

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA

RECHERCHE SCIENTIFIQUE

*Université de Mohamed El-Bachir El-Ibrahimi - Bordj Bou Arreridj*

*Faculté des Sciences et de la technologie*

*Département d'Electronique*

## *Mémoire*

Présenté pour l'obtention du diplôme de

**MASTER**

**Filière :** Télécommunications

**Spécialité :** Systèmes des télécommunications

Par :

➤ **CHAHMI Mohamed Belkheir**

➤ **ATTIA Racim**

*Intitulé :*

**Amélioration de l'image des empreintes digitales en vue  
de leur reconnaissance**

*Soutenue le : 13/09/2023*

*Devant le jury :*

<i>Nom &amp; Prénom</i>	<i>Grade</i>	<i>Qualité</i>	<i>Etablissement</i>
<b>M. FLISSI</b>	<b>MCA</b>	<b>Président</b>	<b>Univ-BBA</b>
<b>S. MEZAACHE</b>	<b>MCB</b>	<b>Encadreur</b>	<b>Univ-BBA</b>
<b>D. BOUDECHICHE</b>	<b>MCA</b>	<b>Examineur</b>	<b>Univ-BBA</b>

*Année Universitaire 2022/2023*

## Remerciements

---

Je tiens à exprimer ma profonde gratitude envers toutes les personnes qui ont contribué à la réalisation de ce mémoire de master. Je tiens tout d'abord à remercier chaleureusement mon superviseur, Dr. S. MEZAACHE, pour sa guidance, ses précieux conseils et son soutien constant tout au long de ce projet. Son expertise a été inestimable pour moi.

Je souhaite également remercier les membres de jury, Dr. M. FLISSI et Dr. D. BOUDECHICHE, pour leurs remarques constructives et leurs suggestions qui ont grandement enrichi ce travail.

Un grand merci à tous mes enseignants et collègues qui m'ont encouragé et partagé leurs connaissances au cours de ces années d'études.

Je n'aurais pas pu accomplir tout cela sans le soutien inconditionnel de ma famille et de mes amis. Votre confiance en moi a été ma source d'inspiration.

Enfin, je tiens à exprimer ma reconnaissance envers toute la communauté du département d'électronique pour les moments passés au sein de l'enceinte universitaire.

Ce travail représente pour moi un accomplissement personnel important, et je suis enthousiaste à l'idée de continuer à explorer de nouvelles opportunités dans le domaine des télécommunications et de l'électronique en général. Merci à tous pour votre soutien et votre encouragement.

M. CHAHMI & R. ATTIA

## Dédicaces

---

*À ma famille, pour leur amour inconditionnel et leur soutien constant. Votre confiance en moi a été ma plus grande motivation. À mes amis, pour les moments de détente et d'encouragement pendant cette période exigeante. À mon superviseur, Dr. S. MEZAAACHE, pour ses précieux conseils et son expertise. À toutes les personnes qui ont contribué à ma formation, je vous remercie du fond du cœur.*

*À mes parents, pour avoir été mes piliers de force tout au long de ce voyage académique. Votre sacrifice et votre amour sont inestimables. À mon ami ....., pour avoir partagé les hauts et les bas de cette aventure avec moi. Ton amitié est un trésor précieux.*

*À mes frères et sœurs, pour vos conseils éclairés, votre soutien inébranlable et votre présence rassurante. Ce mémoire témoigne de notre solide lien familial, et je suis honoré de vous avoir comme frères/sœurs."*

*À tous les collègues et collaborateurs qui ont contribué à ma recherche, votre expertise et votre collaboration ont enrichi ce travail. Je suis reconnaissant de pouvoir compter sur votre soutien dans mon parcours académique.*

## Table des matières

---

Introduction.....	7
1. La Reconnaissance des Empreintes Digitales.....	11
1.1. Introduction.....	11
1.2. Historique.....	11
1.3. Les empreintes digitales, caractéristiques et reconnaissance.....	11
1.4. Reconnaissance des empreintes digitales.....	15
1.4.1. Prétraitement de l’empreinte digitale.....	17
1.4.1.1. Normalisation.....	19
1.4.1.2. Estimation de l’orientation de l’image.....	19
1.4.1.3. Estimation de l’image des fréquences locales.....	21
1.4.1.4. Segmentation de l’image ou masque de région utile.....	23
1.4.1.5. Filtrage.....	24
1.4.2. Extraction des paramètres (minuties).....	25
1.4.2.1. La binarisation de l’image.....	26
1.4.2.2. La squelettisation de l’image.....	26
1.4.2.3. Détection des minuties.....	28
1.4.2.4. Élimination des fausses minuties.....	30
1.4.3. Le fichier signatures.....	30
1.4.4. Phase de Comparaison ou d’appariement.....	31
2. Prétraitement de l’image d’empreinte : partie pratique.....	32
2.1. Introduction.....	32
2.2. Normalisation.....	32
2.3. Calcul de l’image de l’orientation.....	32
2.4. Calcul de l’image des fréquences.....	34
2.5. Calcul du masque de l’image.....	34
2.6. Filtrage de Gabor appliqué à l’image d’empreinte.....	35
2.7. Conclusion.....	36
Conclusion Générale.....	37
Références bibliographiques.....	38

## Table des illustrations

Figure 1: (a) Une empreinte digitale ; (b) Une vue agrandie des crêtes et des vallées.....	12
Figure 2: Les classes d'empreintes selon Henry.....	13
Figure 3: Les types de base des minuties d'une empreinte. (a) Terminaison ;(b) Bifurcation	14
Figure 4: Les types de base des minuties d'une empreinte. (a) Terminaison ;(b) Bifurcation	14
Figure 5: Architecture générale d'un système de reconnaissance d'empreintes [5], [6].....	16
Figure 6 : Organigramme des étapes de l'amélioration de l'image d'empreinte digitale.....	18
Figure 7 : Fenêtre d'orientation et x-signature.....	21
Figure 8: La phase d'extraction de la signature.....	26
Figure 9: Processus de binarisation, image originale.....	26
Figure 10: Processus de binarisation, image binarisée.....	26
Figure 11: Processus de squelettisation, image originale.....	28
Figure 12: Processus de squelettisation, image squelettisée.....	28
Figure 13: Numérotation des pixels pour le calcul de CN.....	29
Figure 14: Les cas des points de type terminaison (CN=1).....	29
Figure 15: Les cas des points de type bifurcation (CN=3).....	29
Figure 16: Résultat de la normalisation de l'image d'empreinte.....	32
Figure 17: Calcul de l'image d'orientation de l'image d'empreinte.....	33
Figure 18: Détails du calcul de l'orientation de l'image d'empreinte.....	33
Figure 19: Agrandissement (zoom) sur l'image d'orientation.....	33
Figure 20: Image fréquentielle cote à cote avec l'image originale en niveaux de gris.....	34
Figure 21: Calcul du masque de région utile de l'empreinte digitale.....	35
Figure 22: Résultat de l'application du filtre de Gabor sur l'image d'empreinte.....	36

## Introduction

---

La biométrie (bios metron = mesure de la vie) se définit comme les méthodes automatisées d'identification ou d'authentification de l'identité d'une personne vivante sur la base d'un ou plusieurs traits physiques ou comportementaux intrinsèques. Un certain nombre de technologies biométriques ont été développées et sont utilisées dans de nombreuses applications telles que les solutions d'identification sécurisée et de vérification personnelle, etc. Les données biométriques sont des données à caractère personnel car elles permettent d'identifier une personne. Elles ont, pour la plupart, la particularité d'être uniques et permanentes (ADN, empreintes digitales, iris, etc.). Bien que la biométrie ait émergé de son utilisation extensive dans l'application de la loi pour identifier les criminels (p. ex. habilitation de sécurité des employés pour les emplois sensibles, détermination de la paternité, criminalistique, et identification positive des condamnés et des prisonniers), il est de plus en plus utilisé aujourd'hui pour établir la reconnaissance des personnes dans un grand nombre d'applications civiles [1].

Selon le contexte de l'application, un système biométrique peut fonctionner en mode de vérification ou en mode d'identification.

En mode de vérification, le système valide l'identité d'une personne en comparant les données biométriques saisies avec ses propres modèles biométriques stockés dans la base de données du système.

Dans un tel système, une personne qui souhaite être reconnue revendique une identité, habituellement au moyen d'un numéro d'identification personnel (NIP), d'un nom d'utilisateur ou d'une carte à puce, et le système effectue une comparaison individuelle pour déterminer si la demande est vraie ou non. (p. ex., Ces données biométriques appartiennent-elles à Mustapha?). La vérification de l'identité est habituellement utilisée à des fins de reconnaissance positive, dans le but d'empêcher plusieurs personnes d'utiliser la même identité [2].

