RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE
ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR
ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITÈ MOHAMMED SADDIK BEN YAHIA
JIJEL

Faculté des sciences exactes et d' informatique
Département d'informatique

PROJET DE FIN D'ÉTUDES

Pour obtenir le diplôme de Master 2
Spécialité : **Informatique Légale et Multimedia**
présentée et soutenue publiquement
par

Nekhla Iness et Yousfi Hadjer

Titre:

LBP ET CARACTÉRISTIQUES D'EMPREINTE POUR L'IDENTIFICATION BIOMÉTRIQUE PAR EMPREINTE DIGITALE

Directeur de thèse: **Mme.Belhadef Mahamdioua.M**

Année Universitaire : 2016 / 2017

RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE
ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR
ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITÈ MOHAMMED SADDIK BEN YAHIA
JIJEL

Faculté des sciences exactes et d' informatique
Département d'informatique

PROJET DE FIN D'ÉTUDES

Pour obtenir le diplôme de Master 2
Spécialité : **Informatique Légale et Multimedia**
présentée et soutenue publiquement
par

Nekhla Iness et Yousfi Hadjer

Titre:

LBP ET CARACTÉRISTIQUES D'EMPREINTE POUR L'IDENTIFICATION BIOMÉTRIQUE PAR EMPREINTE DIGITALE

Directeur de thèse: **Mme.Belhadef Mahamdioua.M**

Année Universitaire : 2016 / 2017

الملخص

إنّ التعرف على بصمات الأصابع مشكلة متناولة بكثرة، والتقنيات الآلية للتعرف و التحقق من البصمة تم تكييفها بنجاح مع التطبيقات المدنية والقانونية منذ عدّة سنوات. وقد تم تطبيق هذه التقنية على نطاق واسع في مجالات التعرف بسبب تفرد بصمة الأصبع، وثباتها، وعادة ما يتمّ استخدام النقاط المهمة لمقارنة بصمات الأصابع. لكنّ هذه التقنيات التي تعتمد على النقاط المهمة تعاني من العديد من المشاكل مثل ظهور النقاط المهمة الخاطئة، ومشكل دوران صور بصمات الأصابع وما إلى ذلك.

نقترح في هذه الأطروحة استعمال طريقة (النمط الثنائي المحلي) في التعرف على بصمات الأصابع، وهو واصف رياضي قويّ، ثابت لتغيرات مستويات الرمادي، وتمييزي للغاية. قمنا باستخدام هذه الطّريقة حول نواة البصمة وبهدف تحسين معدل التّعرف دمجنا نتائج هذه الطّريقة مع نتائج التقنية التي تعتمد على النقاط المهمة حيث نسبقها بمعالجة أولية.

بينت نتائج تجاربنا تحسينات جيدة على مستوى الطرق المقترحة خاصة طريقة الدّمج حيث أعطت نتائج أفضل.

الكلمات المفتاحية : البصمة، النقاط المهمة، النّواة، النمط الثنائي المحلي، معالجة أولية.

Résumé

L'identification de l'empreinte digitale est un problème très étudié, et les techniques automatiques d'identification / vérification de l'empreinte digitale ont été adaptées avec succès aux applications civiles et légales depuis de nombreuses années. Cette modalité à été largement appliquée en reconnaissance, en raison de son unicité, et de son immutabilité, d'où les minuties sont généralement utilisées pour la comparaison des empreintes digitales. Ces techniques à base de minuties souffrent de plusieurs problèmes tels que les fausses minuties trouvées, la rotation des images d'empreintes, ... etc.

Dans ce mémoire nous ciblons l'identification des empreintes digitales à l'aide de la méthode LBP (Local Binary Pattern), qui est un descripteur mathématique puissant, invariant par rapport aux changements de niveaux de gris, et très discriminatif. Nous avons proposé d'utiliser LBP autour du noyau et afin d'améliorer le taux de reconnaissance nous avons opté de fusionner cette méthode avec celle basé sur les minuties qui est précédé d'un prétraitement.

Les résultats de notre expérimentation montrent de bonnes améliorations aux niveaux des méthodes proposées mais la fusion a donné de meilleurs résultats.

Mots clés : Empreinte Digitale ; Minutie ; Noyau ; LBP ; Prétraitement

Abstract

Fingerprint identification is a well-researched problem that has been successfully adapted to both civilian and forensic applications since a long time. This modality has been widely applied in recognition, because of its uniqueness, and its immutability, hence minutiae are generally used for the comparison of fingerprints. However these minutiae-based techniques suffer from several problems such as false minutiae, rotation of fingerprint images, etc.

In this thesis, we focus on the identification of fingerprints using the LBP (Local Binary Pattern) method, which is a powerful mathematical descriptor, invariant with gray scale changes, and very discriminative. We proposed to use the LBP around the core of the fingerprint, and merge it with that based on minutiae preceded by a pre-processing step.

The results of our experimentation show good improvements for the proposed methods especially for the fusion one.

Keywords : Fingerprint ; Minutiae ; Core Point ; LBP ; Pre-processing

Remerciements

Pour commencer, Nous voulons adresser nos remerciements

A notre encadreur de mémoire, Madame BELHADEF MAHAMDIOUA MERIAMA

Vous avez bien voulu nous confier ce travail riche d'intérêt et

nous guider à chaque étape de sa réalisation.

Vous nous avez toujours réservé le meilleur accueil

malgré vos obligations professionnelles.

Vos encouragements inlassables, votre amabilité, votre

gentillesse méritent toute admiration.

Nous saisissons cette occasion pour vous exprimer notre

profonde gratitude tout en vous témoignant notre respect.

A notre juge de thèse et président de jury Monsieur ZAHIR MAHROUK

Vous nous faites l'honneur d'accepter avec une très

grande amabilité de siéger parmi notre jury de thèse.

Veuillez accepter ce travail, en gage de notre

grand respect et notre profonde reconnaissance.

A notre juge de thèse Monsieur LAABANI MARWANE

Vous nous avez honorés d'accepter avec grande

sympathie de siéger parmi notre jury de thèse.

Veuillez trouvez ici l'expression de notre grand respect

et nos vifs remerciements.

Dédicace

Je dédie cette thèse à...

A ma très chère mère LEILA BENYEZZAR

Affable, honorable, aimable : Tu représentes pour moi le symbole de la bonté par excellence, la source de tendresse et l'exemple du dévouement qui n'a pas cessé de m'encourager et de me soutenir.

Tous les sacrifices consentis et ses précieux conseils pour toute son assistance et sa présence dans ma vie reçois à travers ce travail aussi modeste soit-il l'expression de mes sentiments et de mon éternelle gratitude.

A mon très cher père DJAMEL

qui peut être fier et trouver ici le résultat de longues années de sacrifices et de privations pour m'aider à avancer dans la vie

Puisse Dieu faire en sorte que ce travail porte son fruit

Merci pour les valeurs nobles

l'éducation et le soutient permanent venu de toi.

A mes très cher frères Amine et Anis

Mes cher frères présent dans tous mes

moments d'examens par leurs soutien moral et

leurs belles surprises sucrées.

Je vous souhaite un avenir plein de joie

de bonheur, de réussite et de sérénité.

Je vous exprime à travers ce travail

mes sentiments de fraternité et d'amour.

A tous les membres de ma famille, petits et grands

Veuillez trouver dans ce modeste travail l'expression de
mon affection.
Je vous dédie ce travail en témoignage de mon profond

amour. Puisse Dieu, le tout puissant, vous préserver et

vous accorder santé, longue vie et bonheur.

INESS

Dédicace

Avant tout je tiens à remercier le

bon dieu pour m'avoir

aider à accomplir ce

travail dans des bonnes

conditions.

Je dédie ce modeste travail

A TOUTE LA FAMILLE

A MES AMIS FIDELS

A TOUS CEUX QUI ME SONT CHERS

HADJER

Table des matières

Table des figures

Liste des tableaux

Introduction Génerale

DAns la société complexe, en mobile et réseau électronique, la vie privée est devenue une question importante. La reconnaissance biométrique est considérée comme plus fiable que les mots de passe et les codes pins. De plus en plus, les systèmes de reconnaissance biométriques ont été déployés dans les applications gouvernementales, civiles et commerciales.

Le terme "biométrie" provient des mots grecs, «bios» qui veut dire la vie et du mot «métrique» qui veut dire mesure. La biométrie est une mesure des caractéristiques 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'empreinte digitale et du visage).

Parmi toutes ces techniques, l'utilisation de l'empreinte digitale comme un moyen de reconnaissance est la plus courante. La force de ce procédé tient du fait que l'utilisation de l'empreinte digitale est généralement facile à accepter par la majorité des gents, et qu'elle est une des plus efficace et des moins coûteuse comparé aux autres modalités biométriques. Ainsi, l'unicité et l'invariance avec l'âge sont les principales caractéristiques de l'empreinte digitale.

Dans ce contexte, nous nous intéressons dans ce mémoire à l'identification de l'empreinte digitale. Cependant, la plupart des systèmes d'identification des empreintes digitales consiste à extraire en premier lieu de l'image d'empreinte à étudier tous les minuties, et ensuite comparer ces points avec ceux des modèles enregistrés dans une base de données pour trouver le modèle le plus corrélé avec l'empreinte étudiée. Mais Cette approche présente quelques difficultés comme par exemple :

- Il est très difficile d'extraire les minuties d'une image d'empreinte digitale bruitée. Ce problème est très fréquent dans la pratique.
- Le changement d'échelle, de translation et de rotation des empreintes digitales pose des difficultés pour l'étape de mise en correspondance.
- Harmoniser les points de minuties est un passage obligé dans ce système, cependant, le nombre de minuties extraits de chaque empreinte digitale n'est pas uniforme et n'est pas cohérent. Cela rend le temps de calcul de l'étape d'identification très long.

Pour surmonter ces limitations, une étape de prétraitement pour améliorer la clarté de l'image d'empreinte et l'utilisation d'une méthode efficace d'extraction des caractéristiques des images d'empreinte est une nécessité majore.

De ce fait, nous proposons dans ce mémoire d'utilisé l'opérateur LBP (Local Binary Pattern) autour du noyau de l'image d'empreinte digitale améliorée par une méthode de prétraitement. Le LBP est un descripteur très efficace qui est utilisé avec plusieurs modalités (visage, iris, empreinte,...). Après, nous fusionnons les résultats de notre proposition avec ceux de la méthode basée sur les minuties que nous avons

précédés par une étape de prétraitement.

Notre mémoire est scindé en quatre chapitres principaux :

— **Le premier chapitre** est consacré aux notions de base sur la biométrie, l'architecture générale d'un système biométrique, les modalités biométriques les plus couramment utilisées.

— **Le deuxième chapitre** présente la modalité d'empreinte avec ses caractéristiques. Ensuite, les détails des différentes étapes d'un système de reconnaissance d'empreinte digitale sont exposés.

— **Le troisième chapitre** est consacré à la présentation de la méthode LBP, son principe, ces variantes, et un état de l'art sur l'utilisation de cette méthode avec les empreintes digitales.

— **Le quatrième chapitre** expose nos propositions ainsi que les résultats expérimentaux. Nous commençons par la définition de la problématique, puis nous détaillerons les différentes étapes de notre proposition. Ensuite nous terminons ce chapitre par les résultats expérimentaux.

— Enfin nous clôturons notre travail par une conclusion générale.

Chapitre 1

Biométrie

1 Introduction

Les caractéristiques du corps comme le visage et la voix ont toujours étaient utilisées par les êtres-humains pour ce reconnaitre entre eux mais les choses ont beaucoup évolué au milieu du XIXe siècle quand Bertillon, chef de la police scientifique de paris développe et teste une méthode nommé anthropométrie judiciaire, l'idée de la méthode est de prendre un certains nombre de mesures corporelles afin d'identifier les prisonniers. Au moment ou la méthode gagne en popularité une autre méthode beaucoup plus pratique a vu le jour, c'est l'identification par empreinte digitale qui c'est graduellement imposé. Bien que la biométrie ait émergé de son utilisation étendue dans l'application de la loi pour identifier les criminels (par exemple, les étrangers illégaux, la détermination de la paternité, la médecine légale et l'identification positive des condamnés et des prisonniers) elles sont reconnues dans un grand nombre d'applications civiles [A.Jain et al., 2004].

La biométrie est basée sur la reconnaissance automatique d'une personne en utilisant ses traits physiques ou comportementaux telles que l'empreinte digitale, la géométrie de la main, la signature, l'iris, la rétine, le visage, la démarche, l'empreinte palmaire ou l'empreinte vocale. En utilisant la biométrie il est possible d'établir une identité fondée sur qui vous êtes plutôt que par ce que vous possédez (par ex : carte d'identité, badge) ou vous savez (par ex : mot de passe, code pin).

2 Définitions

2.1 Système Biométrique

Un système biométrique est essentiellement un système de reconnaissance de motif qui fonctionne en acquérant des données biométriques d'un individu, en extrayant un ensemble de caractéristiques à partir des données acquises et en comparant ce jeu de caractéristiques avec le modèle défini dans la base de données. Selon le contexte d'application, un système biométrique peut fonctionner en mode de vérification ou en mode d'identification.

2.2 Mode identification

Le système doit deviner l'identité de la personne. Il répond donc à une question de type : « Qui suis-je ? ». Dans ce mode, le système compare le signal mesuré avec les différents modèles contenus dans la base de données (problème de type 1 : n).

2.3 Mode vérification

Le système doit répondre à une question de type : « Suis-je bien la personne que je prétends être ? ». L'utilisateur propose une identité au système et le système doit vérifier que l'identité de l'individu est bien celle proposée. Il suffit donc de comparer le signal avec un seul des modèles présents dans la base de données (problème de type 1 : 1).

3 Architecture d'un système biométrique

Un système biométrique est conçu en utilisant les quatre principaux modules (Voir figure 1.1) [A.Jain et al., 2004].

1. **Module capteur**, qui capture les données biométriques d'un individu. Par exemple, un capteur d'empreinte digitale qui représente la structure des crêtes et des vallées du doigt d'un utilisateur.
2. **Module d'extraction de caractéristique**, dans lequel les données biométriques acquises sont traitées pour extraire un ensemble de caractéristiques discriminatoires. Par exemple, la position et l'orientation de points de minutie dans une image d'empreinte digitale sont extraites dans le module d'extraction de caractéristiques d'un système biométrique d'empreinte digitale.
3. **Module de correspondance**, dans lequel les caractéristiques extraites lors de la reconnaissance sont comparées aux modèles stockés pour générer des scores correspondants. Par exemple, dans le module de correspondance d'un système biométrique à empreinte digitale, le nombre de minuties correspondantes entre l'empreinte digitale d'entrée et les images de modèle est déterminé et un score de correspondance est rapporté. Le module de correspondance encapsule également un module décisionnel, dans lequel l'identité revendiquée d'un utilisateur est confirmée (vérification) ou l'identité d'un utilisateur est établie (identification) sur la base du score correspondant.
4. **Module de base de données système**, qui est utilisé par le système biométrique pour stocker les modèles biométriques des utilisateurs inscrits.

   Le module d'enrôlement est chargé d'inscrire des individus dans la base de données du système biométrique. Pendant la phase d'enrôlement, la caractéristique biométrique d'un individu est d'abord scannée par un lecteur biométrique pour produire une représentation numérique de la caractéristique.

   Un contrôle de qualité est généralement effectué pour s'assurer que l'échantillon acquis peut être traité de manière fiable par des étapes successives. Afin de faciliter la correspondance, la représentation numérique d'entrée est ensuite traitée par un extracteur de caractéristiques pour générer une représentation appelée gabarit.

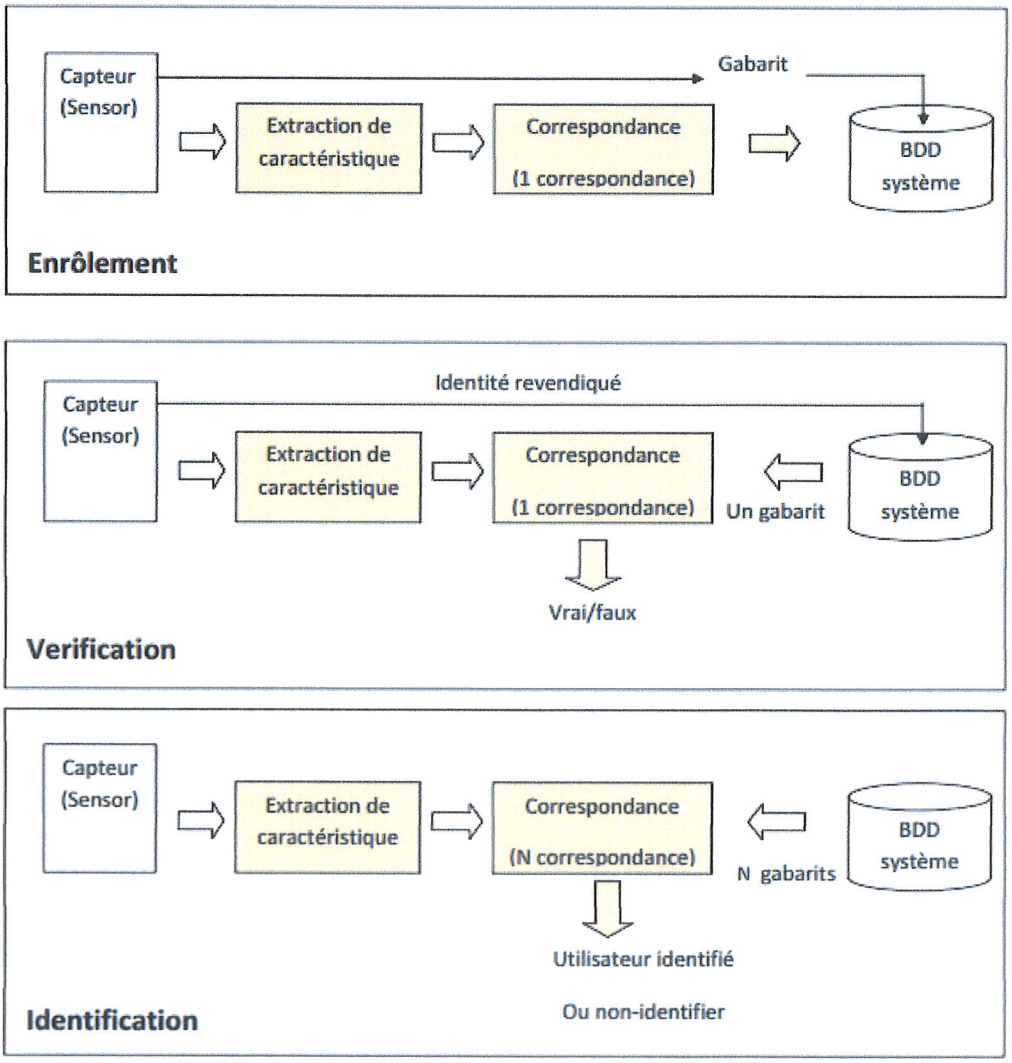


FIGURE 1.1 – Architecture d'un système biométrique [A.Jain et al., 2004].

Le modèle est ensuite stocké dans la base de données centrale du système biométrique ou enregistré sur une carte à puce délivrée à l'individu.

4 Performances des systèmes biométriques

Pour évaluer la performance d'un système biométrique, on peut distinguer les taux suivants [A.Jain et al., 2004] :

- Le **FRR (False Rejet Rate ou Taux de Faux Rejets)** : ce taux représente le pourcentage d'individus censés être reconnus par le système mais qui sont rejetés. C'est le ratio entre le nombre de clients rejets et le nombre total d'accès clients.
- Le **FAR (False Acceptation Rate ou Taux de fausse acceptation)** : c'est le pourcentage d'individus reconnus par le système biométrique, ce système classe alors deux caractéristiques provenant de deux personnes différentes. Il est égale au nombre des imposteurs acceptés divisé par le nombre total d'accès imposteurs.
- **EER (Equal Error Rate)** : c'est le taux d'erreurs égales, un compromis entre les fausses acceptations et les faux rejets, autrement dit c'est le point de mesure sur lequel FAR = FRR. La figure 1.2 illustre le FRR et le FAR à partir de distributions des scores authentiques et imposteurs. Le paramétrage d'un système consiste à trouver le bon équilibre entre ces deux taux, le FAR augmentant lorsque le FRR diminue, et inversement. Un contrôle d'accès très sécurisé aura un FAR très bas, pour garantir qu'aucune personne non autorisée n'accède au site, mais, en contrepartie le FRR sera élevé, ce qui signifie que des utilisateurs valides se verront refuser l'accès.
- **RR (Recognition Rate)** : c'est le taux de reconnaissance, qui est la mesure la plus couramment utilisée pour le mode d'identification. Il est égale au nombre d'individus bien comparées divisé par le nombre total des individus testées.

