'importe quel pays développé. Des recherches récentes ont mis en évidence la vulnérabilité des systèmes biométriques aux « attaques frauduleuses », généralement réalisées en présentant un trait biométrique falsifié ou altéré au capteur, où une fausse empreinte digitale est utilisée pour contourner le système. Il n'est pas difficile maintenant un jour de trouver des directives détaillées sur la façon de créer une empreinte digitale usurpée sur les systèmes biométriques. Pour ces raisons, l'empreinte digitale se démarque des traits biométriques concernant ses vulnérabilités aux attaques par usurpation d'identité. Différencier une empreinte digitale vivante d'une personne avec certaine autre source est appelée détection d'usurpation.

Les systèmes biométriques basés sur les empreintes digitales sont largement adoptés pour la reconnaissance des personnes dans de nombreuses applications nécessitant un haut niveau de sécurité. Cependant, les scanners d'empreintes digitales peuvent être facilement contournés en présentant de faux doigts. Les répliques d'empreintes digitales artificielles ou fausses empreintes digitales, permettent de contourner les systèmes de reconnaissance personnelle basés sur les empreintes digitales, en effet il existe plusieurs façons d'usurper un système biométrique, qu'on peut divisés en deux groupes principaux les attaque directes et indirectes. Le premier envisage la possibilité de générer des échantillons biométriques synthétiques agissant au niveau des capteurs en utilisant des matériaux peu coûteux tels que la gélatine ou le silicium et le second comprend des attaques qui nécessite différents niveaux de connaissances sur le système c'est-à-dire les éventuels liens faibles dans les canaux de communication au sein du système, diverses techniques de détection de faux ont été proposées, un système de détection devrait être en mesure de décider si l'élément placé sur le capteur est comparable ou non à un doigt vivant.

Ce chapitre est organisé de la manière suivante : la section 1 décrit le principe de la biométrie ainsi que ses modalités, la section 2 représente les caractéristiques des empreintes digitales et les différents capteurs utilisés pour les numériser, la section 3 comportent les différentes techniques d'usurpation et d'antiusurpations des empreintes digitales et pour finir la section 4 représentera le traitement d'image des empreintes digitales.

1.3 Contribution

Dans ce mémoire on a travaillé sur un algorithme qui traite les images des empreintes digitales et faire extraire un défaut ou plusieurs sur elles, et compare deux empreintes identiques avec un défaut. On a étudié trois axes principaux :

- Étude de l'empreinte digitale.
- Traitement de l'image d'empreintes.
- Les méthodes de détection de la vivacité des empreintes. Et on a finis par développer un code sur « python » pour détecter les fausses empreintes digitales.

1.4 Problématique

Dans le monde entier les empreintes digitales font partie de l'identification des individus par l'intégration des systèmes spécialisé basent sur des informations données, mais y'a-t-il pas des problèmes générer dans ces systèmes qui ne sont pas résoluble lors du traitement des empreintes digitales ? C'est pour ça on chercher si on va réussir à identifier l'empreinte choisie et détecter si l'empreinte est fausse ou pas.

1.5 Principe de la biometrie

1.5.1 Qu'est ce que la biométrie ?

Le mot biométrie est une traduction du mot anglais « biométrics » qui correspond en français à l'anthropométrie.

La biométrie est une mesure des caractéristiques biologiques pour l'identification ou l'authentification d'un individu à partir de certaines de ses caractéristiques : comportementales (exemple de la dynamique de frappe au clavier), physiques ou physiologiques (exemple de l'ADN). Cette technique est utilisée de plus en plus aujourd'hui pour établir la reconnaissance des personnes dans un grand nombre d'applications diverses. Il peut y avoir plusieurs types de caractéristiques, les unes plus fiables que d'autres, mais toutes doivent être infalsifiables et uniques pour pouvoir être représentatives d'un et un seul individu . [6].

1.5.2 Caracteristiques de la biométrie

Les caractéristiques physiologiques et/ou comportementales peuvent être utilisées comme un Identificateur biométrique pour reconnaître des personnes si et seulement si elle satisfait les conditions suivantes :

— **Universalité :** chaque personne possède l'attribut biométrique.

— **Distinction :** la caractéristique possédée est suffisamment différente entre deux personnes.

— **Permanence :** elle reste invariable pendant une période de temps.

— **Récupérable :** peut être mesurée quantitativement [13].

1.5.3 Modalités biométriques

Il existe plusieurs modalités biométriques utilisées dans divers secteur, On peut distinguer trois grandes catégories qui sont :

— **Modalités morphologiques :** Les modalités biométriques de cette catégorie sont les plus utilisées, elles sont basées sur les traits physiques qui sont uniques et permanents, cette catégorie regroupe l'empreinte digitale, l'empreinte palmaire, la géométrie de la main, l'iris, le visage, le réseaux veineux de la rétine, la géométrie de l'oreille, etc.

— **Modalités comportementales :** Les modalités biométriques comportementales sont basées sur l'analyse de certains comportements d'une personne, cette catégorie regroupe la reconnaissances vocale, dynamique de frappe de clavier, la signature manuscrite, l'analyse de la démarche, etc.
Elle reste encore assez peu utilisée mais dont l'usage à tendances à se développer.

— **Modalités biologiques :** La dernière catégorie consiste à l'étude des traces biologiques, elle regroupe des caractéristiques telles que les veines de la main, ADN, la thermographie faciales, l'odeur, le sang et le salive, etc. [43].

Le shema de la figure 1.1 montre ces differentes caracteristiques.

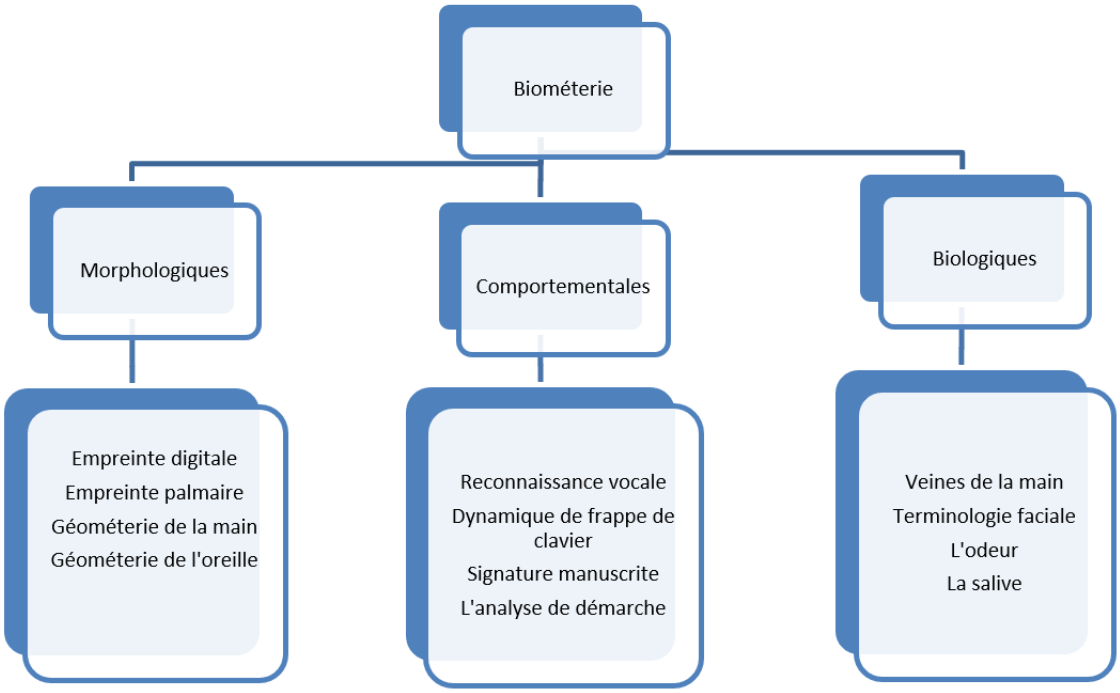

FIGURE 1.1 – Classification d'un certain nombre de modalités biométriques [43].

1.5.4 Qu'est ce que l'authentification ?

L'authentification consiste à indiquer l'entité, c'est, elle peut consister à valider des documents d'identité personnels ou encore à vérifier l'authenticité d'un site web à l'aide d'un certificat numérique.

L'authentification biométrique est un concept de sécurité des données. Les solutions d'authentification biométrique créent un modèle généré par les données qui représente l'individu. Avec ce modèle et ces informations biométriques, les systèmes de sécurité peuvent authentifier l'accès aux applications et aux autres ressources du réseau . [7].

1.5.5 Authentification biométrique digitale

Un système d'authentification de reconnaissance d'empreintes digitales est une chaîne de processus qui à partir du doigt d'un utilisateur en entrée renvoie un résultat en sortie, permettant ainsi à l utilisateur d accéder ou non à des éléments nécessitant une protection.

La réalisation d'un tel système a fait l'objet de très nombreuses recherches et des méthodes très différentes de traitement ont été proposées, mais ces systèmes répondent toujours à la même structure (Figure I-7). La première phase permet d obtenir une image de l'empreinte de l utilisateur (acquisition), laquelle va subir un prétraitement pour extraire l'information utile de l image (signature) suivi éventuellement d un traitement supplémentaire permettant d'éliminer de possibles fausses informations qui se seraient glissées entre temps dans la chaîne de traitement. Ensuite si l'utilisation du système consiste juste à créer une base de données (stockage) la signature est éventuellement compressée puis stockée dans la base de données au moyen d'une technique d'archivage (classification). Pour un système d'identification l'ensemble des empreintes présentes dans la base de données

pouvant correspondre à celle de l'utilisateur (modèle identique) sont désarchivées et comparées (appariement) une à une avec celle de l'utilisateur, si une éventuelle correspondance est trouvée des informations personnelles concernant l'utilisateur sont renvoyées par le système , la figure 1.2 représente l'architecture générale d'un système complet de reconnaissance d'empreintes. [48].

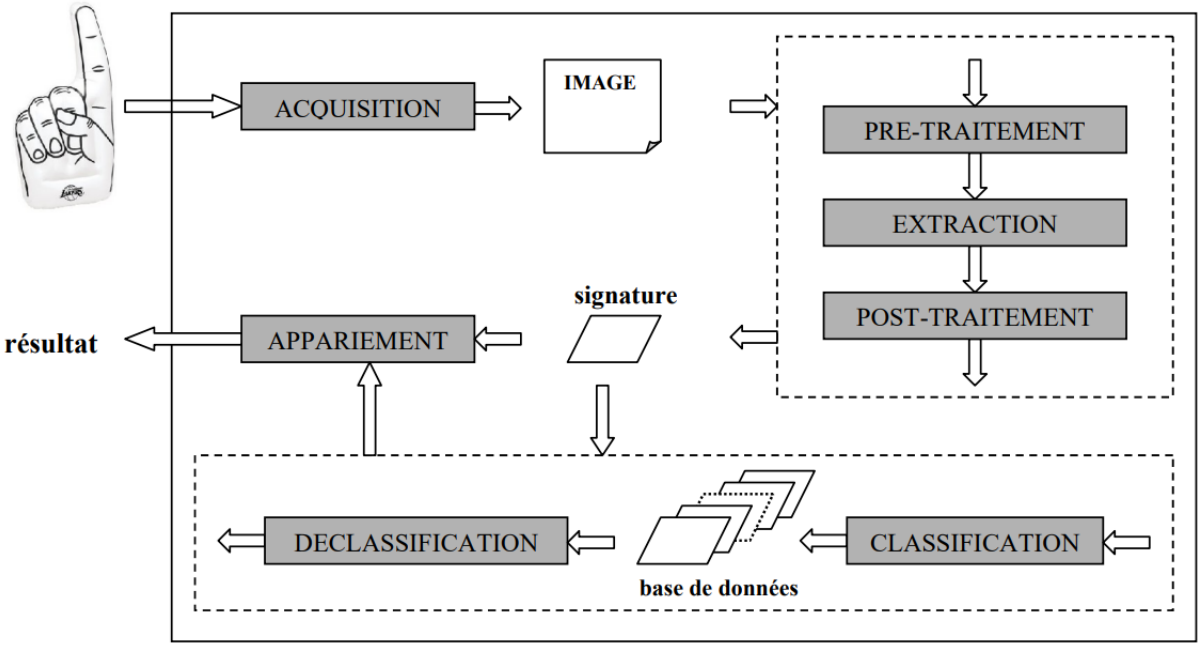

FIGURE 1.2 – Architecture générale d'un système complet de reconnaissance d'empreintes. [48].

1.6 Empreintes digitales

1.6.1 Définition d'une empreinte digitale

Une empreinte digitale ou dactylogramme est le dessin formé par un doigt sur un support suffisamment lisse pour qu'y restent marqués les dermatoglyphes.

Les empreintes digitales sont des motifs graphiques de crêtes et de vallées à la surface du bout des doigts, la fin de la crête et la bifurcation de la crête sont appelées minuties.

Chaque personne a une empreinte digitale unique de toute autre personne, L'identification des empreintes digitales est basée sur deux hypothèses de base Invariance et Singularité :

- **Invariance :** signifie que les caractéristiques des empreintes digitales ne changent pas tout au long de la vie.
- **Singularité :** signifie que l'empreinte digitale est unique et que deux personnes n'ont pas le même motif d'empreintes digitales .

Les empreintes digitales sont des motifs uniques, constitués de crêtes de friction (en relief) et de sillons (en retrait), qui apparaissent sur les coussinets des doigts et des pouces, les empreintes des paumes, des orteils et des pieds sont également uniques ; cependant, ceux-ci sont moins souvent utilisés pour l'identification.

Le motif d'empreintes digitales comme l'empreinte laissée lorsqu'un doigt encré est pressé sur du papier, est celui des crêtes de friction sur ce doigt particulier, les motifs de crêtes de friction sont regroupés en trois types distincts qui sont les boucles les verticilles et les arcs chacun avec des variations uniques, en fonction de la forme et de la relation des crêtes.

Le motif d'empreintes digitales avec lequel une personne est née est le motif d'empreintes digitales exact qu'elle aura toute sa vie, chaque modèle est distinct et le restera de la petite enfance à la vieillesse, la rareté des empreintes digitales individuelles et leur nature durable est également ce qui en fait d'excellents outils d'identification [14].

1.6.2 Caractéristiques d'une empreinte digitale

Les empreintes digitales sont les suggestions d'une impression des crêtes de friction de n'importe quelle partie d'une main humaine.

S'il est vrai que chaque empreinte digitale est différente de l'autre, il est également vrai que toutes les empreintes digitales ont des caractéristiques communes entre elles, ces caractéristiques communes rendent possible la classification des empreintes digitales.

Maltoni et al [40] ont classés les fonctions d'empreintes digitales en trois niveaux :

Fonctionnalités de niveau 1 :

telles que les crêtes, les noyaux et les deltas, figure 1.3 (a)

— **Les crêtes :** Sont en relief avec la peaux et représente des trace qui peuvent laisser des marques sur des supports du bout des doigts .

— **Les noyaux :** Le noyau est le point central du motif, le noyau est approximativement le centre de l'empreinte du doigt.

— **Les deltas :** Les deltas sont formés lorsqu'une crête bifurque et que deux bras de la crête bifurquant divergent ou lorsque deux crêtes adjacentes s'étendant côte à côte divergent, provoquant un espace intermédiaire dans lequel se trouve le motif.

Fonctionnalités de niveau 2 :

Concernent les détails, une minutie est un détail infime sur les crêtes d'une empreinte digitale, souvent la fin de crête ou la bifurcation, figure 1.3 (b)

— **Les munities :** Les minuties sont extraites à partir des deux empreintes digitales et stockées sous forme d'un ensemble de points dans le plan de deux dimensions.

Fonctionnalités de niveau 3 :

Sont des détails intra-ridge observables au niveau très fin, tels que contours des crêtes, pores sudoripares et les points, figure 1.3 (c)

— **Les pores sudoripares :** Situés le long des crêtes, ces pores exocrines secrètent en permanence de petites perles de sueur et il est impossible de ne pas laisser d'empreinte. La sueur est constituée d'environ 99 % d'eau, lorsqu'elle s'évapore elle laisse des traces de sels d'acides aminés et de graisses.

— **Point** C'est des Strie ponctuelle.

La figure 1.3 montre ces caractéristiques d'empreintes digitales

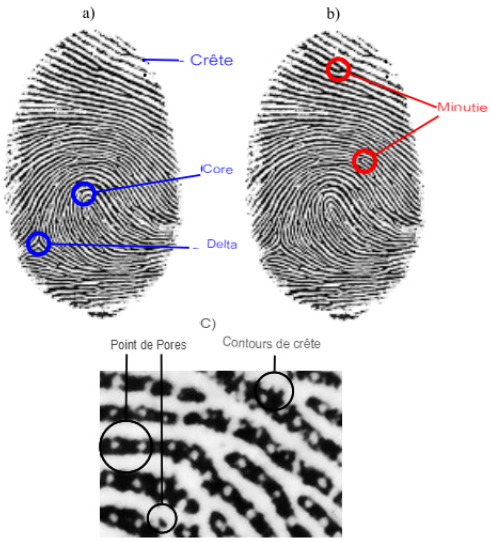

FIGURE 1.3 – Caractéristiques d'empreintes digitales [16].