En mode d'identification, le système reconnaît un individu en recherchant les modèles de tous les utilisateurs de la base de données pour une correspondance. Par conséquent, le système effectue une comparaison de un à plusieurs pour établir l'identité d'une personne (ou échoue si la personne n'est pas inscrite dans la base de données du système) sans que la personne en cause ait à demander une identité (p. ex. « À qui appartiennent ces données biométriques? »). L'identification est un élément essentiel dans les demandes de reconnaissance négative

lorsque le système établit si la personne est celle qu'elle nie (implicitement ou explicitement). Le but de la reconnaissance négative est d'empêcher une seule personne d'utiliser des identités multiples [2].

Un système biométrique est conçu à l'aide des quatre modules principaux suivants (voir figure 1) [1].

1. Module d'acquisition qui capture les données biométriques d'une personne. Un exemple est un capteur d'empreintes digitales qui représente la crête et la structure de la vallée du doigt d'un utilisateur.
2. Module d'extraction de caractéristiques, dans lequel les données biométriques acquises sont traitées pour extraire un ensemble de caractéristiques discriminatives. Par exemple, la position et l'orientation des points de minutie (singularités locales de crête et de vallée) dans une image d'empreinte digitale sont extraites dans le module d'extraction de caractéristiques d'un système biométrique basé sur les empreintes digitales.
3. Module de calcul de similarité, dans lequel les paramètres extraits lors de la reconnaissance sont comparés aux modèles stockés pour générer des scores correspondants. Par exemple, dans le module d'appariement d'un système biométrique basé sur les empreintes digitales, un certain nombre d'appariement de minuties entre l'entrée et les images d'empreintes digitales du modèle est déterminé et un score correspondant est calculé. Ce module englobe également un module de prise de décision, dans lequel l'identité revendiquée d'un utilisateur est confirmée (vérification) ou l'identité d'un utilisateur est établie (identification) en fonction du score correspondant.
4. Module de base de données système, utilisé par le système biométrique pour stocker les modèles biométriques des utilisateurs inscrits. Le module d'inscription est chargé d'inscrire les personnes dans la base de données du système biométrique.

Il ne semble y avoir pratiquement aucune limite aux parties du corps, aux caractéristiques personnelles et aux méthodes d'imagerie suggérées et utilisées pour l'identification biométrique: les doigts, les mains, les pieds, le visage, les yeux, les oreilles, les dents, les veines, la voix, la signature, etc. Quelle caractéristique est la meilleure? Les principales préoccupations sont au moins cinq : la robustesse, le caractère distinctif, l'accessibilité, l'acceptabilité et la disponibilité du modèle biométrique. Par robuste, nous entendons reproductible, non sujet à de grands changements dans le temps. Par distinctif, nous entendons

l'existence de grandes différences dans la structure de la population. Par accessible, nous entendons qu'il soit facilement présenté à un capteur d'imagerie. Par acceptable, nous entendons qu'il soit perçu comme non intrusif par l'utilisateur. Par disponible, nous entendons qu'un certain nombre de mesures indépendantes peuvent être présentées par chaque utilisateur [2].

Les humains ont utilisés les empreintes digitales pour l'identification personnelle depuis de nombreux siècles et il a été démontré que l'exactitude de la correspondance à l'aide des empreintes digitales est très élevée [3]. Une empreinte digitale est le motif des crêtes et des vallées à la surface d'un bout de doigt, dont la formation est déterminée au cours des sept premiers mois du développement fœtal. Les empreintes digitales de jumeaux identiques sont différentes, tout comme les empreintes sur chaque doigt de la même personne. À l'heure actuelle, un scanner d'empreintes digitales ne coute presque rien, et le coût marginal de l'intégration de données biométriques fondées sur les empreintes digitales dans un système (p. ex., ordinateur portable) est devenu abordable dans un grand nombre d'applications.

L'exactitude des systèmes de reconnaissance des empreintes digitales actuellement disponibles est adéquate pour les systèmes de vérification et les systèmes d'identification à petite et moyenne échelle impliquant quelques centaines d'utilisateurs. Les multiples empreintes digitales d'une personne fournissent des renseignements supplémentaires pour permettre la reconnaissance à grande échelle de millions d'identités. L'un des problèmes avec les systèmes actuels de reconnaissance des empreintes digitales est qu'ils nécessitent une grande quantité de ressources informatiques, surtout en mode d'identification [3].

L'acquisition des images d'empreintes digitales est considérée comme l'étape la plus critique d'un système de reconnaissance, car elle produit la qualité d'image finale d'empreintes digitales, ce qui est très important pour les performances globales du système et pour atteindre la meilleure qualité. Le filtre Gabor, également connu sous le nom de filtre de détection des bords, est largement utilisé pour l'amélioration de la qualité de l'image [4].

L'objectif principal est d'utiliser des techniques de filtrage de type Gabor sur une image d'empreinte qui sera filtrée pour obtenir une image de sortie de meilleur qualité. En fait, le filtre Gabor est utilisé pour la détection des bords. Les filtres de Gabor sont essentiellement des filtres passe-bande qui sont principalement utilisés dans le traitement d'image. Un filtre de Gabor produit une réponse élevée aux coins et exactement au point où la texture change. Le filtre Gabor est largement utilisé pour la détection des contours et l'extraction des textures d'image, la suppression ainsi que pour la détection des contours des objets et les effets de

perception visuelle .

Ce projet vise principalement à améliorer la qualité d'une image d'empreinte digitale en entrée par l'utilisation de techniques de filtrage Gabor où l'image d'entrée est segmentée en fonction de la texture des couleurs et filtrée.

Le présent mémoire est divisé en deux chapitres :

Dans le premier chapitre, nous donnons une étude théorique sur les aspects essentiels de la reconnaissance des empreintes digitales. Nous allons détailler la partie prétraitement de l'image d'empreinte digitale et mentionner brièvement les autres étapes.

Dans le deuxième chapitre, nous présentons les résultats de la partie de prétraitement et nous terminons par une conclusion générale et des perspectives.

## Chapitre 1

# La Reconnaissance des Empreintes Digitales



## **1. La Reconnaissance des Empreintes Digitales**

---

### **1.1.Introduction**

L'empreinte digitale est un outil d'identification rapide, fiable et moins coûteux que les autres outils. L'utilisation des empreintes digitales comme moyen d'identification d'une personne ne sont pas nouvelles. En effet, c'est la technologie biométrique la plus ancienne et la plus mature. L'empreinte a été officiellement acceptée comme identifiant personnel valide dès le début du siècle. Ils ont d'abord été utilisés dans les milieux juridiques avant de devenir une technologie d'authentification valide [5].

### **1.2.Historique**

Les empreintes digitales ont été utilisées dans les temps anciens, et il existe des preuves [5]; cependant, il n'y a pas des preuves qu'ils ont été utilisés comme moyen d'identification personnelle.

Le premier enregistrement fiable vient de Sir William Herschel. En 1858, il était employé de la Compagnie des Indes orientales en Inde. Alors qu'il préparait un contrat avec un homme local pour des matériaux de construction, il a décidé de prendre une empreinte de la paume de l'individu au lieu d'utiliser la signature plus conventionnelle. Sa motivation était « d'effrayer l'entrepreneur de toute pensée de répudier sa signature par la suite ». Herschel a rapidement reconnu le potentiel de l'utilisation des empreintes digitales comme moyen d'identification personnelle et a étudié la question comme un passe-temps pendant des années après son expérience initiale. La première publication scientifique proposant l'utilisation des empreintes digitales pour l'identification est due à Henry Faulds en 1880, et à la fin des années 1880, Sir Francis Galton a commencé une étude rigoureuse de l'identification basée sur les empreintes digitales .

La première adoption généralisée d'un système d'identification basé sur les empreintes digitales a eu lieu en Inde en 1893. Edward Henry, un chercheur sur les empreintes, a complété le système anthropométrique utilisé avec des empreintes de pouce. Encouragée par le succès du système, la Grande-Bretagne a mis en place un programme similaire l'année suivante. Les forces de l'ordre du monde entier ont utilisé ensuite des systèmes d'identification entièrement basés sur les empreintes digitales [6].

### **1.3.Les empreintes digitales, caractéristiques et reconnaissance**

La peau de la paume et des doigts de la main humaine ainsi que la peau de la plante du pied et

des orteils du pied ont la propriété unique d'être ondulées par un motif de crêtes et de vallées étroites (également appelées sillons ou ravins). Les crêtes et les vallées au bout des doigts, connues sous le nom d'empreintes digitales, sont particulièrement intéressantes.

On distingue trois niveaux de structure dans une empreinte digitale. Le premier niveau de structure est le schéma global des crêtes et des vallées. Par exemple, certaines des crêtes de la figure 1 [6] entrent par le bas à gauche de l'image, bouclent autour d'un point central commun et sortent sur la gauche. C'est le modèle global des crêtes d'empreintes digitales, et la plupart des empreintes digitales tombent clairement dans l'une des nombreuses classes de modèles.