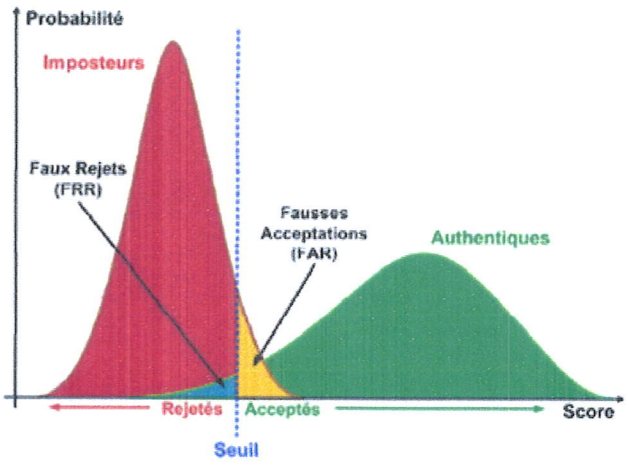


FIGURE 1.2 – Illustration du FRR et du FAR [I.Benchennane, 2015].

5 Modalités biométriques

5.1 Définition d'une modalité

Une modalité biométrique est la combinaison d'un trait biométrique, d'un type de capteur et d'algorithmes pour extraire et traiter les représentations numériques du trait. Elle fait référence à un système conçu pour reconnaître un trait biométrique particulier. Visage, empreinte digitale, géométrie de la main, empreinte palmaire, iris, balayage rétinien, voix, signature, démarche et dynamique des touches sont des exemples de traits biométriques. Dans le contexte d'un système et d'une application donné, la présentation d'une caractéristique biométrique d'un utilisateur comporte à la fois des aspects biologiques et comportementaux. Les modalités biométriques les plus connues décrites par[A.Jain et al., 2004] sont résumés brièvement ci dessous.

5.2 Empreinte digitale

La reconnaissance des empreintes digitales est la technique biométrique la plus utilisée. Une empreinte digitale est le modèle des crêtes et des vallées sur la surface d'un doigt, dont la formation est déterminée au cours des sept premiers mois de développement fœtal. Les empreintes digitales des jumeaux identiques sont différentes et aussi les imprime sur chaque doigt de la même personne. Les lecteurs d'empreintes digitales scannent puis relèvent des éléments permettant de différencier les empreintes. Ces éléments sont appelés minuties (figure1.3).

Ce type de technique biométrique est utilisé par les institutions financières pour leurs clients et se trouve en même temps dans les hôpitaux, les écoles, les aéroports... etc. Toute fois cette technique n'est pas sans inconvénients car elle nécessite la coopération de l'utilisateur pour posé correctement le doigt sur le lecteur, et aussi le problème de contraste (doigt propre et sec devient trop clair tandis qu'un doit humide devient très foncé)..etc.

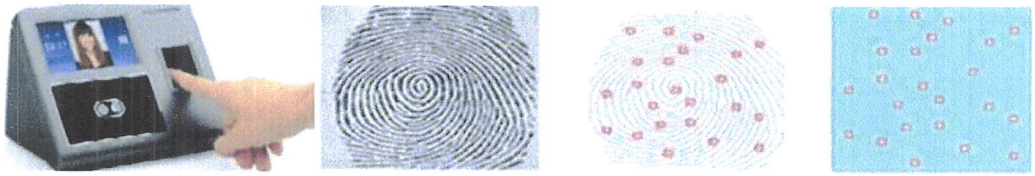


FIGURE 1.3 – Empreinte digitale.

5.3 Visage

La reconnaissance faciale est une méthode non intrusive, et les images faciales sont probablement la caractéristique biométrique la plus communément utilisée par les humains pour faire une reconnaissance personnelle. Les approches les plus populaires pour la reconnaissance faciale sont basées sur :

— L'emplacement et la forme des attributs du visage comme les yeux, les sourcils, le nez, les lèvres et le menton, et leurs relations spatiales (voir figure1.4).

— L'ensemble (Globale) de l'image du visage qui représente un visage comme une combinaison pondérée d'un certain nombre de faces canoniques. Elles imposent un certain nombre de restrictions sur la façon dont les images faciales sont obtenues, nécessitant parfois un fond fixe et simple ou une illumination spéciale.

Ces systèmes ont également des difficultés à reconnaître un visage à partir d'images capturées à partir de deux vues radicalement différentes et sous des conditions d'éclairage différentes. Pour qu'un système de reconnaissance faciale fonctionne bien en pratique, il devrait automatiquement : détecter si un visage est présent dans l'image acquise, localiser le visage s'il y en a un, et reconnaître le visage d'un point de vue général (c'est-à-dire, de toute pose).

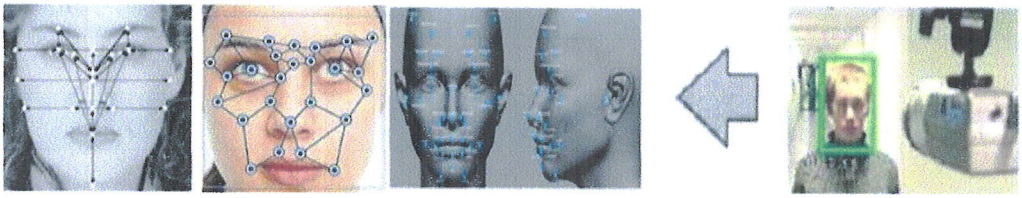


FIGURE 1.4 – Visage.

5.4 Empreinte palmaire

Les paumes des mains humaines contiennent des motifs de crêtes et de vallées comme les empreintes digitales. La zone de la paume est beaucoup plus grande que la surface d'un doigt et, comme résultat, les empreintes palmaires sont attendues pour être encore plus distinctif que les empreintes digitales. Étant donné que les scanneurs de l'empreinte palmaire ont besoin de capteur d'une grande surface, ils sont plus encombrants et plus coûteux que les capteurs d'empreintes digitales. Les palmiers humains contiennent également des caractéristiques distinctives supplémentaires telles que les lignes principales et les rides qui peuvent être capturés même avec un scanner de résolution inférieure, ce qui serait moins cher.

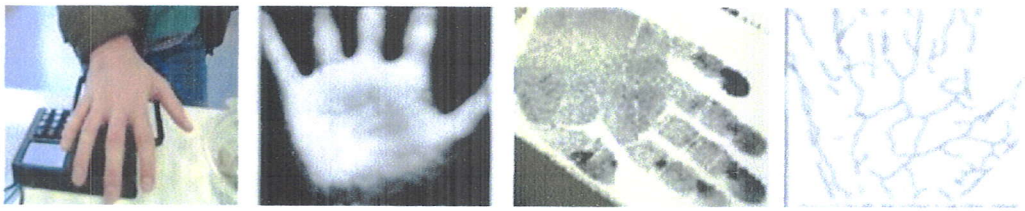


FIGURE 1.5 – Empreinte palmaire.

5.5 Géométrie de la main

La géométrie de la main se réfère à la forme de la main humaine, la taille de la paume et les longueurs et largeurs des doigts. Les avantages de cette modalité

sont qu'il est relativement simple et facile à utiliser. Les systèmes sont généralement utilisés pour la vérification plutôt que pour l'identification. En outre, du fait que les dispositifs de capture doivent avoir au moins la taille d'une main, Ils sont trop grands pour les appareils comme les ordinateurs portables.

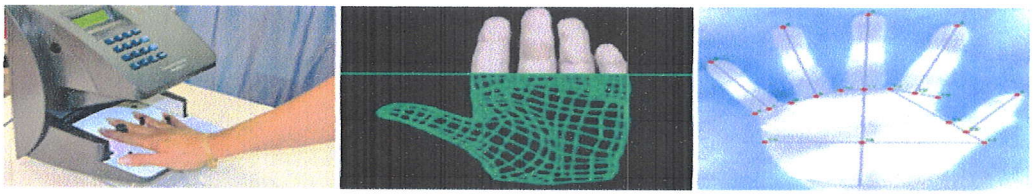


FIGURE 1.6 – Géométrie de la main.

5.6 Iris

L'iris est la région annulaire de l'œil délimitée par la pupille et la sclère (blanc de l'œil) de chaque côté. La texture visuelle de l'iris se forme pendant le développement du fœtus et se stabilise durant les deux premières années de vie. La texture complexe de l'iris porte des informations très distinctives utile pour la reconnaissance personnelle. La précision et la vitesse des systèmes de reconnaissance basés sur l'iris actuellement déployés est prometteurs et mettent en évidence la faisabilité de systèmes d'identification à grande échelle basés sur l'information sur l'iris.

Chaque iris est distinctif et comme les empreintes digitales, même les iris des jumeaux identiques sont différents. Il est extrêmement difficile de manipuler chirurgicalement la texture de l'iris. En outre, il est assez facile de détecter des iris artificiels (par exemple, des lentilles de contact). l'image de l'iris est capturée par un appareil qui contient une caméra infrarouge, lorsque la personne se place à une courte distance de l'appareil (voir figure1.7).

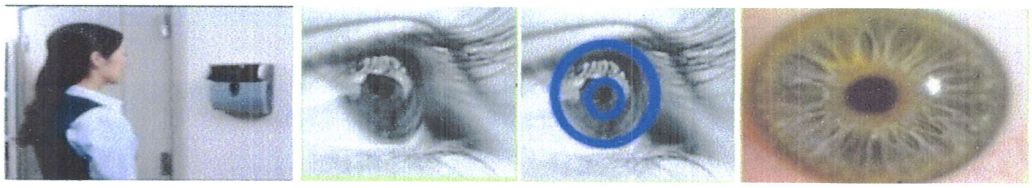


FIGURE 1.7 – Iris.

5.7 Balayage rétinien

La vascularisation rétinienne est riche en structure et est censé être une caractéristique de chaque individu et de chaque œil. Il est affirmé être la biométrie la

plus sécurisé car il n'est pas facile de modifier ou de reproduire le système vasculaire rétinien. L'acquisition d'image nécessite une personne qui s'installer à proximité du lecteur rétinien (quelques centimètres) et se concentrer sur un point spécifique dans le champ visuel de sorte qu'une partie prédéterminée de la vascularisation rétinienne pourrait être imagée. L'acquisition d'images implique la coopération du sujet, et nécessite un effort conscient de la part de l'utilisateur. Tous ces facteurs nuisent à l'acceptabilité publique de la biométrie rétinienne. La vascularisation rétinienne peut révéler certaines conditions médicales, par exemple l'hypertension, qui est un autre facteur qui dissuade l'acceptation publique de la biométrie basée sur le balayage rétinien.

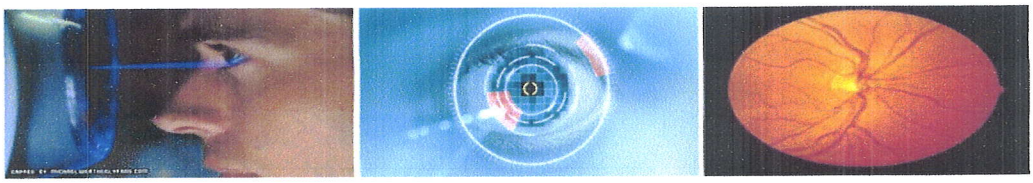


FIGURE 1.8 – Balayage rétinien.

5.8 Voix

La voix combine directement les caractéristiques biologiques et comportementales. Le son que produit un individu lorsqu'il parle est basé sur des aspects physiques du corps (bouche, nez, lèvres, cordes vocales, etc.) et peuvent être affectés par l'âge, l'état émotionnel, la langue maternelle et les conditions médicales. La qualité du dispositif d'enregistrement et le bruit ambiant influencent également les taux de reconnaissance. La voix n'est pas très distinctive et peut ne pas être approprié pour l'identification à grande échelle. On peut trouver deux types de système de reconnaissance vocale :

Un système de reconnaissance vocale dépendant du texte est basé sur la prononciation d'une phrase prédéterminée fixe. Un système de reconnaissance vocale indépendant du texte reconnaît l'orateur indépendamment de ce qu'il dit.

Un système indépendant du texte est plus difficile à concevoir qu'un système dépendant du texte mais offre plus de protection contre la fraude.

FIGURE 1.9 – Signale de voix.

5.9 Signature

La façon dont une personne signe son nom change habituellement au fil du temps. Il peut également être fortement influencé par le contexte, y compris les conditions

physiques et l'état émotionnel du signataire. Malgré que les signatures requièrent un contact avec l'instrument d'écriture et un effort de la part de l'utilisateur, ils ont été acceptés dans les transactions gouvernementales, juridiques et les transactions commerciales comme méthode de vérification. De nombreuses expériences ont aussi montré que les signatures sont relativement faciles à forger.

FIGURE 1.10 – Signature.

5.10 Démarche

Chaque individu, en fonction de son corps et plus spécifiquement de sa musculature, développe une démarche qui lui est propre.

La démarche a un potentiel pour la reconnaissance à distance et potentiellement, sur une longue période de temps. Les systèmes de reconnaissance de la marche sont basés sur le traitement d'image pour détecter la silhouette humaine et les attributs spatiotemporels associés. La marche peut être affectée par plusieurs facteurs, dont le choix des chaussures, la surface de marche et les vêtements. Les systèmes de reconnaissance de la marche sont encore au stade de développement.

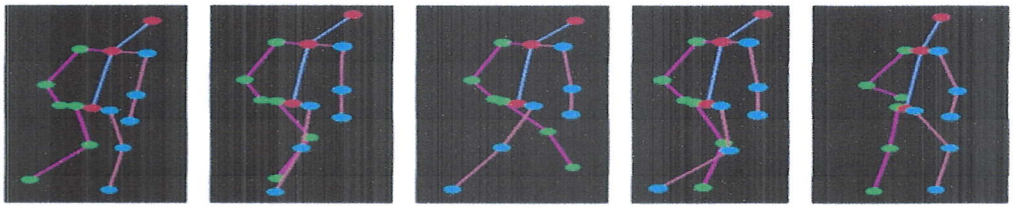


FIGURE 1.11 – Démarche.

5.11 Dynamique de frappe sur clavier

Il est hypothéqué que chaque personne tape sur un clavier d'une manière caractéristique. Cette biométrie comportementale n'est pas attendue d'être unique à chaque individu mais elle offre suffisamment d'informations discriminatoires pour permettre une vérification d'identité. La dynamique de frappe est un comportement biométrique ; fortement affecté par le contexte, tel que l'état émotionnel de la personne, son sa posture, le type de clavier, etc. Les frappes d'une personne utilisant un système pourraient être surveillées discrètement quand cette personne saisit des informations.

FIGURE 1.12 – Dynamique de frappe sur clavier.

6 Comparaison des Modalités

Chaque modalité biométrique a ses avantages et ses inconvénients, dont certains sont mentionnés dans les descriptions ci-dessus. De plus, même si certains des inconvénients pouvaient être surmontés, une modalité elle-même pourrait avoir des défaillances inhérentes, bien que très peu de recherches aient été faites sur ça. Donc, le choix d'un trait biométrique pour une application particulière dépend des problèmes en plus de la performance correspondante. Raphael et Young ont identifiés un certain nombre de facteurs qui rendent un trait physique ou comportemental approprié pour une application biométrique [D.Raphael et al., 1974].

- **Universalité :** chaque personne qui accède à l'application doit posséder le trait.
- **Unicité :** le trait donné doit être suffisamment différent en travers des membres de la population.
- **Permanence :** le trait biométrique d'un individu doit être suffisamment invariant dans le temps par rapport à un algorithme d'appariement donné.
- **Mesurabilité :** il devrait être possible d'acquérir et de numériser le trait biométrique en utilisant des dispositifs appropriés qui ne gênent pas indûment l'individu. En outre, les données brutes acquises devraient être accommodé au traitement pour extraire des caractéristiques représentatives.
- **Performance :** la précision de la reconnaissance et les ressources nécessaires pour atteindre cette précision devrait répondre aux exigences de l'application.
- **Acceptabilité :** les individus de la population ciblée qui utiliseront l'application doivent être prêts à présenter leur trait biométrique au système.
- **Imitable :** la facilité avec laquelle un trait biométrique peut être imité à l'aide de méthodes frauduleuses.

7 Applications de la biométrie

Aujourd'hui, les principales applications sont la production de titres d'identité, le contrôle d'accès à des sites sécurisés, le contrôle des frontières, l'accès aux réseaux, systèmes d'information et stations de travail, le paiement électronique, la signature électronique et même le chiffrement de données.

Modalité Biométrique	Universalité	Unicité	Permanence	Mesurabilité	Performance	Acceptabilité	Imitable
Empreinte digitale	Moyen	Élevé	Élevé	Moyen	Élevé	Moyen	Moyen
Visage	Élevé	Faible	Moyen	Élevé	Faible	Élevé	Élevé
Empreinte palmaire	Moyen	Élevé	Élevé	Moyen	Élevé	Moyen	Moyen
Géométrie de la main	Moyen	Moyen	Moyen	Élevé	Moyen	Moyen	Moyen
Iris	Élevé	Élevé	Élevé	Moyen	Élevé	Faible	Faible
Balayage rétinien	Élevé	Élevé	Moyen	Faible	Élevé	Faible	Faible
Voix	Moyen	Faible	Faible	Moyen	Faible	Élevé	Élevé
Signature	Faible	Faible	Faible	Élevé	Faible	Élevé	Élevé
Démarche	Moyen	Faible	Faible	Élevé	Faible	Élevé	Moyen
Dynamique de frappe	Faible	Faible	Faible	Moyen	Faible	Moyen	Moyen

TABLE 1.1 – Comparaison entre les modalités biométriques [I.Benchennane, 2015].

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

- **Application commerciales :** telles que l'accès au réseau informatique, la sécurité de données électroniques, le commerce électronique, l'accès d'internet, l'ATM, la carte de crédit, le contrôle d'accès physique, le téléphone portable, le PDA, la gestion des registres médicales, etc.
- **Applications de gouvernement :** telles que la carte nationale d'identifications, le permis de conduite, la sécurité sociale, le contrôle de passeport, etc.
- **Applications juridiques :** telles que l'identification de cadavre, la recherche criminelle, l'identification de terroriste, les enfants disparus, etc.

8 Avantages et limites de la biométrie

8.1 Avantages de la biométrie

La biométrie est une technologie récente et commence à être adoptée par de grands constructeurs de matériel informatique. L'usage de la biométrie est une méthode parmis les méthodes d'authentification comme des mots de passe, des badges, des cartes à puce :

- Suppression des mots de passe, suppressions des clés : Au lieu de retaper son mot de passe dès que le PC se met en veille, une simple pression de l'empreinte digitale sur le capteur suffit et permet facilement de changer la session d'utilisateur.
- Utilisation d'une signature biométrique : offre une grande sécurité, intransmissible à une autre personne. Une identité vérifiée (Le destinataire est bien la personne autorisée à visualiser ou à utiliser les données). Lors de transactions financières, il est capital de savoir quel moyen de paiement du consommateur est le plus sûr.
- Diminution de la fraude.
- Rehaussement de l'intégrité des informations et la sécurité.
- Réduction des attaques à l'égard des programmes gouvernementaux.
- Croissance de la confiance envers les systèmes de sécurité.
- Accélération des services.