—

1.6.3 Types d'empreintes digitales :

Après contact, les empreintes digitales peuvent rester sur une surface solide, y compris le corps humain, les empreintes digitales entrent dans l'une des trois catégories selon le type de surface sur laquelle elles se trouvent et si elles sont visibles ou invisibles :

— **Empreintes latentes :** Empreintes digitales invisibles faites de sueur et d'huile à la surface du corps humain.

— **Empreintes digitales en plastique :** Impressions tridimensionnelles faciles à voir sur des surfaces souples, y compris la cire et la peinture humide.

— **Empreintes du brevet :** Les empreintes se forment lorsque la saleté, le sang, l'encre, la peinture et d'autres liquides entrent en contact avec le bout des doigts, puis se transfèrent sur une surface solide, les empreintes digitales des brevets peuvent être vues à l'œil nu [46].

1.6.4 Représentations des empreintes digitales

Les empreintes digitales sont inaltérables, de la naissance à la mort de l'individu, elles subissent des transformations homothétiques ou des distorsions modélisables par des similitudes dues à la croissance, lorsque l'épiderme est altéré, celui-ci se régénère de façon identique.

Plusieurs représentations des empreintes digitales sont proposées, et elles sont classifiées dans deux types principaux caractérisée par le motif (représentations globales) et les points singuliers (représentations locales), généralement des représentations globales sont employées pour la classification d'empreinte digitale et des représentations locales sont employées pour la comparaison d'empreinte digitale [33].

A/Représentation globale :

Chaque empreinte digitale a un ensemble des points singuliers globaux qui sont les centres et les deltas. Le centre est le lieu de convergence des stries (il est aussi appelé le core), alors que le deltacorrespond au lieu de divergence.

La position et le nombre de ces points permettent la classification des empreintes digitales, c'est ainsi que Francis Galton les a subdivisées en trois grandes familles la figure 1.4 représente les différents types globales d'une empreinte digitale.

FIGURE 1.4 – Représentation des types globales d'une empreinte digitale [33].

— **Boucles (Loops) :** Une empreinte est de classe boucle si ses stries rentrent d'un côté et ressortent du même côté et si elle possède un point singulier de type boucle et un point singulier de type delta, les boucles représentent 65% des empreintes des doigts humains.

— **Spires (Whorls) :** Une empreinte appartient 'à la classe spire si elle possède au moins une strie qui fait 360◦, elle peut aussi contenir jusqu'a deux régions singulières de type boucles et deux régions singulières de type deltas, les spires représentent 30% des empreintes des doigts humains.

— **Arches (Archs) :** Une empreinte est de classe arche si elle possède des stries qui rentrent d'un côté et ressortent du côté opposé et si elle ne contient ni boucle ni delta comme points singuliers. Les arches ne représentent que 5% des empreintes des doigts humains.

B/Représentation locale :

Il s'agit des caractéristiques les plus utilisées "les minuties" (littéralement : petits détails), qui sont en fait les points d'irrégularités qui se trouvent sur les lignes capillaires.

Nous pouvons distinguer jusqu'à six types de minuties différentes, mais dans les algorithmes on ne s'en intéresse qu'aux deux types suivants parce qu'ils sont facilement détectables :

— **Bifurcation :** C'est le point où la strie se divise en deux.

— **Terminaison :** C'est le point où la strie s'arrête.

— **Ile :** Assimilée à deux terminaisons.

— **Lac :** Assimilée à deux bifurcations [33].

1.6.5 Scanners d'empreintes digitales

Le scanner d'empreinte digitales est un type de technologie qui identifie et authentifie les empreintes digitales d'un individu afin d'accorder ou de refuser l'accès à un système informatique ou à une installation physique.

Chaque type de scanner reconnaît les empreintes digitales à sa manière. Il existe de nombreux lecteur d'empreintes digitales aujourd'hui, voici quelques types de lecteurs d'empreintes digitales actuellement disponibles sur le marché :

— **Scanners optiques d'empreintes digitales :**

Les diodes électroluminescentes créent un échantillon numérique de l'empreinte digitale, lors de l'utilisation du terminal, l'employé place son doigt sur la zone de lecture, une image de l'empreinte digitale est ensuite enregistrée tandis que l'algorithme compare les séquences binaires au modèle binaire stocker, un exemple est montré dans la figure 1.5.

FIGURE 1.5 – Exemple d'un scanner optique d'empreinte digitale [41].

— **Scanners capacitifs d'empreintes digitales :**

Fonctionne de la même manière que les capteurs optiques, le motif numérique est généré par une tension électrique, contrairement au scanner optique, l'utilisateur passe son doigt sur la surface de numérisation, le système offre une excellente qualité d'image et permet une installation petite et compacte, un exemple est montré dans la figure 1.6.

FIGURE 1.6 – Exemple d'un scanner capacitif d'empreinte digitale [41].

— **Scanners d'empreintes digitales à ultrasons :**

Des ondes ultrasonores sont émises lorsque les doigts sont placés sur la surface, un motif spécifique du doigt est créé, permet de fixer le capteur sous la vitre de l'écran, le doigt n'a plus besoin d'être placé sur un point précis et limité, un exemple est montré dans la figure 1.7

FIGURE 1.7 – Exemple d'un scanner d'empreinte digitale à ultrason [41].

— **Scanners d'empreintes digitales thermiques :**

Les capteurs déterminent les différences de température minimales entre les lignes des doigts et génèrent une image thermique du doigt placé dessus, un exemple est montré dans la figure 1.8 [41].

FIGURE 1.8 – Exemple d'un scanner d'empreinte digitale thermique [41].

1.6.6 Avantages et inconvénients d'utilisation des empreintes digitales

La biométrie est l'un des meilleurs moyens d'identification, c'est un domaine émergeant où la technologie améliore notre capacité à identifier une personne, chaque être humain a sa propre empreinte unique qui peuvent être utilisés pour identifier les personnes à de nombreuses fins, de prévention de la fraude à résoudre des crimes.

Les empreintes digitales utilisées pour prendre manuellement avec de l'encre et des cartes , mais avec l'apparition des nouvelles technologie qui a fait informatisé les empreintes digitales de la méthode standard maintenant l'empreinte informatisé comporte des avantages et des inconvénients qui sont représentés par :

1.6.6.1 Avantages

— La technologie la plus utilisée et la plus acceptée par le grand public

— La taille du lecteur biométrique d'empreinte digital n'est pas volumineuse et le système reste très simple à mettre en place.

— Bon compromis entre le taux de faux rejet et le taux de fausse acceptation.

— L'utilisation est facile, il suffit de poser son doigt dessus.

— Traitement rapide.

1.6.6.2 Inconvénients

— Certaines personnes peuvent créer de "faux doigt" en utilisant l'empreinte digitale d'une autre personne (par moulage, utilisation de doigt coupé...).

— Difficulté de lecture : sensibilité aux altérations pouvant survenir au cours de la vie (égratignure, cicatrice, vieillissement ou autre) et à certaines variations (température, humidité, saleté).

— Manque d'hygiène, les traces de doigts se succèdent sur ce lecteur et ainsi les microbes se dispersent sur tout le lecteur ce qui rend celui-ci très sale.

— Besoin de la coopération de l'utilisateur (pose correcte du doigt sur le lecteur).

— Cette technologie est ressentie comme intrusive [47].

1.7 Méthodes basés sur la qualitées d'images

1.7.1 Reconnaissance d'une empreinte digitale

Le principe de la reconnaissance des empreintes digitales consiste à comparer une empreinte fournie au système, à une ou plusieurs autres empreintes (les templates) dont le système dispose préalablement dans sa base de données biométrique. Le système biométrique renvoie un résultat positif au cas où l'empreinte fournie à l'entrée correspond à l'une des templates, et un résultat négatif dans le cas contraire La structure d'un système de reconnaissance d'empreinte digitale est présentée dans la figure 1.9 [15].

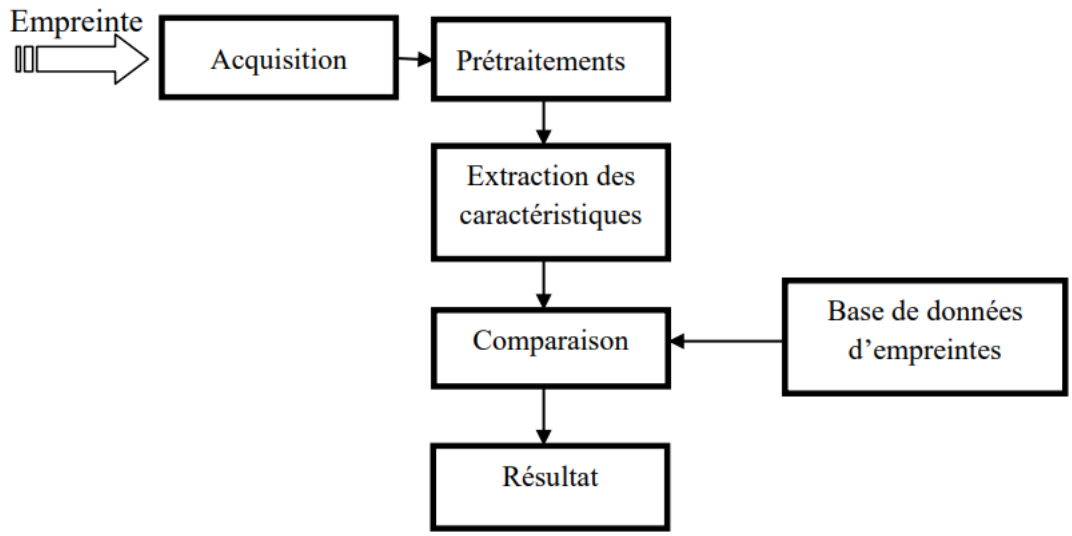

FIGURE 1.9 – Architecture générale d'un système de reconnaissance d'empreintes digitales [15].

Les détails de la reconnaissance des empreintes digitales sont généralement décomposés en trois niveaux distincts :

— **Niveau un :** Au premier niveau, le logiciel de reconnaissance d'empreintes digitales imagera les motifs d'empreintes digitales dans leur ensemble, plutôt que de mettre l'accent sur les spécificités de l'empreinte.

— **Niveau deux :** Les points minutieux de l'empreinte digitale sont rassemblés plus en détail, à partir desquels la majeure partie des caractéristiques uniques est extraite.

— **Niveau trois :** Cela inclut les formes et les images des crêtes et de leurs pores associés. Il s'agit du niveau le plus sophistiqué et le plus détaillé et il n'est généralement pas largement adopté dans les cas d'utilisation [36].

1.7.2 La texture des empreintes et leur description

L'analyse de la texture joue un rôle primordial dans le domaine de l'analyse et du traitement d'images, car les images traitées sont souvent formées des objets présentent à la fois un aspect textural et structurel. L'analyse de la texture d'image peut être trouvée dans de nombreuses applications du monde réel telles que la reconnaissance d'objets, l'analyse des images médicales pour aide au diagnostic et dans le domaine industriel pour le contrôle et la classification de qualité. La texture est considérée comme une variation spatiale d'intensités de pixels, ou d'une façon plus générale c'est la reproduction d'un motif de base dans plusieurs directions spatiales, ou la texture est une structure spatiale constituée par l'organisation des motifs (primitives) de base ayant chacune un aspect aléatoire. Elle est considérée comme un phénomène bidimensionnel : la description primitive de base à partir desquels sont formée la texture et la description des relations spatiales entre ces primitives. On distingue généralement deux types de texture tactile et optique. La texture tactile fait référence à la sensation tangible d'une surface et la texture visuelle fait référence à la forme ou au contenu de l'image d'une manière efficace et pertinente par le descripteur. Un processus de classification se fait généralement en deux phases :

Extraction des fonctionnalités : qui extraire les propriétés texturales. Le but est de créer un modèle pour chacune des textures qui existent dans la plate-forme de formation.

Classification : qui consiste à déterminer la classe de la texture de l'image à partir d'échantillon de test par un algorithme de classification.

Nous pouvons citer plusieurs méthodes d'extraction de caractéristiques mais on c'est basée sur les méthodes locales qui utilisent les descripteurs de texture locaux. La fonction du descripteur local est de convertir l'information au niveau du pixel en une forme utile qui capture le contenu le plus important mais insensible aux variations causées par l'environnement, ce qui révèle que ces approches sont les plus efficaces dans les conditions réelles. Pour les empreintes, ces méthodes sont basées sur les connaissances des crête et les arc et s'appuient généralement sur ses points caractéristiques (point singulier, etc.).

1.7.3 Quelques Filtres utilisées sur les images d'empreintes digitales

1.7.3.1 weber local descripteur

Weber local qui utilisent les descripteurs de texture locaux. La fonction du descripteur local est de convertir l'information au niveau du pixel en une forme utile qui capture le contenu le plus important mais insensible aux

variations causées par l'environnement, ce qui révèle que ces approches sont les plus efficaces dans les conditions réellesdescripteur (WLD) C'est un descripteur puissant et robuste récemment proposé pour la classification des textures, c'est à dire les informations des crêtes (ridges) et points singuliers globaux (delta et core) peu à peu prennent leur place dans le domaine de reconnaissance d'empreintes digitales, basée sur la loi de Weber qui définit la différence entre deux stimuliqui est :

I=k.log(S)

ou

I est l'intensité de la sensation

S la grandeur du stimulus

k une constante

Étant donné que la même différence entre un pixel central et les valeurs des pixels environnants peut être à peine distinguable dans une région de haute intensité et plus significative dans d'autres régions, cette différence est normalisée par rapport à l'intensité du pixel central lui-même. Il se compose de deux composantes, l'excitation différentielle et l'orientation, évaluées pour chaque pixel de l'image [10].

1.7.3.2 Modèle binaire locale (LBP)

l'opérateur LBP (en anglais : local binary pattern) est l'un des descripteurs d'analyse de texture les plus performants. Il a été proposé à la fin des années 90 par Ojala et al [4]. dans le but de caractériser la texture d'une image. Ses avantages se résument dans son invariance pour les changements monotones de l'intensité (niveaux de gris) et son efficacité de calcul . Le motif LBP est une mesure de texture invariante à l'échelle de gris. Son concept est simple, il propose d'assigner un code binaire à un pixel en fonction de son voisinage. Ce code est calculé par un seuillage d'un voisinage de 3*3 de chaque pixel avec le niveau de gris du pixel central. La Figure ci-joint présente le processus de calcul du code LBP. Afin de générer un motif binaire, tous les voisins prendront alors une valeur 1 si leur valeur est supérieure ou égale à la valeur du pixel central sinon le résultat est mis à zéro. Le code LBP du pixel central est ensuite obtenu en multipliant les résultats par des poids donnés par les puissances de deux (2^{poids}) et en les résumant ensemble. On obtient alors pour toute l'image, des pixels dont l'intensité se situe entre 0 et 255 comme dans une image à 8 bits ordinaire. On peut choisir comme descripteur de texture un histogramme de dimension 255. Le calcul des codes LBP peut être facilement effectué en un seul balayage à travers l'image. La valeur du code LBP d'un pixel (Xc, Yc) est donnée comme suit :

$LBP^{P,R}(X_c, Y_c) = \sum_{i=1}^{P} U(g_i^{P,R} - g_c)2^{i-1}$

Avec :

Xc et Yc : sont les coordonnées du pixel central.

Et g_i, g_c : sont respectivement les niveaux de gris d'un pixel voisin et du pixel central.

U : la fonction de seuillage qui est définie comme suit :

$$U = \begin{cases} 1 & \text{si} \quad Si > 0 \\ 0 & \text{sinon} \end{cases} \tag{1.1}$$

.

Les occurrences des codes LBP dans l'image sont collectées dans un histogramme. La classification est ensuite effectuée en calculant les similitudes d'histogramme. La notation (P, R) est généralement utilisée pour les voisinages de pixel pour se référer à P points d'échantillonnage sur un cercle de rayon R.

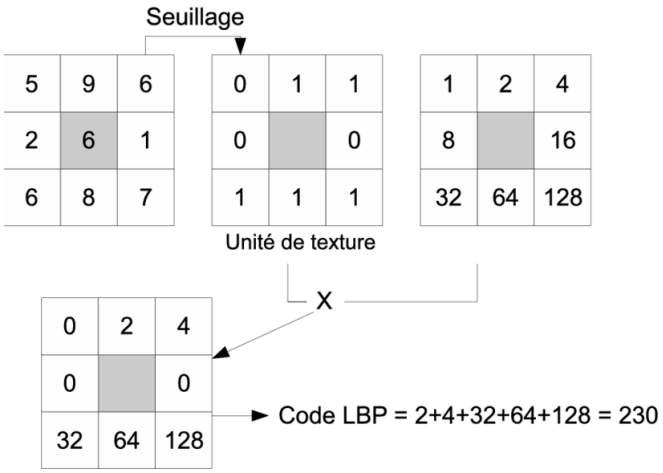

FIGURE 1.10 – Exemple de calcul de l'opérateur LBP appliqué à une image [29].