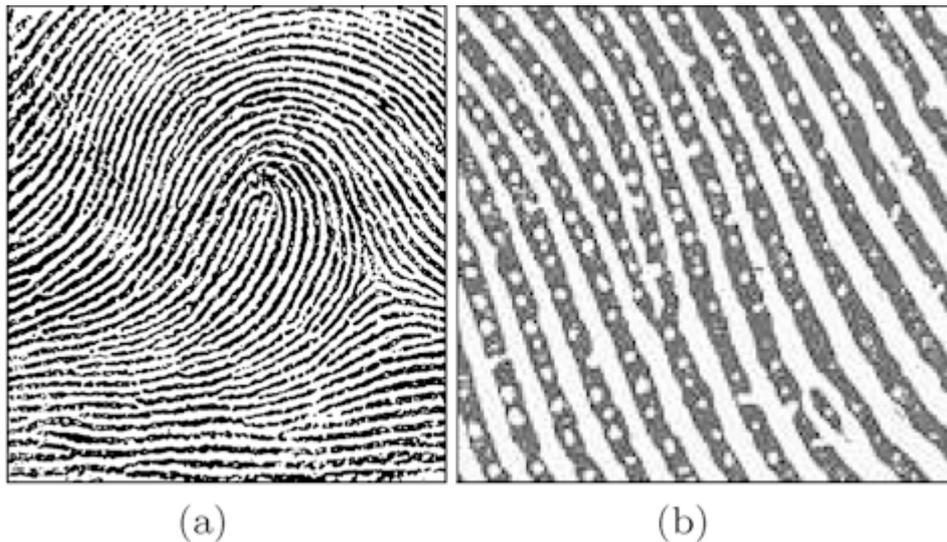


Figure 1: **(a)** Une empreinte digitale ; **(b)** Une vue agrandie des crêtes et des vallées

Le schéma de classification le plus courant est connu sous le nom de classification de Henry et est illustré à la figure 2. La classification de Henry (et d'autres basées sur celle-ci) est connue comme exclusive parce qu'elle divise les empreintes digitales en catégories mutuellement exclusives.

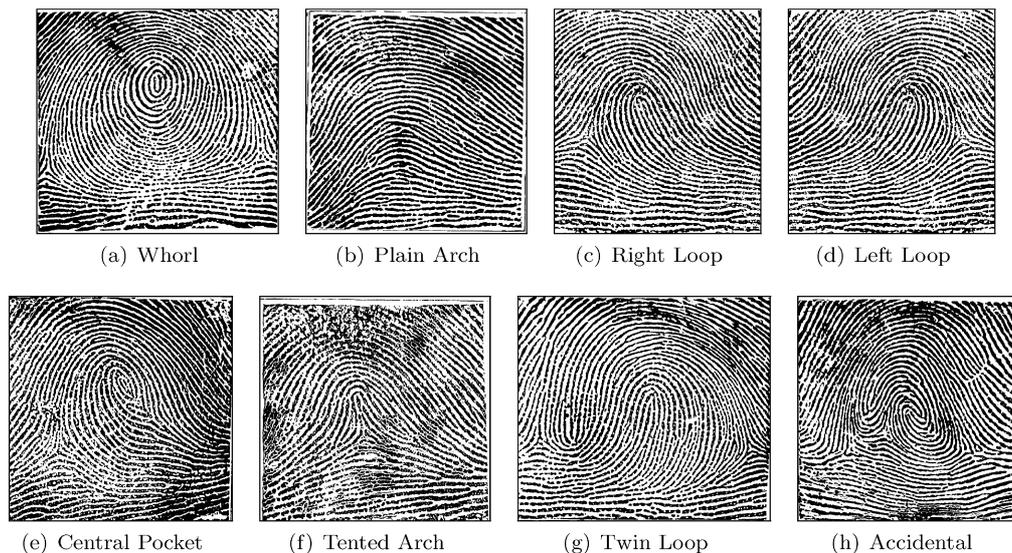


Figure 2: Les classes d'empreintes selon Henry

Une empreinte digitale peut être catégorisée en cinq classes en fonction de son type, à savoir : 1) Arche, 2) Boucle à gauche, 3) Boucle à droite, 4) Tente et 5) Spirale.

Le deuxième niveau de structure se produit dans les régions d'empreintes digitales locales. On peut voir que près du centre de la figure 1.(b), l'une des crêtes se divise en deux crêtes distinctes. On peut également voir que près du coin inférieur droit de l'image, il y a une très courte crête. Ces discontinuités de crête locales, connues sous le nom de minuties, ont peu d'effet sur le modèle global de crêtes-vallées.

Cependant, c'est l'existence et l'emplacement de ces détails (minuties) qui incarnent une grande partie de l'individualité d'une empreinte digitale. Pour cette raison, ils sont la caractéristique discriminante la plus importante et la plus courante utilisée par les experts humains [6].

Il existe deux types de base de minuties : les terminaisons de crête (extrémités des crêtes) et les bifurcations. Les extrémités des crêtes sont des endroits où les crêtes se terminent et les bifurcations sont des endroits où une seule crête se sépare en deux crêtes (figure 3).

Il existe d'autres types de minuties, mais ce sont des combinaisons de terminaisons de crêtes et de bifurcations. Une empreinte digitale typique contient jusqu'à 80 minuties ; cependant, beaucoup moins seront présents dans une empreinte latente ou une empreinte capturée à partir d'un petit scanner.

Le troisième niveau de structure d'empreintes digitales comprend des caractéristiques de bas

niveau telles que les emplacements des pores sudoripares et les formes de crêtes. Ces caractéristiques sont parfois utilisées par des experts humains lors de la comparaison d'impressions. Cependant, ils sont rarement utilisés dans les systèmes automatisés, car ils nécessitent des analyses à très haute résolution pour une extraction fiable des caractéristiques.

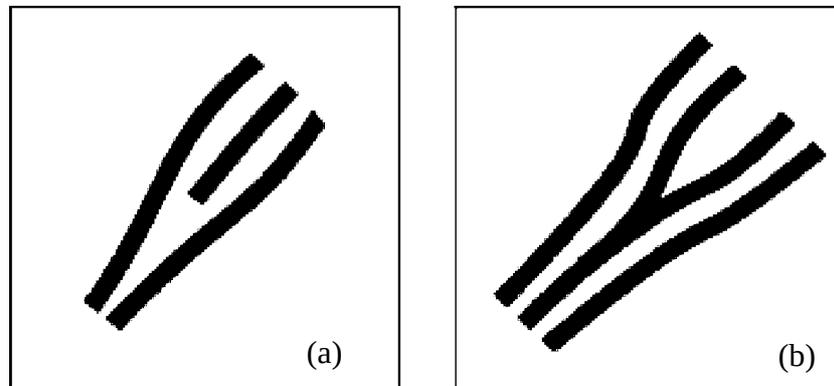


Figure 3: Les types de base des minuties d'une empreinte. **(a)** Terminaison ; **(b)** Bifurcation

Les singularités sont une autre structure importante des empreintes digitales qui ont des propriétés à la fois globales et locales. Globalement, une singularité est une région d'une empreinte digitale où le motif de crête la rend visuellement proéminente. Il existe deux types de singularités : les noyaux et les deltas. Localement, un noyau est le tournant d'une crête la plus intérieure et un delta est un endroit où deux crêtes côte à côte divergent. Les points centraux et delta sont mieux illustrés par des exemples (figure 4).

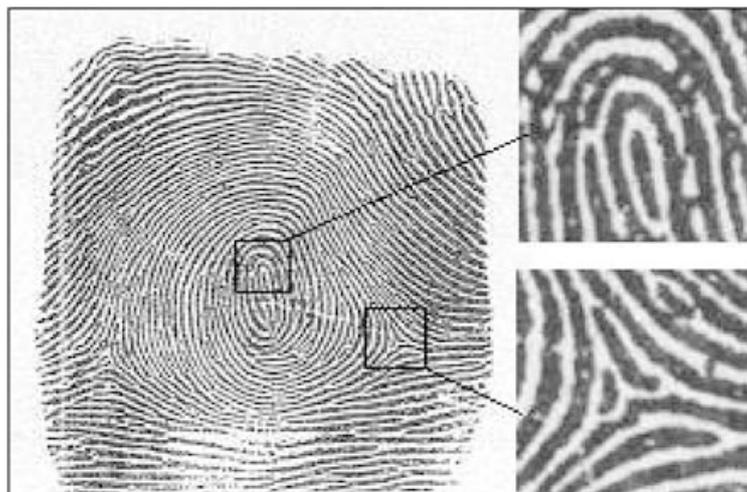


Figure 4: Les types de base des minuties d'une empreinte. **(a)** Terminaison ; **(b)** Bifurcation

Les singularités sont utiles pour déterminer la classe d'une empreinte digitale. Par exemple, les boucles de gauche (comme sur la figure 4) ont un point central près du centre de

l'impression et un point delta en bas à droite. Les singularités ont également d'autres utilisations, telles que l'alignement des empreintes digitales et comme outil de discrimination grossière.