8.2 Limites de la biométrie

La biométrie présente malheureusement un certain nombre d'inconvénients parmi eux :

- **Les limites fonctionnelles** : les systèmes biométriques laissent la place à un certain nombre de faux rejets et de fausses acceptations. Ils ne peuvent à eux seuls garantir à 100 pour 100 que seules les personnes autorisées pourront passer le contrôle. Ils ne peuvent même pas garantir qu'une personne autorisée ne sera pas rejetée par le système. Il y aura toujours une marge d'erreur à prendre en compte, ce qui n'est pas forcément très rassurant.
- **Les limites techniques** : les données biométriques peuvent être imitées, notamment celles qui laissent des traces sur le passage de l'individu telles que les empreintes digitales.
  Un individu mal intentionné peut récupérer les empreintes digitales sur un objet tenu par la victime, les imiter et tenter de passer le contrôle biométrique à l'aide de ces empreintes.

9 Conclusion

La biométrie est une mesure des caractéristiques biologiques pour l'identification ou l'authentification d'un individu à partir de certaines de ses caractéristiques. Cette technique est utilisée de plus en plus aujourd'hui pour établir la reconnaissance de la personne dans un grand nombre d'applications diverses.

Dans ce chapitre nous avons introduit le concept de la biométrie, l'architecture de systèmes biométriques, ses différentes modalités, ces avantages ainsi que ses limites et ses différentes applications. Dans le chapitre suivant nous nous intéresserons à la reconnaissance par empreintes digitales.

Chapitre 2

Reconnaissance par empreinte digitale

1 Introduction

DAns ce chapitre, nous ciblons la reconnaissance par empreintes digitales pour les raisons suivantes :

- L'empreinte digitale domine le marché de la biométrie aussi bien sur un plan privé que public ou gouvernemental.
- La reconnaissance des empreintes digitales est la technique biométrique la plus ancienne et la plus mature. Elles ne se modifient donc pas au cours du temps (sauf par accident comme une brûlure par exemple).
- La probabilité de trouver deux empreintes digitales similaires est de 10^{-24}. Les jumeaux, par exemple auront des empreintes très proches mais pas semblables.

Dans ce chapitre, nous présentons la définition et les différentes représentations d'empreinte digitale, puis nous citons les différentes étapes de la reconnaissance des empreintes digitales basé sur les minuties. On terminera par les différents problèmes rencontrés lors de l'extraction des minuties.

2 Définition d'une empreinte digitale

Une empreinte digitale est le dessin formé par les lignes de la peau des doigts. Elles sont uniques et immuables, elles ne se modifient donc pas au cours du temps (sauf par accident) mis à part leur qualité qui peut se dégrader.
Une empreinte digitale est constituée d'un ensemble de lignes localement parallèles formant un motif unique pour chaque individu. On distingue :

- **Les crêtes** : ce sont les lignes en contact avec une surface au touché.
- **Les vallées** : ce sont les creux entre deux crêtes.

A l'intérieur de ce motif, il y a un très grand nombre d'éléments qui nous différencient les uns des autres.
L'empreinte digitale est la caractéristique d'un doigt. On estime que les empreintes digitales commencent à se former entre la 10è et la 16è semaine de vie du fœtus, par un plissement des couches cellulaires. Les circonvolutions des crêtes leur donnant leur dessin caractéristique vont dépendre de nombreux facteurs, comme la vitesse de

croissance des doigts, l'alimentation du fœtus, sa pression sanguine, etc. Ce qui fait que non seulement chaque individu, mais aussi chaque doigt, a sa propre empreinte [K.Jain et al., 2004].

3 Représentation des empreintes digitales

Une empreinte digitale est la reproduction de l'épiderme d'un doigt, produit quand un doigt est pressé contre une surface lisse. La caractéristique structurelle la plus évidente d'une empreinte digitale est un modèle entrelacé de crêtes et de vallées. Dans une image d'empreinte digitale, crêtes (aussi appelées lignes de crête) sont sombres alors que les vallées sont claires (voir la figure 2.1).

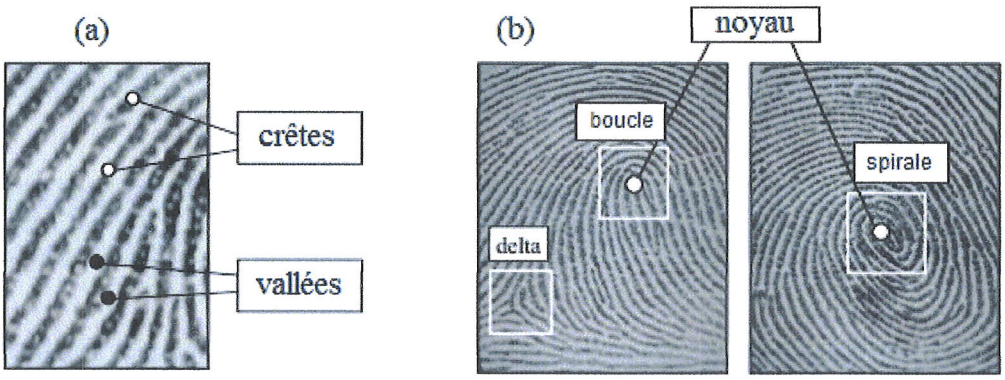


FIGURE 2.1 – Représentation d'une empreinte digitale, (a) Les crêtes et les vallées sur une image d'empreinte digitale, (b) régions singulières (cases blanches) et les points noyau (petits cercles dans les images d'empreintes digitales) [D.Maltoni et al., 2003].

Il existe deux représentations des empreintes digitales et elles sont classées en deux types principales : représentation globale et représentation locale [B.Vibert et al., 2016].

3.1 Représentation globale

Lorsqu'il est analysé au niveau global, le motif d'empreinte digitale présente une ou plusieurs régions où les lignes de crêtes prennent des formes distinctives (caractérisées par une courbure élevée, une terminaison fréquente, etc.).On distingue cinq régions [B.Vibert et al., 2016] :

a) Arche

b) Boucle à gauche

c) Boucle à droite

d) Tente

e) Spirale

La figure 2.2 donne un exemple de chacune des cinq classes.

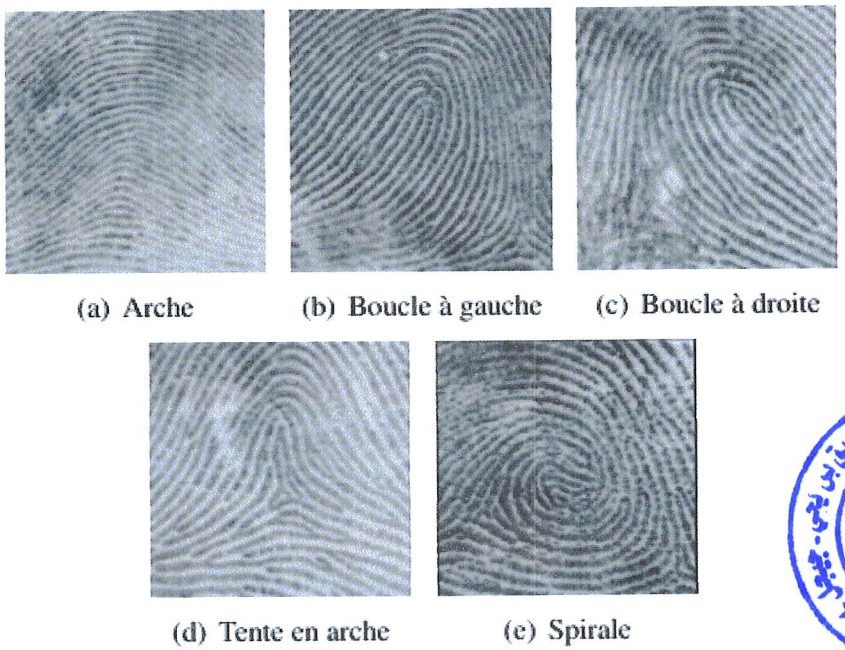


FIGURE 2.2 – Les 5 grands types d'empreintes définis par Henry [B.Vibert et al., 2016].

Plusieurs algorithmes d'adaptation d'empreintes digitales pré-alignent les images d'empreintes digitales en fonction d'un point de repère ou d'un point central, appelé **noyau**. Le point noyau correspond au centre de la singularité du type de boucle la plus au nord. Pour les empreintes digitales qui ne contiennent pas de singularités en boucle ou en spirale (ceux qui appartiennent à la classe Arche dans la figure 2.2), il est difficile de définir le noyau. Dans ces cas, le noyau est généralement associé au point de courbure maximale de la ligne de crête.
Malheureusement, en raison de la grande variabilité des motifs d'empreintes digitales, il est difficile de localiser le point (noyau) dans toutes les images d'empreintes digitales.
Les régions singulières sont couramment utilisées pour la classification des empreintes digitales (voir la figure 2.2), c'est-à-dire attribuer une empreinte digitale à une classe parmi un ensemble de classes distinctes, dans le but de simplifier la recherche et la récupération.

3.2 Représentation locale

Au niveau local, d'autres caractéristiques importantes, appelées **minuties** (figure 2.3), peuvent être trouvé dans les empreintes digitales. Les Minuties se réfèrent à diverses façons à laquelle les crêtes peuvent être discontinues. Par exemple, une crête peut soudainement se terminer (**terminaison**), ou peut se diviser en deux crêtes (**bifurcation**). Les deux types de minuties qui sont principalement utilisées pour la reconnaissance d'empreintes digitales sont les terminaisons et les bifurcations :

chaque minutie est désignée par sa classe, les coordonnées x et y et l'angle entre la tangente à la ligne de crête à la position de minutie et l'axe horizontal (voir figure 2.4) [D.Maltoni et al., 2003].

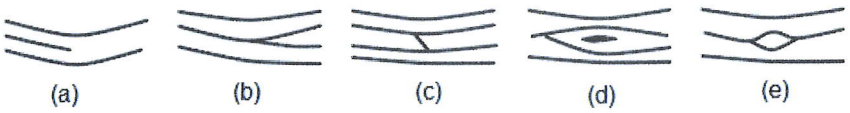


FIGURE 2.3 – Différents types de minuties, (a) terminaison, (b) bifurcation, (c) pont, (d) île et (e) lac [D.Maltoni et al., 2003].

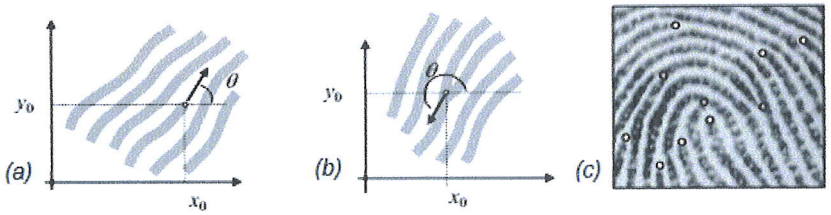


FIGURE 2.4 – Coordonnées $[x_0, y_0]$de minutie,(a)terminaison, (b) bifurcation, (c) terminaison (blanc) et bifurcation (gris) dans une empreinte digitale.

4 Techniques pour la reconnaissance d'empreintes digitales

Dans la littérature, les algorithmes de reconnaissance d'empreintes digitales adoptent l'une des approches [D.Maio et al., 2001] :

- **Technique à base de corrélation :** deux images d'empreintes digitales sont superposées et la corrélation entre les pixels correspondants est calculée pour différents alignements (Par exemple, divers déplacements et rotations).
- **Technique à base des caractéristiques de crêtes :** les approches de cette famille comparent les empreintes digitales en termes de caractéristiques (orientation, texture, forme de crête, etc.) extraites du motif de crête.
- **Technique à base de minuties :** les minuties sont extraites des deux empreintes digitales et stockés sous forme de points dans le plan bidimensionnel. La correspondance basée sur les minuties consiste essentiellement à trouver la correspondance entre le gabarit et la minutie entrée qui donne le nombre maximal de jumelages de minuties.

la plupart des systèmes de reconnaissance d'empreintes digitales emploient les minuties comme des caractéristiques des empreintes digitales. [A.Jain et al., 2004] [D.Maio et al., 2001] et c'est elle d'ont nous allons nous intéressés.

5 Conception du système de reconnaissance des empreintes digitales

Un système de reconnaissance des empreintes digitales est un système automatique de reconnaissance de formes qui se compose de quatre étapes principales(figure 2.5) [M.Fons et al., 2006] :

- **Acquisition :** les empreintes digitales sont capturées et stockées sous forme d'images numériques en niveaux de gris.
- **Prétraitement :** afin d'améliorer la qualité de l'impression d'entrée, plusieurs étapes de prétraitement sont appliquées à l'image d'origine.
- **Extraction des caractéristiques (minuties) :** les caractéristiques essentielles sont extraites à partir des images. Dans cette phase nous allons considérées les caractéristiques de minuties.
- **Comparaison des caractéristiques :** les caractéristiques acquises sont comparées avec les caractéristiques stockées dans une base de données et à partir du résultat de cette comparaison ; une décision est prise.

5.1 Acquisition des empreintes digitales

La première phase d'un système de reconnaissance consiste à obtenir une image de l'empreinte du doigt. Il existe 2 méthodes pour l'acquisition d'une image d'empreinte digitale :

5.1.1 Acquisition hors ligne

Il existe deux méthodes :

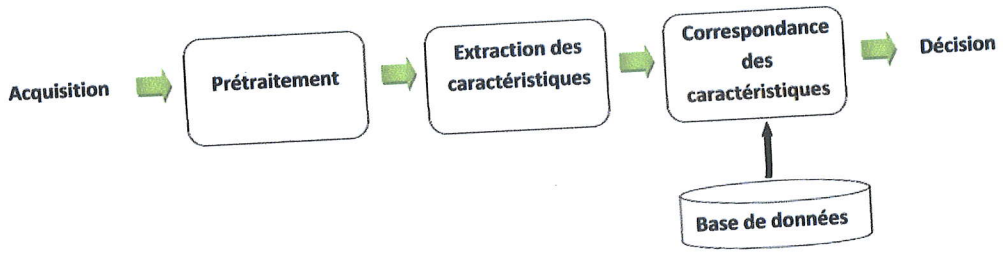


FIGURE 2.5 – Conception d'un système biométrique basé sur les empreintes digitales [M.Fons et al., 2006].

5.1.1.1 Empreinte acquise par encre

Dans la technique de l'encre, la peau du doigt est d'abord étalée à l'encre noire puis pressée contre une carte à papier ; La carte est ensuite convertie sous forme numérique au moyen d'un capteur de papier ou en utilisant une caméra CCD de haute qualité (voir figure 2.6).

La résolution par défaut est de 500 ppp. Si elle n'est pas exécutée avec soin, la technique de l'encre produit des Images avec des régions où l'information manque, due à un excès d'encre ou a une carence en encre.

FIGURE 2.6 – Images d'empreintes digitales roulées acquises hors ligne avec la technique de l'encre [D.Maltoni et al., 2003].

5.1.1.2 Empreinte latente

C'est une trace invisible à l'œil nu qui est le résultat d'un dépôt de sueur et autres composés présents sur les crêtes. la trace sera observable uniquement après l'utilisation d'une technique de révélation (par exemple poudre dactyloscopiqu, voir figure 2.7).

5.1.2 Acquisition directe

La partie la plus importante d'un scanner d'empreintes digitales est le capteur (ou l'élément de détection) qui est la composante où l'image d'empreinte digitale est formée. Les capteurs utilisées pour la mesure sont diverses [I.Benchennane, 2015] : cap-

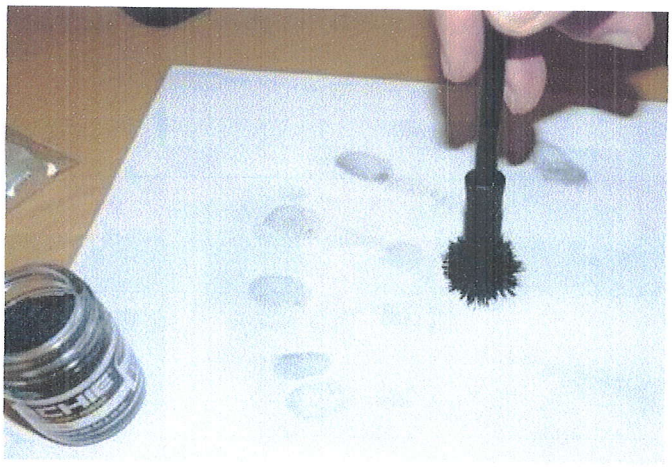


FIGURE 2.7 – Empreinte latente prise à l'aide d'une poudre spéciale.

teurs optiques (caméras CCD/CMOS), capteurs ultrasoniques, capteurs de champ électrique, de capacité, de température.

5.1.2.1 Capteur optique

Le capteur optique s'assimile à une mini caméra. Le doigt est apposé sur une platine en plastique dur ou en quartz, qui est en vis-à-vis de la mini caméra (voir figure 2.8). Il résiste très bien aux fluctuations de température, mais est gêné par une lumière ambiante trop forte. De plus il est assez volumineux. Son coût est intéressant, et il est intrinsèquement protégé contre les décharges électrostatiques. Il permet d'avoir des images précises et nettes. Ce procédé de capture d'image est le plus ancien après l'encre. Il est fréquemment utilisé particulièrement dans les applications judiciaires pour la qualité des images.

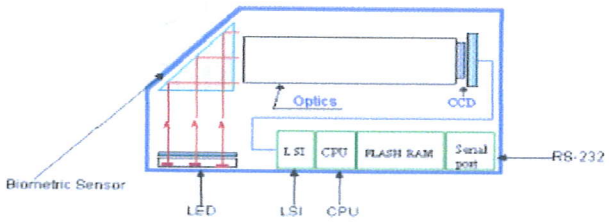


FIGURE 2.8 – Capteur optique [I.Benchennane, 2015].

5.1.2.2 Capteur en silicium

Le Silicium est un semi-conducteur qui permet de mesurer de l'effet piezo-électrique, l'effet capacitif, l'effet thermo-électrique et l'effet photo-électrique. Il est en général de très petite taille, d'une durée de vie assez longue, et son coût est très intéressant. Mais, comme tout composant, il est fragile aux décharges électrostatiques et il peut-être détruit si des règles de fabrication et d'installation ne sont pas

observées. Ces nouvelles technologies visent surtout les applications de masses, grâce à une taille réduite et des coûts moins importants que les lecteurs optiques.

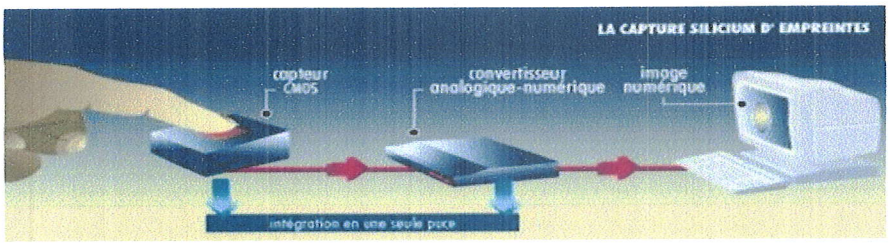


FIGURE 2.9 – Capteur en silicium.

5.1.2.3 Capteur thermique

La technique de capture thermique est utilisée par le FingerChip d'Atmel. Le capteur mesure une différence de température obtenue selon que la peau touche (dans le cas d'une crête de l'empreinte) ou ne touche pas (pour une vallée) le capteur. Cette technologie thermique présente de nombreux avantages. En particulier, elle permet d'obtenir une image de très grande qualité avec des empreintes « difficiles », par exemple quand les crêtes et les vallées sont très peu marquées.

5.1.2.4 Capteur à ultra sons

Il utilise une onde ultra sonore qu'il envoie vers le doigt, puis calcule le temps mis par l'onde pour faire un aller-retour et, point par point, fournit l'image de l'empreinte. Il est très précis, et hérite des propriétés des ultrasons de traverser certains matériaux (gants en latex, saletés, etc.). Mais il est volumineux et très coûteux. Il est intéressant pour une population d'utilisateurs très hétérogène.