1.7.3.3 Descripteur binaire local de Weber (WLBP)

C'est un descripteur de texture qui combine efficacement les avantages de WLD et LBP. Plus précisément, WLBP se compose de deux composants : excitation différentielle et LBP. L'excitation différentielle extrait les caractéristiques de perception par la loi de Weber, tandis que le LBP (Local Binary Pattern) peut décrire à merveille les caractéristiques locales. En calculant les deux composantes, on obtient deux images : image d'excitation différentielle et image LBP, à partir desquelles un histogramme WLBP est construit [10].

1.7.3.4 Local Phase Quantization (LPQ)

La quantification de la phase locale ou le descripteur LPQ a été désigné pour la première fois par Ojansivu et Heikkilä pour l'utiliser dans la classification de textures pour les images floues. Il permet d'améliorer la classification de textures pour être robuste aux facteurs générés par le flou présent dans une image .[24]

Le descripteur de quantification de phase locale est basé sur la quantification de la phase de transformée de Fourier dans les voisinages locaux. La fréquence locale pourrait être calculée en utilisant une transformée de Fourier à court terme sur les locaux M × M, et le voisinage Np pour chaque pixel P de l'image définie par

$F(u,p) = \sum_{yNp} f(p-y)e^{-j2u^T y}$

La transformation est évaluée efficacement pour toutes les positions P=p1,p2,...pN lisant des convolutions 1-D pour les lignes et colonnes successivement. Dans LPQ, seuls quatre coefficients complexes sont considérés,

correspondant aux fréquences 2D $u_1 = [a, 0]^T, u_2 = [0, a]^T, u_3 = [a, a]^T, u_4 = [a, -a]^T$ ou est un scalaire suffisamment petit pour satisfaire $H(u_i) > 0$ soit : $F_p^c = [F(u_1, p), F(u_2, p), F(u_3, p), F(u_4, p)]$ et $F_p = [R_e$ F$_p^c)$,Im $F_p^c)]$

Ou R et Im la partie réelle et la partie imaginaire d'un nombre complexe, la correspondant matrice de transformation 8 par M2 est

$W = [R_e(w_u1, w_u2, w_u3, w_u4), Im(w_u1, w_u2, w_u3, w_u4)]^T$

alors $F_p = Wf_x$

Les informations de phase dans les coefficients de Fourier sont enregistrées en regardent les signes des partie réelles et imaginaires de chaque composant dans Fp cela se fait en utilisant un simple scalaire quantificateur.

$$U = \begin{cases} 1 & \text{si} \quad Si\ gj > 0 \\ 0 & \text{sinon} \end{cases} \tag{1.2}$$

.

Ou j et la composante du vecteur $G(P) = [R_e(F_p), Im(F_p)]$ les résultats des huit binaires coefficients qj sont représentés comme des valeurs entre 0-255 en utilisant le codage binaire $F_{LPQ}(P) = \sum_{j=1}^{8} q_j 2^{i-1}$

Et comme résultat en obtient l'image d'étiquette f dont les valeurs sont les étiquettes LPQ invariables de flou comme la indique l'image suivante.

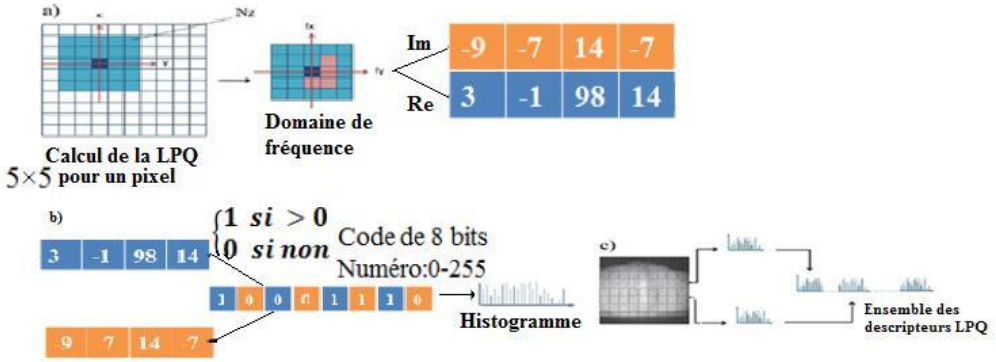

FIGURE 1.11 – Exemple de calcul de l'opérateur LPQ [34].

1.7.3.5 Caractéristiques des images statistiques binarisées (BSIF)

Le descripteur BSIF est inspiré par la méthodologie LBP et LPQ, c'est un code binaire pour chaque pixel est calculé en projetant linéairement des patchs locaux de l'image sur un sous-espace, dont les vecteurs de base sont appris à partir d'images naturelles par l'analyse en composantes indépendantes (Independent Component Analysis, ICA), en utilisant la binarisation des coordonnées dans cette base par le seuillage. L'objectif du descripteur BSIF est d'obtenir une représentation significative d'une image basée sur les caractéristiques statistiques [24].

1.7.4 Prétraitement d'une empreinte digitale

La reconnaissance d'une empreinte digitale est directement liée à la qualité de l'image obtenue au moyen du capteur. Ainsi dans la plupart des cas, un pré-traitement est nécessaire pour améliorer la qualité de l'image. Pour limiter les calculs des étapes suivantes du système l'image brute de l'empreinte est filtrée. Une opération de filtrage utilisant les caractéristiques locales de l'empreinte est ensuite appliquée à l'image de manière à améliorer sa qualité en éliminant le bruit [35]. Les algorithmes de reconnaissance des empreintes digitales sont sensibles

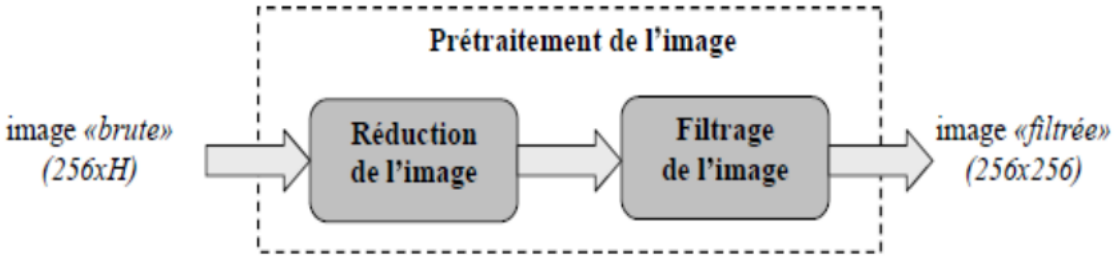

FIGURE 1.12 – Principe de prétrétement de l'image [35].

à la qualité des images d'empreintes digitales obtenue lors de l'acquisition. La qualité de ces images dépend de plusieurs facteurs comme

— Les substances parasites présentes sur le doigt (encre, graisse, saletés...).

— La personne (cicatrices, métiers manuels, âge....).

— L'environnement où se produit l'acquisition (température de l'air, degré d'humidité....).

— Les caractéristiques spécifiques du moyen d'acquisition utilisé.

— La profondeur de rides/vallée, etc

Alors l'étape de prétraitement est nécessaire avant d'effectuer les étapes suivantes. Typiquement le prétraitement peut se composer de lissage, segmentation et filtrage du domaine spatiale/ fréquence [21].

1.7.5 Extractions des caractéristiques d'empreintes digitales

La méthode la plus répandue consiste à extraire les minuties à partir d'un squelette de l'image. Comme le montre la figure 1.13 l'image est d'abord préparée à l'étape d'extraction au moyen d une binarisation et d'une squelettisation, ensuite un fichier signature est extrait de l'empreinte après la détection et l'extraction des minuties [35].

La plupart des systèmes de reconnaissance des empreintes digitales emploient des minuties comme caractéristiques des empreintes digitales. Alors cette partie présentera les méthodes pour extraire des minuties à partir des empreintes digitales. Un extracteur de minuties cherche des terminaisons de stries et des bifurcations dans les empreintes. Si les stries sont bien déterminées, alors l'extraction de minuties est une tâche relativement simple. Cependant, dans la pratique, il n'est pas toujours possible d'obtenir une carte parfaite de stries. Donc la

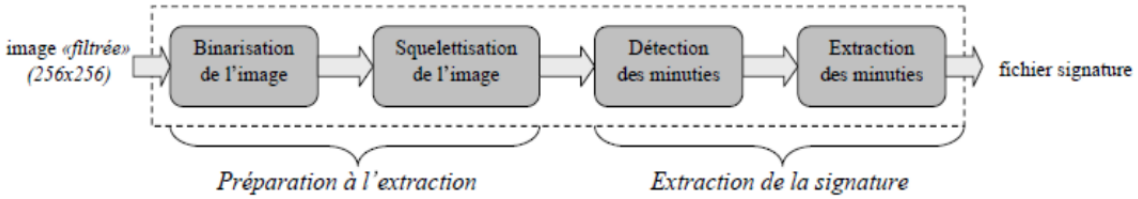

FIGURE 1.13 – Phase d'extraction de la signature [35].

performance des algorithmes d'extraction de minuties dépend fortement de la qualité des images des empreintes digitales d'entrée [28].

1.8 Usurpations des empreintes digitales

L'authentification biométrique est l'une des méthodes efficaces pour déverrouiller ou exécuter n'importe quel appareils intelligent dans l'environnement. Les vivants moments de l'individu ou toute information fonctionnelle sera détecté par l'ajout de détection de vivacité des empreintes digitales ou cette dernière est la solution pour l'usurpation des empreintes. [1]

1.8.1 Usurpation d'identité biométriques

L'usurpation d'identité est une méthode d'attaque des systèmes biométriques où des objets artificiels sont présentés à un système d'acquisition biométrique qui imite des caractéristiques comportementales.

Une attaque est la présence d'un article fabriqué ou d'un attribut humain dans un système biométrique, plusieurs attaques peuvent être imposées pour compromettre la sécurité d'un système, Ratha et al [37] ont décrit ces attaques comme le montre la Figure 1.14.

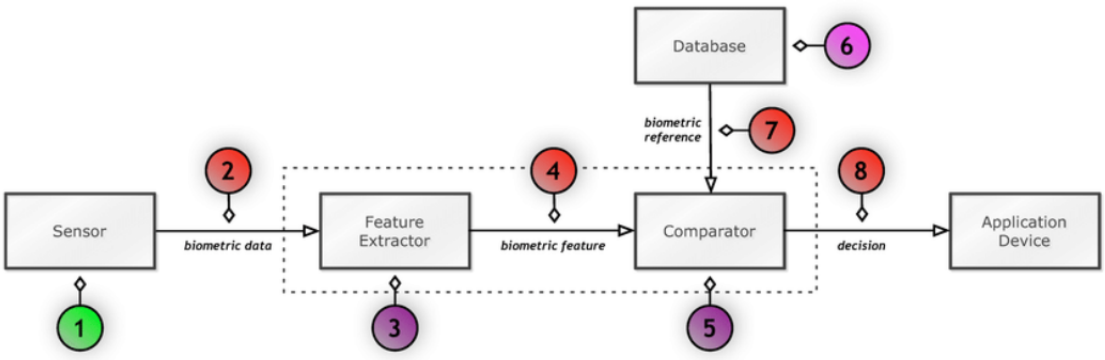

FIGURE 1.14 – Points d'attaque vulnérables dans un système biométrique [37].

1. Une reproduction de la modalité biométrique est présentée comme entrée du capteur.
2. Le capteur est contourné et les données biométriques précédemment stockées sont soumises à nouveau.

1. Matcher pour indiquer l'appariement de données et encore moins pour désigner des logiciels ou des bases de données.

3. L'extracteur de caractéristiques modifient les fonctionnalités.
4. Attaque et Remplacement des fonctionnalités.
5. Attaque contre le système d'appariement le Matcher.
6. Remplacement du modèle de base de données
7. Modification des données via le canal
8. Modification de la décision.

La reconnaissance d'empreintes digitales est une technique biométrique mature pour toute application d'authentification ou de vérification d'individus. Même si la reconnaissance des empreintes digitales est particulièrement sécurisée, aucun système biométrique n'est à l'abri d'une faille.

L'usurpation c'est un nouveau coup dur pour l'authentification par empreinte digitale, des études avaient déjà montré qu'il était possible de piéger les lecteurs avec un faux doigt, réalisés à partir de la simple photo d'une phalangette et un peu de colle à bois , d'où l'un des majeur technique présenté pour tromper un capteur est l'empreinte digitale artificielle.

1.8.2 Empreinte digitale artificielle

L'empreinte digitale artificielle connue sous le nom d'artefacts falsifiés et présentée à un capteur d'empreintes digitales pour tromper les systèmes de reconnaissances, elles sont utilisés pour vaincre les lecteurs biométriques.

Ces attaques représentent une préoccupation importante au niveau du monde, en mars 2013, un médecin brésilien a été accusé d'avoir utilisé de faux doigts pour enregistrer les collègues qui n'étaient pas présents sur le lieu de travail, en septembre 2013, quelques jours seulement après la sortie de l'iPhone 5S équipé du capteur d'empreintes digitales Touch ID libéré, un groupe allemand a annoncé que le capteur pouvait être trompé en utilisant une feuille de latex ou de la colle à bois hébergeant les crêtes des empreintes digitales d'une personne [42].

1.8.3 Méthodes d'usurpations d'empreintes digitales

On distingue deux méthodes d'usurpations coopératives et non coopératives representés par le shema de la figure 1.15 :

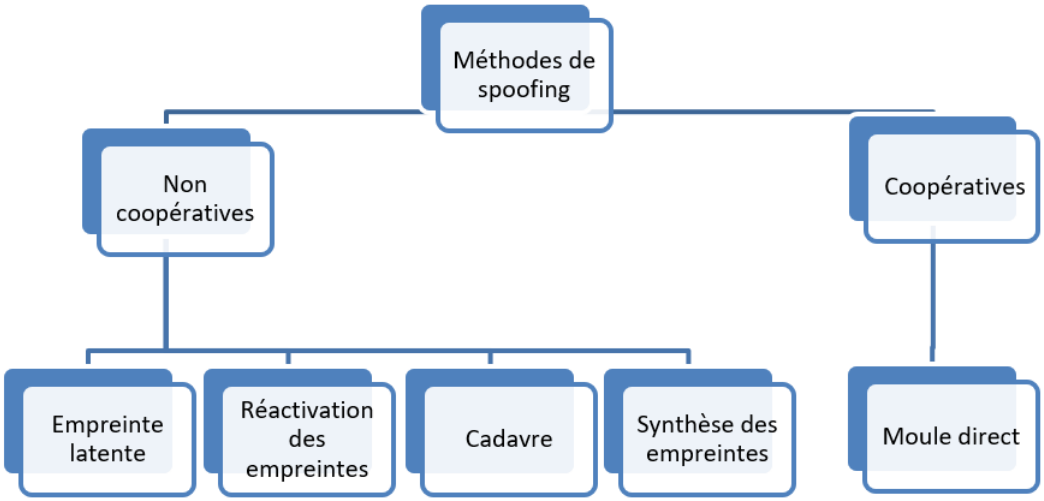

FIGURE 1.15 – Schéma illustrant les différentes méthodes d'usurpation d'empreinte digital [1].

1.8.3.1 Usurpation coopérative

Dans l'usurpation d'identité coopérative les empreintes digitales artificielles sont généralement faites de matériaux qui peuvent être scannés par les scanners d'empreintes digitales commerciaux existants, des articles comme Play-Doh et de l'argile sont de bons matériaux en raison de leur texture à base d'humidité, un attaquant qui souhaite fabriquer une empreinte digitale artificielle doit disposer d'une représentation de l'empreinte originale.

L'usurpation est formée à l'aide d'un moule à doigt vivant le doigt est pressé sur une surface et l'impression négative de l'empreinte digitale est fixée et le moule est pris. Le moule est ensuite rempli d'un matériau à base d'humidité et une parodie est formée, la figure 1.16 montre un exemple d'une réalisation d'une empreinte digitale artificielle directement à partir d'un doigt vivant [1].

FIGURE 1.16 – Réalisation d'une empreinte digitale artificielle directement à partir d'un doigt vivant [1].

1.8.3.2 Usurpation non coopérative

Il existe quatre types d'usurpation d'identité non coopérative qui sont :

— **Empreinte digitale latente :**

Ce sont les impressions qui sont produites par la peau rigide connue sous le nom de crêtes de frottement sur le doigt humain, ce sont les marques laissées dans la zone et peuvent ne pas être visibles à l'œil nu. Pour les flasher, la surface sur laquelle est laissée l'empreinte digitale est poudrée au pinceau, La poudre de fond est retirée et l'impression soulevée est placée sur le capteur et exposée à la lumière [17].

— **Réactivation des empreintes digitales :**

Dans cette méthode, la poudre de graphite est brossée sur le capteur où l'empreinte latente déposée sur le capteur est réactivée.