#### **1.4.Reconnaissance des empreintes digitales**

Un système automatique complet de reconnaissance (figure 5) d'empreintes digitales est une chaîne de processus qui à partir du doigt d'un utilisateur en entrée renvoie un résultat en sortie, permettant ainsi à l'utilisateur d'accéder ou non à des éléments nécessitant une protection.

Un système de reconnaissance d'empreintes digitales opère en deux phases ; une phase d'entraînement et une phase de test ; pendant la phase d'entraînement les données biométriques d'un individu client appartenant au système sont stockées dans une base de données. Typiquement, les données biométriques acquises par un lecteur d'empreintes digitales sont traitées par le module d'extraction des paramètres qui seront stockées dans la base de données. Pendant la phase de reconnaissance, les paramètres extraits à partir des empreintes d'une personne de test sont comparés avec ceux stockés par le module d'appariement ou de comparaison. La détermination de l'identité de l'utilisateur se fait par le module de décision.

La phase d'acquisition : La première phase permet d'obtenir une image de l'empreinte de l'utilisateur par l'utilisation de capteur d'empreintes digitales.

La phase d'extraction des paramètres : Une fois qu'une empreinte digitale a été acquise sous forme numérique, un système de reconnaissance doit sélectionner une représentation de stockage appropriée. La quasi-totalité des systèmes utilisent la représentation par les minuties.

La phase d'extraction des paramètres comprend plusieurs phases :

- **Phase de pré-traitement** : une étape très importante d'un système de reconnaissance est l'étape de prétraitement. En effet, de nombreuses caractéristiques discriminantes d'une empreinte digitale sont de minuscules irrégularités de crête qui sont très difficiles à extraire pour des images de faible qualité. Les performances d'un algorithme d'appariement d'empreintes digitales sont étroitement liées à la fiabilité de son étape d'extraction de paramètres. Par conséquent, de nombreuses recherches ont été menées sur le problème du prétraitement des empreintes digitales et de l'amélioration de l'extraction des paramètres. Dans une zone locale, les crêtes et les vallées d'une empreinte digitale ont une fréquence et une orientation bien définies. Par conséquent, il

est naturel d'utiliser des outils d'analyse fréquentielle pour améliorer les informations de crête, tels que les transformées de Fourier [7]–[10], les filtres de Gabor [11]–[13] et les ondelettes [14], [15]. L'estimation du champ d'orientation, la binarisation et l'amincissement ou la squeletisation sont également des étapes de prétraitement courantes et importantes (en particulier pour l'extraction des minuties) [6].

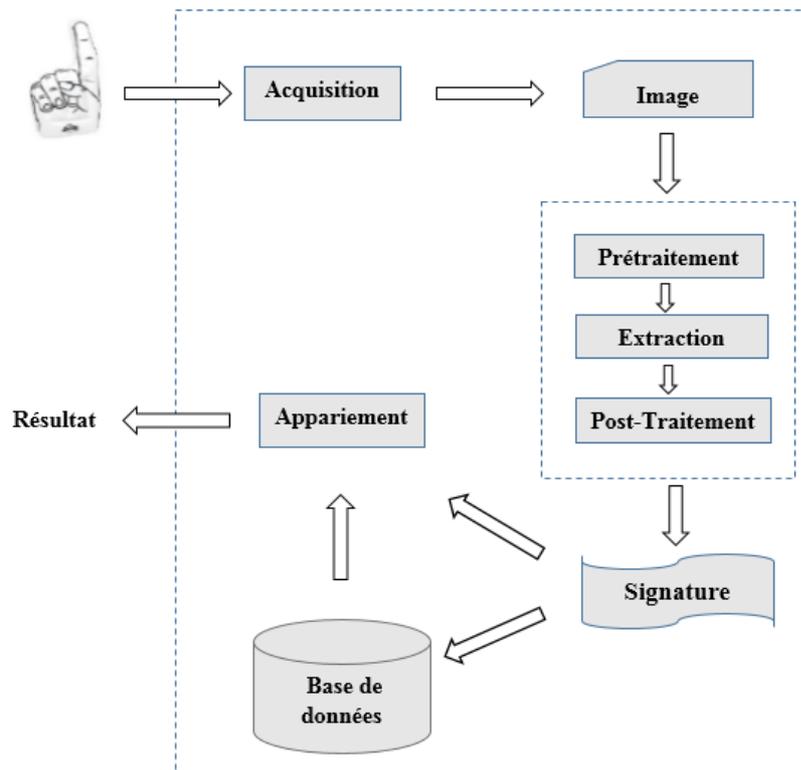


Figure 5: Architecture générale d'un système de reconnaissance d'empreintes [5], [6]

**La phase d'extraction des paramètres:** L'étape d'extraction des paramètres consiste en l'obtention de la signature d'une empreinte digitale et qui correspond à l'information utile nécessaire à l'identification fiable de la personne ou à l'archivage dans la base de données. Elle permet de caractériser de manière unique la personne. La très grande majorité des techniques de reconnaissance sont basées sur la détection locale des minuties et l'extraction de leurs caractéristiques [5].

**La phase d'appariement :** La phase d'appariement est l'étape critique du système, elle reçoit en entrée deux signatures issues de deux acquisitions différentes d'empreinte et renvoie en sortie un résultat binaire indiquant si oui ou non les deux signatures proviennent de la même empreinte. Bien entendu deux empreintes provenant de la même personne ne seront jamais identiques en raison de l'élasticité de la peau, de la présence de poussière, de l'orientation du doigt lors de l'acquisition. La phase d'appariement va donc calculer le degré de similarité (taux d'appariement ou un score) entre les deux signatures et décider si elles peuvent être considérées identiques en fonction d'une valeur seuil ([22]).

#### **1.4.1. Prétraitement de l'empreinte digitale**

Les images d'empreintes digitales sont rarement d'une qualité directement exploitable. Ils peuvent être dégradés et corrompus par des éléments de bruit dus à de nombreux facteurs, notamment les variations de l'état de la peau et de l'impression. Cette dégradation peut entraîner la création d'un nombre important de faux minuties et l'ignorance de minuties authentiques. Une étape critique dans un système de reconnaissance d'empreintes digitales consiste à extraire de manière fiable les détails des images d'empreintes digitales. Ainsi, il est nécessaire d'employer des techniques d'amélioration d'image avant l'extraction des minuties pour obtenir une estimation plus fiable des emplacements des minuties.

D'une manière générale, l'amélioration de l'image des empreintes digitales englobe, mais sans s'y limiter, les étapes telles que l'amélioration du contraste, le calcul de l'orientation des crêtes et l'estimation de leurs fréquences, la segmentation ou la binarisation et le filtrage.

L'organigramme des étapes les plus usuelles d'amélioration des empreintes digitales est illustré à la figure 6. Les principales étapes de l'algorithme comprennent [11] :

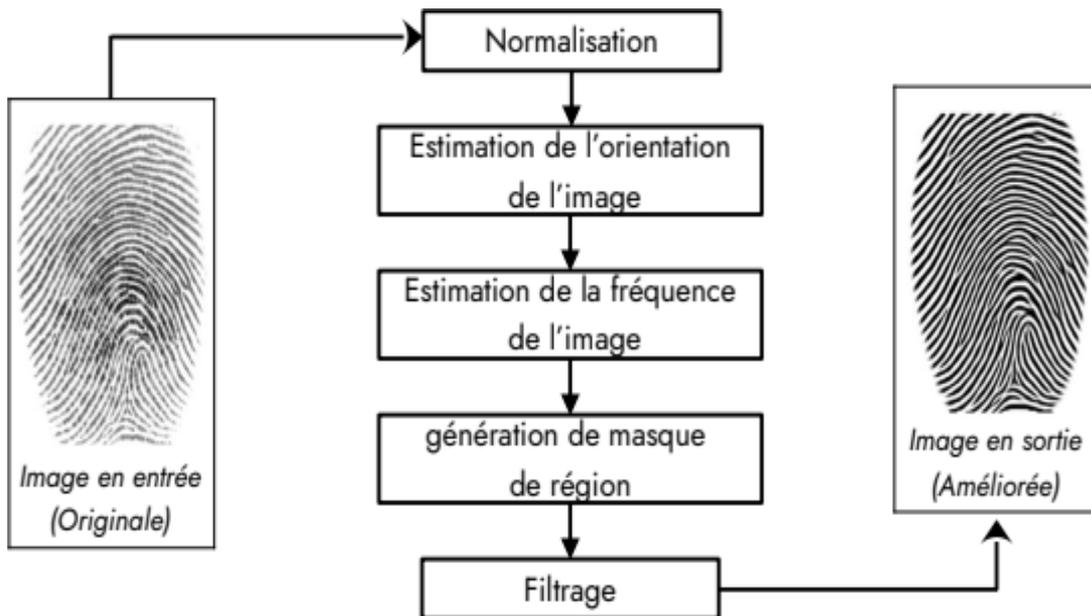


Figure 6 : Organigramme des étapes de l'amélioration de l'image d'empreinte digitale