5.2 Prétraitement

Les algorithmes de reconnaissance des empreintes digitales sont sensibles à la qualité des images de celles-ci, l'étape de prétraitement est alors nécessaire avant d'effectuer les étapes suivantes [J.Lim et al., 2013]. La qualité des images d'empreintes digitales dépend de plusieurs facteurs comme : le contact avec le sonde, la qualité de la sonde, la profondeur des crêtes /bifurcations, etc.

Généralement, le pré-traitement se compose du lissage, l'amélioration de contraste, le filtrage de domaine spatiale/ fréquentielle. Dans les cas extrêmes, une empreinte digitale avec une qualité très pauvre peut être automatiquement renforcée en utilisant le filtrage par exemple.

5.3 Extraction de caractéristiques (Minuties)

Un extracteur de minuties cherche des fins de crêtes et des bifurcations dans les empreintes digitales. Si les crêtes 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 crêtes. Donc la performance des algorithmes actuellement disponibles d'extraction de minuties dépend fortement de la qualité des images des empreintes digitales.

Généralement, un algorithme d'extraction de minuties se compose des étapes suivantes[D.Maltoni et al., 2003] :

- Estimation d'orientation
- Segmentation
- Binarisation
- Squelletisation
- Extraction des minuties
- Elimination des fausses minuties

5.3.1 Estimation d'orientation

Les images d'empreintes digitales peuvent être considérées comme un motif de texture orienté. Le champ d'orientation d'une image d'empreinte digitale prescrit l'orientation locale des crêtes, contenue dans l'empreinte digitale [L.Wieclaw, 2009]. Par conséquent, le champ d'orientation définit la direction des minuties (figure 2.10).

FIGURE 2.10 – Champ d'orientation d'une image d'empreinte digitale [D.Maltoni et al., 2003].

Il y a eu plusieurs approches pour estimer le champ d'orientation d'une image d'empreinte digitale. L'approche la plus simple et la plus naturelle pour l'estimation du champ d'orientation à était proposé par Anil Jain et al., dans [A.Jain et al., 2005]. Elle est basée sur le calcul des gradients dans l'image d'empreinte digitale.

L'orientation locale au pixel (i, j) peut alors être estimée en utilisant les équations suivantes :

$$V_x(i,j) = \sum_{u=i-\frac{W}{2}}^{i+\frac{W}{2}} \sum_{v=j-\frac{W}{2}}^{j+\frac{W}{2}} 2G_x(u,v)G_y(u,v) \tag{2.1}$$

$$V_y(i,j) = \sum_{u=i-\frac{W}{2}}^{i+\frac{W}{2}} \sum_{v=j-\frac{W}{2}}^{j+\frac{W}{2}} G_x^2(u,v)G_y^2(u,v) \tag{2.2}$$

Où :

W : est la taille de la fenêtre locale.

G_x, G_y : sont les grandeurs de gradient (l'opérateur Sobel) dans les directions x et y.

$$\theta(i,j) = \frac{1}{2} tan^{-1} \frac{Y_y(i,j)}{Y_x(i,j)} \tag{2.3}$$

Où :

$\theta(i,j)$: est l'estimation la moins approximative de l'orientation locale au bloc centré au pixel (i, j).

les gradients Gx et Gy à chaque pixel de l'image d'empreinte digitale sont calculés, où l'opérateur gradient est estimé comme opérateur Sobel [L.Wieclaw, 2009] :

$$G_x = \begin{bmatrix} -1 & 0 & 1 \\ -2 & 0 & 2 \\ -1 & 0 & 1 \end{bmatrix}, G_y = \begin{bmatrix} -1 & -2 & -1 \\ 0 & 0 & 0 \\ 1 & 2 & 1 \end{bmatrix} \tag{2.4}$$

5.3.2 Segmentation

La segmentation des images d'empreintes digitales est une étape importante dans un système automatique de reconnaissance d'empreintes digitales. Elle se réfère à la séparation de la zone d'empreinte digitale (premier plan) du fond de l'image.

La segmentation est utile pour éviter l'extraction des caractéristiques dans les zones bruyantes des empreintes digitales ou de l'arrière-plan. La segmentation est une phase très importante puisqu'elle empêche le traitement ultérieur sur l'image entière, permet de gagner du temps, mais aussi réduire la détection des fausses minuties [M.Fons et al., 2006].

5.3.3 Binarisation

Le but de la binarisation dans le cas d'une empreinte digitale est de repérer les crêtes. La technique la plus utilisée est la méthode de seuillage simple, elle consiste à se fixer un seuil global T, puis la valeur de chaque pixel I(x, y) est comparée au seuil T et si cette valeur est supérieure au seuil le pixel prend la valeur de un (noir), sinon il prend la valeur de zéro (blanc) [F.Zhao et al., 2002].

$$I_T(x,y) = \begin{cases} 1 & \text{si I(x,y)} > T \\ 0 & \text{si I(x,y)} \leq \text{T} \end{cases} \tag{2.5}$$

5.3.4 Squelettisation (amincissement)

Dans l'image binarisée (noir et blanc), les lignes se voient clairement mais elles ont des tailles différentes(figure 2.11). Pour pouvoir détecter rapidement les minuties (terminaisons, bifurcations), il est nécessaire d'obtenir une image plus schématique de l'empreinte, dans laquelle toutes les lignes ont la même épaisseur (1 pixel) [F.Zhao et al., 2002].

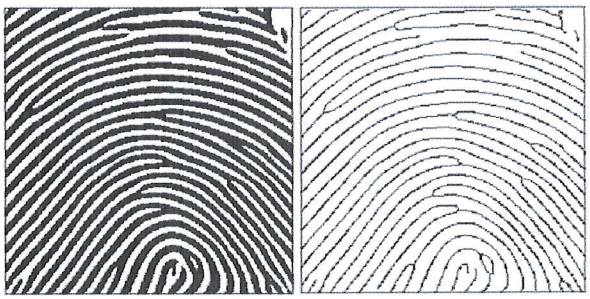


FIGURE 2.11 – Squelette de l'image binaire de l'empreinte.

5.3.5 Extraction des minuties

Les deux étapes de préparation à l'extraction (binarisation et squelettisation) ont grandement facilité cette phase.

L'extraction de minuuties consiste a calculer le nombre de connexion CN de chaque pixel blanc avec ces 8 voisins afin de déterminer le type d'un pixel (voir figure 2.12), il s'agit de la technique du **crossing number**, initiée par Arcelli [N.Galy, 2005].

Le crossing number cn(p) d'un pixel p se calcule par la formule suivante :

$$cn(p) = \frac{1}{2}\sum_{i=1}^{8} |val(P_i mod 8) - val(P_{i-1})| \tag{2.6}$$

$p_0, p_1, \ldots, p_7$ sont les 8 pixels au voisinage de p et val(p) $\in$ 0,1. Alors, un pixel p dont val(p) = 1, le calcul de CN prend les valeurs suivantes :

- CN (P) = 1 : correspond à une minutie de type terminaison.
- CN (P) = 2 : correspond à un point d'une ligne de l'empreinte, il n'ya pas de minutie.
- CN (P) $\geq$ 3 : correspond à une bifurcation.

Bien que l'utilisation du nombre CN facilite la détection, elle provoque aussi la détection d'un nombre très important de minuties (quelques centaines) introduites pour la plupart lors des étapes de binarisation et de squelettisation (Figure 2.13) [N.Galy, 2005].

Afin d'extraire directement la signature : un traitement supplémentaire est nécessaire pour éliminer le plus de fausses minuties possibles.

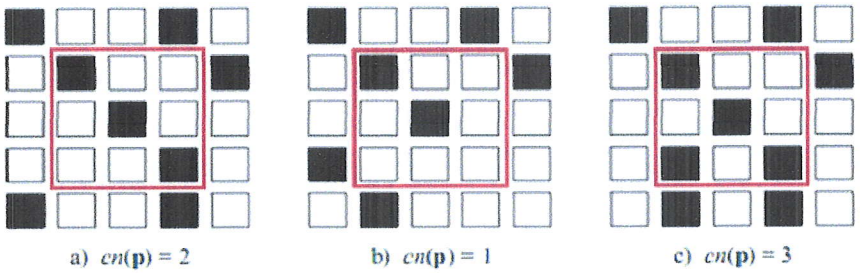


FIGURE 2.12 – Exemple de détermination du type de minutie en fonction du calcul de CN (Dans chaque cas on considère le pixel au centre du carré) [N.Galy, 2005].

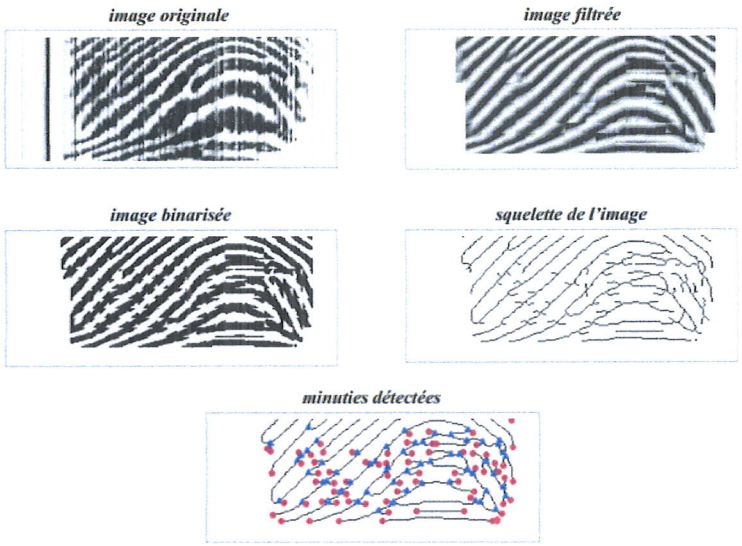


FIGURE 2.13 – Exemple de détection de fausses minuties [N.Galy, 2005].

5.3.6 Elimination de fausses minuties

L'étape d'extraction de minuties est souvent suivie par un post traitement pour éliminer la multitude de fausses minuties produites au cours des étapes de binarisation et de squelettisation [F.Zhao et al., 2002]. Comme le montre la figure 2.14 ces fausses minuties sont diverses et variées. L'objectif de ce processus est d'en éliminer le maximum tout en conservant les vraies minuties détectées.

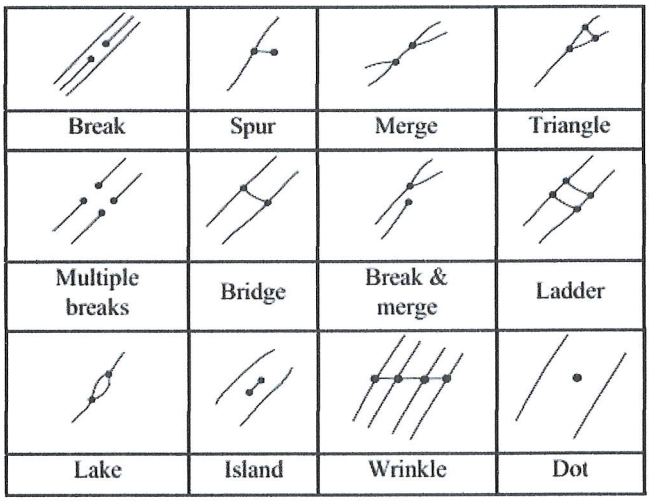


FIGURE 2.14 – Exemples de fausses minuties (Les Points Noir) [F.Zhao et al., 2002].

5.3.6.1 Traitement de terminaisons détectées

Un point $T(x_T, y_T)$ est considéré, ce point est une terminaison si (CN(T)=1), afin d'éliminet les fausses minuties, on suit les régles suivantes [N.Galy, 2005] :

- vérifier si T se situe au bord de l'image car, la majorités des fausses terminaisons se trouvent aux bord de l'image.
- Pour les terminaisons restantes T, parcourez la crête qui lui est associée sur une distance maximum K jusqu'à atteindre le point A (d=$\widehat{TA}$ $\leq$ K, figure 2.15).

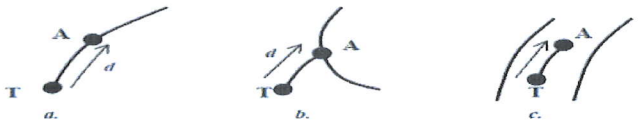


FIGURE 2.15 – Validation des terminaisons détectées, (a) vraie terminaison , (b) branche parasite, (c) segment trop court [N.Galy, 2005].

5.3.6.2 Traitement de bifurcations détectée

Lorsque un point B candidat pour le titre de bifurcation (CN(B)=3) est détecter, on parcourt les trois crêtes qui lui sont associées sur une distance maximum de K, jusqu'à atteindre 3 point A_1, A_2 et A_3 (figure 2.16). $d_1 = \widehat{BA_1}$, $d_2 = \widehat{BA_2}$, $d_3 = \widehat{BA_3}$

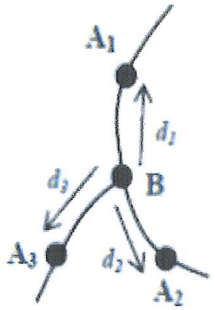


FIGURE 2.16 – Définitions associées à une bifurcation lors de la phase de validation [N.Galy, 2005].

5.4 Comparaison(Matching)

Un système d'appariement d'empreintes digitales basé sur les minuties renvoie habituellement le nombre des minuties correspondantes sur les empreintes digitales de requête et de référence pour indiquer si oui ou non les deux ensembles de minuties proviennent de la même empreinte [D.Miao et al., 2001].

6 Limites de la reconnaissance d'empreinte digitale basée sur les minuties

La reconnaissance d'empreinte digitale basée sur les minuties présente malheureusement un certain nombre d'inconvénients parmi eux :

- Le nombre de minutie extraite varie selon la qualité de l'image, soit il est très grand soit il est beaucoup moins élevé, ce qui peu affecter les performance du système de reconnaissance.
- Les étapes de reconnaissance basé sur les minuties prennent beaucoup de temps.
- Le changement d'échelle, de translation et de rotation des empreintes digitales pose des difficultés pour l'étape de mise en correspondance.

7 Conclusion

Dans ce chapitre nous avons abordé en détail la reconnaissance par empreinte digital qui est très utilisée. Nous avons également présentées l'approche basé sur les minuties d'une empreinte digitale. Cette technique détecte les minuties à partir

d'un squelette binaire de l'image, néanmoins elle est couteuse en temps et requière un traitement supplémentaire pour éliminer les nombreuses fausses minuties détectées.

Pour remédier a ces désavantages, plusieurs techniques sont largement utilisées principalement, l'opérateur LBP (Local Binary Pattern) avec un ensemble de ses variantes que nous aborderons dans le chapitre suivant.

Chapitre 3

Motifs binaires locaux (LBP)

1 Introduction

La reconnaissance par empreinte digitale a tiré une grande intention dans le domaine de la reconnaissance biométrique. Les principaux défis est de trouver des issues aux problèmes reliées à la nature de l'image d'empreinte tel que l'orientation, et la qualité d'image. Ces problèmes peuvent compliquer le processus de reconnaissance d'empreinte digitale, de ce fait, plusieurs techniques de reconnaissance d'empreintes ont était proposées durant les années passées. Parmi ces méthodes on trouve la méthode Local Binary Pattern (LBP) qui fait partir de la famille des méthodes basées sur les descripteurs, et qui est l'objectif de ce chapitre. Par définition, un descripteur d'image permet de décrire d'abord les parties/régions de l'image avant de calculer le vecteur caractéristique. Ce dernier permet de caractériser l'image de manière robuste dans des conditions défavorable comme la variation d'éclairage, altération due la rotation, le zoom, etc. [T.Jabid et al., 2010].

Mais avant de présenter le détail de cette méthode, nous voulons d'abord la localiser dans la famille des méthodes de reconnaissance des images.

2 Méthodes de reconnaissance des images

La reconnaissance d'images en générale fait appel soit à des méthodes globales qui caractérisent l'ensemble de l'image, soit à des méthodes locales appliquées sur des régions ou des points caractéristiques.

2.1 Méthodes locales et méthodes globales

On peut utiliser des méthodes globales traitant la totalité de l'image ou des méthodes locales caractérisant les différentes parties de l'image.

Les techniques modernes en imagerie tendent à privilégier les méthodes locales par rapport à celles globales car elles sont plus efficaces et elles permettent une recherche plus fine et absorbent mieux certaines variations.

Dans le cas de méthodes globales, un seul vecteur décrit la totalité de l'image, cela les rend robustes au bruit qui peut affecter le signal. L'inconvénient de ces méthodes est qu'elles ne permettent pas de distinguer des parties de l'image, ils ne distinguent pas, par exemple, les objets dans l'image, sauf dans le cas où l'image ne contient qu'un seule objet dans un fond uni.

Parmi les méthodes globales : les PCA (Analyse en Composante Principale), ICA (Analyse en Composante Indépendantes) et LDA (Analyse Discriminante Linéaire) [M.Mehrubeoglu, 2007]. Par opposition, les méthodes locales décrient les parties/régions de l'image qu'on commence par détecter avant de calculer le vecteur caractéristique, cette partie peut concerner un objet par exemple, la détection se fait indépendamment de la position dans l'image, ce qui assure l'invariance par translation.

Parmi les techniques utilisées pour l'extraction des caractéristiques locales : Les Ondelettes de Gabor [J.Lim et al., 2013], les transformées de Fourier [D.Zhang, 2002], les caractéristiques basées sur les indices LBP [Ojala et al., 1996], SIFT (Scale Invariant Feature Transform) [D. Lowe, 2004].

Ces méthodes utilisées dans la reconnaissance des images en générale, sont aussi utilisées pour la reconnaissance des images d'empreinte.

L'approche locale est intéressante pour notre problématique d'où nous privilégierons cette approche par rapport à l'approche globale. Dans ce contexte, nous présentons dans le reste de ce chapitre, une méthode d'extraction des caractéristiques couramment utilisées en vision par ordinateur : le descripteur Local binaire (LBP), cet opérateur est très discriminatif et bénéficie de l'efficacité du calcul [S.Sam et al., 2016].

3 Motif binaire local(LBP)

L'opérateur LBP en anglais (Local Binary Pattern) a été proposé en 1996 par Ojala et al. [Ojala et al., 1996]. Cet opérateur propose de représenter chaque pixel par un code binaire calculé à partir des 8 pixels voisins. Chacun des pixels voisins se verra représenter par un 1 si sa valeur est supérieure au pixel courant. Dans le cas contraire, ce pixel sera représenté par un 0.

Le code LBP du pixel courant est alors produit en concaténant ces 8 valeurs pour former un code binaire. La valeur LBP du pixel courant est obtenue par multiplication de la matrice binaire avec la matrice des poids LBP et on sommant le tous (la figure 3.1 montre un exemple du calcul de LBP).

On obtient donc, comme pour une image à niveaux de gris, une image des valeurs LBP contenant des pixels dont l'intensité se situe entre 0 et 255. Plutôt que de décrire l'image par la séquence des motifs LBP, on peut choisir pour descripteur un histogramme de dimension 255. Le code de LBP est définit par la formule suivante :

$$LBP = \sum_{p=0}^{7} S(g_p - g_c)2^p \tag{3.1}$$

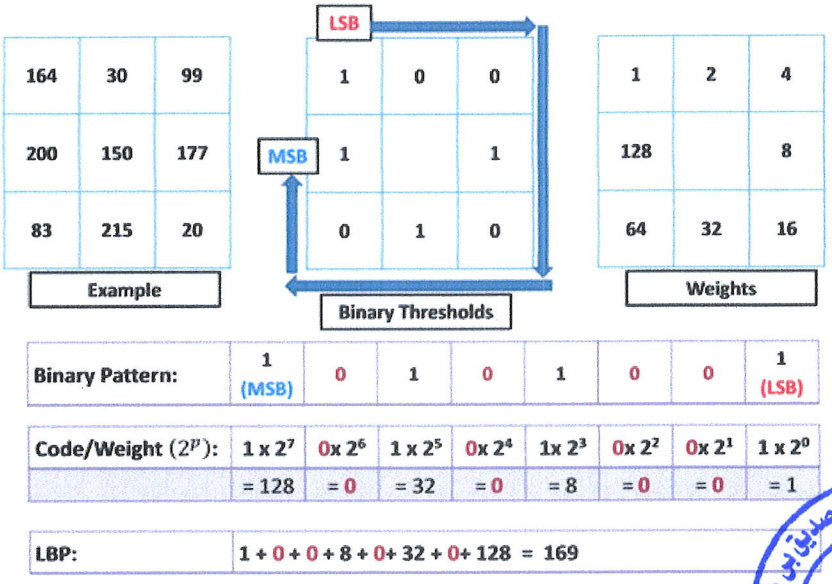


FIGURE 3.1 – Exemple de calcul de LBP [L.Paulhac, 2011].