— **Cadavre :**

Dans cette méthode ces les doits morts qui sont utilisées pour l'usurpation.

— **Synthèse des empreintes digitales :**

Dans cette méthode, l'image de l'empreinte digitale est reconstruite à l'aide de modèles, tels que des points de minuties sur l'empreinte digitale après ça une image numérique est capturée et transférée à l'artefact d'usurpation [20].

1.8.4 Techniques anti-usurpations d'empreintes digitales

Il existe plusieurs types de techniques anti-usurpation qui pourraient être utilisées pour rendre plus difficile l'usurpation d'un système.

Elles sont généralement divisées en deux grandes catégories la première se base sur le matériel et la deuxième sur les logiciels representés par le shema de la figure 1.17.

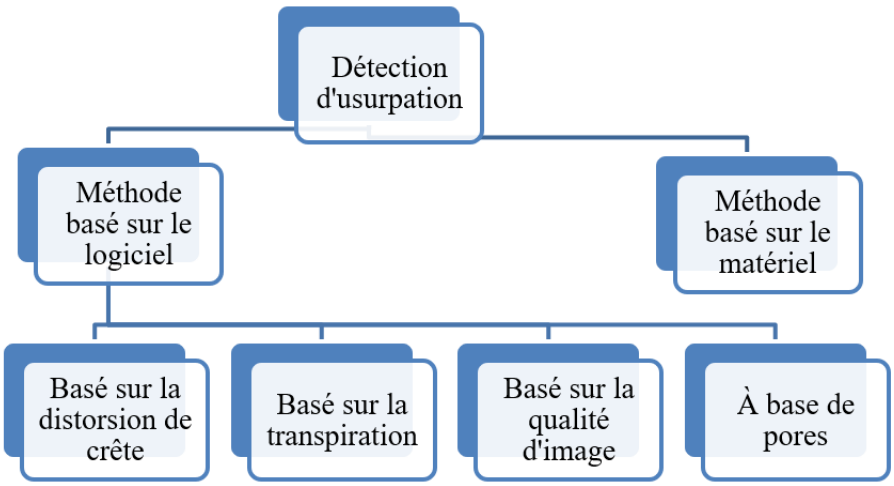

FIGURE 1.17 – Schéma illustrant les différentes méthodes d'anti usurpation d'empreinte digital [3].

1.8.4.1 Méthodes basées sur le matériel

Ces techniques utilisent un équipement supplémentaire pour évaluer les propriétés thermiques et électriques du doigt elles réalisent l'individualité de la vitalité telle que la température, la conductivité électrique, l'oxymétrie de pouls, la résistance de la peau, etc. Néanmoins, l'utilisation d'un équipement supplémentaire augmente les frais généraux du système et rendent l'appareil coûteux [3].

1.8.4.2 Méthodes basées sur le logiciel

Les solutions logicielles utilisent une analyse sophistiquée des images capturées par des lecteurs standard pour détecter les signes de vie dans les empreintes digitales acquises, elles extraient les principales caractéristiques des images pour séparer les échantillons vivants et usurpés.

— **Basé sur la transpiration :**

La méthode de transpiration utilise un doigt vivant basé sur la détection de la transpiration entre la peau humaine et d'autres matériaux, car la sueur part des pores et se diffuse le long des crêtes, il rend la région entre les pores plus sombre. Le motif d'humidité résultant peut être capturé. Les empreintes digitales vivantes présentent une non-uniformité due à la transpiration, tandis que les empreintes digitales factices présentent une grande uniformité [39].

— **Basé sur la distorsion de crête :**

Basé sur la distorsion produite par un vrai doigt lors de la pression et du déplacement sur un scanner. Ces distorsions sont analysées en traitant une séquence d'images à une fréquence d'images très élevée. Le doigt est supposé non déformé au départ et ses mouvements sont analysés par flux optique. Le résultat et les performances de cette méthode dépendent de la précision de l'extraction et de l'appariement des minuties [45].

— **À base de pores :**

Cette une méthode qui utilise un capteur à très haute résolution pour acquérir l'image en appliquant deux filtres, Le filtre passe-haut pour extraire les pores qui se situe le long des crêtes qui sont actifs tandis que le filtre de corrélation est utilisé pour localiser la position des pores.

— **Basé sur la qualité d'image :**

Cette méthode a pour but d'obtenir les caractéristiques discriminantes des empreintes digitales pour l'étude de la vivacité, en effectuant des différents prétraitements sur l'image afin d'améliorer sa qualité pour distinguer les vraies empreintes des fausses [3].

1.9 Conclusion

Ce chapitre avait pour but de donner une vue d'ensemble sur le sujet des empreintes digitales et du traitement d'image d'empreinte digitale, c'est en effet, un chapitre introductif aux techniques d'usurpation des empreintes digitales. Nous avons, en premier lieu définie la biométrie ainsi que ses modalités, nous avons ensuite présenter

les empreintes digitales ainsi que les différentes techniques d'usurpation et d'anti usurpation de cette identité biométrique et pour finir nous avons exposé le principe du traitement d'image pour le traitement des images d'empreintes digitales. Dans le chapitre suivant nous allons présenter un état de l'art sur les techniques d'anti usurpations des empreintes digitales.

Chapitre 2

Etat de l'art sur les techniques d'anti-usurpation des empreintes digitales

2.1 Introduction

Bien que nous ne nous en rendions pas toujours compte, notre identité est vérifiée quotidiennement par de multiples organisations, chaque personne s'efforce d'assurer la sécurité de ses appareils électroniques, en raison des informations personnelles et sensibles qu'ils contiennent, beaucoup de technique son représentée pour protéger les ressource personnel telle les empreinte digitales en effet se sont les plus utilisées dans les systèmes d'authentification puisqu'elles garantissent une haute précision d'identification. Cependant, ces systèmes ne sont pas à l'abri des attaques malveillantes.

En effet les systèmes de reconnaissance d'empreintes digitales sont largement déployés pour l'authentification dans de nombreuses applications. Cependant, ce type de systèmes de reconnaissance peut être falsifié par des empreintes digitales artificielles fabriquées à partir de divers matériaux. Ainsi, il est nécessaire d'ajouter un module de détection de la vivacité des empreintes digitales pour maintenir ce type de systèmes de reconnaissance à un bon niveau de sécurité. La détection de la vivacité des empreintes digitales vise à déterminer si une image d'empreinte digitale donnée est capturée à partir d'un vrai doigt ou d'un faux.

Il existe plusieurs méthodes pour reconnaitre une empreinte digitale quelconque. Au début les méthodes classiques étaient l'outil unique pour reconnaitre et classifier une empreinte, ces méthodes se basent sur l'observation avec l'œil nue à l'aide d'une loupe. Jour après jour la science se développe, la numérisation des images devient une clé essentielle pour améliorer les processus de ce domaine. Les outils mathématiques aident les systèmes de reconnaissance à effectuer plusieurs opérations sur les empreintes digitales dès l'acquisition jusqu'à l'identification des personnes.

Dans ce chapitre nous allons présenter les différent travaux et études proposées par des chercheurs afin d'améliorer la sécurité des empreintes digitales et éviter leurs l'usurpassions en utilisant des méthodes basées sur le logiciel à savoir les caractéristiques des images statistiques binarisées (BSIF) et le descripteur local weber

simplifié (SWLD) et les réseau de neurone convolutif (CNN).

2.2 La méthode de descripteur local binaire de weber

Zhihua et al [49]ont proposer une nouvelle méthode logicielle basé sur un descripteur local nommé descripteur binaire local de Weber pour la détection de la vivacité des empreintes digitales. La méthode consiste en deux composantes : la composante d'excitation différentielle binaire locale qui extrait les caractéristiques d'intensité-variance et la composante d'orientation du gradient binaire local qui extrait les caractéristiques d'orientation. Ensuite les deux composants sont combinés pour former un histogramme 2D, qui est défini comme le descripteur binaire local de Weber (WLBD) final. La probabilité de cooccurrence des deux composantes est calculée pour construire un vecteur des caractéristiques qui est introduit dans les classificateurs de la machine à vecteurs de support (SVM) pour entraîner les classificateurs avec la proposition descripteur local. Des expériences sont réalisées sur deux bases de données publiques de compétitions de 2011 et 2013. Les résultats ont prouvé que la méthode proposée obtient la meilleure précision de détection parmi les descripteurs locaux d'images existants dans la détection de vivacité des empreintes digitales.

Diego et al [11] ont proposé une méthode de détection de la vivacité des empreintes digitales basée sur le descripteur d'image local Weber proposé pour la classification des textures avec la construction des histogrammes conjoints de ces composants pour former un classificateur SVM à noyau linéaire. Les résultats expérimentaux avec différentes bases de données et différents capteurs montrent que le descripteur d'image local Weber (WLD) fonctionne favorablement par rapport aux méthodes de pointe en matière de détection de la vivacité des empreintes digitales.

2.3 Filtres de gabor pour la détection de la vivacité

Xia et al [50]ont proposer une nouvelle méthode d'extraction de caractéristiques efficace pour la détection de la vivacité des empreintes digitales, basée sur la caractéristique de Gabor à symétrie circulaire (CSGF), qui est conçus pour être invariants en. Les filtres de Gabor ont été utilisés pour extraire les caractéristiques de texture des images d'empreintes digitales, et le composant CSGF extrait les caractéristiques discriminantes dans le domaine fréquentiel. Les composantes de (CSGF) sont extrait pour générer un histogramme bidimensionnel dont les éléments sont utilisés comme caractéristiques finales. Les fonctionnalités proposées sont utilisées pour former des classificateurs SVM séparément sur deux bases de données dans Fingerprint Liveness Detection Competition 2011 et 2013, les résultats expérimentaux sur deux bases de données publiques ont démontré l'efficacité de la méthode.

2.4 Les réseaux de neurone dans la détection de la vivacité des empreintes

Rodrigo et al [44] ont proposer une méthode de détection de la vivacité des empreintes digitales à l'aide des réseaux de neurones convolutifs en faisant une comparaison de trois modèles différents de réseaux convolutifs. Le premier, c'est un réseau de neurone convolutif aléatoire (CNN-Random) utilise uniquement un filtre aléatoire les poids sont tirés d'une distribution gaussienne et un classificateur machine à vecteurs de support (SVM) avec un réseau à fonctions de base radiales (RBF) utilisés comme classifieur. Le deuxième modèle, CNN-Alexnet, utilisé pour améliorer la précision dans une variété d'autres points de repère le réseau préformé fournit un bon point de départ pour apprendre les poids du réseau. Le troisième modèle, CNN-VGG, un CNN à 19 couches qui a obtenu la deuxième place dans la tâche de détection du défi ImageNet 2014, et un (SVM) comme classificateur. Les études ont montré que ces modèles ont une bonne précision sur de très petits ensembles d'apprentissage.

Park et al [19]ont proposé une nouvelle méthode de détection de la vivacité des empreintes digitales à l'aide des fonctionnalités des réseaux de neurones convolutif (CNN) sur des patchs aléatoires, la méthode proposée consiste en deux phases : apprentissage et le test. Dans la phase d'apprentissage, le (CNN) est appliqué à un ensemble de données de patch augmenté à partir d'une image d'empreinte digitale. Dans la phase de test, les résultats finaux sont renvoyés à l'aide d'un schéma de vote sur tous les correctifs extraits. Tout d'abord, les empreintes digitales sont segmentées, puis une augmentation des données est effectuée pour augmenter la taille des données d'apprentissage. Deuxièmement, sur l'empreinte digitale augmentée, les emplacements des patchs sont déterminés par des distributions normales de zones segmentées de l'image de l'empreinte digitale. Les résultats expérimentaux montrent que la méthode proposée peut être appliquée à la détection de la vivacité des empreintes digitales avec une grande précision sur un ensemble de données de capteur Identix LivDet2009.

Shervin et al [31] ont proposé une méthode d'apprentissage en profondeur pour la reconnaissance d'empreintes digitales à l'aide de réseaux de neurones convolutifs, c'est une approche d'apprentissage par transfert en affinant un réseau neuronal avec l'utilisation d'un modèle ResNet50 formé sur l'ensemble de données ImageNet avec des filtres prédéfinis. Pour effectuer la reconnaissance sur l'ensemble de données d'empreintes digitales, ils ont affiné un modèle ResNet avec 50 couches sur l'ensemble d'apprentissage augmenté, en appliquant plusieurs techniques d'augmentation des données pour augmenter le nombre d'échantillons d'apprentissage qui est déterminé en fonction des performances sur un ensemble de validation, pour l'évaluer sur l'ensemble de test. Les résultats sont prometteurs ils surpassent les approches précédentes sur l'ensemble de données testés.

2.5 La méthode des caractéristiques des images statistiques binarisées

Luca et al [24] on proposer l'utilisation d'un algorithme de classification de texture le BSIF (Caractéristiques des images statistiques binarisées). Il s'agit d'un descripteur d'image local construit en binarisant les réponses

aux filtres linéaires mais les filtres sont appris à partir d'images naturelles. L'approche consiste à partir de la représentation des empreintes digitales à appliquer l'apprentissage, au lieu d'un réglage manuel, pour obtenir une représentation statistiquement significative des données d'empreintes digitales, ce qui permet un codage efficace des informations à l'aide d'une simple quantification élément par élément. L'apprentissage offre également un moyen simple et flexible d'ajuster la longueur du descripteur et de s'adapter aux applications présentant des caractéristiques d'image inhabituelles telles que les empreintes digitales. L'ensemble de filtres est appris à partir d'un ensemble d'apprentissage de patchs d'images naturelles en maximisant l'indépendance statistique des réponses des filtres. Les résultats montrent clairement que les caractéristiques des images statistiques binarisées, avec un assez grand nombre de bits, surpassent les autres algorithmes, mais ils montrent qu'une réduction de bits diminue fortement les performances de l'algorithme.

Patil et al [5] on utiliser une méthode qui consiste à effectuer un prétraitement puis effectuées une étape de calcul des caractéristiques, qui traite de l'extraction d'informations texturales en utilisant la fusion de motifs binaires locaux multi blocs et de filtres des caractéristiques des images statistiques binarisées, et après ça effectuer un prétraitement de l'image de l'empreinte digitale dont la méthode est évaluée avec un classificateur binaire différent. Et enfin établir la fusion au niveau des caractéristiques du motif binaire local multi-blocs de descripteur de texture bien connu et des caractéristiques pour implémenter les caractéristiques d'image statistiques binaires. L'approche proposée est testée sur le jeu de données multimodal SDUMLA-HMT (Groupe d'apprentissage automatique et applications, Université du Shandong) et comparée à l'état de l'art en termes de précision avec les techniques d'extraction de caractéristiques de soustraction d'arrière-plan sont mises en œuvre respectivement et en utilisant le classificateur de machine à vecteurs de support.

Marasco et al [18]ont proposé une approche qui est évalué sur les empreintes digitales acquises auprès de 494 participants de l'université de Virginie-Occidentale à l'aide de quatre capteurs optiques à haute résolution et de la méthode traditionnelle à base d'encre. Cette méthode consiste de compenser la distorsion due à la diversité des appareils et de réduire son impact sur les performances du système global de reconnaissance d'empreintes digitales, on utilisons un schéma de classification qui fusionne ces caractéristiques avec des scores de correspondance pour développer un modèle pour améliorer le taux de correspondance entre appareils à montrer une réduction significative des taux d'erreur par rapport à la référence ainsi qu'une amélioration des performances par rapport aux recherches précédentes.

2.6 Conclusion

Ce chapitre a pour but de représenter l'état de l'art sur les différentes techniques d'anti usurpations des empreintes digitales avec les deux méthodes SWLD (simplified weber local descriptor) et la méthode BSIF (binarized statistical image features) et nous avons aussi comparer ses différentes méthodes. Dans le chapitre suivant nous allons présenter notre méthode d'anti usurpations des empreintes digitales en utilisant les deux

méthodes BSIF et SWLD.

Chapitre 3

Méthodes d'anti-usurpation des empreintes digitales

3.1 Introduction

A travers ce chapitre, nous allons présenter la méthode de prétraitement utilisée pour les empreintes digitales ainsi que les méthodes d'extraction des caractéristiques en particulier et leur classification.

L'extraction de caractéristiques discriminantes est une étape fondamentale du processus de reconnaissance des empreintes digitales Les caractéristiques sont obtenues par une quantification de l'image et permettent de représenter l'image par un nombre minimal des paramètres. Il existe plusieurs méthodes pour l'extraction des caractéristiques trouvées dans la littérature. En utilisant des méthodes différentes qui consiste à mettre en œuvre une méthode basée sur le logiciel qui permettra de détecter les vraies empreintes des fausses. La première représente une présentions des méthodes de prétraitement appliquées aux images d'empreintes digitales qui sont les filtre simplifiée weber local descripteurs (SWLD) et fonctionnalité d'image statique binarisée (BSIF).