Une image d'empreinte digitale est généralement une image en niveaux de gris représentée par une matrice  $(\mathfrak{I})$   $N \times N$  éléments, où  $\mathfrak{I}(i, j)$  représente l'intensité du pixel à la  $i^{\text{ème}}$  ligne et à la  $j^{\text{ème}}$  colonne. Les images sont numérisées à une résolution donnée (exemple : 500 points par pouce (dpi)). La moyenne et la variance d'une image d'empreintes digitales en niveaux de gris, sont données par :

$$M(\mathfrak{I}) = \frac{1}{N^2} \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} \mathfrak{I}(i, j)$$

$$\text{VAR}(\mathfrak{I}) = \frac{1}{N^2} \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} (\mathfrak{I}(i, j) - M(\mathfrak{I}))^2$$

1. **Normalisation** : une image d'empreinte digitale d'entrée est normalisée de sorte qu'elle ait une moyenne et une variance prédéfinies.
2. **Estimation de l'orientation locale** : l'image d'orientation est estimée à partir de l'image d'empreinte digitale d'entrée normalisée.
3. **Estimation de fréquence locale** : l'image de fréquence est calculée à partir de l'image d'empreinte digitale d'entrée normalisée et de l'image d'orientation estimée.
4. **Estimation du masque de région** : le masque de région est obtenu en classant chaque bloc dans l'image d'empreinte digitale d'entrée normalisée en un bloc récupérable ou irrécupérable.
5. **Filtrage** : une banque de filtres de Gabor qui est accordée à l'orientation et à la fréquence de crête locales est appliquée aux pixels de crête et de vallée dans l'image

d'empreinte digitale d'entrée normalisée pour obtenir une image d'empreinte digitale améliorée.

#### 1.4.1.1. Normalisation

Soit  $\mathfrak{I}(i, j)$  la valeur de niveau de gris au pixel  $(i, j)$ ,  $M$  et  $VAR$  la moyenne et la variance estimées de  $\mathfrak{I}$  respectivement, et  $G(i, j)$  la valeur de niveau de gris normalisée au pixel  $(i, j)$ . L'image normalisée est définie comme suit :

$$G(i, j) = \begin{cases} M_0 + \sqrt{\frac{VAR_0 \cdot (\mathfrak{I}(i, j) - M)^2}{VAR}} & \text{si } \mathfrak{I}(i, j) > M \\ M_0 - \sqrt{\frac{VAR_0 \cdot (\mathfrak{I}(i, j) - M)^2}{VAR}} & \text{sinon} \end{cases} \quad (1)$$

où  $M_0$  et  $VAR_0$  sont respectivement les valeurs de moyenne et de variance souhaitées. La normalisation est une opération pixel par pixel. Cela ne change pas la clarté des structures de la crête et de la vallée. L'objectif principal de la normalisation est de réduire les variations des valeurs de niveau de gris le long des crêtes et des vallées, ce qui facilite les étapes de traitement ultérieures.

#### 1.4.1.2. Estimation de l'orientation de l'image

L'estimation de l'orientation de l'image d'empreinte dite image d'orientation représente une propriété intrinsèque des images d'empreintes digitales et définit des coordonnées invariantes pour les crêtes et les vallées dans un voisinage local. En considérant une image d'empreinte digitale comme une texture orientée, un certain nombre de méthodes ont été proposées pour estimer le champ d'orientation des images d'empreintes digitales [11]. Nous décrivons ici un algorithme d'estimation de l'orientation basé sur les moindres carrés. Étant donné une image normalisée,  $G$ , les principales étapes de l'algorithme sont les suivantes :

1. Découper  $G$  en bloc de taille  $w \times w$  ( $16 \times 16$ )
2. Calculer les gradients  $\partial_x(i, j)$  et  $\partial_y(i, j)$  à chaque pixel,  $(i, j)$ . L'opérateur de gradient utilisé peut être un simple opérateur de Sobel ou un autre opérateur plus complexe (Marr-Hildreth)
3. Estimer l'orientation locale de chaque bloc centré au pixel  $(i, j)$  en utilisant les équations suivantes [16] :

$$v_x(i, j) = \sum_{u=i-\frac{w}{2}}^{i+\frac{w}{2}} \sum_{v=j-\frac{w}{2}}^{j+\frac{w}{2}} 2\partial_x(u, v)\partial_y(u, v) \quad (2)$$

$$v_y(i, j) = \sum_{u=i-\frac{w}{2}}^{i+\frac{w}{2}} \sum_{v=j-\frac{w}{2}}^{j+\frac{w}{2}} \partial_x^2(u, v)\partial_y^2(u, v) \quad (3)$$

$$\theta(i, j) = \frac{1}{2} \tan^{-1} \left( \frac{v_y(i, j)}{v_x(i, j)} \right) \quad (4)$$

où  $\theta(i, j)$  est l'estimation des moindres carrés de l'orientation locale de la crête au niveau du bloc centré au pixel  $(i, j)$ . Mathématiquement, il représente la direction orthogonale à la direction dominante du spectre de Fourier de la fenêtre  $w \times w$ .

4. En raison de la présence de bruit, de structures de crêtes et de vallées corrompues, de détails, etc. dans l'image d'entrée, l'orientation de crête locale estimée,  $\theta(i, j)$ , peut ne pas toujours être correcte. Étant donné que l'orientation locale de la crête varie lentement dans un voisinage local où aucun point singulier n'apparaît, un filtre passe-bas peut être utilisé pour modifier l'orientation incorrecte. Afin d'effectuer le filtrage passe-bas, l'image d'orientation doit être convertie en un champ vectoriel continu, qui est défini comme suit :

$$\Phi_x(i, j) = \cos(2\theta(i, j)) \quad (5)$$

$$\Phi_y(i, j) = \sin(2\theta(i, j)) \quad (6)$$

où  $\Phi_x$  et  $\Phi_y$  sont respectivement les composantes x et y du champ vectoriel. Avec le champ vectoriel résultant, le filtrage passe-bas peut alors être effectué comme suit :

$$\Phi'_x(i, j) = \sum_{u=-w_\phi/2}^{w_\phi/2} \sum_{v=-w_\phi/2}^{w_\phi/2} W(u, v)\Phi_x(i-uw, j-vw) \quad (7)$$

$$\Phi'_y(i, j) = \sum_{u=-w_\phi/2}^{w_\phi/2} \sum_{v=-w_\phi/2}^{w_\phi/2} W(u, v)\Phi_y(i-uw, j-vw) \quad (8)$$

où  $W$  est un filtre passe-bas bidimensionnel et  $w_\phi \times w_\phi$  spécifie la taille du filtre. La taille par défaut du filtre est  $5 \times 5$ .

5. Calculer l'orientation locale de la crête en  $(i, j)$  en utilisant :

$$O(i, j) = \frac{1}{2} \tan^{-1} \left( \frac{\Phi'_y(i, j)}{\Phi'_x(i, j)} \right) \quad (9)$$

### 1.4.1.3. Estimation de l'image des fréquences locales

Dans un voisinage local où aucune minutie et aucun point singulier n'apparaissent, les niveaux de gris le long des crêtes et des vallées peuvent être modélisés comme une onde de forme sinusoïdale le long d'une direction normale à l'orientation locale de la crête (figure 7). Par conséquent, la fréquence de crête locale est une autre propriété intrinsèque d'une image d'empreinte digitale. Soit  $G$  l'image normalisée et  $O$  l'image d'orientation, alors les étapes impliquées dans l'estimation de la fréquence de la crête locale sont les suivantes :

1. Diviser l'image  $G$  en bloc de taille  $w \times w$  (  $16 \times 16$  ) ;
2. Pour chaque bloc centré au pixel  $(i, j)$  , calculer une fenêtre orientée de taille  $l \times w$  (  $32 \times 16$  ) définie dans le système de coordonnées des crêtes (figure 7). ;