Où s () est la fonction signe :

$$S(x) = \begin{cases} 1 & \text{si } x \geq 0 \\ 0 & \text{si } x < 0 \end{cases} \tag{3.2}$$

Et où :

g_p et g_c sont respectivement les niveaux de gris d'un pixel voisin et du pixel central.

3.1 Intérêt du descripteur LBP

Les avantages majeurs de cette opérateur est qu'il est : invariant a la rotation, robuste contre les changements de niveaux de gris et à une faible complexité de calcule. De plus le LBP est idéale pour les applications nécessitant l'extraction de caractéristiques rapide. En raison de sa simplicité et de performance, de nombreuses personnes l'ont appliqué à un certain nombre d'applications différentes [T.Mäenpää, 2003].

Cette méthode est utilisée avec succès dans divers domaines comme la biométrie (la reconnaissance par empreinte digitale, la reconnaissance faciale, ..). En termes d'efficacité discriminante, cette méthode offre de bonnes performances et contient des informations structurelles et statistiques [L.Paulhac, 2011].

3.2 Dérivateurs de LBP

Par la suite Ojala et al., ont proposé deux variantes de la méthode LBP dans [T.Ojala et al., 2001] et [T.Ojala et al., 2002] :

1. LBP multi-échelle : méthode définie pour des voisinages de différentes tailles, ce qui permet de traiter la texture à différentes échelles.

2. LBP uniforme.

3.3 LBP multi échelle

Le LBP standard est calculé dans un voisinage de 3 * 3, mais la technique LBP a été étendue ultérieurement en utilisant des voisinages de taille déférente, pour pouvoir capturer des caractéristiques discriminatifs à différentes échelles [T.Ojala et al., 2002].
Un voisinage pour un pixel central est réparti sur un cercle et construit à partir de deux paramètres : le nombre de voisins (P) sur le cercle et un rayon (R) pour définir une distance entre un pixel central et ses P voisins.

Quand les P voisins ne se situe pas exactement au centre d'un pixel (Comme nous pouvons le voir à la figure 3.2), leurs valeur est obtenue par interpolation, déterminé par :

$$x_p = x + Rcos(2\pi p/P) \tag{3.3}$$

$$y_p = y - Rsin(2\pi p/P) \tag{3.4}$$

L'opérateur LBP est désigné par LBP (P, R). La notation (P, R) est utilisée pour définir le voisinage de P points de rayon R d'un pixel. La figure 3.2, illustre trois voisinages pour des valeurs de R et P différentes.

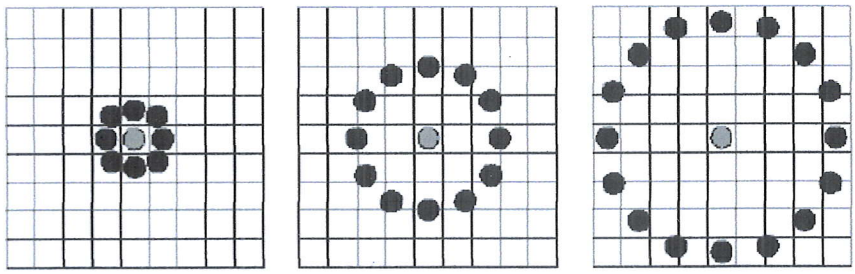


FIGURE 3.2 – LBP multi-échelle. Trois voisinages pour des valeurs de R et P différentes [L.Paulhac, 2011].

Comme pour LBP de base, le LBP multi-échelle est obtenue par multiplication des valeurs binaires avec la matrice des poids et on sommant le tous. L'opérateur $LBP_(P, R)$ est définit par :

$$LBP_{P,R}(x_c, y_c) = \sum_{p=0}^{P-1} S(g_p - g_c)2^p \tag{3.5}$$

Où s () est la fonction signe :

$$S(x) = \begin{cases} 1 & \text{si x} \geq 0 \\ 0 & \text{si x} < 0 \end{cases} \tag{3.6}$$

Et Où :
— x_c, y_c : sont les coordonnées du pixel courant,
— g_c : le niveau de gris du pixel central,
— $g_p(p = 1 \ldots P)$: les niveaux de gris de ses voisins.

3.4 LBP uniforme

Une autre extension de l'opérateur d'origine est le LBP uniforme. Un LBP est appelé uniforme si le nombre de transitions binaires (de 0 à 1, de 1 à 0) est au plus 2 lorsque la chaîne binaire est considérée circulaire. Le tableau 3.1 suivant représente quelque code LBP uniforme et non uniforme :

Code LBP	Nombre de transitions	LBP Uniforme
00000000	0	Oui
11111111	0	Oui
01110000	2	Oui
11001111	2	Oui
11001001	4	Non
01010011	6	Non

TABLE 3.1 – Exemple des LBP uniforme et non uniforme.

L'utilisation d'un code LBP uniforme, noté **LBPu2** à deux avantages :
— Le premier est le gain en mémoire et en temps calcul.
— Le deuxième est que LBPu2 permet de détecter uniquement les motifs locales importantes, comme les spots, les fins de ligne, les bords et les coins (voir figure 3.3, pour des exemples de ces textures particulières). En effet, Ojala et al., ont montré que les LBPs uniformes contiennent plus de 90% de l'information d'une image [Ojala et al., 2001].

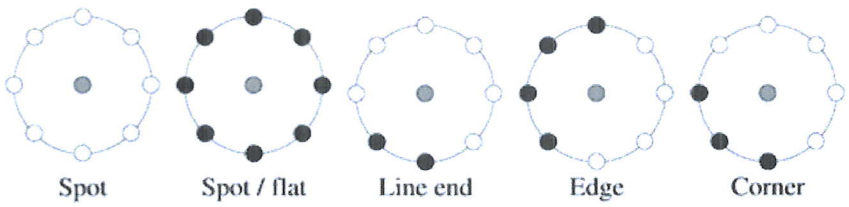


FIGURE 3.3 – Motifs particulières détectées par LBPu2 [L.Paulhac, 2011].

L'opérateur LBP uniforme est définit comme suit [Ojala et al., 2001] :

$$LBP^{u2}_{P,R}(x,y) = \begin{cases} I(LBP_{P,R}(x,y)) & \text{si U(LBP}_{P,R}) \leq 2,\ \text{I(z)} \in [0,\text{(P-1)P+2}[\\ (P-1)P+2 & \text{sinon} \end{cases} \quad (3.7)$$

Le **u2** représenté dans l'équation 3.7 indique que la définition se rapporte à des modes uniformes avec une valeur U au plus 2.

Si **U(x)** est inférieur ou égale à 2, le pixel en cours est étiqueté par une fonction d'index I(z), sinon, il lui sera assigné la valeur **P(P-1)+2** [Ojala et al., 2001].

Autrement, le nombre de codes possibles en utilisant uniquement des codes uniformes est réduit à P(P-1) +2, où P est le nombre de points du voisinage.

La fonction d'index **I(z)**, contenant P(P-1) +2 indices, est utilisée pour attribuer un index particulier de chacun des modèles uniformes.

Un exemple de huit voisins (P=8) des motifs binaires locaux uniformes est présenté dans la figure 3.4.

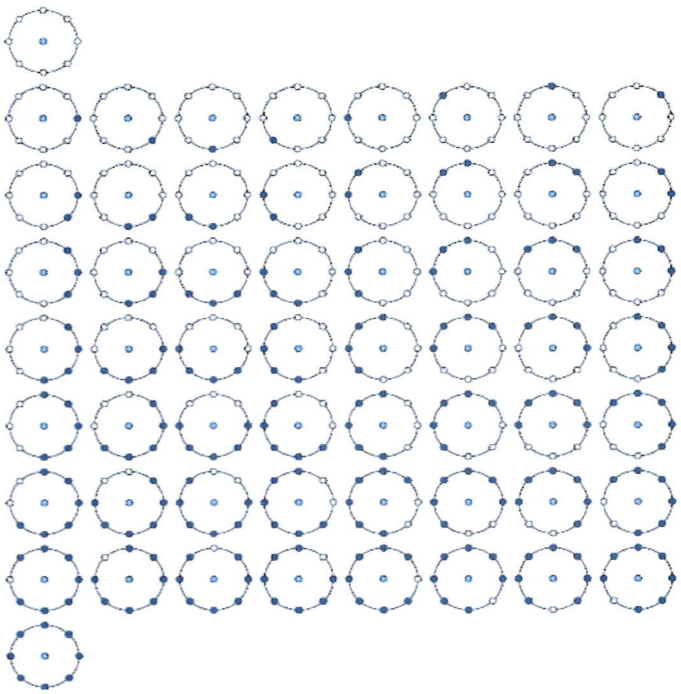


FIGURE 3.4 – Les 58 motifs uniformes différents dans le voisinage (8, R). [M.Pietikäinen et al., 2011]

4 Histogramme LBP

Ojala et al., a constaté que seuls 58 des 256 motifs LBP sont uniformes [Ojala et al., 2001]. Dans ce cas, la dimension de l'histogramme LBP peut être réduite de manière importante avec un histogramme de dimension 59 (selon l'équation 3.7). Chacune des 58 premières catégories contiendra le nombre d'occurrences de l'un des motifs uniformes. La dernière contiendra le nombre d'occurrences de tous les motifs non-uniformes, ce regroupement permet de réduire la dimension du descripteur sans perdre trop d'information.

Par exemple :
Quand P = 8, le nombre de code uniforme est obtenue par :
- Nombre de codes uniformes = 8 (8-1) +2 = 58 codes uniformes.
- Et les codes non uniforme sont regroupés à un seul indice.
- Alors l'histogramme sera de dimension 59.

Où :
- P : nombre de points du voisinage.

De même manière P = 6 produit un histogramme de dimension 33.

4.1 Comparaison des histogrammes

Étant donner deux histogrammes de LBP S, M de deux images, l'étape suivante est d'utiliser une métrique pour calculer la similarité entre deux histogrammes. Selon [T.Ahonen et al., 2006] la métrique chi-square est la plus adaptée avec LBP.

la distance chi-square est calculée par la formule suivante :

$$X^2(S, M) = \sum_{i-1}^{n} \frac{(S_i - M_i)^2}{(S_i + M_i)} \tag{3.8}$$

Où :
- S_i : i éme valeur de bin de l'histogramme de l'image de référence.
- M_i : i éme valeur de bin de l'histogramme de l'image de teste.
- n : le nombre de bins (éléments) dans l'histogramme.

5 Etat de l'art

Dans la littérature, peu de travaux se sont focalisés sur la reconnaissance d'empreinte digitale basée sur LBP, dont on présente dans cette section les principales approches proposées pour l'empreinte digitale utilisant l'opérateur LBP :
- Loris Nanni et Alessandra Lumini ont proposé un système hybride de correspondance d'empreinte basé sur des modèles binaires locaux. La première

étape du système hybride est l'amélioration de la qualité de l'image d'empreinte. Étant donné que l'image d'entrée peut être bruyante, elle est d'abord améliorée afin d'améliorer la clarté des crêtes et des structures de crêtes et de vallées en utilisant la technique du domaine de Fourier pour améliorer les images d'empreintes digitales. Ensuite, l'empreinte inconnue est alignée sur le modèle stocké en utilisant les minuties [L.Nanni et al., 2008]. Pour l'extraction des caractéristiques, l'image est décomposée en plusieurs sous-fenêtres avec des dimensions fixes ; Seules les sous-fenêtres de premier plan sont conservées, selon une procédure de segmentation. L'extraction des fonctionnalités de chaque sous-fenêtre consiste en l'application d'une banque de filtres Gabor et dans le calcul des histogrammes LBP à partir des images filtrés. Le vecteur caractéristique est obtenu en concaténant les histogrammes LBP. Enfin, la comparaison entre les sous-fenêtres correspondantes de l'empreinte inconnue alignée et le modèle stocké est effectuée en calculant leur distance euclidienne. Les vecteurs caractéristiques résultants ont des propriétés très souhaitables : ils sont assez robustes au bruit (due à Gabor et LBP).

— V. Talele et al., ont proposées une méthode pour la reconnaissance d'empreinte digitale partielle. Leur principe est que l'identification d'empreinte digitale partielle s'effectue en utilisant les caractéristiques de pores à l'aide de LBP pour améliorer la précision de correspondance. La première étape consiste à extraire les pores de l'image partielle. Ces pores agissent en tant que points d'ancrage et une sous-fenêtre (32 * 32) est formée autour des pores. La correspondance d'image partielle et complète est basée sur une distance chi-carré entre deux histogrammes LBP pour calculer la distance minimale entre eux afin de trouver le meilleur score de correspondance. [V.Talele et al., 2014]. Les résultats expérimentaux ont étés testés sur la base de données NIST SD30 et présentent un score de correspondance élevé lors de la correspondance partiel avec la base de données complète d'empreintes digitales.

— S. Kulkarni et Dr. Hemprasad, ont proposé dans [S.Kulkarni et al., 2016]un système de détection d'empreintes digitales falsifiées utilisant LBP. Principalement une technique de reconnaissance d'imitation où LBP et la transformée de Shearlet ont étés utilisées comme extracteur de caractéristiques pour évaluer l'image d'empreinte digitale, qu'elle soit réelle ou falsifiée à l'aide du classifieur SVM. L'image d'empreinte digitale est prétraitée en utilisant cinq opérations de prétraitement : premièrement les images sont réduites en utilisant une "Interpolation bilinéaire". Deuxièmement une région d'intérêt (ROI) est appliquer sur les empreintes digitales afin de les centrées. Troisièmement une égalisation d'image est appliquer on utilisant la technique d'égalisation d'histogramme adaptatif limité contrasté, quatrièmement un filtrage passe haut et utilisée avant d'extraire les caractéristiques pour distinguer entre l'empreinte digitale réelle et falsifiée dans les composants haute fréquence de l'image. Cinquièmement l'élimination du bruit à l'aide d'un filtre passe-bas pour améliorer les résultats. L'image prétraitée est donnée à l'algorithme de modèle binaire local. Les caractéristiques extraites de ces histogrammes sont concaténées pour donner 59 vecteurs de caractéristique. Ces vecteurs de

caractéristique sont sauvegardés dans une BDD.

6 Conclusion

Ce chapitre était consacré à la présentation d'une méthode très importante qui est utilisé dans la reconnaissance. Nous étions intéressées par l'utilisation de la méthode des motifs binaires locaux. Dans ce contexte nous avons détaillés les différentes étapes de cette méthode, puis nous avons présentés un état de l'art des différentes approches qui ont utilisée cette méthode pour les empreintes digitales. Dans le chapitre suivant, nous présenterons notre système proposé et testerons le système dans son environnement afin d'évaluer ses performances pour en déduire les paramètres optimaux qui garantissent une meilleure efficacité du système.

Chapitre 4

Développement d'application

1 Introduction

Pour chaque système de reconnaissance des empreintes digitales, l'utilisation d'une étape de prétraitement et une méthode de reconnaissance fiable est une nécessité pour améliorer le taux de reconnaissance qui est souvent médiocre par rapport aux systèmes classiques.

Dans ce dernier chapitre, nous présentons notre proposition en commençant par la problématique, ensuite nous expliquerons le principe et les étapes de notre application, et nous terminerons par une partie d'expérimentation où les résultats obtenus sont présentés. Ces résultats permettent de mesurer les performances de notre proposition.

2 Problématique

Bien que l'identification des empreintes digitales basées sur les minuties soit largement utilisée, car l'information de minutie est très discriminante, des améliorations doivent encore être apportées dans ce domaine.

La méthode classique de reconnaissance d'empreinte digitale souffre de plusieurs problèmes :

- Si la qualité des images est dégradée, l'image résultante du processus de reconnaissance (image squelette) contient des faux branchements et par conséquent un ensemble large des fausses minuties est trouvées, ce qui amène à la fausse comparaison de ces dernières.
- Le système est affecté par la translation/ rotation des images d'empreintes digitales, d'où il faut utiliser une méthode efficace de translation/ rotation des images comparées basé sur les minuties seulement et ignorer l'utilisation des autres informations des images d'empreinte.

Afin de remédier à ces problèmes, nos propositions s'articulent sur les points suivants :

- Amélioration de la qualité d'image par l'utilisation d'une étape de prétraitement ;
- Utilisation d'autre information que les minuties : noyau de l'empreinte ;
- Utilisation d'autre méthode que la méthode classique : la méthode LBP ;
- Utilisation du principe de multi-algorithmique : fusion des minuties et LBP.

3 Proposition

Dans notre travail, nous proposons trois systèmes d'identification d'empreinte digitale (comme montré dans la figure 4.1) basés sur des méthodes différentes :

- La première est une amélioration de la méthode classique basée sur les minuties en proposant une étape de prétraitement.
- La deuxième est une amélioration de la reconnaissance d'empreinte digitale par LBP en appliquant cette dernière autour du noyau de l'empreinte.
- La troisième est basée sur le principe de multi-algorithmiques où plusieurs algorithmes et caractéristiques sont utilisés au moins dans une étape de processus de reconnaissance. La méthode proposée ici est une fusion des deux propositions précédentes (LBP et minuties).

Notre proposition touche principalement trois niveaux :

- Le premier consiste à améliorer la qualité des images d'empreinte digitale, pour cela on utilise la correction de Gamma et un Banc de filtres de Gabor pour la première méthode basée sur les minuties, et seulement la correction de Gamma pour la deuxième méthode basée sur LBP.
- Le deuxième est au niveau de l'extraction des caractéristiques d'empreinte digitale, où nous utilisons les minuties pour la première méthode et l'histogramme LBP autour du noyau pour la deuxième méthode.
- Le troisième au niveau de la décision où nous proposons une nouvelle méthode basée sur la combinaison des scores obtenue durant l'étape de comparaison des deux premières méthodes.

Les détails de notre système sont présentés dans les sous sections suivantes.

3.1 Proposition 1 : Algorithme d'identification par minuties

Notre première méthode est basée sur l'identification par les minuties. Tout d'abord nous proposons d'améliorer la qualité d'image par un prétraitement pour réduire les éventuels problèmes rencontrés lors de l'extraction des minuties comme le grand nombre de fausses minuties, ce qui influe directement sur l'efficacité de cette méthode. Les étapes de cette dernière sont détaillées ci-dessous.

3.1.1 Prétraitement

La performance de système de reconnaissance des empreintes est très liée à la qualité d'image d'entré. Pour résoudre le problème de mauvaise qualité des images d'empreinte digitale et qui influe dramatiquement sur la bonne extraction des détails d'empreinte et ses caractéristiques, nous combinons les résultats de deux algorithmes d'amélioration de la qualité d'image :

- **Correction de Gamma :** est l'opération d'amélioration de la luminosité la plus largement utilisée pour le traitement d'image numérique comme mentionné dans [G.Cao et al., 2010]. Elle permet d'éclaircir les zones sombres, ou au contraire assombrir les zones claires.
- **Banc de Gabor :** l'intérêt principal de cette opération est d'améliorer la clarté des crêtes et des vallées dans les images des empreintes digitales.