La seconde sera consacrée à l'extraction des caractéristiques, une méthode basée sur une architecture spécifique du caffenet dans les réseaux de neurones qui a été utilisé dans notre application. En troisième étape nous abordons la fusion des caractéristiques de chaque résultat apporté dans les CNN, résultats générés à l'étape précédente, afin d'augmenter la fiabilité du système de reconnaissance. Nous allons tester et comparer ces descripteurs sur les images de la base de données FVC 2002, pour mettre en évidence ses performances et ses précisions dans la reconnaissance des empreintes digitales des individus. Ces descripteurs sont comparés selon des conditions de traitement prédéfini, et également aussi en fonction du type de classifieur utilisé.ET pour terminer on va classifier les résultats obtenus avec un classifieur SVM.

3.2 Environnement de développement

3.2.1 Matériels

Nous avons utilisés deux machines avec les caractéristiques suivantes :

Caractéristiques	**Machine 1**
Processeur	Intel(R) Core(TM) i5-8250U CPU @ 1.60GHz 1.80 GHz
RAM	8,00 Go
Système d'exploitation	Ubuntu linux 20.04

TABLE 3.1 – Matériels utilisés

3.2.2 Logiciels

L'environnement logiciel utilisé pour la réalisation de notre application est : Python Nous avons utilisés la

FIGURE 3.1 – Logo python [38].

version Python 3.9 comme langage de programmation, parmi les raisons de cette utilisation :

— Python fonctionne sur différentes plateformes (Windows, Mac, Linux).

— Il a une syntaxe simple claire, respecte les standards du domaine. Similaire a la langue anglaise.

— langage peut être traité de manière procédurale, de manière orientée objet ou de manière fonctionnelle [38].

3.2.3 Modules et bibliothèques

Une bibliothèque est une ensemble de fonctions. Elles sont regroupées et mises à disposition afin de pouvoir être utilisées sans avoir à les réécrire. Celles-ci permettent de faire : du calcul numérique, du graphisme, de la programmation internet ou réseau, du formatage de texte, de la génération de documents... Parmi les différentes bibliothèques utilisés dans notre travaille on peux cité :

Module PIL :

La bibliothèque PIL (Python Imaging Librairie) permet la manipulation de tout type d'images et fournit quelques fonctions de traitement d'images de base. **Numpy :**

Numpy est une biblioth'eque num´erique apportant le support efficace de larges tableaux multidimensionnels, et de routines math´ematiques de haut niveau.

Matplotlib :

Matplotlib est une bibliothèque destinée à tracer et visualiser des données sous formes de graphiques.

SciPy :

La librairie SciPy contient de nombreuses boites à outils consacrées aux méthodes de calcul scientifique. Ses différents sous-modules correspondent à différentes applications scientifiques, comme les méthodes d'interpolation, d'intégration, d'optimisation, de traitement d'image, de statistiques, de fonctions mathématiques spéciales, etc.

OpenCV :

Cette bibliothèque permet de manipuler les structures de base, réaliser des opérations sur des matrices, dessiner sur des images, sauvegarder et charger des données. Une grande partie de notre application repose sur l'utilisation de la bibliothèque spécialisée dans le Computer Vision, OpenCV version 4.1. Il permet aussi de partager les bibliothèques dynamiques entre les différentes applications dans le même appareil en même temps.

Tensorflow :

TensorFlow est un framework de programmation pour le calcul numérique qui a été rendu Open Source par Google en Novembre 2015. Depuis son release, TensorFlow n'a cessé de gagner en popularité, pour devenir très rapidement l'un des frameworks les plus utilisés pour le système d'apprentissage en profondeur et donc les réseaux de neurones. Son nom est notamment inspiré du fait que les opérations courantes sur des réseaux de neurones sont principalement faites via des tables de données multi-dimensionnelles, appelées Tenseurs (en anglais : Tensor).

Un Tensor à deux dimensions est l'équivalent d'une matrice. Aujourd'hui, les principaux produits de Google sont basés sur TensorFlow : Gmail, Google Photos, Reconnaissance de voix. Le fonctionnement interne de Tensorflow est la clé de son succès. Un calcul TensorFlow est décrit par un graphe, qui se compose d'un ensemble de nœuds. Le graphe représente un flux de données et ses transformations, avec des extensions permettant à certains types de nœuds de maintenir et de mettre à jour des états persistants. Les différents clients (Python, C++, autres) permettent de générer ce type de graphe de calcul.

Kiras :

keras est une API (application programming interface) réservée pour les réseaux neuronaux de haut niveau pour un développement et une expérimentation rapide . Il fonctionne au-dessus de TensorFlow, CNTK, ou Theano,c'est l'outil le plus utilisé en deep learning et en reconnaissance d'image, cette librairie open-source, créée par François Chollet permet de créer facilement et rapidement des réseaux neurones, en se basant sur les principaux frameworks (tensorflow), il est l'API officielle de haut niveau de tensorflow car il il permet un prototypage rapide et facile (par sa convivialité, sa modularité et son extensibilité) [38].

3.3 Proposition de notre travail

3.3.1 Présentation du travail

Notre travaille consiste a réaliser un nouveau système de détection de la vivacité des empreintes digitales basé sur des caractéristiques locales Simplified Weber Local Descriptor (SWLD) et Binarized Statistical Image Features (BSIF) en tant que descripteur local de texture codé par des modèles CNN et traité avec CaffeNet. La fonction SWLD et le vecteur de fonction BSIF sont combinés pour assurer la préservation des informations d'intensité locale et le gradient d'orientation dans WLD est remplacé par une récente fonctionnalité d'image statistique binarisée (BSIF). Après une sélection de fonctionnalités appropriée, un classificateur SVM à noyau linéaire formé prend la décision finale en direct/faux. Notre analyse expérimentale sur deux bases de données accessibles au public LivDet2011 et LivDet2013, comprenant des ensembles de données collectées à partir de divers capteurs, la figure 3.2 représente la structure de notre travaille.

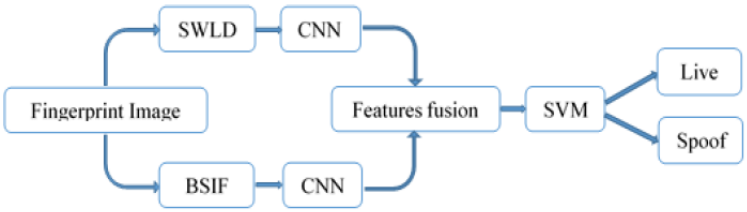

FIGURE 3.2 – Shémat de travail [30].

3.3.2 BSIF

Le descripteur BSIF (Binarized Statistical Image Features) a été proposé par J. Kannala et al en 2012 pour la reconnaissance faciale et la classification de texture.[27]. Il est inspiré par la méthodologie LBP et LPQ, BSIF calcule également un code binaire pour chaque pixel dans une image pour représenter la structure locale d'une image, La valeur du code d'un pixel est considérée comme un descripteur local du motif d'intensité de l'image dans l'environnement du pixel. Contrairement à LBP et LPQ qui peuvent être utilisées pour calculer les statistiques d'étiquettes dans les voisinages des pixels locaux, BSIF utilise un ensemble prédéfini manuellement des filtres linéaires et binarisation des réponses du filtre. De plus, les histogrammes des valeurs de code des pixels permettent de caractériser les propriétés des textures des patchs (dans les sous-régions) des images

Description :

La valeur de chaque bit dans une chaîne de code binaire est calculée en binarisant la réponse d'un filtre linéaire avec un seuil à zéro. Chaque bit est associé à un filtre différent et la longueur désirée de la chaîne de bits détermine le nombre de filtres utilisés. L'ensemble de filtres sont automatiquement appris basés sur des propriétés statistiques d'un petit ensemble d'images naturelles. L'ensemble des filtres est entrainé à partir d'un ensemble de patchs d'images naturelles en maximisant l'indépendance statistique des réponses des filtres. Par conséquent, les propriétés statistiques des patchs d'images naturelles déterminent les descripteurs et c'est pourquoi, on les nomme descripteurs d'images statistiques binarisées (BSIF). Compte tenu d'un patch image X de taille l × l pixels et un filtre linéaire Wi de la même taille, la réponse du filtre Si est donnée par l'équation suivante :

$$Si = \sum Wi(u,v)X_i^T(x,v) = wx(u,v). \tag{3.1}$$

Où les vecteurs w et x contiennent les pixels de Wi et X respectivement. La chaîne de code binaire b est obtenue par la binarisation de chaque élément Si. La fonction binarisée bi est calculée par :

$$bi = \begin{cases} 0 & \text{si} \quad Si > 0 \\ 1 & \text{sinon} \end{cases} \tag{3.2}$$

.

Etant donné n filtres linéaires Wi, nous pouvons les empiler sur une matrice W de taille n × l. La longueur de la chaîne de bits n avec la taille du filtre l sont des paramètres variables pour évaluer le descripteur BSIF. Toutes les réponses sont calculées à la fois, c'est-à-dire [27] :

$$S = Wx. \tag{3.3}$$

Appliquage du filtre BSIF a l'image d'emprente digitale :

FIGURE 3.3 – Filtre BSIF

3.3.3 SWLD

Le WLD (Weber local descriptor) est un nouvel opérateur récemment développé par Chen et al [12]. Il a été introduit pour caractériser les textures dans les images et a été illustrée sur des images brutes en considérant le rapport des changements d'intensité des pixels qui peuvent être considérés comme des informations de stimulus pour la perception visuelle. Le descripteur local simple est inspiré de la loi de Weber qui a été proposée par le physiologiste allemand Ernst Weber en 1834, très puissant et robuste, il est basé sur le fait que la perception humaine d'un motif dépend non seulement du changement d'un stimulus (comme le son, l'éclairage), mais aussi de l'intensité originale du stimulus. Plus précisément, WLD se compose de deux composants : l'excitation différentielle et l'orientation. La composante d'excitation différentielle est fonction du rapport entre deux termes : l'un est les différences d'intensité relative d'un pixel de courant par rapport à ses voisins, l'autre est l'intensité du pixel de courant. Le SWLD(simplified weber local descriptor) est une simplification du WLD en enlevant la phase d'orientation, il détecte les bords et enregistre leurs valeurs d'intensité qui sont des opérateurs complémentaires quant au type d'informations qu'ils encodent [26].

Description :

Il capture les modèles visuels saillants locaux[13]. Par exemple, une valeur d'excitation différentielle élevée indique que le pixel central appartient potentiellement à un bord ou à un spot car il existe une forte différence d'intensité de pixel entre le pixel central et ses voisins. L'excitation différentielle est calculée comme une fonction arc tangente du rapport de la différence d'intensité entre le pixel central et ses voisins à l'intensité du pixel central. L'excitation différentielle du pixel central y(xc) est calculée comme suite :

$$\varepsilon(xc) = \arctan\{\sum_{i=0}^{P-1}((xi - xc)/xc)\} \tag{3.4}$$

Où xc est la valeur d'intensité du pixel central et P est le nombre de voisins sur un cercle de rayon R. Si y(xc) est positif, il simule le cas où l'environnement est plus clair que le pixel actuel. En revanche, si y(xc) est négatif, il

simule le cas où l'environnement est plus sombre que le pixel courant [26]. La fonction Arctangente est continue et strictement croissante sur. C'est une conséquence directe du théorème des fonctions réciproques On note arctan la fonction réciproque telleque :

arctan $\implies tang = x$

Appliquage du filtre SWLD a l'image d'emprente digitale :

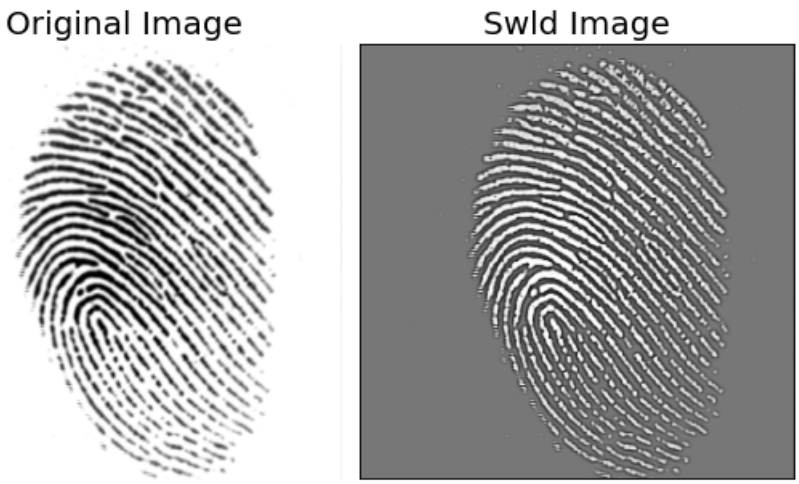

FIGURE 3.4 – Filtre SWLD

3.3.4 Discussion

Notre travail consiste à réaliser un système de détection de la vivacité des empreintes digitales. D'abord on prend une image dans la base de données FCV 2002, c'est un concours de vérification d'empreintes digitales et qui été établie pour tester un algorithme d'extraction et de correspondances des empreintes, ou a chaque image est associé un vecteur des caractéristiques. Ces caractéristiques sont supposées être invariantes pour une même personne, et différentes d'une personne à l'autre. La reconnaissance consiste alors à comparer le vecteur de caractéristiques du l'empreinte à reconnaitre avec celui de chacun des empreintes de la base de données. Puis pour l'extraction des caractéristiques on a choisi deux méthode BSIF et SWLD. Cette étape représente le cœur du système de reconnaissance, on extrait de l'image les informations qui seront sauvegardées en mémoire pour être utilisées plus tard dans la phase de décision. L'extraction des caractéristiques utilise plusieurs méthodes on a utilisé BSIF car il est utilisé pour convertir les caractéristiques des texture d'image d'empreinte digitale en code binaire pour chaque pixel en fonction des réponses des filtre, et SWLD est introduit pour caractériser les texture dans les image dépend de l'intensité original de stimulus ,on a choisie c'est deux méthodes car leur principe est de prend en entrée les données biométriques acquises par le module de capture et extrait seulement l'information pertinente afin de former une nouvelle représentation des données. A la fin de cette étape on a pouvez passez directement a la classification avec le SVM mais le problème de cette méthodes est qu'elle n'est pas capable de déterminer à quelle catégorie cette entrée appartient,c'est pour ça on a appliqué le CNN car les deux classe ne sont pas séparables ,donc on a appliqué le CNN car quand on augmente les caractéristiques les classe commence a apparaitre et les résultats serrant facile à séparer , et en fin on applique la classification

avec SVM pour les deux classe . On a utilisé ce classificateur car Les SVM sont une famille d'algorithmes d'apprentissage automatique qui permettent de résoudre des problèmes tant de classification que de régression ou de détection d'anomalie.

3.3.5 Réseau de neurones convolutifs :

Un réseau neuronal convolutif (CNN) est un type de réseau neuronal artificiel utilisé dans la reconnaissance et le traitement d'images qui est spécifiquement conçu pour traiter les données de pixels. Les CNN sont un traitement d'image puissant, une intelligence artificielle (IA) qui utilise l'apprentissage en profondeur pour effectuer des tâches à la fois génératives et descriptives, souvent en utilisant une vision machine qui inclut la reconnaissance d'images et de vidéos, ainsi que des systèmes de recommandation et le traitement du langage naturel (NLP). Un réseau de neurones est un système matériel et/ou logiciel calqué sur le fonctionnement des neurones du cerveau humain. Les réseaux de neurones traditionnels ne sont pas idéaux pour le traitement d'images et doivent être alimentés en images en morceaux à résolution réduite. Les CNN ont leurs «neurones» disposés davantage comme ceux du lobe frontal, la zone responsable du traitement des stimuli visuels chez les humains et les autres animaux. Les couches de neurones sont agencées de manière à couvrir tout le champ visuel en évitant le problème de traitement d'image fragmentaire des réseaux de neurones traditionnels. Un CNN utilise un système un peu comme un perceptron multicouche qui a été conçu pour des exigences de traitement réduites. Les couches d'un CNN se composent d'une couche d'entrée, d'une couche de sortie et d'une couche cachée qui comprend plusieurs couches convolutionnelles, des couches de regroupement, des couches entièrement connectées et des couches de normalisation. La suppression des limitations et l'augmentation de l'efficacité du traitement d'image se traduisent par un système beaucoup plus efficace, plus simple pour les trains limités au traitement d'image et au traitement du langage naturel [9].

3.3.5.1 Couche convolutive

Une couche convolutive est le bloc de construction principal d'un CNN. Il contient un ensemble de filtres (ou noyaux) dont les paramètres sont à apprendre tout au long de la formation. La taille des filtres est généralement plus petite que l'image réelle. Chaque filtre convolue avec l'image et crée une carte d'activation. Pour la convolution, le filtre a glissé à traversla hauteur et la largeur de l'image et le produit scalaire entre chaque élément du filtre et l'entrée sont calculés à chaque position spatiale. Le volume de sortie de la couche convolutionnelle est généré en empilant les cartes d'activation de chaque filtre le long de la dimension de profondeur. Chaque composant de la carte d'activation peut être considéré comme la sortie d'un neurone. Par conséquent, chaque neurone est connecté à une petite région locale dans l'image d'entrée, et la taille de la zone est égale à la taille du filtre. Tous les neurones d'une carte d'activation partagent également des paramètres entre eux. En raison de la connectivité locale de la couche convolutive, le réseau est obligé d'apprendre les filtres qui ont la réponse maximale à une région locale de l'entrée [44]. Les couches convolutionnelles initiales capturent les caractéristiques de bas niveau (par exemple, les lignes) des images, tandis que les couches ultérieures extraient les caractéristiques de haut niveau (par exemple, les formes et les objets spécifiques) [23].