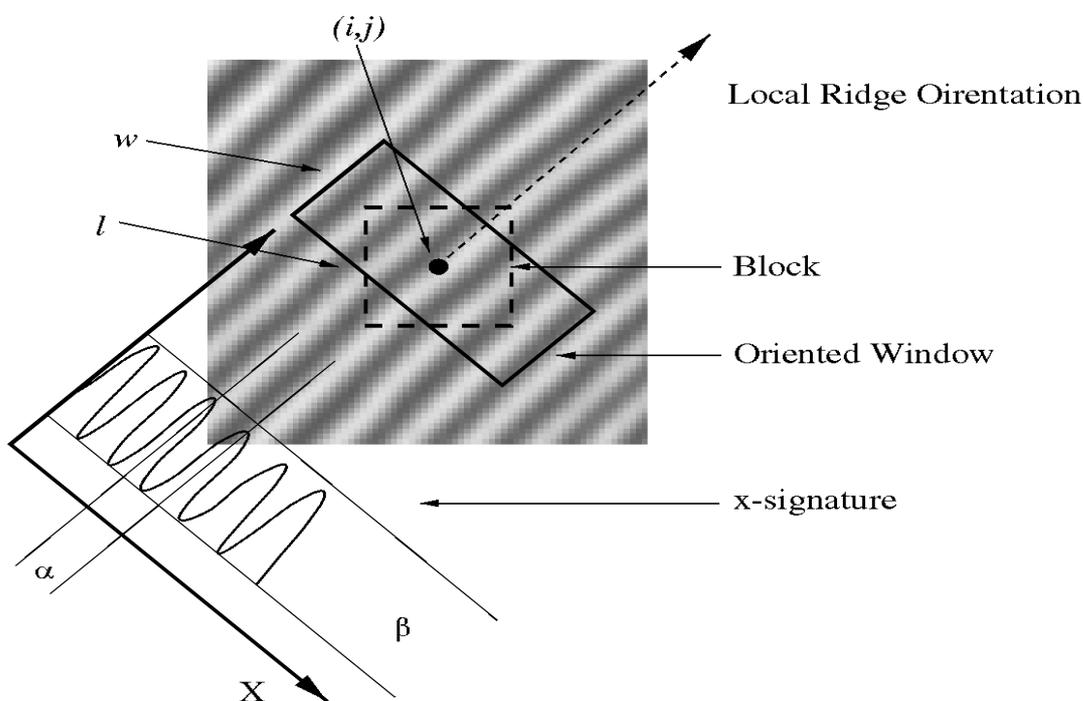


Figure 7 : Fenêtre d'orientation et x-signature

3. Pour chaque bloc centré au pixel  $(i, j)$  , calculer la x-signature,  $X[0], X[1], \dots, X[l-1]$  , des crêtes et vallées à l'intérieur de la fenêtre d'orientation, où

$$X[k] = \frac{1}{w} \sum_{d=0}^{w-1} G(u, v) \quad k=0, 1, \dots, l-1, \quad (10)$$

$$u = i + \left(d - \frac{w}{2}\right) \cos(O(i, j)) + \left(k - \frac{l}{2}\right) \sin(O(i, j)) \quad (11)$$

$$v = j + \left(d - \frac{w}{2}\right) \sin(O(i, j)) + \left(\frac{l}{2} - k\right) \cos(O(i, j)) \quad (12)$$

Si aucune minutie et aucun point singulier n'apparaissent dans la fenêtre orientée, la x-

signature forme une onde de forme sinusoïdale discrète, qui a la même fréquence que celle des crêtes et des vallées dans la fenêtre orientée. Par conséquent, la fréquence des crêtes et des vallées peut être estimée à partir de la x-signature. Soit  $\Gamma(i, j)$  la moyenne du nombre de pixel entre deux pics consécutifs de x-signature, alors, la fréquence  $\Omega(i, j)$  est donnée par :  $\Omega(i, j) = 1/\Gamma(i, j)$ . Dans le cas où des pics consécutifs ne sont pas détectés, alors la fréquence se voit attribuer la valeur  $-1$  pour la différencier d'une valeur valide.

4. Pour une image d'empreinte digitale scannée à une résolution fixe, la valeur de la fréquence des crêtes et des vallées dans un voisinage local se situe dans une certaine plage. Pour une image de 500 dpi (point par pouce ou Dot Per Inch), cette plage est  $[1/3, 1/25]$ . Par conséquent, si la valeur estimée de la fréquence est hors de cette plage, alors la fréquence se voit attribuer une valeur de  $-1$  pour indiquer qu'une fréquence valide ne peut pas être obtenue.

5. Les blocs dans lesquels apparaissent des minuties et/ou des points singuliers et/ou des crêtes et des vallées qui sont corrompus ne forment pas une onde de forme sinusoïdale bien définie. Les valeurs de fréquence de ces blocs doivent être interpolées à partir de la fréquence des blocs voisins. L'interpolation est effectuée comme suit :

a. Pour chaque bloc centré en  $(i, j)$  :

$$\Omega'(i, j) = \begin{cases} \Omega(i, j) & \text{si } \Omega(i, j) \neq -1 \\ \frac{\sum_{u=-w_\Omega/2}^{w_\Omega/2} \sum_{v=-w_\Omega/2}^{w_\Omega/2} W_g(u, v) \mu(\Omega(i-uw, j-vw))}{\sum_{u=-w_\Omega/2}^{w_\Omega/2} \sum_{v=-w_\Omega/2}^{w_\Omega/2} W_g(u, v) \delta(\Omega(i-uw, j-vw)+1)} & \text{sinon} \end{cases} \quad (13)$$

Où

$$\mu(x) = \begin{cases} 0 & \text{si } x \leq 0 \\ x & \text{sinon} \end{cases} \quad (14)$$

$$\delta(x) = \begin{cases} 0 & \text{si } x \leq 0 \\ 1 & \text{sinon} \end{cases} \quad (15)$$

$W_g$  est un noyau gaussien discret avec une moyenne et une variance de zéro et neuf, respectivement, et  $w_\Omega = 7$  est la taille du noyau.

b. S'il existe au moins un bloc avec une valeur de fréquence de  $-1$ , alors échangez  $\Omega$  et  $\Omega'$  et passez à l'étape (a).

6. Les distances entre les crêtes changent lentement dans un voisinage local. Un filtre passe-bas peut être utilisé pour supprimer les valeurs aberrantes dans  $f'$  :

$$F(i, j) = \sum_{u=-w_i/2}^{w_i/2} \sum_{v=-w_i/2}^{w_i/2} W_i(u, v) \Omega'(i-uw, j-vw) \quad (16)$$

où  $W_i$  est un filtre passe-bas bidimensionnel avec un intégrale unitaire et  $w_i=7$  est la taille du filtre.

#### 1.4.1.4. Segmentation de 'l'image ou masque de région utile

Comme mentionné précédemment, un pixel (ou un bloc) dans une image d'empreinte digitale peut se trouver soit dans une région récupérable, soit dans une région irrécupérable. La classification des pixels en catégories récupérables et irrécupérables peut être effectuée sur la base de l'évaluation de la forme de l'onde formée par les crêtes et les vallées locales. Dans le présent algorithme [11], trois caractéristiques sont utilisées pour caractériser l'onde de forme

sinusoïdale : l'amplitude ( $\alpha$ ), la fréquence ( $\beta$ ) et la variance ( $\gamma$ ). Soit  $X[1], X[2], \dots, X[l]$  la x-signature d'un bloc centré en  $(i, j)$ . Les trois paramètres correspondant au pixel (bloc)  $(i, j)$  sont calculées comme suit :

1.  $\alpha$  = (hauteur moyenne des pics – profondeur moyenne des vallées).
2.  $\beta = 1/T(i, j)$ , où  $T(i, j)$  est le nombre moyen de pixels entre deux pics consécutifs.
3.  $\gamma = \frac{1}{l} \sum_{i=1}^l \left( X[i] - \left( \frac{1}{l} \sum_{i=1}^l X[i] \right) \right)^2$

Plusieurs images d'empreintes digitales typiques où les régions récupérables et irrécupérables ont été étiquetées manuellement ont été sélectionnées les trois paramètres ont été calculés pour ces régions. Au total, 2000 motifs tridimensionnels ont été obtenus. Afin de trouver des modèles représentatifs pour les deux classes (récupérable et non récupérable), les 2000 motifs ont été présentés à un algorithme de classification basé sur les moindres carrés qui a identifié six classes. Quatre de ces classes correspondent à des régions récupérables et les deux autres correspondent à des régions irrécupérables. Les six prototypes (correspondant aux six centres des classes) ont été utilisés dans un classificateur de type 1NN ou voisin le plus proche pour classer chaque bloc  $w \times w$  d'une image d'empreinte digitale en entrée en des blocs récupérables ou irrécupérables. Si un bloc centré en  $(i, j)$  est récupérable, alors  $R(i, j)=1$ , sinon  $R(i, j)=0$ . Une fois l'image  $R$  obtenue, le pourcentage des régions récupérables est calculé. Si le pourcentage des régions récupérables est inférieur à un seuil,  $\Gamma_{récupérable} = 40$ , alors l'image d'empreinte digitale d'entrée est rejetée. L'image acceptée est ensuite passée à un filtre [11].