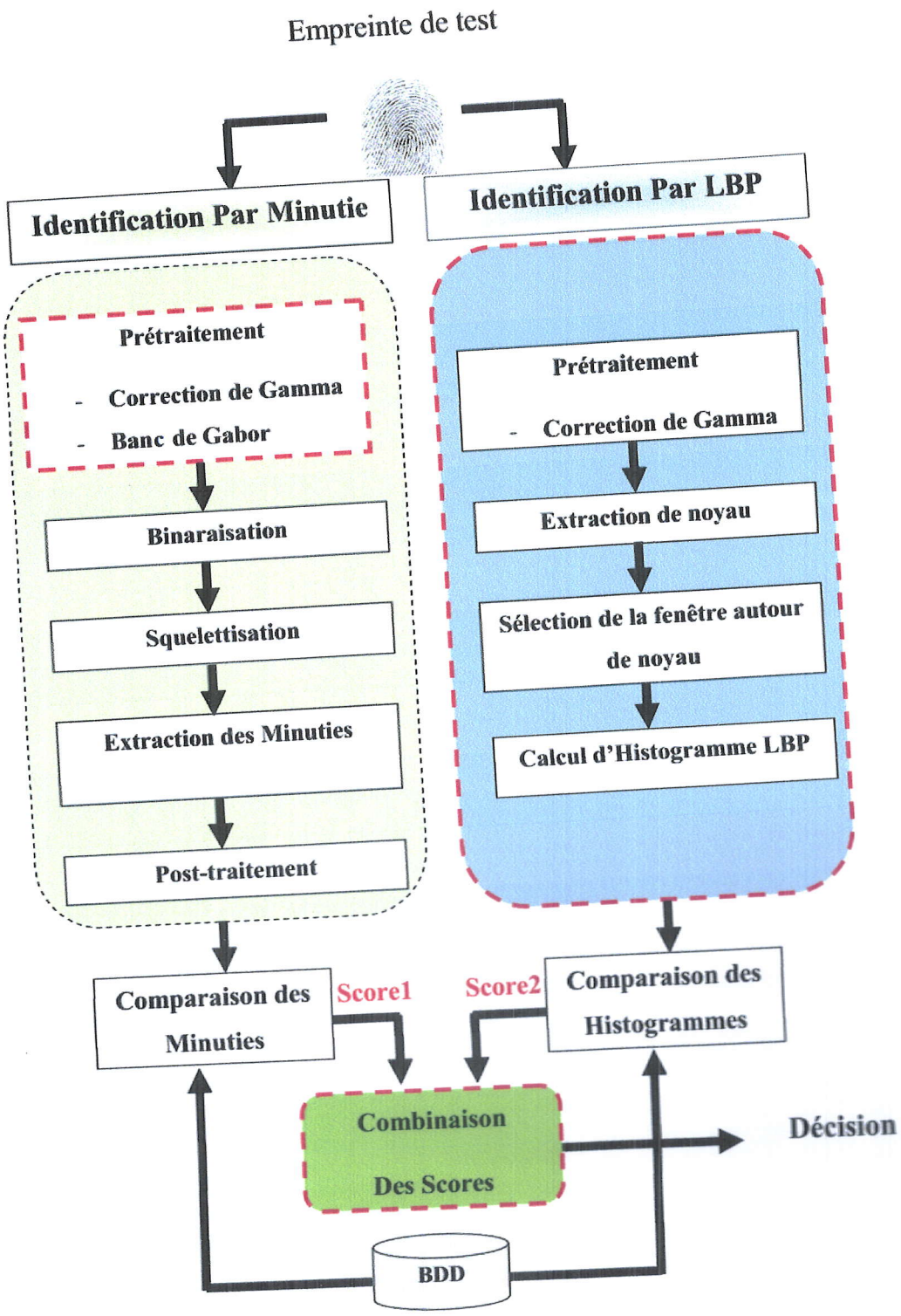


FIGURE 4.1 – Schéma générale du système d'identification des empreintes digital par la méthode proposé.

[L.Hong et al., 1998]. Il a étais largement utilisé dans l'étape de prétraitement pour les images d'empreintes digitales [L.Nanni et al., 2008].

Le choix de ces deux méthodes de prétraitement est basé sur notre expérimentation et les travaux antérieurs comme [L.Hong et al., 1998], [P.Moreno et al., 2005] et [S.Kahlsnan et al., 2013].

3.1.1.1 Correction de Gamma

La correction de gamma est un procédé qui permet de régler l'illumination de l'image, selon la fonction suivante :

$$V_{out} = V_{in}^{\gamma} \tag{4.1}$$

- $V_{in} \epsilon$ [0,1] : sont les valeurs des pixels de l'image d'entré.
- $V_{out} \epsilon$ [0,1] : sont les valeurs de pixels de l'image améliorée.

Selon la valeur de gamma (γ), l'image soit plus claire ou bien plus noire :
- Si gamma<1, l'image est plus claire que l'image d'entré.
- Si gamma>1, l'image résultante est plus noire.
- Si gamma=1, l'image qui en résulte est la même que celle d'entré.

La figure 4.2 montre les résultats de l'application de la correction de Gamma avec différentes valeurs de Gamma (γ) sur une image d'empreinte digitale :

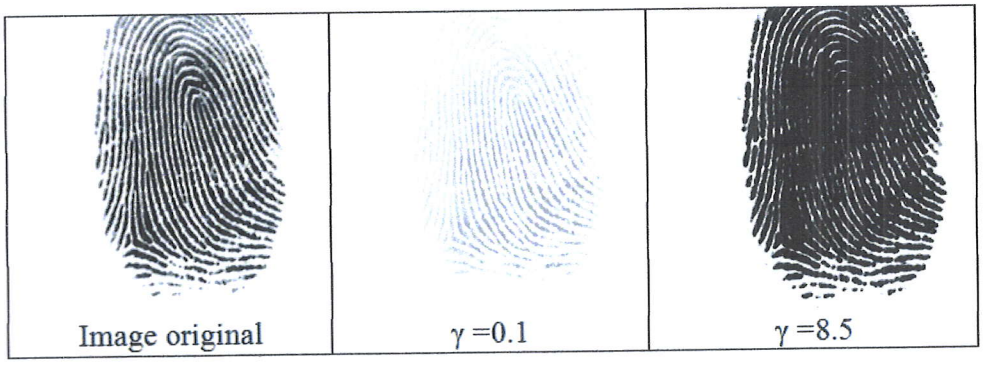


FIGURE 4.2 – Application de la correction de Gamma avec différentes valeur de γ.

La valeur de gamma dans notre proposition est choisie automatiquement selon la qualité d'image d'empreinte. Pour cela, nous avons procédés dans notre expérimentation comme suit :
- Calcul de la région d'intérêt de l'empreinte digitale (ROI).
- Calcul de la moyenne des valeurs des pixels de l'image d'empreinte digitale dans la ROI.
- Selon la valeur de la moyenne, on fixe la valeur de Gamma. La moyenne des images dans des conditions d'éclairage est :
- Si moyenne (img)$\leq$ 0.4 alors Gamma=0.3

— Si moyenne (img)≥ 0.6 alors Gamma=1.5
— Si moyenne (img) appartient à [0.4 ; 0.6] alors l'éclairage de l'image est considérée de bonne qualité, et la valeur de gamma=1.

La figure 4.3 ci-dessous montre les résultats obtenues par l'application de notre choix des valeurs de gamma sur deux empreintes une sombre (moyenne de ROI)≤ 0.4) et l'autre clair (moyenne de ROI) ≥ 0.6) :

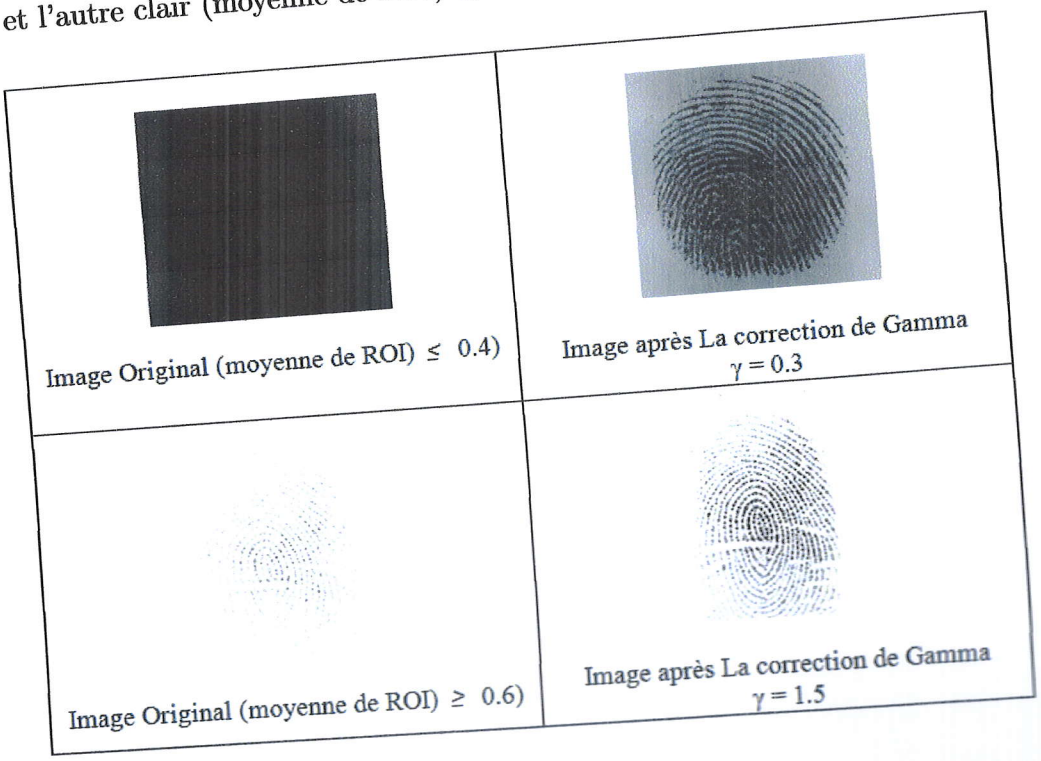


FIGURE 4.3 – Application de la correction de Gamma sur deux empreintes une sombre et l'autre clair.

3.1.1.2 Gabor

Un filtre de Gabor est un filtre linéaire utilisé pour la détection de bord. La fréquence et l'orientation des représentations de filtres de Gabor sont semblables à celles du système visuel humain, elle est une sinusoïde multipliée par une enveloppe gaussienne, comme indiqué dans la formule suivante :

$$G(x, y, \theta, f_0) = \exp\left\{-\frac{1}{2}\left[\frac{x_\theta^2}{\sigma_x^2} + \frac{y_\theta^2}{\sigma_y^2}\right]\right\} * cos(2\pi f_0 x_0) \tag{4.2}$$

$$\begin{bmatrix} x_0 \\ y_0 \end{bmatrix} = \begin{bmatrix} sin\theta & cos\theta \\ -cos\theta & sin\theta \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \tag{4.3}$$

Où :

— θ : est l'orientation de crête respectée à l'axe verticale.
— f_0 : est la fréquence de crête sélectionnée dans x_0 – direction.

— σ_x, σ_y : (Respectivement) l'écart-type de la gaussienne selon l'axe des abscisses (respectivement des ordonnées).

3.1.1.2.1 Banc de Gabor

Les filtres de Gabor permettent d'isoler les contours d'une image d'orientation perpendiculaire à thêta et répondant à une certaine épaisseur, qui dépend de f. Ce ci justifier le fait de détecter l'ensemble des contours d'une image, on lui applique généralement un ensemble de filtres de Gabor que nous appelons Banc.

Un Banc de Gabor est décrit par la fréquence centrale f_0, la largeur σ des filtres et le nombre de filtres N (dans l'image).

La figure 4.4 suivante montre les résultats de l'application d'un Banc de filtre de Gabor sur une image d'empreinte digitale :

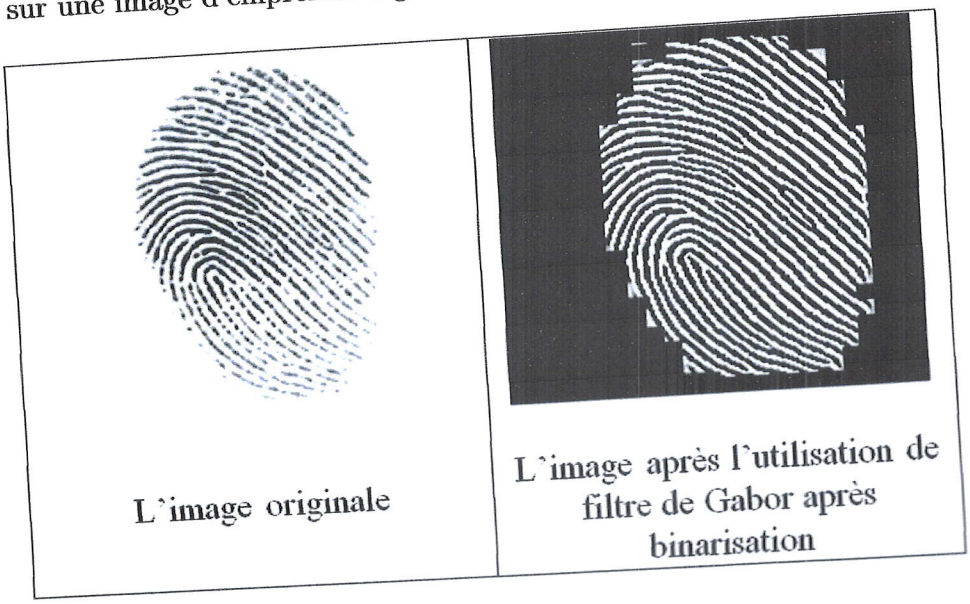


FIGURE 4.4 – Résultat d'application d'un Banc de Gabor sur une empreinte digitale.

Après l'étape de prétraitement, nous passons à l'extraction des minuties.

3.1.2 Extraction des minuties

Dans cette étape, nous utilisons les étapes basiques d'extraction des minuties (comme montrée dans la figure 4.5) :

— Segmentation.
— Binarisation.
— Squelettisation.
— Extraction des minuties.
— Post-traitement (élimination de fausses minuties).

Ces étapes ont été détaillées dans le chapitre 2, section 5.3. Chaque minutie dans ce cas est définie par (x, y, θ, type).

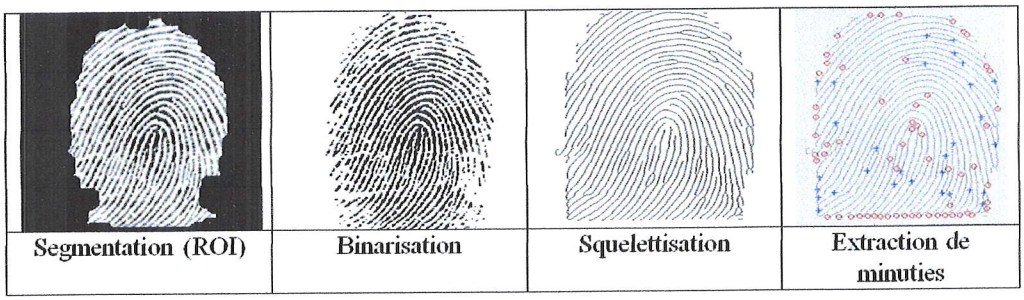


FIGURE 4.5 – Résultats des étapes d'extraction des minuties.

3.1.3 Comparaison

Un système de correspondance d'empreintes digitales basés sur les minuties retourne habituellement le nombre des minuties correspondantes entre l'empreinte de teste et l'empreinte de référence et les utilisent pour générer les scores de similarité.

La comparaison des minuties passe par les étapes suivantes :

- On commence par la sélection d'une minutie de l'image d'entré (m_i) et une autre (m'_j) de l'image dans la base de donnée et de faire une translations des autres minuties.
- Après l'alignement, on passe à l'étape de correspondance, d'où une paire de minutie mi et mj sont considérer comme correspondues si la distance spatiale (sd) est inférieure à un seuil donnée r_0, la différence de direction (dd) est inférieure à une tolérance angulaire donnée θ_0.
- On termine par le calcul de score de similarité Score1.

Parmi les distances spatiales nous avons utilisés la distance euclidienne qui est la plus utilisée dans la littérature pour la comparaison des empreintes digitales (minuties) [A.Ghany et al., 2014], à cause de sa simplicité de calcule et aussi pour les bons résultats qu'il offre.

La distance euclidienne est définit par la formule suivante :

$$sd(m'_j, m_i) = \sqrt{(x'_j - x_i)^2 + (y'_j - y_i)^2} \leq r_0 \tag{4.4}$$

La différence de direction (dd) est définit par la formule suivante :

$$dd(m'_j, m_i) = min(|\theta'_j - \theta_i|.360^0 - |\theta'_j - \theta_i|) \leq \theta_0. \tag{4.5}$$

Dans notre expérimentation, r_0 est fixé à 15, θ_0 est fixé à 14.

Pour le score de similarité, il est générer en effectuant le calcul suivant :

$$\text{Score1} = \sqrt{\frac{N^2}{C1 * C2}} \tag{4.6}$$

Où :

— N : le nombre de minutie qui sont considérer comme correspondues.
— C1 : le nombre de minutie dans l'empreinte de test.
— C2 : le nombre de minutie dans l'empreinte de référence.

Le score1 maximal est celui qui correspond à la meilleure image d'empreinte identifié.

3.2 Proposition 2 : Algorithme d'identification par LBP autour du noyau

La deuxième méthode est basée sur l'extraction des informations locales (noyau) avec l'utilisation de l'opérateur LBP qui est un descripteur mathématique dont son principe consiste à assigner un code binaire à tout les pixels d'une image en fonction de leurs voisinages. Ensuite on calcul l'histogramme LBP de cette image pour former un vecteur de caractéristiques représentant l'image d'empreinte digitale.

Nous avons utilisé LBP pour ces multiples avantages comme : la robustesse au bruit, l'invariance au changement de niveaux de gris et surtout pour ça rapidité de calcule. Cette opérateur est utilisées avec succès dans différents travaux sur les empreintes digitales (voir les détailles au chapitre 3).

Les étapes de la proposition sont détaillées ci-dessous.

3.2.1 Prétraitement

Pour régler l'illumination des images nous avons utilisées la correction de gamma, avec les mêmes paramètres utilisé dans notre première méthode.

3.2.2 Extraction des histogrammes LBP

Au lieu de calculer le code LBP pour toute l'image, nous avons choisit de calculer le code LBP autour du noyau (Core) de l'empreinte digitale, qui apporte beaucoup d'information de l'image d'empreinte. Pour cela nous procédons en premier lieu à la détection du noyau, après on sélectionne une fenêtre de taille w*w (par expérimentation w=61) autour de celui-ci. Enfin on termine par le calcul d'histogramme LBP de cette fenêtre pour former un vecteur de caractéristiques représentant l'image d'empreinte (comme montré dans la figure 4.7).

Dans notre expérimentation, nous avons utilisé la version LBP Uniforme (P, R) d'où les valeurs de P, R sont choisit par expérimentation $P = 8$, $R = 2$.

3.2.2.1 Détection de point noyau

La détection de point noyau est une tâche non triviale. Un noyau est défini comme un point dans le champ d'orientation où l'orientation dans un petit voisinage local autour du point présente une tendance semi-circulaire. D'où l'orientation joue un rôle crucial dans l'estimation du point noyau sur une image d'empreinte digitale. Pour déterminer l'emplacement du point noyau, le champ d'orientation de l'empreinte digitale doit d'abord être estimé. Cette fonctionnalité est utilisée pour localiser la

région du point noyau. Cette méthode est basée sur le fait que les points noyau ont un motif spécifique du champ d'orientation [H.Kekre et al.]. Un exemple de champ d'orientation de la région du point noyau est illustré à la figure 4.6.

FIGURE 4.6 – Champ d'orientation du point noyau.