3.3.5.2 Couche de mise en commun maximale

Le regroupement maximal, ou regroupement maximal, est une opération de regroupement qui calcule la valeur maximale, ou la plus grande, dans chaque patch de chaque carte d'entités. Les résultats sont des cartes de fonctionnalités sous-échantillonnées ou regroupées qui mettent en évidence la fonctionnalité la plus présente dans le patch, et non la présence moyenne de la fonctionnalité dans le cas d'un regroupement moyen. Il a été constaté que cela fonctionnait mieux dans la pratique que la mise en commun moyenne pour les tâches de vision par ordinateur telles que la classification des images. En un mot, la raison en est que les caractéristiques ont tendance à coder la présence spatiale d'un modèle ou d'un concept sur les différentes tuiles de la carte des caractéristiques (d'où le terme carte des caractéristiques), et il est plus informatif de regarder la présence maximale de différentes caractéristiques qu'à leur présence moyenne. Nous pouvons concrétiser l'opération de mise en commun maximale en l'appliquant à nouveau à la carte des caractéristiques de sortie de l'opération convolutive du détecteur de ligne et calculer manuellement la première ligne de la carte des caractéristiques regroupées [32].

3.3.5.3 Couches entièrement connectées

Les couches entièrement connectées dans un réseau de neurones sont les couches où toutes les entrées d'une couche sont connectées à chaque unité d'activation de la couche suivante. Dans les modèles d'apprentissage automatique les plus populaires, les dernières couches sont des couches entièrement connectées qui compilent les données extraites par les couches précédentes pour former la sortie finale [22].

3.3.6 Architecture utilisés dans notre travaille

Nous choisissons d'utiliser CNN pour apprendre la représentation des caractéristiques à partir d'images d'empreintes digitales. Nous implémentons une structure CNN canonique pour l'apprentissage des fonctionnalités. Plus précisément, nous adoptons la configuration basée sur CaffeNet , l'architecture CNN contient cinq couches convolutives (Conv) et trois couches entièrement connectées (FC). Les couches de normalisation de réponse sont utilisées pour la sortie des deux premières couches convolutives. Les couches de regroupement maximum sont utilisées pour produire la sortie des 1ère, 2ème et 5ème couches Conv. De plus, les 6e, 7e et 8e couches sont des couches entièrement connectées. 6ème et 7ème couche contenant 4096 neurones tandis que la 8ème couche contient 1000 neurones. Une non-linéarité ReLU est appliquée à la sortie de chaque couche entièrement connectée et Conv. Cependant, les 3ème et 4ème couches ont 384 canaux suivis d'une 5ème couche convolutive avec 256 canaux. Les caractéristiques de texture sont calculées à partir de l'image SWLD et de l'image BSIF. De cette manière, les fonctionnalités apprises devraient avoir une meilleure capacité de généralisation.

A la fin Les fonctionnalités CNN-SWLD et CNN-BSIF sont combinées pour garantir la capacité de classification des fonctionnalités CNN, une amélioration du descripteur local Weber (WLD) contient une composante d'excitation différentielle et l e gradient d'orientation dans WLD est remplacé par une récente fonctionnalité d'image statistique binarisée. (BSIF) comme descripteur local de texture. On s'attend donc à ce que les informations codées à l'aide de ces opérateurs se combinent bien.

Après avoir appris les CNN, nous extrayons les caractéristiques de la dernière couche entièrement connectée. Ensuite, la machine à vecteurs de support (SVM) est utilisée pour apprendre les classificateurs à partir des données de train pour la détection de la vivacité des empreintes digitales.

3.3.7 Classification SVM

Le SVM est une nouvelle technique d'apprentissage statistique utilisée pour l'analyse des données et la reconnaissance des formes, proposé par Cortes et Vapnik. Au début et dans sa forme de base, le SVM est utilisé comme une méthode de classification binaire basé sur un problème à deux classes. L'algorithme SVM a été développé au cours des années 1990 à des fins industrielles Les classifieurs SVM utilisent l'idée de l'hyperplan Optimal pour calculer une frontière entre des nuages de points. Elles projettent les données dans l'espace de caractéristiques en utilisant des fonctions non-linéaires. Dans cet espace on construit l'hyperplan optimal qui sépare les données transformées. L'idée principale est de construire une surface de séparation linéaire dans l'espace des caractéristiques qui correspond à une surface non-linéaire dans l'espace d'entrée. Le SVM binaire cherche à trouver l'hyperplan de séparation optimale entre les deux classes en maximisant la marge entre l'hyperplan et les deux classes qui sont étiquetées avec -1 et 1. Supposons que A est un ensemble de données, xi(i=1,2,...,K) sont les vecteurs caractéristiques d'apprentissage en K dimension et Yi sont les étiquettes (labels) :

$$A = \{(xi, yi) \mid xi \in Rk, yi \in \{-1, 1\}\} \tag{3.5}$$

Pour le SVM linéaire, l'hyperplan de séparation optimale peut être exprimé par la fonction suivante :

$$f(x) = (w \,.\, x) + b \tag{3.6}$$

Le SVM est généralisé pour résoudre le problème multi-classes. Les algorithmes SVM multi-classes peuvent être divisés en deux catégories : One-Versus-All et One-Versus-One. Lorsque le nombre de classes des personnes dans notre système de reconnaissance est assez grand, nous utilisons la stratégie One-Versus-All basé sur le noyau RBF pour effectuer la vérification des images faciales entre les imposteurs et les clients. One-Versus-All est une méthode simple dans laquelle nous utilisons M classificateurs, un pour chaque classe, les M classificateurs sont combinés pour prendre la décision finale [8].

3.3.8 Hyperplan

On appelle hyperplan séparateur un hyperplan qui sépare les deux classes (Figure 2), en particulier il sépare leurs points d'apprentissage.[2]. De cette notion nous pouvons dire qu'il est évident de trouver une multitude d'hyperplans, mais la propriété délicate des SVM est d'avoir l'hyperplan dont la distance minimale aux exemples d'apprentissage est maximale, cet hyperplan est appelé L'hyperplan optimal, et ce dernier va maximiser la marge .

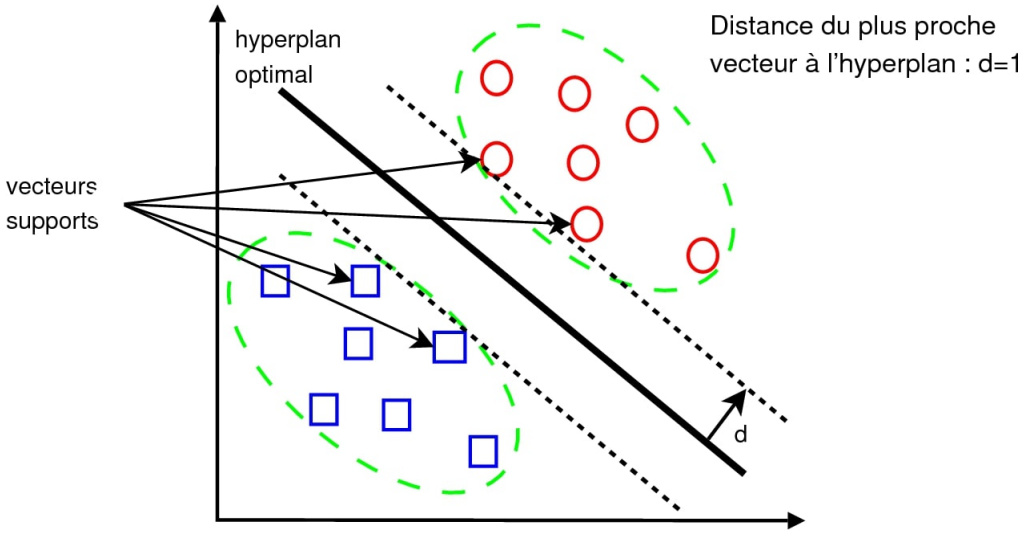

FIGURE 3.5 – L'hyperplan H qui sépare les deux ensembles de points.[38].

3.4 Conclusion

Dans ce chapitre, les travaux biométriques présentés ont conduit à l'élaboration d'un système d'identification des personnes par reconnaissance d'empreintes des doigts. Pour ce faire, nous avons proposé plusieurs systèmes biométriques. Ces différents systèmes sont testés dans le but d'améliorer le taux d'identification dans les modes d'identification. Nous avons généré deux types de descripteurs notamment : BSIF et SWLD. Également, la fusion des descripteurs a été évaluée pour assurer une éventuelle amélioration.

Au module d'extraction des caractéristiques, les systèmes de reconnaissances faits des étapes plus importantes avant le stockage des informations dans ces bases de données. Ces étapes sont basées sur des algorithmes spécifiques comme suit : Le prétraitement des images des empreintes digitales, ensuite l'extraction de caractéristiques : pour obtenir les caractéristiques pertinentes de chaque image acquise, en forme de vecteur d'où on a utilisé les deux méthodes telle que le BSIF et SWLD. Classification des données : dernière étape fait classer les caractéristiques semblables d'un ou plusieurs individus à la même classe, cette étape est appliquée par des algorithmes comme SVM.

Chapitre 4

Tests et résultats expérimentaux

4.1 Introduction

Dans le chapitre précédent, nous avons présenter un aperçu général sur la phase pratique de notre travail largement utilisée en caractérisation des images texturées, ainsi que ces extensions les plus populaires en analyse de texture des filtre BSIF et SWLD et décrire l'environnement de programmation qu'on a travailler .

Ce chapitre est dédié à la présentation des résultats obtenus pour la validation de notre système. La description de la base de données utilisée est tout d'abord présentée. Puis plusieurs expériences sont menées pour l'étude de l'influence des paramètres initiaux sur les performances du système. Les résultats obtenus sont présentés avec la combinaison des différentes catégories de caractéristiques. Ces résultats permettent de mesurer les performances de notre approche. Et pour tester l'approche, nous allons utiliser une méthodes de classification et le séparateur à vaste marge (SVM) qui est le meilleur classificateur entre deux classe qui est le cas de notre travaille . L'évaluation et la comparaison sont effectuées en utilisant le mode et puis examinerons attentivement ses résultats sur la données .

4.2 Mesures des Performances

Les erreurs de classification correspondent aux erreurs de décision des systèmes.L'accuracy, le recall et la precision sont à utiliser ensemble pour donner une vision complète de la performance , ces erreurs de décision sont [40] :

4.2.1 L'accuracy

il indique le pourcentage de bonnes prédictions. C'est un très bon indicateur parce qu'il est très simple à comprendre. 4.1.

$$\text{Accuracy} = \frac{Vrai\ positif + Vrai\ négatif}{Total}$$

FIGURE 4.1 – Lequation de l'accuracy [40].

4.2.2 Le recall

il se concentre uniquement sur les clients qui ont réellement résilié et donne une indication sur la part de faux négatifs. Les faux négatifs ce sont les clients qui résilient mais qui ne sont pas détectés par le score. 4.2.

$$\text{Recall} = \frac{Vrai\ positif}{Vrai\ positif + faux\ négatif}$$

FIGURE 4.2 – L'equation de recall [40].

4.2.3 La precision

il se concentre uniquement sur les clients pour lesquels le modèle a prédit une résiliation et donne une indication sur les faux positifs. Les faux positifs ce sont les clients pour lesquels le score a prédit une résiliation mais qui sont restés abonnés.

4.3.

$$\text{Precision} = \frac{Vrai\ positif}{Vrai\ positif + Faux\ positif}$$

FIGURE 4.3 – L'equation de la precision [40].

4.3 Base de donnée utilisée

Pour évaluer la méthode proposée dans ce mémoire nous l'avons appliqué sur certain images de la base FVC 2004, la résolution de ces images est (388 × 374) ainsi que son format est TIFF.. Il existe dans cette base de données huit échantillons par doigt ce qui permet aux algorithmes de comprendre les variations entre les doigts correspondants. La figure4.4 et **??** montrent une partie de la base de données utilisées.

FIGURE 4.4 – Une image d'empreinte digitale de chaque base de données

Quatre bases de données constituent le benchmark FVC2002, Trois scanners différents et le générateur synthétique SFinGE ont été utilisés pour collecter les empreintes digitales, ils ont collecté pour chaque base de données un total de 120 doigts et 12 impressions par doigt (1440 impressions) à l'aide de 30 volontaires. La taille de chaque base de données à utiliser dans le test FVC2002 est cependant établie à 110 doigts, 8 empreintes par doigt (880 empreintes) [12], le tableau suivant montre les différents scanners et technologies utilisées pour la collecte des bases de données FVC2002.

En raison de leur simplicité et de leur efficacité, les descripteurs basés sur les textures sont très utilisés dans la tâche de reconnaissance d'empreintes digitales. Dans ce travail, nous utilisons deux descripteurs basés sur la texture appelé caractéristiques d'image statistiques binarisées (BSIF) et descripteur local Weber simplifié (SWLD). Les expérimentations ont été menées sur la base de données standard FVC2002. Nous avons extrait les caractéristiques de l'image de l'empreinte digitale avec chaque filtre et les avons concaténés pour construire le vecteur de caractéristiques final. Les expériences ont montré qu'un nombre croissant de sous-images extraites entraînait une augmentation du taux de reconnaissance. Les résultats ont montré que l'utilisation de la méthode de sélection des caractéristiques pouvait réduire la dimensionnalité conduisant à une moindre complexité de calcul.

Dans ce tableau , nous listons les performances en termes d'erreur de classification moyenne sur les ensembles de test de compétition standard FVC2002.

Base de données	1	2	3	4
Scanner	Identix	Biometrika	Precise Biometrics	SFinGE
Numéro de modèle	TouchView II	FX2000	100 SC	v2.51
Rés.(dpi)	500 dpi	569 dpi	500 dpi	500 dpi
Taille de l'image	388×374	296×560	300×300	288×384
Échantillons de formation en direct	100	100	100	100
Échantillons d'entraînement frauduleux	10	10	10	10
Échantillons de test en direct	1000	1000	1000	1000
Échantillons de test d'usurpation d'identité	1000	1000	1000	1000
Matériaux utilisés pour parodie échantillons	programmes informatiques exécutables	programmes informatiques exécutables	programmes informatiques exécutables	programmes informatiques exécutables

TABLE 4.1 – Caractéristiques du jeu de données FVC2002.

En ce qui concerne les méthodes actuellement les plus performantes sur (1) Biometrika, Italdata, Dig ital et Sagem Luca et al [1] ont proposé une méthode de détection de la vivacité des empreintes digitales basée sur

BSIF (les meilleurs résultats obtenus sur Biometrika), l'approche a une erreur de 0,50 % de [25]. Enfin notre approche a une erreur moyenne de 0,80 % par rapport aux 0,5 % de BSIF [1] (les meilleurs résultats obtenus), par contre nous avons obtenu des performances compétitives pour l'ensemble de données FCV2000, comme indiqué dans le tableau.