### 1.4.1.5. Filtrage

La configuration des crêtes et des vallées parallèles avec une fréquence et une orientation bien définies dans une image d'empreinte digitale fournissent des informations utiles qui aident à éliminer le bruit indésirable. Les ondes de forme sinusoïdale des crêtes et des vallées varient lentement dans une orientation locale constante. Par conséquent, un filtre passe-bande qui est accordé sur la fréquence et l'orientation correspondantes peut éliminer efficacement le bruit indésirable et préserver les véritables structures de crête et de vallée [11].

Les filtres de Gabor ont à la fois des propriétés sélectives en fréquence et sélectives en orientation et ont une résolution conjointe optimale dans les domaines spatial et fréquentiel [17]. Par conséquent, il convient d'utiliser des filtres de Gabor comme filtres passe-bande pour éliminer le bruit et préserver les véritables structures crête/vallée.

Le filtre de Gabor symétrique a la forme générale :

$$h(x, y: \phi, f) = \exp\left(-\frac{1}{2}\left[\frac{x_\phi^2}{\delta_x^2} + \frac{y_\phi^2}{\delta_y^2}\right]\right) \cos(2\pi f x_\phi) \quad (17)$$

$$x_\phi = x \cos(\phi) + y \sin(\phi) \quad (18)$$

$$y_\phi = -x \sin(\phi) + y \cos(\phi) \quad (19)$$

où  $\phi$  est l'orientation du filtre de Gabor,  $f$  est la fréquence d'une onde plane sinusoïdale, et  $\delta_x$  et  $\delta_y$  sont les constantes d'espace de l'enveloppe gaussienne le long des axes  $x$  et  $y$ , respectivement.

Les propriétés sélectives en fréquence – et orientation – du filtre de Gabor sont plus explicites dans sa représentation dans le domaine fréquentiel. La représentation dans le domaine de Fourier est donnée par :

$$H(u, v: \phi, f) = 2\pi \delta_x \delta_y \exp\left(-\frac{1}{2}\left[\frac{(u_\phi^2 - u_0)^2}{\delta_u^2} + \frac{(v_\phi^2 - v_0)^2}{\delta_v^2}\right]\right) + 2\pi \delta_x \delta_y \exp\left(-\frac{1}{2}\left[\frac{(u_\phi^2 + u_0)^2}{\delta_u^2} + \frac{(v_\phi^2 + v_0)^2}{\delta_v^2}\right]\right) \quad (20)$$

$$u_\phi = u \cos(\phi) + v \sin(\phi) \quad (21)$$

$$v_\phi = -u \sin(\phi) + v \cos(\phi) \quad (22)$$

$$u = \frac{2\pi \cos \phi}{f} \quad (23)$$

$$v = \frac{2\pi \sin \phi}{f} \quad (24)$$

Et  $\delta u = 1/2 \pi \delta x$  et  $\delta v = 1/2 \pi \delta y$

La représentation dans le domaine de Fourier spécifie la quantité par laquelle le filtre modifie ou module chaque composante de fréquence de l'image d'entrée. Ces représentations sont donc appelées fonctions de transfert de modulation ( Modulation Transfer Function, MTF) [17].

Pour appliquer le filtre de Gabor à une image, trois paramètres doivent être spécifiés :

1. la fréquence de l'onde plane sinusoïdale,  $f$  ;
2. l'orientation du filtre ;
3. les écarts-types de l'enveloppe gaussienne,  $\delta_x$  et  $\delta_y$  .

Il est évident que la fréquence du filtre,  $f$  , est complètement déterminée par la fréquence de crête locale et l'orientation est déterminée par l'orientation de crête locale. La sélection des valeurs de  $\delta_x$  et  $\delta_y$  implique un compromis. Plus les valeurs sont élevées, plus les filtres sont robustes au bruit, mais plus on risque de créer des crêtes et des vallées parasites, et vice versa.

Soient  $G$  l'image d'empreintes digitales normalisées,  $O$  l'image d'orientation,  $F$  l'image des fréquences et  $R$  le masque des régions récupérables, l'image améliorée  $E$  s'obtient comme suit :

$$E(i, j) = \begin{cases} 255 & \text{si } R(i, j) = 0 \\ \sum_{u=-w_g/2}^{w_g/2} \sum_{v=-w_g/2}^{w_g/2} h(u, v; O(i, j), F(i, j)) G(i-u, j-v) & \text{sinon} \end{cases} \quad (25)$$

Où  $w_g = 11$  correspond à la taille du filtre de Gabor.

#### 1.4.2. Extraction des paramètres (minuties)

La plupart des algorithmes de vérification d'empreintes digitales s'appuient dans une certaine mesure sur des informations de minuties, et ces algorithmes ne peuvent être aussi robustes que les informations de minuties sous-jacentes. Par conséquent, une extraction fiable des minuties est vitale pour les performances d'un tel système. Il existe deux approches principales pour l'extraction des minuties. La première approche utilise une squelette de l'image de la structure de crête binaire, connue sous le nom de squelette. La deuxième approche tente d'extraire les emplacements des détails de l'image en niveaux de gris elle-même.

Certains systèmes d'identification automatique des empreintes (Automated Fingerprint Identification System AFIS) incluent une étape de post-traitement pour confirmer que des

minuties valides ont été extraites, et c'est ce qu'on appelle la vérification des minuties.

La méthode la plus répandue consiste à extraire les minuties à partir d'un squelette de l'image. Comme le montre la figure, l'image est d'abord préparée à l'étape d'extraction au moyen d'une binarisation et d'une squelettisation, ensuite un fichier signature est extrait de l'empreinte après la détection et l'extraction des minuties [5].



Figure 8: La phase d'extraction de la signature.

#### 1.4.2.1. La binarisation de l'image

La binarisation, également connue sous le nom de seuillage binaire, transforme une image après ajustement de contraste en une image composée uniquement de pixels ayant la valeur 0 ou 1, en utilisant un seuil spécifique. Cette étape revêt une grande importance dans le processus de squelettisation de l'image.

Afin de réaliser ce traitement, chaque pixel  $E(i, j)$  est comparé à un seuil donné, et s'il est supérieur à ce seuil, le pixel est assigné la valeur 1 (noir), sinon, il est attribué la valeur 0 (blanc) (Figure 9, Figure 10).



Figure 9: Processus de binarisation, image originale

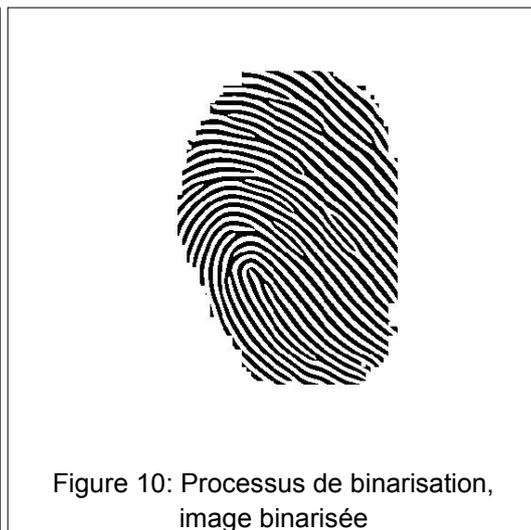


Figure 10: Processus de binarisation, image binarisée

#### 1.4.2.2. La squelettisation de l'image

La squelettisation d'une image d'empreinte digitale est une étape cruciale dans le processus de reconnaissance des empreintes. Cette technique vise à extraire le motif central et

caractéristique de l'empreinte digitale, ce que l'on appelle le squelette.

Pour parvenir à la squelettisation, plusieurs méthodes et algorithmes ont été développés au fil des années. L'une des approches courantes consiste à suivre les crêtes de l'empreinte digitale et à réduire progressivement leur largeur jusqu'à ce qu'elles deviennent des lignes d'une seule unité de pixel. Ce processus permet de représenter de manière compacte les informations cruciales tout en éliminant les variations mineures qui pourraient affecter la précision de la comparaison d'empreintes digitales.

La squelettisation est généralement réalisée en appliquant des opérations morphologiques, telles que l'érosion, la dilatation et la minceur, pour extraire les caractéristiques squelettiques de l'image. Ce processus peut être suivi d'étapes de post-traitement pour éliminer les artefacts indésirables et améliorer la qualité de la représentation squelettique.

La plupart des techniques utilisent des algorithmes d'amincissement itératif, ou plus précisément, des algorithmes qui suppriment successivement des couches de pixels sur la limite du motif jusqu'à ce qu'il ne reste plus qu'un squelette. La suppression ou la conservation d'un pixel (noir)  $p$  dépendrait de la configuration des pixels dans un voisinage local contenant  $p$ . Selon la manière dont ils examinent les pixels, ces algorithmes peuvent être classés comme séquentiels ou parallèles. Dans un algorithme séquentiel, les pixels sont examinés pour la suppression dans une séquence fixe à chaque itération, et la suppression de  $p$  dans la  $n$ -ième itération dépend de toutes les opérations qui ont été effectuées jusqu'à présent, c'est-à-dire du résultat de la  $(n-1)$ -ème itération ainsi que des pixels déjà traités dans la  $n$ -ième itération. En revanche, dans un algorithme parallèle, la suppression des pixels dans la  $n$ -ième itération dépendrait uniquement du résultat qui subsiste après la  $(n-1)$ -ème ; par conséquent, tous les pixels peuvent être examinés indépendamment de manière parallèle à chaque itération.