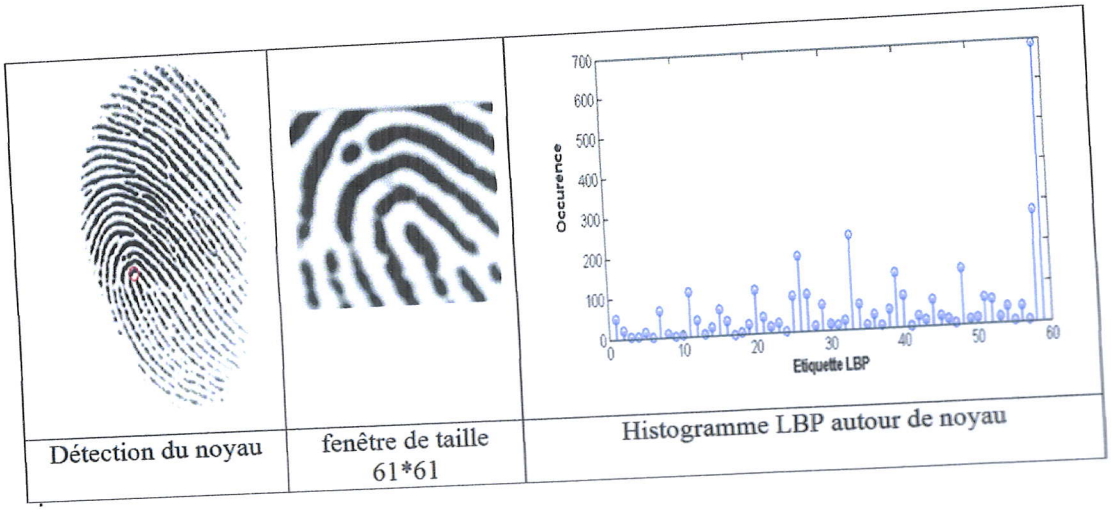


FIGURE 4.7 – Résultats des étapes d'extraction de l'histogramme LBP.

3.2.3 Comparaison des histogrammes LBP

Le calcul de la similarité entre les images est la seule solution utilisée pour la reconnaissance des objets. Selon [T.Ahonen et al., 2006], la métrique la plus adaptée avec LBP et qui permet d'obtenir de meilleurs résultats est la métrique Chi-square. C'est pour ça que nous l'avons choisit dans notre travail.

On calcule la distance chi-square entre deux histogrammes S et M, par la formule suivante :

$$X^2(S,M) = \sum_{i-1}^{n} \frac{(S_i - M_i)^2}{(S_i + M_i)} \tag{4.7}$$

Le meilleur score de correspondance est celui qui se réfère à la distance minimum entre deux histogrammes.

Après avoir calculé les distances de l'image de teste avec toute celles de références de la base de données, nous proposons une formule pour le calcul de score de LBP, selon la formule suivante :

$$\text{Score2} = \frac{\text{Max} - D}{\text{Max}} \tag{4.8}$$

Où :

- D : est la distance entre les histogrammes LBP de l'empreinte de teste et de référence.
- Max : est la distance maximale résultante de la comparaison d'une image avec toutes les images de la base de donnes.

3.3 Proposition 3 : Fusion des deux méthodes

Notre proposition globale combine les deux méthodes précédentes, en les fusionnant au niveau de score.

Pour cela, nous combinons les deux scores de minuties et de LBP, avec la formule suivante :

$$\text{Score final} = \frac{(\text{Score1} + \text{Score2})}{2} \tag{4.9}$$

L'image choisit est celle ayant le « score final » maximale.

4 Implémentation de l'application

Pour réaliser notre application ont sait baser sur les outils présentés dans ce qui suit :

4.1 Outil de développement

Nous avons eu recours lors de l'élaboration de notre système à Matlab (R2013b) (8.2.0.701) que nous présenterons ci-dessous.

Matlab et son environnement interactif est un langage de haut niveau qui permet l'exécution de tâches nécessitant une grande puissance de calcul et dont la mise en œuvre sera bien plus simple et rapide qu'avec des langages de programmation traditionnels tels que le C, C++. Il dispose de plusieurs boites à outils en particulier celle du traitement d'images « Image Processing ToolBox » qui propose un ensemble d'algorithme et d'outils graphiques de référence pour le traitement, l'analyse, la visualisation et le développement d'algorithmes de traitement d'images.

4.2 Base de données

Nous avons utilisé dans notre expérimentation deux familles de bases de données :

1. **FVC2002**(Fingerprint Verification Competition 2002) :
   - Composé de quatre bases (DB1_B, DB2_B, DB3_B, DB4_B). Chacune d'elle comporte 80 images correspondantes à 10 personnes (8 acquisitions pour chacune).
   - FVC2002 contient des images d'empreintes digitales de format TIF.

   Les figures 4.8, 4.9, 4.10 et 4.11 montrent quelques exemples des bases de FVC2002.
2. **UPEK** : Elle comporte 128 images (de format PNG) correspondantes à 16 personnes (8 acquisitions pour chacune)

La figure 4.12 contient des exemples des images de cette base de données.

FIGURE 4.8 – Echantillon d'empreintes de la base de données DB1_B de FVC2002.

FIGURE 4.9 – Echantillon d'empreintes de la base de données DB2_B de FVC2002.

FIGURE 4.10 – Echantillon d'empreintes de la base de données DB3_B de FVC2002.

FIGURE 4.11 – Echantillon d'empreintes de la base de données DB4_B de FVC2002.

FIGURE 4.12 – Echantillon d'empreintes de la base de données UPEK.

4.3 Présentation de l'application

On présente dans cette section les différents aspects de notre système d'identification.

4.3.1 Interface de Présentation du projet

C'est une interface destinée aux utilisateurs, elle est simple et permet d'illustrer les principaux processus du système d'identification, Ces opérations sont effectuées sur les bases de données (FVC2002 et UPEK) décrites auparavant.

Elle se compose de deux interfaces :

4.3.1.1 Accueil

Nous commençons par l'interface principale de notre logiciel. C'est une interface simple et contient trois boutons (Identification System, LBP Process, Minutiea Process), et une barre de menu qui contient quatre onglets (File, LBP Process, Minutiea Process, About), Comme le montre la figure 4.13.

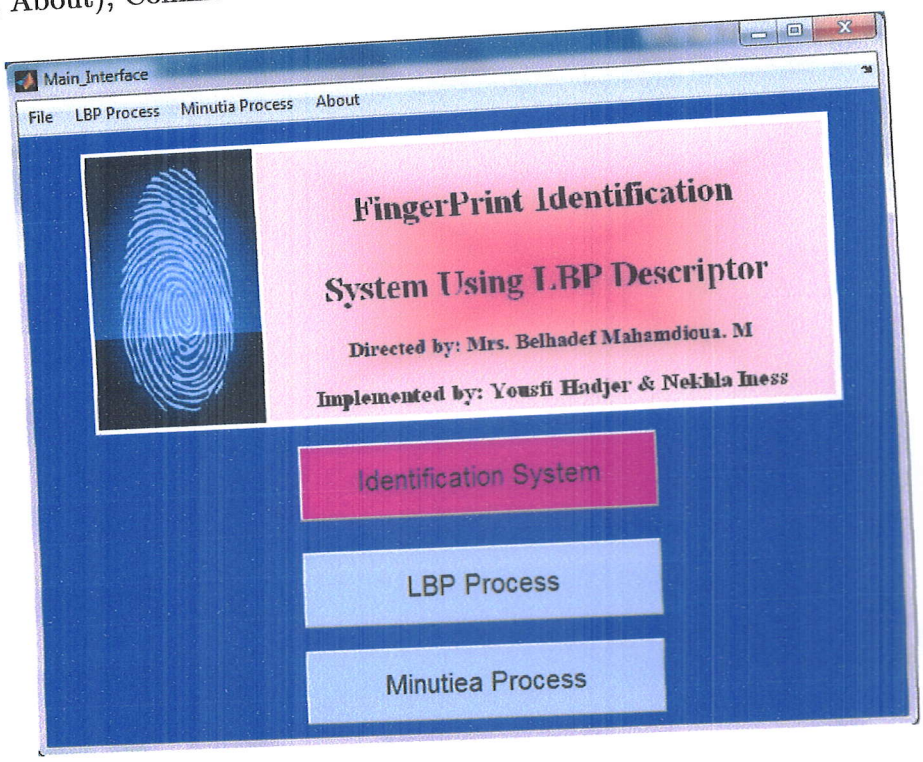


FIGURE 4.13 – Interface principale (accueil).

Les fonctionnalités des Boutons de l'interface sont :

— Le bouton **«Identification System »** : permet d'accéder à l'interface « Identification.fig » qui contient les différentes taches de notre application.

— Le bouton **« LBP Process »** : permet d'accéder à l'interface **« DealWithImage.fig »** qui contient les étapes le l'algorithme (LBP autour de noyau).

— Le bouton « **Minutiea Process**» : permet d'accéder à l'interface « **DealWithImage.fig** » qui contient les étapes le l'algorithme.

On peut aussi accéder a ces fonctionnalités à partir de la barre du menu.

Les fonctionnalités de la barre du menu de l'interface sont :

— Le menu « **file** » : contient trois sous-menus :

1. Le sous-menu « **Identification System** » : à la même fonctionnalité que le bouton « Identification System »
2. Le sous-menu « **Close** » : pour fermer la fenêtre en cours.
3. Le sous-menu « **Close All**» : pour fermer toutes les fenêtres.

— Les menus « **LBP Process** » et « **Minutiea Process**» : ont les mêmes fonctionnalités que les boutons du même nom.

— Le menu « **About** » : permet d'accéder à l'interface « **About.fig** » qui contient une brève explication sur notre application.

4.3.1.2 Interface d'identification

Elle se compose de cinq panneaux (comme montré dans la figure 4.14) :

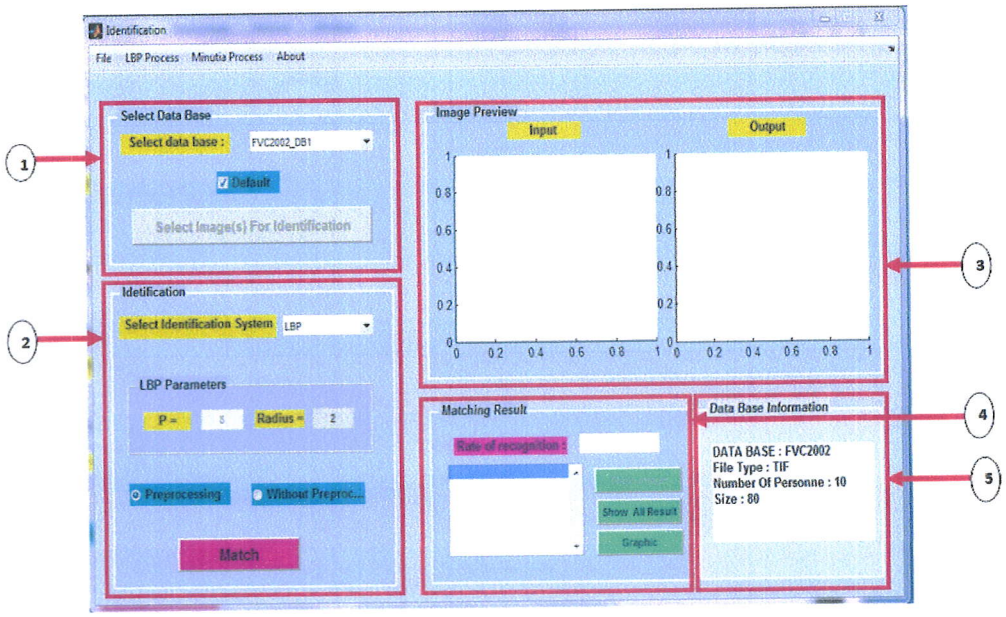
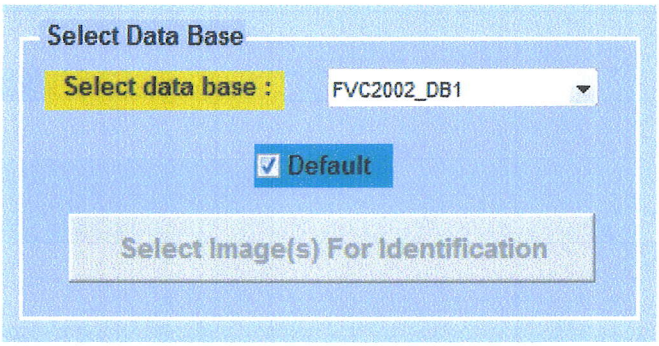
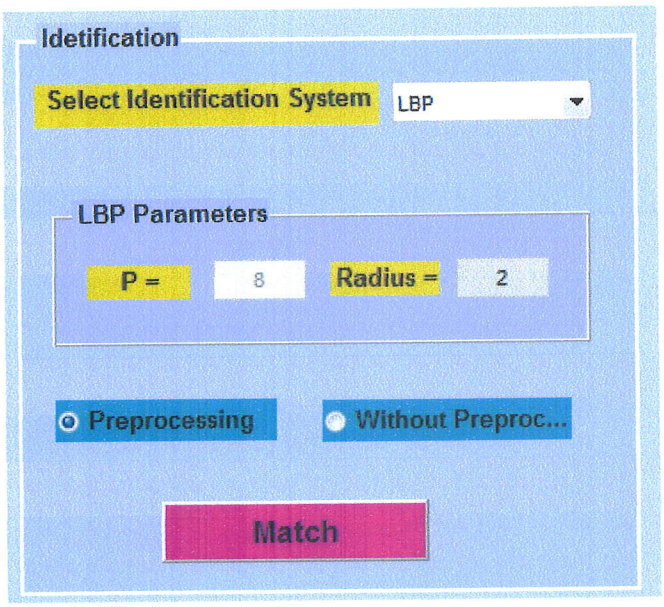


FIGURE 4.14 – Interface d'identification.

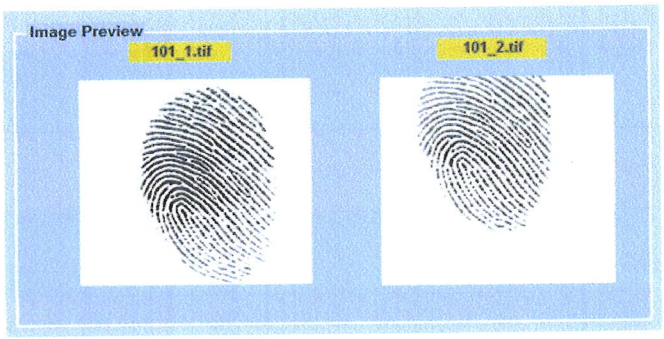
1. Le premier panneau nommé « **Select data base** » : permet de sélectionner la base de donnés sur laquelle on veut travailler, si on coche la case « **default** », le système va choisir par défaut 10 images de teste et 70 de référence pour la base de donné choisit au par avant et le bouton « **select image(s) for identification** » va être désactivé. Autrement le choix des images (teste/référence) s'effectue manuellement en cliquant sur le bouton « select image(s) for identification ».



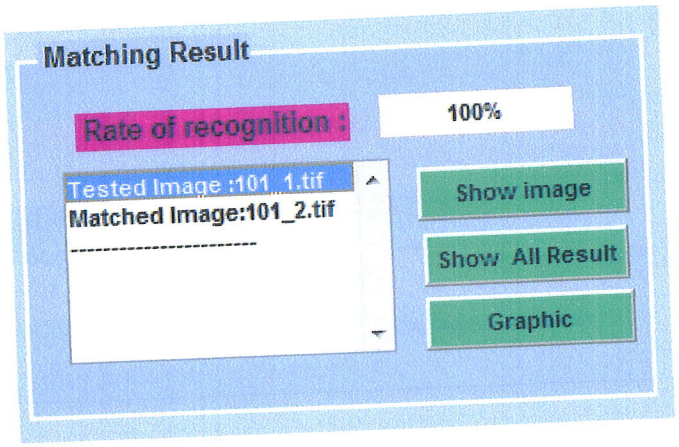
2. Le deuxième panneau nommé « **Identification** » : permet de choisir la méthode à utiliser pour l'identification (LBP, Minuties ou la méthode globale). Et fixées les paramètres d'identification (Radius, Preprocessing, Without Preprocessing).



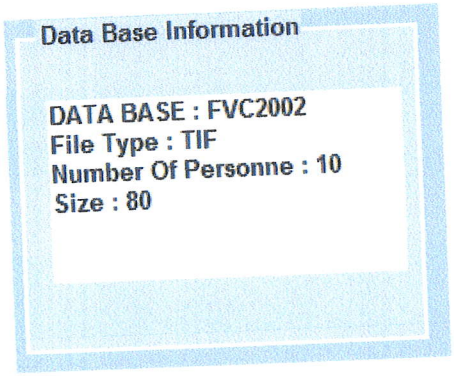
3. Le troisième panneau nommé « **Image Preview** » : permet d'afficher les résultats d'application de l'algorithme choisi.



4. Le quatrième panneau nommé « **Matching Result** » : permet d'afficher les résultats de correspondance (Taux de reconnaissance).



5. Le cinquième nommé « **Data Base Information** » : qui permet d'afficher des information sur la base de données choisit.



4.3.1.3 Interface de traitement

Permet de visualisé les différents traitements faits sur l'empreinte durant la phase d'identification pour chaque algorithme (identification par minutie et identification par LBP). Il se compose de 3 panneaux (comme montré dans la figure 4.15) :

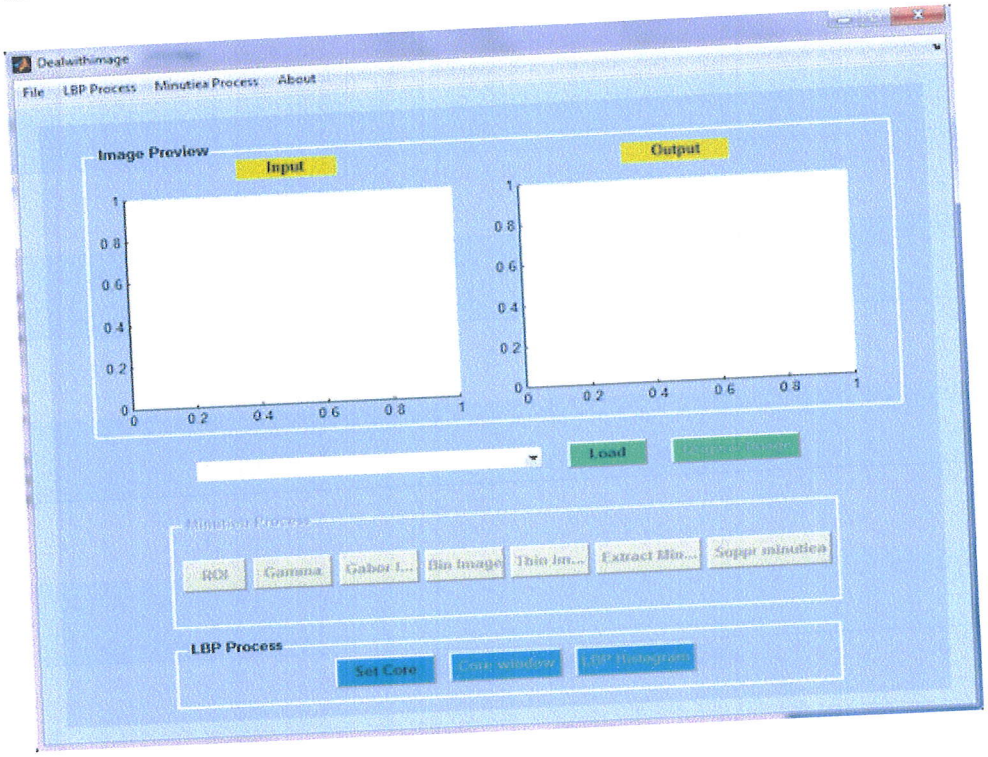


FIGURE 4.15 – Interface de traitement.

— Le premier nommé « **Image Preview** » : permet d'afficher les résultats d'application de l'algorithme choisi.

— Le deuxième et le troisième panneau « **Minutiea Process** » et « **LBP Process** » qui contiennent les différents traitements par laquelle passent les deux méthodes.

4.3.1.4 Interface d'aide

permet d'accéder à l'interface « About.fig » qui contient une brève explication sur notre application (comme montré dans la figure 4.16).