4.3.1 Résultat et discussion

En ce qui concerne les méthodes actuellement les plus performantes sur (1) Biometrika, Italdata, Dig ital et Sagem Luca et al [1] ont proposé une méthode de détection de la vivacité des empreintes digitales basée sur BSIF (les meilleurs résultats obtenus sur Biometrika), l'approche a une erreur de 0,50 de .[4]. Nous avons utiliser python pour réaliser un système de vérification d'usurpation d'une empreinte dans une base de donne FCV on appliquant les deux méthode BSIF et SWLD pour la phase d'extraction des caractéristiques car ces deux méthodes sert a collecter tous les texture de l'empreinte (les crête, lac ..) puis on a traite chaque cas avec le CNN et afficher les résultats puis on a combiner chaque méthode avec l'autre ; Nous avons d'abord traité les

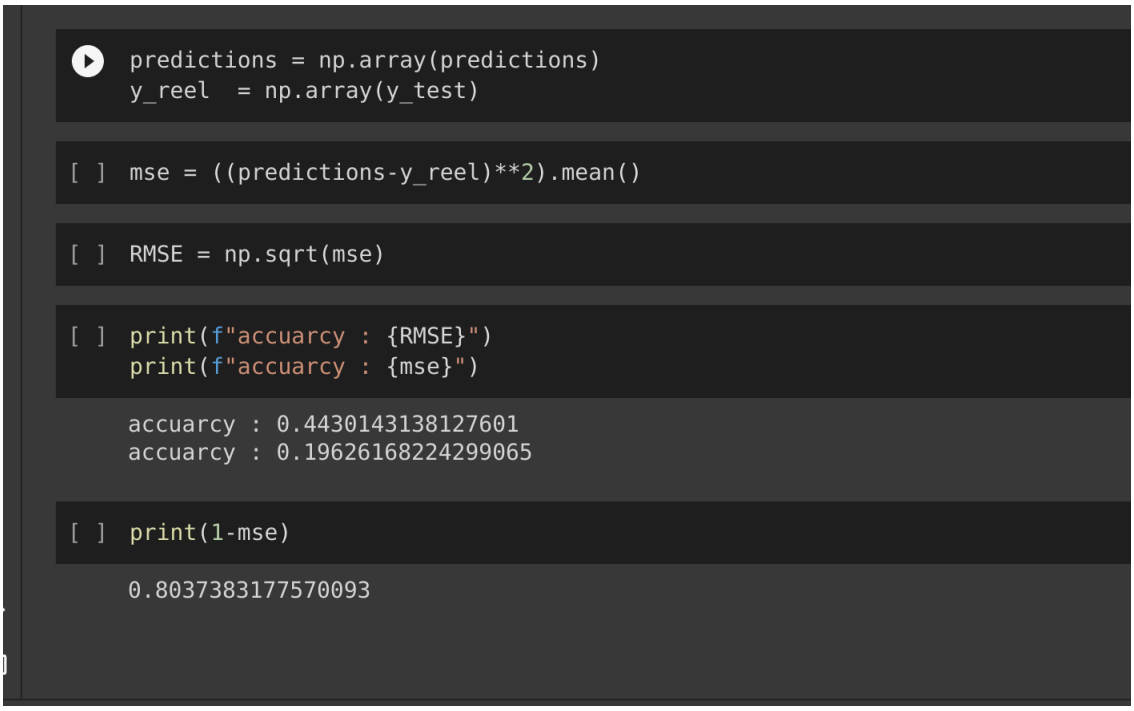

FIGURE 4.5 – Une image des résultats obtenus dans notre travail

résultats de BSIF est on a un résultat de 0.69 , puis les résultat de SWLD et on a eu a résultat de 0 .61 puis la combinaison des deux résultats nous a donner une valeur de 0.80 comme la représente les figures suivante . d'où on a remarqué que la combinaison des deux méthodes nous a donne une meilleur valeur pour le résultat.

Nous avons obtenu des performances compétitives pour l'ensemble des donnés FCV , notre approche a un taux de précision de 80 .

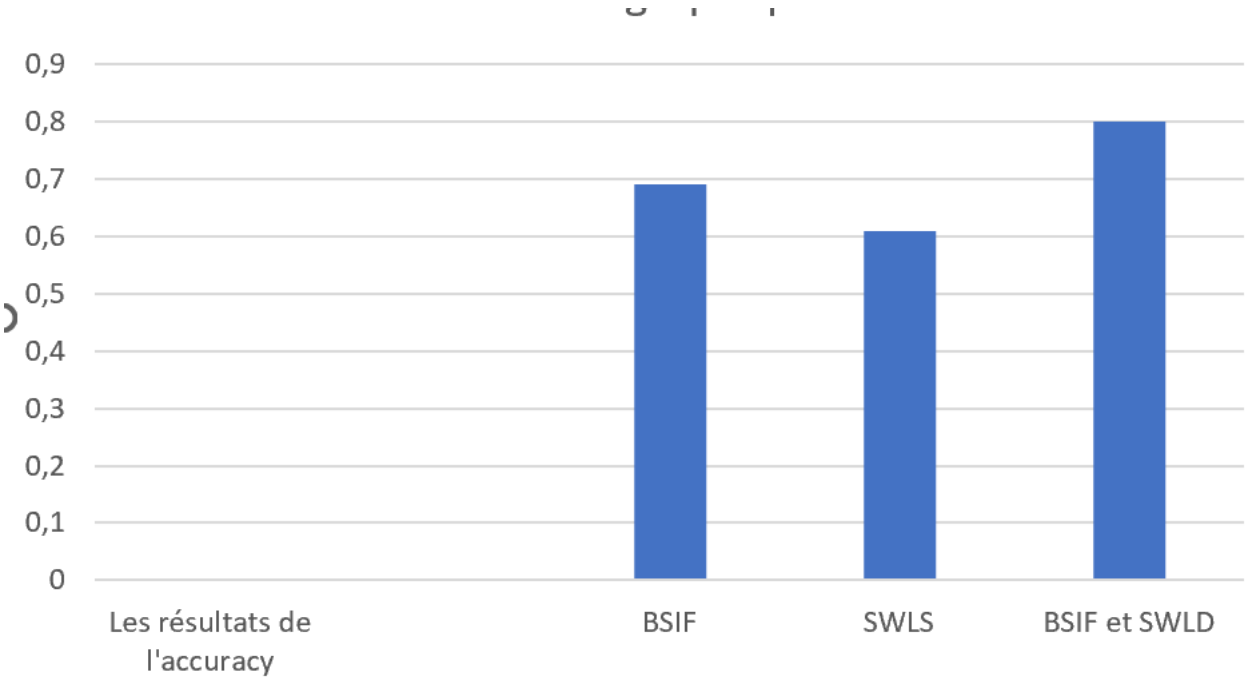

FIGURE 4.6 – Un histogramme qui représente les résultats obtenus dans notre travail

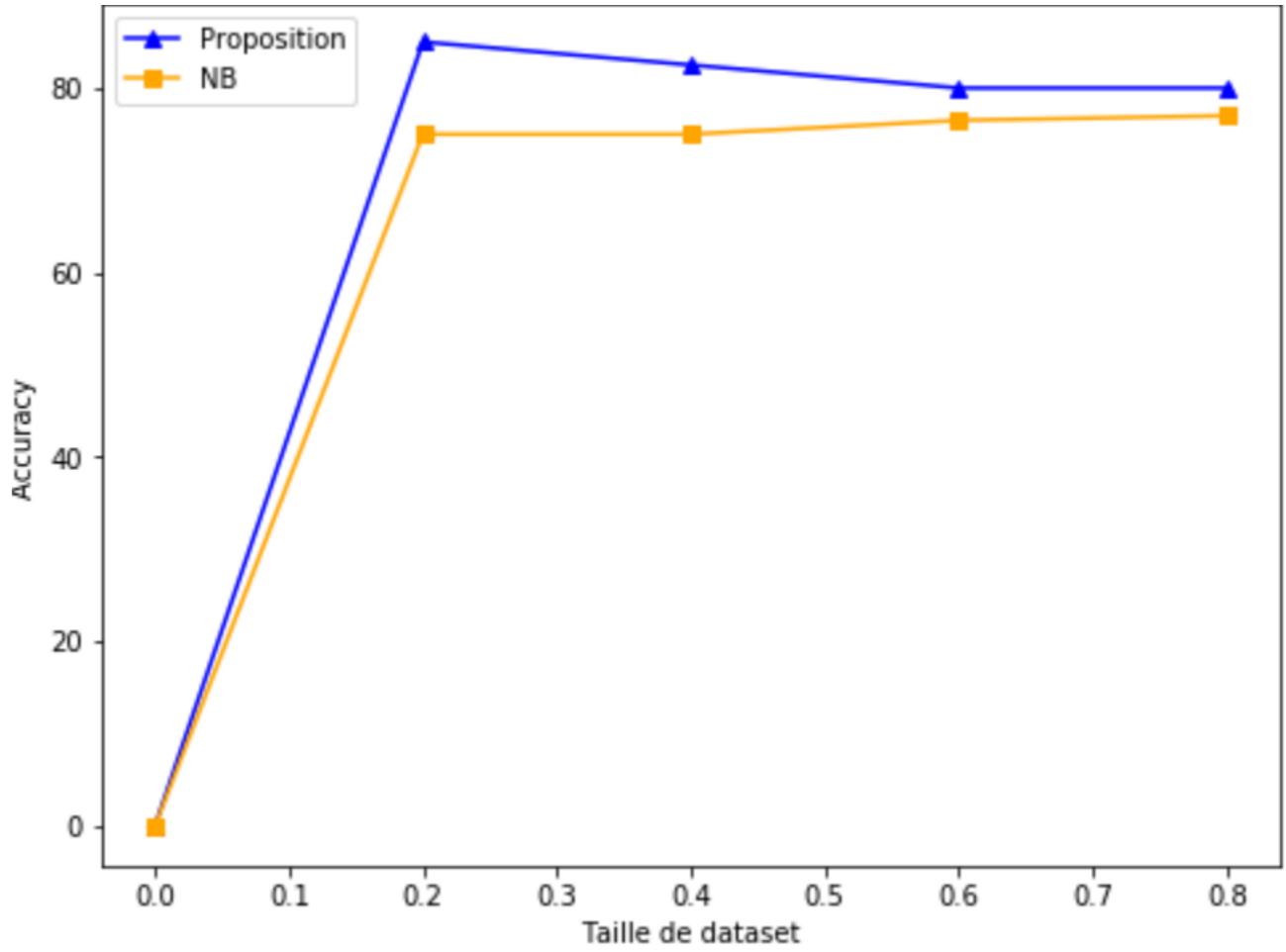

FIGURE 4.7 – Une courbe d'accuracy qui représnete les résultats des données test et validations obtenus dans notre travail

4.4 Interfaces

4.4.1 Affichage de l'interface

Cette page représente l'interface de l'image elle contient tous bouton essentiellement le bouton de browse qui permet de charger une image.

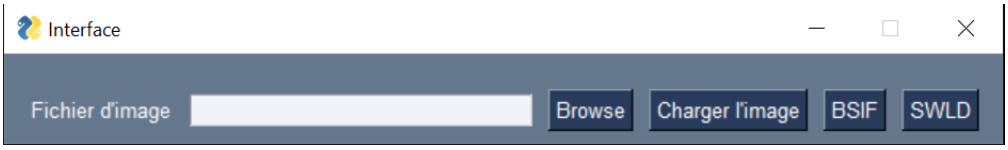

FIGURE 4.8 – Affichage

4.4.2 Parcourire la base de données

Cette page représente la sélection d'une image qu'un utilisateur pourrait sélectionner sur son bureau