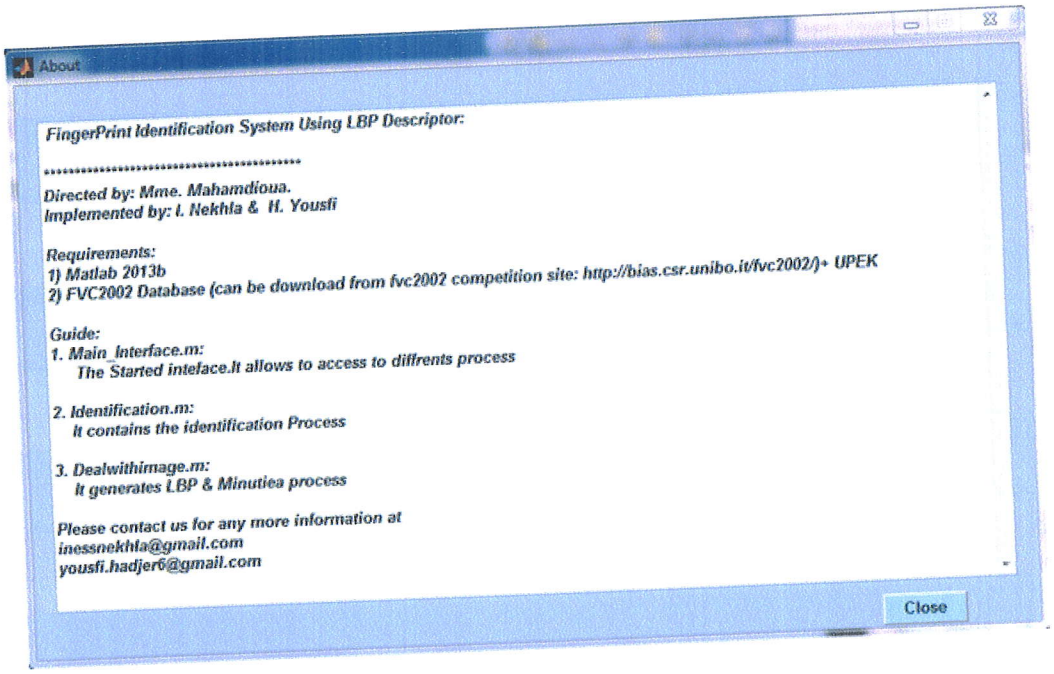


FIGURE 4.16 – Interface d'aide.

5 Résultats expérimentaux et discussion

Pour évaluer l'efficacité de nos propositions, nous avons opté pour une validation sur des bases de données standard (les quatre bases de données de « FVC2002 » et « UPEK »).

5.1 Principe d'identification

L'identification consiste à comparer l'image d'empreintes avec toutes les images de référence de la base de données. Afin de tester une application d'identification d'empreinte digitale, il est nécessaire de disposer de deux bases de données : une base pour les empreintes de référence et une autre pour les empreintes de test.

Le but est d'évaluer le taux de reconnaissance de différents algorithmes présenté et montrer leur importance, en suivant un protocole de test basé sur la mesure de taux de reconnaissance suivante :

$$\text{Taux de reconnaissance} = \frac{\text{nombre d'image de teste reconnues}}{\text{totale des images de teste}} \tag{4.10}$$

5.2 Intérêt d'amélioration

Pour montrer l'intérêt des améliorations apportés avec la première méthode proposé (prétraitement plus minuties) ainsi que la deuxième proposition (LBP autour de noyau). Nous allons effectuer un test monotone pour chaque méthode.

Dans le premier test, nous comparons le résultat obtenu à partir de la première

méthode proposé et le résultat obtenu par H.Douara et al., dans [H.Douara et al., 2016] pour la méthode basée sur les minuties sans prétraitement.

Le deuxième test était entre la deuxième méthode proposée qui est LBP autour de noyau et la méthode LBP sur l'image entière (plus exactement l'image de la région d'intérêt).

5.2.1 Minuties avec prétraitement

Nous avons utilisé un sous ensemble de la base FVC2002(DB1_B), constitué de 10 images de test et 23 images de référence.

Les résultats obtenus sont montré dans le tableau 4.1 :

Minutie avec prétraitement	Minutie sans prétraitement
80%	10%

TABLE 4.1 – Comparaison de la méthode minuties avec prétraitement et minuties sans prétraitement.

Comme nous pouvons le voir dans le tableau 4.1, le taux de reconnaissance de notre méthode basée sur les minuties avec prétraitement appliquée sur la base de données citée précédemment est de 80%, ce qui signifie que le système n'a pas connu seulement deux images parmi les images testées. Ces images dans notre expérimentation a été de très mauvaise qualité.

Pour la méthode qui utilise les minuties sans prétraitement, le taux de reconnaissance est de 10%. Nous voyons bien la grande différence entre les deux résultats.

5.2.2 LBP autour du noyau

Cette fois-ci, nous utilisons la base FVC2002 (DB1_B) complète, où nous avons utilisé 10 images de test et 70 images de référence. Nous obtenons les résultats suivants :

LBP autour du noyau	LBP sur l'image entière
90%	50%

TABLE 4.2 – Comparaison de la méthode LBP autour du noyau et LBP sur l'image entière.

Les résultats montrent la supériorité de la méthode proposée, cela explique l'importance de l'information autour du noyau.

5.3 Etude comparative des méthodes proposées

Dans la section précédente, nous avons illustré l'efficacité de nos ajouts par rapport aux méthodes originales. Dans cette section, nous comparons les trois méthodes proposée en effectuant une séries de tests sur plusieurs bases de données qui ont étés scindées de la façon suivante :

— **Images tests :**
  — Pour la base FVC2002 : les 10 premières empreintes de chaque personne.
  — Pour la base UPEK : les 16 premières empreintes de chaque personne.
— **Images références :**
  — Pour la base FVC2002 : les 70 empreintes restantes servent de référence.
  — Pour la base UPEK : les 112 empreintes restantes servent de référence.

5.3.1 Résultats

Le tableau 4.3 représente le taux de reconnaissance pour chaque méthode proposée. Les résultats sont variés d'une méthode à une autre. Nous observons clairement que la méthode globale donne de bon résultat dans tous les cas sauf dans le cas de DB3. D'autre côté, l'utilisation individuelle du descripteur LBP autour de noyau donne 90%, 100% 100%, 80% et 93.75% respectivement pour les bases DB1, DB2, DB3, DB4 et UPEK contre 100%, 80%, 90%, 70%, 87.5% pour l'utilisation des minuties pour les mêmes bases.

Base de données	Prétraitement +Minutie	LBP autour du noyau	Méthode Global
DB1	100%	90%	100%
DB2	80%	100%	100%
DB3	90%	100%	90%
DB4	70%	80%	90%
UPEK	87.5%	93.75%	93.75%

TABLE 4.3 – Taux de reconnaissance obtenus pour chaque méthode.

La représentation graphique ci-dessous présente mieux cette comparaison entre les trois approches pour chaque base de données.

6 Conclusion

Ce chapitre a été consacré à la présentation des méthodes d'identification d'empreinte digitale proposées dans notre travail en l'occurrence de la méthode de reconnaissance par minuties et celle basée sur l'utilisation du descripteur LBP autour du noyau, en arrivant à la troisième qui résulte de la fusion des deux.

Notre système d'identification des empreintes digitales, est appliqué sur 2 familles des bases de données d'empreinte FVC2002 et UPEK qui sont bien présentées dans

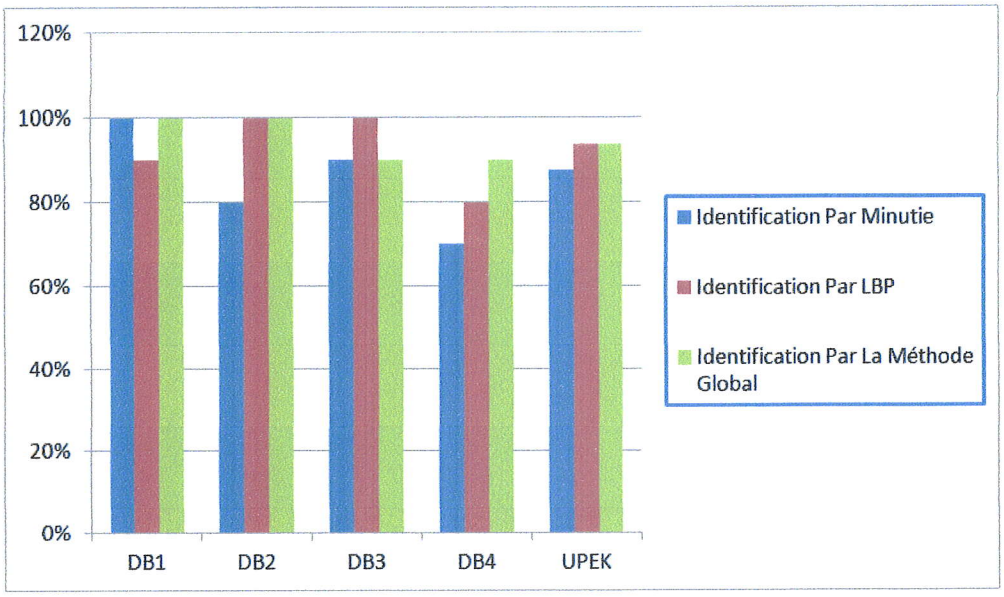


FIGURE 4.17 – Comparaison des trois approches proposées.

la partie implémentation de l'application. Les résultats trouvés illustrent clairement l'intérêt de nos propositions pour l'identification d'empreinte digitale.

Pour conclure, nous pouvons noter que chaque méthode à prouver son efficacité. Cependant, la fusion proposée dans notre système d'identification a montré un taux d'amélioration visible par rapport au deux autre méthodes.

Conclusion générale

DANS ce mémoire nous nous sommes intéressés au système d'identification par empreinte digitale dans le but d'améliorer la reconnaissance des individus. Nous avons présenté la biométrie de manière générale. Ensuite nous avons exposé la reconnaissance par empreinte digitale, un domaine qui a reçu une attention accrue de la part des chercheurs.

Nous avons donc décrit les différentes étapes nécessaires à la construction d'un système de reconnaissance des empreintes digitales à savoir : le prétraitement, l'extraction des caractéristiques et la comparaison. Ensuite nous avons détaillés la méthode LBP (Local Binary Pattern), qui est un descripteur très discriminatif pour l'extraction de caractéristiques, ainsi qu'un état de l'art de son utilisation avec les empreintes digitales.

La performance d'un algorithme d'extraction et de mise en correspondance des images d'empreintes digitales dépend fortement de la qualité de l'image en entrée. Cependant, dans la pratique un pourcentage signifiant d'images est en mauvaise qualité. Cela est dû des conditions d'acquisition, de l'état de l'épiderme, de dispositif de prise de vue, et d'une mauvaise coopération du sujet. Cela peut engendrer un ensemble des problèmes tels que la création de fausses minuties, l'ignorance de vraies minuties, l'introduction d'erreurs de localisation (rotation/translation) ...etc. Une étape de prétraitement pour améliorer la clarté s'avère donc nécessaire. De même l'utilisation d'une méthode fiable pour la reconnaissance d'empreintes se révèle être une nécessité cruciale.

Dans ce contexte, nous avons proposé d'améliore la qualité d'image d'empreinte et d'utiliser la méthode LBP autour du noyau. Puis, nous fusionnons cette méthode avec celle basé sur les minuties extraites de l'image améliorée. Cette fusion que nous avons nommée méthode globale est effectuée au niveau des scores générés par les deux méthodes.

Le prétraitement utilisé pour LBP est la correction de gamma qui permet d'améliorer le contraste et la clarté de l'image. Pour l'extraction de minuties, nous avons basé essentiellement sur la Correction de Gamma et un Banc de Gabor.

Pour illustrer l'intérêt de nos propositions, nous avons effectué des expérimentations sur les bases de données FVC2002 et UPEK. Les résultats expérimentaux ont montré une très bonne efficacité pour nos propositions, particulièrement la méthode globale (la fusion).

Bibliographie

[A.Jain et al., 2004] A.K. Jain, A. Ross, S. Prabhakar. : 'An introduction to biometric recognition'. In IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics. VOL. 14, pp. 4–6, Janvier, 2004.

[I.Benchennane, 2015] I. Benchennane. : 'Etude et mise au point d'un procédé biométrique multimodale pour la reconnaissance des individus'. Thèse de Doctorat, Université des Sciences et de la Technologie d'Oran Mohamed Boudiaf, 2015.

[D.Raphael et al., 1974] D.E. Raphael and J.R. Young. : 'Automated Personal Identifcation', Palo Alto, Calif. [cité par Joseph N. Pato and Lynette I. Millett, Biometric Recognition : Challenges and Opportunities. In Whither Biometrics Committee, National Research Council, 182p, 2007.

[D.Maltoni et al., 2003] Davide Maltoni. : 'A tutorial on fingerprint recognition in biometric systems laboratory' - DEIS - University of Bologna., Cesena (FC), Italy, pp. 51-62, A Portions reprinted from : D. Maltoni, D. Maio, A.K. Jain and S. Prabhakar. Handbook of fingerprint recognition, In Springer, 2003.

[B.Vibert et al., 2016] B. Vibert J.M. Le Bars, C. Charrier et C. Rosenberger. : ' Analyse d'empreintes digitales a partir de paramètres structurels calculès sur une référence réduite de l'image'. In Conférence 18éme éditions de CORESA , NANCY, France, Mai, 2016.

[A.Jain et al., 2005] A.K. Jain, K. Nandakumar et A. Ross. : 'Score normalization in multimodal biometric systems'. In Pattern Recognition. Vol. 38, no. 12, pp. 2270–2285 , December, 2005.

[F.Zhao et al., 2002] F. Zhao, X. Tang. : ' Duality-based post-processing for fingerprint minutiae extraction'. In Department of Information Engineering The Chinese University of Hong Kong, pp. 36, 2002.

[N.Galy, 2005] Nicolas Galy. : ' Etude d'un système complet de reconnaissance d'empreintes digitales pour un capteur microsystème balayage'. Thèse de Doctorat, Ecole Doctorale Electrotechnique, Automatique, Télécommunication, Signal, Institut National Polytechnique de Grenoble, 2005.

[M.Fons et al., 2006] M. Fons , F. Fons . : ' Design of an Embedded Fingerprint Matcher System4. In Proc IEEE on Consumer Electronics, pp 1–6, Canto, 2006.

[X.Jia et al., 2014] X. Jia , X. Yang , K. Cao , Y. Zang , N. Zhang , Ruwei Dai , X. Zhu , J. Tian. : ' Multi-scale local binary pattern with filters for spoof fingerprint detection In Information Sciences', Elsevier, pp.91–102, 2014.

[D.Maio et al., 2001] D. Maio and D.maltoni. : ' Direct gray-scale minutiae detection in fingerprints'. In IEEE Transactions on Pattern Recognition, Vol. 34, pp. 999-1013, 2001.

[J.Lim et al., 2013] J. F. Lim, R. K. Y. Chin. : ' Enhancing fingerprint recognition using minutiae-based and image-based matching techniques'. In First International Conference on Artificial Intelligence, Modelling and Simulation. 2013.

[T.Ojala et al., 1996] T. Ojala, M. Pietikäinen, D. Harwood. : 'A comparative study of texture measures with classification based on feature distributions'. In Pattern Recognit. Vol. 29, no. 1, pp. 51–59, 1996.

[D.Lowe, 2004] D.G. Lowe. : 'Distinctive image features from scale-invariant keypoints', In International Journal of Computer Vision. Vol. 60, no. 2, pp. 91–110, 2004.

[S.Sam et al., 2016] S.Samruddhi, Dr. Kulkarni, Y. H. Patil. : ' A fingerprint spoofing detection system using LBP'. In International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), 2016.

[L.Paulhac, 2011] L. Paulhac. : ' Outils et méthodes d'analyse d'images 3D texturées : Application à la segmentation des images échographiques'. pp. 32–35, 2011.

[T.Ojala et al., 2001] T. Ojala, M. Pietikäinen, and T. Mäenpää. : 'A generalized local binary pattern operator for multiresolution gray scale and rotation invariant texture classification'. In Advances in Pattern Recognition - ICAPR. Vol. 2013 : Springer Berlin Heidelberg, pp. 399–408, 2001.

[T.Ojala et al., 2002] T. Ojala, M. Pietikäinen, and T. Mäenpää. : ' Multiresolution gray-scale and rotation invariant texture classification with local binary patterns'. In IEEE Trans. Pattern Anal. Mach. Intell. No. 7, 971–987, 2002.

[M.Pietikäinen et al., 2011] M. Pietikäinen, A. Hadid, G. Zhao, T. Ahonen . : ' Computer vision using local binary patterns'. Computational Imaging and Vision 40 . 2011.

[T.Mäenpää, 2003] T. Mäenpää. : ' The Local Binary Pattern Approach To Texture Analysis'. In Extensions And Applications, 2003.

[T.Ahonen et al., 2006] T. Ahonen, A. Hadid, et M. Pietikäinen. : ' Face description with local binary patterns : Application to Face Recognition'. In IEEE, Department of Electrical and Information Engineering, University of Oulu, Finland, pp. 2037–2041, 2006.

[L.Nanni et al., 2008] L. Nanni, A. Lumini. : 'Local binary patterns for a hybrid fingerprint matcher '. In Pattern Recognition, University of Bologna, via Venezia ,Cesena, Italy, 2008.

[V.Talele et al., 2014] V. M. Talele, V. P. Talele, S. N. Bhutada. : 'Study of local binary pattern for partial fingerprint identification', Journal Of Modern Engineering Research (IJMER). Vol. 4, Septembre, 2014.

[S.Kulkarni et al., 2016] S.Samruddhi, Dr. Kulkarni, Y. H. Patil. : 'A fingerprint spoofing detection system using LBP'. In International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT). Sapat College of Engineering, Management Studies and Research. India Maharashtra, Nashik, 2016.

[G.Cao et al., 2010] G. Cao, Y. Zhao, Rongrong Ni. : 'Forensic estimation of gamma correction in digital images'. Institute of Information Science, Beijing Jiaotong

University, Proceedings IEEE 17th International Conference on Image Processing, Hong Kong. September, 2010.

[L.Hong et al., 1998] L. Hong, Y. Wan ; A. Jain. : 'Fingerprint image enhancement : algorithm and performance evaluation'. Dept. of Computer Science. Michigan State University. East Lansing, MI, USA. In IEEE Transactions on Pattern Analysis and Machine Intelligence. Vol. 20, Aoute 1998.

[L.Wieclaw, 2009] Lukasz Wieclaw. : 'A minutiae-based matching algorithms in fingerprint recognition systems'. In Journal of Medical Informatics and Technologies. Vol. 13, pp. 65–68. 2009.

[A.Ghany et al., 2014] K. Kamal A. Ghany , A. E. Hassanien and G. Schaefer. : 'Similarity Measures for Fingerprint Matching'. Faculty of Computers and Information, Cairo University, Department of Computer Science, Loughborough University, U.K. Juillet, 2014.

[H.Kekre et al.] H.B. Kekre, V.A. Bharadi. : ' Fingerprint core point detection algorithm using orientation field based multiple features'. In International journal of computer applications. Department of computer science Mukesh Patel School of technology management and engineering, NMIMS University Mumbai, India. Vol. 1, no. 15, s. d. pp. 100–101.

[H.Douara et al., 2016] H.E Douara, M. Feltane . : ' Reconnaissance d' empreinte digitale par fusion multi-algorithmique'. Thèse de Master 2, Département d'informatique, Université de JIJEL, 2016.

[S.Kahlsnan et al., 2013] S. Kahlsnan, N. Zihga. : ' Comparaison des méthodes d'amélioration de la qualité d'image d'empreinte digitale'. Département d'informatique, Université de Jijel. 2013.

[M.Mehrubeoglu, 2007] M. Mehrubeoglu , L. McLauchlan. : 'Identification of degraded fingerprints using PCA- and ICA-based features', Proc. Applications of Digital Image Processing, 2007.

[P.Moreno et al., 2005] P. Moreno, A. Bernardino, J. Santos-Victor. : ' Gabor Parameter Selection for Local Feature Detection'. 2nd Iberian Conference on Pattern Recognition and Image Analysis, Estoril, Portugal. Juin, 2005.