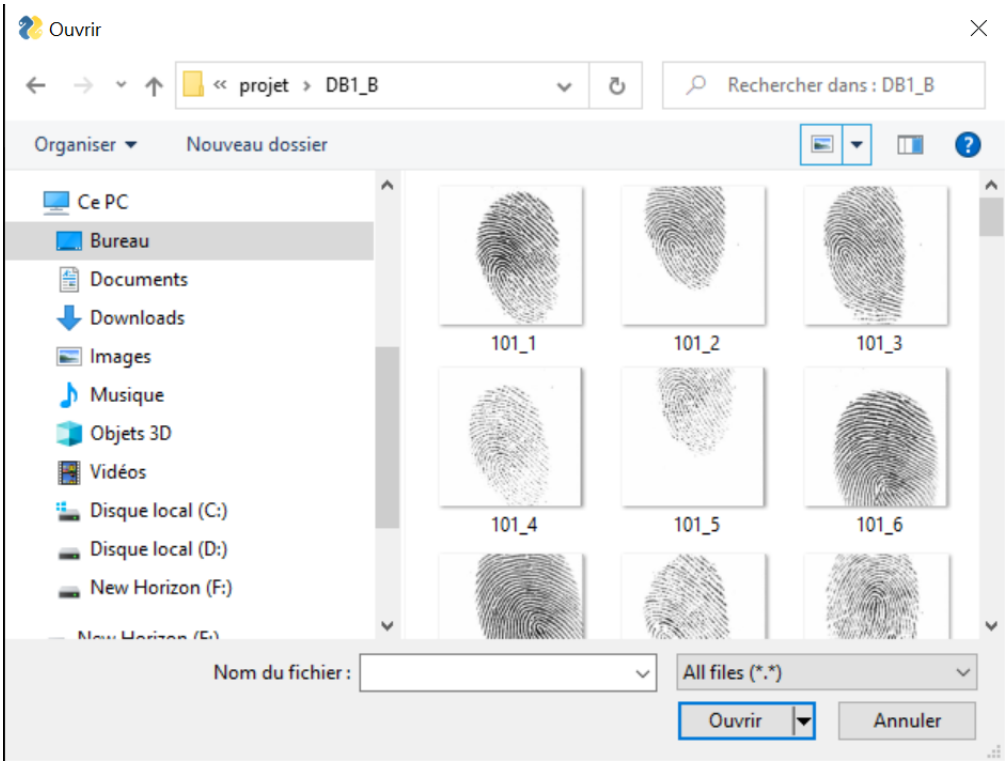

FIGURE 4.9 – Parcourir

4.4.3 Chargement de l'image

Cette page représte l'image sélectionner à partir de la base données existante

FIGURE 4.10 – Chargement de l'image

4.4.4 Filtre BSIF

Cette page représente l'application du filtre BSIF à l'image déjà sélectionner

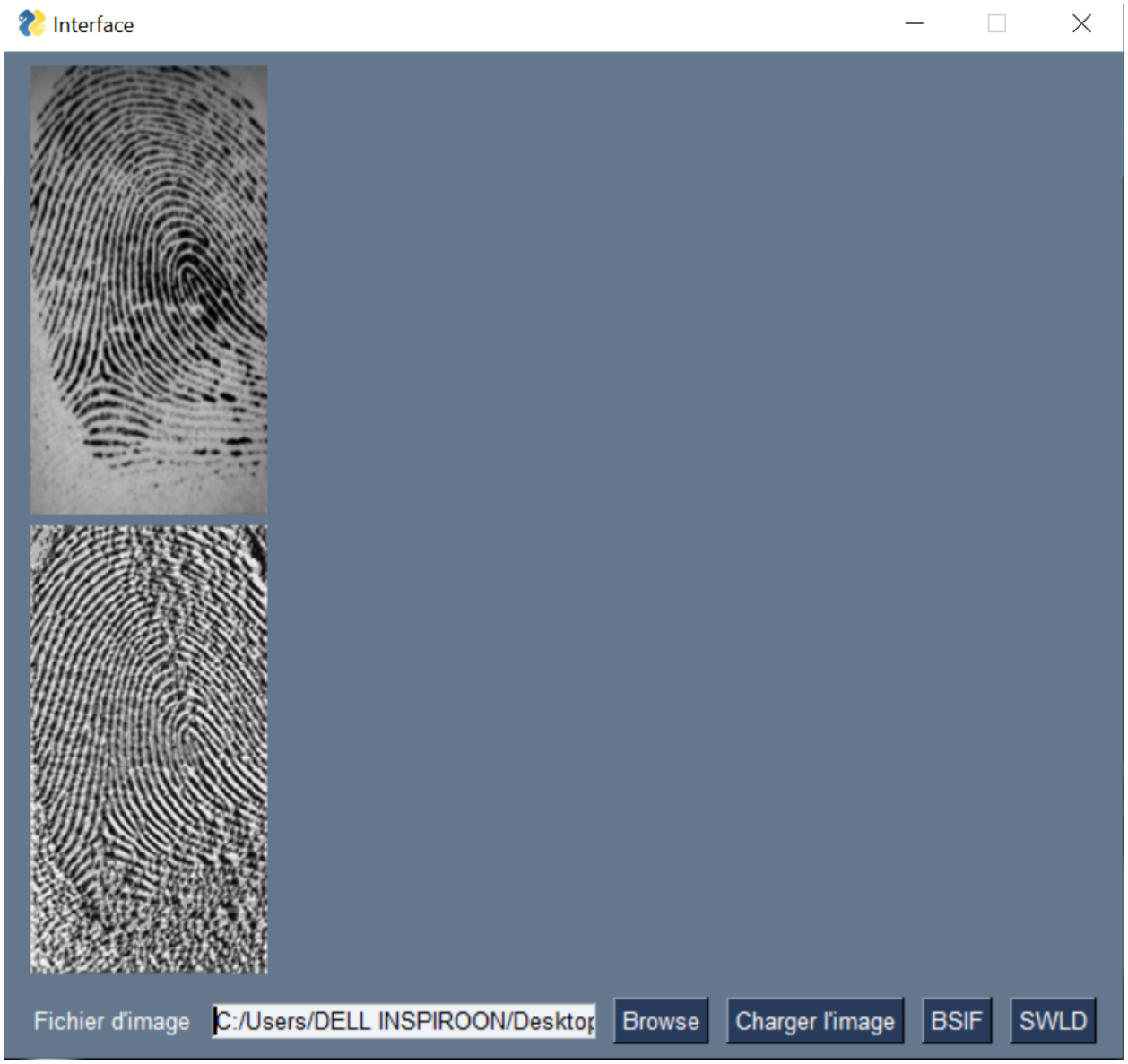

FIGURE 4.11 – Image BSIF

4.4.5 Filtre SWLD

Cette page représente l'application du filtre SWLD à l'image déjà sélectionner

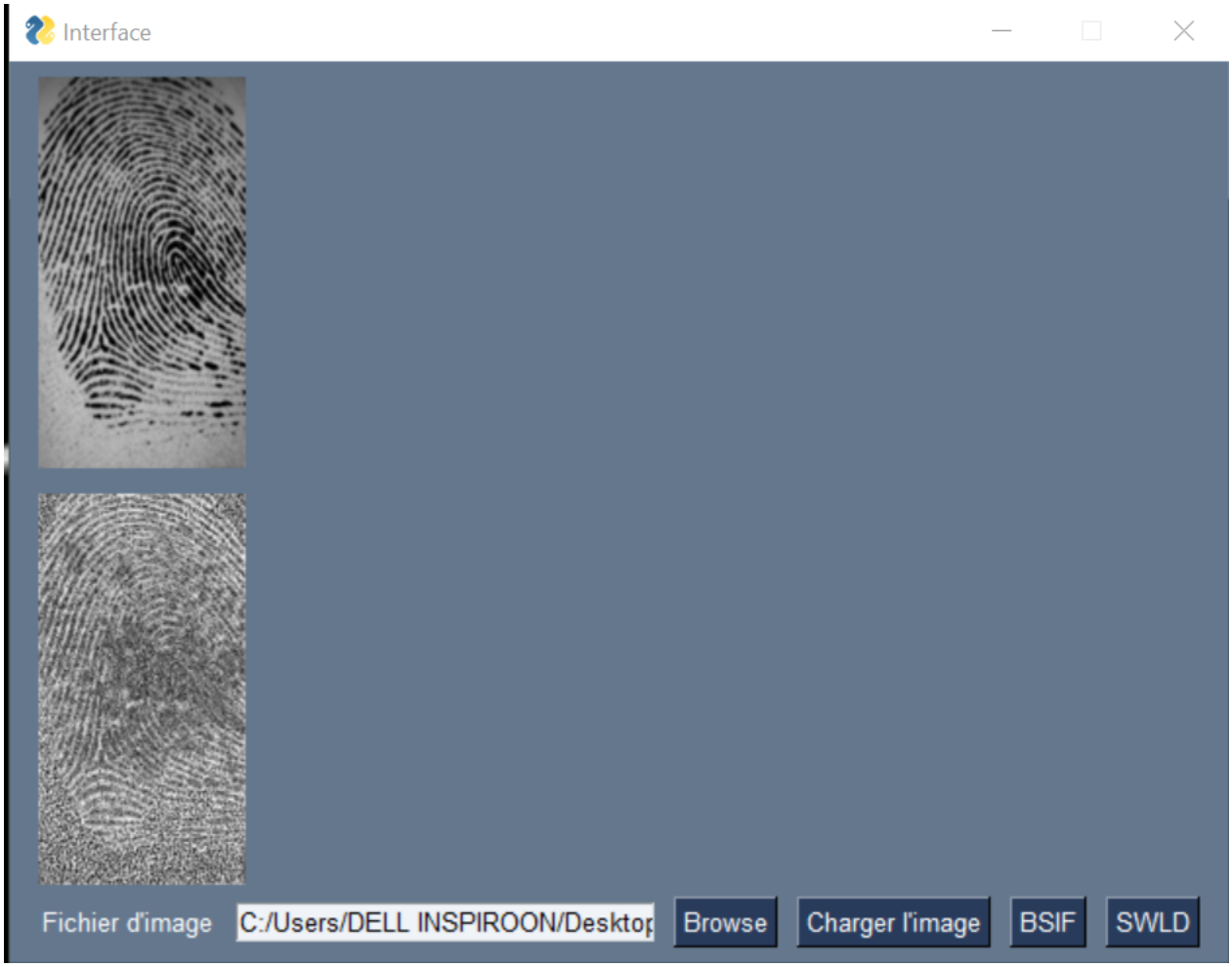

FIGURE 4.12 – Image SWLD

4.5 Conclusion

Dans ce chapitre, nous avons présenté et interpréter les résultats obtenus pour la classification des images des empreintes digitales. Classer une empreintes en considérant les images vrais ou fausse est très difficile car les images des empreintes obtenues d'une personne qui est vrais ressemblent beaucoup à celles qui est falsifié. Pour cela, nous avons utilisé une méthode d'extraction des caractéristiques binaires de l'image en utilisant les descripteurs BSIF (Binarized Statistical Image Features) et SWLD (simplified weber local descriptor) pour la description des images puis on à appliquer l'architecture de CNN (caffenet) pour l'extraction des caractéristique et fusionner les résultat obtenus dans chaque traitement. Pour la phase de classification, nous avons opté dans notre étude à la classification supervisée à savoir le SVM . Les résultats obtenus sans présélection ni prétraitement, ont montré que les modèles proposés sont prometteurs. ET pour finir nous avons présentez les différentes méthodes utilisées pour l'implémentation des différents modules du système.

Conclusion générale

Ce projet nous permis de découvrir une nouvelle discipline, à savoir la reconnaissance automatique d'empreintes digitales, et plus généralement la biométrie, tout en renforçant nos connaissances sur le traitement d'images et la programmation, notamment le python. A travers l'étude des résultats, il est assez facile d'arriver à se rendre compte de la problématique importante de l'analyse et de la comparaison d'empreintes digitales. Encore aujourd'hui, il est assez difficile d'obtenir des algorithmes qui répondent à plusieurs problèmes simultanément, comme pour l'amélioration d'image où l'on doit réussir à améliorer à la fois les captures d'empreintes trop sèches, trop humides, mal cadrées,. . . De plus, la partie extraction de caractéristiques a elle aussi son lot de problèmes, à savoir comment déterminer si une minutie se révèle être ou non un faux positif. Il s'agit donc d'avoir une vraie réflexion de fond sur le problème et de fournir un travail assez conséquent pour pouvoir donner un niveau de garantie sûr en matière de reconnaissance positive ou négative.

L'objectif de ce travail est la mise en œuvre et l'évaluation de plusieurs méthodes d'extraction de caractéristiques pour la reconnaissance des empreintes digitales en utilisant des filtre et classificateur. Nous avons donc décrit dans ce mémoire les différentes étapes nécessaires à la construction d'un système de reconnaissance des empreintes digitales à savoir : les pré-traitements, l'extraction des caractéristiques et la classification.

Dans le premier chapitre nous avons vus des généralité et sur la biométrie des empreintes digitales qui a été traitée plus particulièrement dans notre travaille. Nous avons visez surtout deux objectifs. Le premier est de présenter les principaux éléments théoriques liés aux empreintes digitales et à la biométrie associée, utiles à la bonne compréhension de notre problématique. Le deuxième est de discuter des problèmes actuels rencontrés en biométrie des empreintes digitales, puis des grands enjeux qui ont justifié notre étude sur l'utilisation.

dans le deuxième chapitre de nombreuses études ont été proposées dans la littérature. Notre orientation s'est focalisée sur les caractéristiques A travers ce premier chapitre, nous avons présenté un état de l'art sur les technique d'usurpation des empreintes digitales basées sur le logiciel, les différentes modalités ainsi que les critères d'évaluation des performances de ce type de systèmes. Ensuite, nous avons mis en évidence une comparaison entre ces technique , tout en accordant une attention particulière à la reconnaissance des empreintes, puisqu'elles constituent un bon choix, en termes de praticabilité, robustesse, acceptabilité et nouveauté, afin d'évaluer les descripteurs de texture locaux proposés dans ce projet. Finalement, nous avons terminé le chapitre par une brève conclusion, qui constitue un défi très important que nous voulons exploiter dans le futur travail, par l'application et le développement des descripteurs de texture locaux proposés.

Dans le troisième chapitre on à présenter un aperçu général sur la phase pratique de notre travail qui consiste à mettre en œuvre une méthode basée sur le logiciel . Nous avons donc présenté d'une part les méthodes et les techniques utilisées pour le traitement des image telle que le BSIF et SWLD , et on à mis en évidence des tests sur l'application et les résultats obtenue . D'autre part, nous avons extraire les caractéristiques des empreintes en utilisant une architecture spécifique CNN et pour terminer on a classifier les résultat obtenus avec un classifieur SVM . Finalement, nous avons terminé le chapitre par la présentation des résultat de notre projet.

Nous avons enfin présenté les résultats expérimentaux de ces approches dans le quatrième chapitre. Nous avons exposé premièrement des notions liés à décrivez les critères les plus souvent employés pour évaluer la performance des systèmes de reconnaissance en phase de généralisation, puis on a fait la description de la base de données utilisée.Et nous avons fait plusieurs tests afin de trouver les paramètres optimaux du système et afficher les résultats obtenus.

Bibliographie

[1] A. Anjos, J. Komulainen, S. Marcel, A. Hadid, and M. Pietikäinen. Face anti-spoofing : Visual approach. *Advances in Computer Vision and Pattern Recognition*, page 65–82, 2014.

[2] A. Benishak. *Sélection de variables par les machines a vecteurs supports pour la discrimination binaire et multi classe en grande dimension.* Thèse doctorat, Université de Tunis, 2007.

[3] A. Habib, and A. Selwal. Robust anti-spoofing techniques for fingerprint liveness detection : A survey. *IOP Conference Series : Materials Science and Engineering*, 1033(012026), 2021.

[4] A. Nait-Ali, R. Fournier. Traitement du signal et de l'image pour la biométrie. *L'OUASIR*, 2012.

[5] A. Patil, R. Kruthi and S. Gornal . Analysis of multi-modal biometrics system for gender classification using face, iris and fingerprint images. *I.J. Image, Graphics and Signal Processing*, 5 :34–43, 2019.

[6] A.K. Jain, L. Hong and S. Pankanti . Biometrics : Promising frontiers for emerging identification market. *Comm. ACM*, pages 91,98, 2000.

[7] `https://www.onespan.com/fr/topics/authentification-biometrique`, (consulté le 13/08/2022).

[8] C. Cortes and V. Vapnik. Support-vector networks. *Machine learning*, 20 :273–297, 1995.

[9] `https://www.techtarget.com/searchenterpriseai/definition/convolutional-neural-network`, (consulté le 07/06/2022).

[10] D. Gragnaniello, G. Poggi, C. Sansone. Fingerprint liveness detection based on weber's local image descriptor. *IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications (BIOMS)*, pages 46–50, 2013.

[11] D. Gragnaniello, G. Poggi, C. Sansone, and L. Verdoliva. Fingerprint liveness detection based on weber local image descriptor. *IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications*, 2013.

[12] D. Maio, D. Maltoni, R. Cappelli, J.L. Wayman, A.K. Jain. Fvc2002 : Second fingerprint verification competition. *Object Recognition Supported by User Interaction for Service Robots*, 2002.

[13] D. Maltoni, D. Maio, A.K. Jain, S. Prabhakar. Handbook of fingerprint recognition. *Springer New York*, 2003.

[14] D. Maltoni, D. Maio, A.K. Jain, S. Prabhakar. *Handbook of Fingerprint Recognition*, pages 1–52. Springer Professional Computing, New York, 1st edition, 2003.

[15] D. Tony. " la reconnaissance des empreintes digitales. *BA3-INFO Université Libre de Bruxelles*, 2009.

[16] D. Valdes-Ramirez, M.A. Medina-Perez, R. Monroy, O. Loyola-Gonzalez, J. Rodriguez, A. Morales and F. Herrera. A review of fingerprint feature representations and their applications for latent fingerprint identification : Trends and evaluation. *IIEEE Access*, 2019.

[17] E. Marasco, and A. Ross. A survey on antispoofing schemes for fingerprint recognition systems. *ACM Computing Surveys*, 47(2), 2014.

[18] E. Marasco, Z. Chapman, B. Cukic . Impoving fingerprint interoperability by integrating wavelet entropy and binarised statical image features. *Lecture Notes in informatic*, 2016.

[19] E. Park, W. Kim, Q. Li, J. Kim, and H. Kim. Fingerprint liveness detection using cnn features of random sample patches. *2016 International Conference of the Biometrics Special Interest Group (BIOSIG)*, 2016.

[20] F. Annalisa, and M. Davide. Fingerprint synthesis and detection of usurpations. *Springer London*, 2008.

[21] F.Parrain. Capteur intégré tactile d'empreintes digitales à microstructures piezorésistives. *Ph.D. dissertation, INPG, TIMA Laboratory*, 2002.

[22] `https://iq.opengenus.org/fully-connected-layer`, (consulté le 07/06/2022).

[23] G. Carneiro, J. Nascimento†, A.P. Bradley. Deep learning models for classifying mammogram exams containing unregistered multi-view images and segmentation maps of lesions. *University of Queensland, Brisbane, QLD, Australia*, 2017.

[24] G. Luca, H. Abdenour, L. Gian and R. Fabio . Fingerprint liveness detection using local texture features. *The Institution of Engineering and Technology*, 6(3) :224–231, 2017.

[25] G.Luca, H.Abdenour, M.Gian, R.Fabio. Fingerprint liveness detection using binarized statistical image features. *IEEE Sixth International Conference on Biometrics*, 2013.

[26] J. Chen, S. Shan, C. He, G. Zhao, M. Pietikinen, X. Chen, W. Gao. Wld : un descripteur d'image local robuste. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 32 :1705–1720, 2009.

[27] J. CKannala, E. Rahtu. Bsif : Binarized statistical image features. in pattern recognition. *(ICPR)21st International Conference on*, pages 1363–1366, 2012.

[28] J.D. Stosz and L.A. Alyea. Automated system for fingerprint authentication using pores and ridge structure. *Proceedings of SPIE in Automatic Systems for the Identification and Inspection of Humans*, 2277 :210–223, 1994.

[29] L. Paulhac. *Weber pattern and Binarized Statistical Image Features encoded CNN for fingerprint liveness detection.* 2009.

[30] M. Khammari. *Weber pattern and Binarized Statistical Image Features encoded CNN for fingerprint liveness detection.* International Conference on Image and Signal Processing and their Applications (ISPA), 2019.

[31] M. Shervin, A. Elham, A. Amirali. Fingernet : Pushing the limits of fingerprint recognition using convolutional neural network. *arXiv Cornell University*, 2019.

[32] https://machinelearningmastery.com/pooling-layers-for-convolutional-neural-networks/, (consulté le 07/06/2022).

[33] M.Madina, B.Salah . Crypto système biométrique pour la protection du template d'empreinte digitale. *Mémoire de fin d'études Master Option Informatique Légale et Multimédia, Université Mohamed Seddik Benyahia Jijel*, 2020.

[34] N. Morizet. *Reconnaissance Biométrique par Fusion Multimodale du Visage et de l'Iris.* Ecole Nationale Supérieure des Télécommunications, 2009.

[35] Nicolas Galy. Etude d'un syst'eme complet de reconnaissance d'empreintes digitales pour un capteur microsystème à balayage. *PhD thesis, Institut National Polytechnique de Grenoble-INPG*, 2005.

[36] https://www.forensicsciencesimplified.org/prints/principles.html, (consulté le 07/06/2022).

[37] N.K. Ratha, J.H. Connell, and R.M. Bolle. Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal*, 40(3) :614–634, 2001.

[38] https://docs.python.org/3/, (consulté le 10/05/2022).

[39] R. Derakhshani, S.A.C. Schuckers, L.A.Hornak, and L. O'Gorman,. Determination of vitality from a non-invasive biomedical measurement for use in fingerprint scanners. *Pattern Recognition*, 36(2) :383–396, 2003.

[40] (Consulté le 22/08/2022).

[41] https://almas-industries.com/blog/fingerprint-scanners-types, (consulté le 28/02/2022).

[42] https://www.lemondeinformatique.fr/actualites/lire-des-hackers-ont-trompe-le-capteur-\
\biometrique-de-l-iphone-5s-55113.html, (Consulté le 01/03/2022).

[43] R.Benjanna. Protéger l'échange d'information via un système crypto-biométrique. *Mémoire de fin d'études Master Option Système d'information, Université Larbi tebessi -Tebessa*, 2021.

[44] R.F. Nogueira, R. Alencar Lotufo, and R. Campos Machado. Fingerprint liveness detection using convolutional neural networks. *IEEE Transactions on Information Forensics and Security*, 11(6) :1206–1213, 2016.

[45] S.S. Kulkarni, and H.Y.Patil. Survey on fingerprint spoofing, detection techniques and databases. *International Journal of Computer Applications*, 2015.

[46] https://legalbeagle.com/6498833-importance-fingerprints-forensic-science.html, (consulté le 17/06/2022).

[47] V. Messéant, P. Nizou, N. Villain . Modélisation des empreintes digitales. *Université Paris VII*, 2006.

[48] X. Tong, J. Huang, X. Tang and D. Shi. Fingerprint minutiae matching using the adjacent feature vector. *Pattern Recognition Letters*, 2005.

[49] Z. Xia , C. Yuan, R. Lv, X. Sun, N. Xiong and Y. Shi. A novel weber local binary descriptor for fingerprint liveness detection. *IEEE Transactions on Systems, Man, and Cybernetics : Systems*, page 1–11, 2018.

[50] Z. Xia, R. Lv, and X. Sun. Rotation-invariant weber pattern and gabor feature for fingerprint liveness detection. *Multimedia Tools and Applications*, 77(14) :18187–18200, 2017.