Cette étape n'est pas essentielle dans notre travail, nous avons utilisé un programme disponible [18].

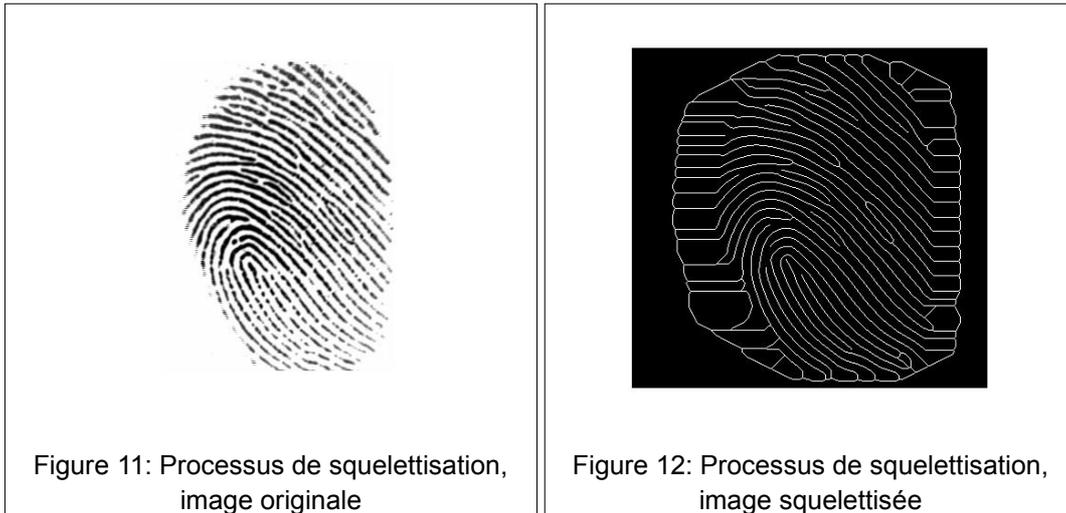


Figure 11: Processus de squelettisation, image originale

Figure 12: Processus de squelettisation, image squelettisée

### 1.4.2.3. Détection des minuties

La détection de ces minuties permet de créer une représentation abstraite de l'empreinte digitale, ce qui facilite sa comparaison et son identification.

Pour détecter les minuties, un algorithme analyse l'image de l'empreinte digitale pixel par pixel, en recherchant des motifs de crêtes qui se divisent (bifurcations) ou se terminent (terminaisons). Lorsque de tels motifs sont identifiés, ils sont enregistrés en tant que minuties. Cette étape de détection est souvent suivie d'une étape de post-traitement visant à éliminer les fausses minuties ou à combler les gaps entre les minuties détectées, pour obtenir une représentation plus fiable.

Les minuties ainsi détectées sont ensuite utilisées pour créer une « carte » des minuties, également appelée « carte minutieuse », qui contient des informations sur l'emplacement, l'orientation et les types de minuties dans l'empreinte digitale. Cette carte est ensuite comparée à d'autres empreintes digitales pour effectuer des vérifications d'identité ou des recherches dans des bases de données d'empreintes digitales.

Les deux étapes de préparation pour l'extraction, à savoir la binarisation et la squelettisation, ont grandement simplifié cette phase. En effet, nous disposons après ces deux étapes de préparation d'une image binaire squelettisée où un pixel noir est représenté par la valeur 1 et un pixel blanc par la valeur 0, avec une largeur de stries égale à 1 pixel. En calculant le nombre de transitions divisé par 2 entre un pixel blanc et un pixel noir pour chaque point du squelette, nous obtenons le nombre  $CN$  (Crossing Number) de stries partant de ce point. Cela nous permet de déterminer le type d'un pixel.

pour chaque pixel  $P$  appartenant à une strie (c'est-à-dire pour chaque pixel ayant une valeur

de 1) le calcul de  $CN$  est basé sur le voisinage comme indiqué sur la Figure 13 .

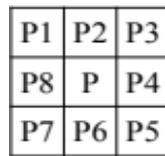


Figure 13: Numérotation des pixels pour le calcul de CN

Le calcul de CN est donné par :

$$CN(P) = \frac{1}{2} \sum_{i=1}^8 |P_i - P_{i-1}| \quad \text{et} \quad P_0 = P_8, \quad P_i \in \{0,1\}$$

Chaque point terminaison ou bifurcation est détecté par la méthode de voisinage ; si le nombre de voisinage autour d'un pixel est égal à zéro, il s'agit d'un pixel isolé.

Par exemple, Si  $CN(P)=1$  : dans ce cas nous avons à faire à une minutie de type terminaison (Figure 14).

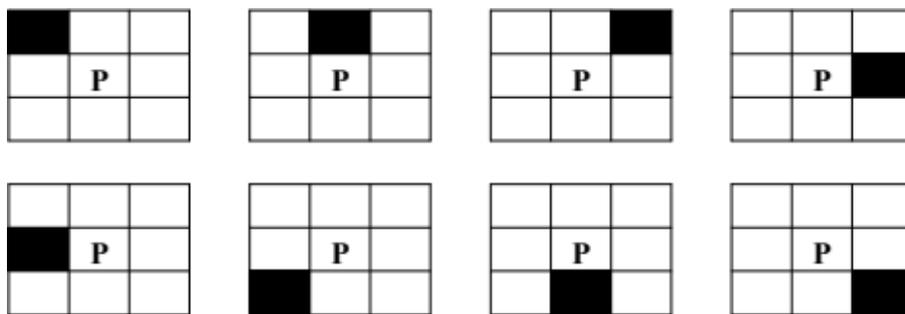


Figure 14: Les cas des points de type terminaison (CN=1)

Le cas de  $CN=3$  indique la présence d'une bifurcation triple (Figure 15).

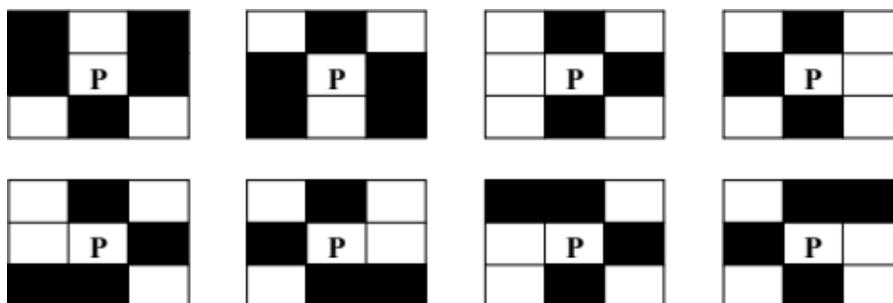


Figure 15: Les cas des points de type bifurcation (CN=3)

Malgré les avantages qu'offre l'utilisation du nombre  $CN$  pour faciliter la détection, elle engendre également la détection d'un grand nombre de minuties supplémentaires (généralement quelques centaines), principalement introduites lors des étapes de binarisation

et de squelettisation. Par conséquent, l'extraction directe de la signature n'est pas possible, ce qui rend impératif d'appliquer un traitement supplémentaire visant à éliminer le plus grand nombre possible de fausses minuties [5].

#### **1.4.2.4. Élimination des fausses minuties**

Le but de ce processus est de maximiser l'élimination des fausses minuties tout en préservant les minuties authentiques qui ont été détectées. Cela s'accomplit en se basant sur des observations empiriques qui reposent sur le principe que la distance entre deux minuties voisines est généralement supérieure à un seuil déterminé. En pratique, il est très rare de trouver deux vraies minuties très proches l'une de l'autre, alors que l'on constate presque toujours une concentration locale de plusieurs fausses minuties [5].

Parmi les méthodes courantes pour l'élimination des fausses minuties, on peut citer :

**Filtrage spatial** : Supprimer les minuties trop proches les unes des autres, car elles pourraient représenter le même point.

**Analyse de la courbure** : Éliminer les minuties qui ne suivent pas les modèles de courbure typiques des empreintes digitales humaines.

Il est important de noter que la précision de l'algorithme d'élimination des fausses minuties est cruciale pour garantir la fiabilité de la vérification d'empreintes digitales. Une mauvaise suppression de minuties peut entraîner des erreurs de vérification, tandis qu'une élimination excessive de minuties peut réduire la capacité de discrimination de l'empreinte digitale. Par conséquent, l'optimisation de cet algorithme est essentielle dans les systèmes de reconnaissance d'empreintes digitales.

#### **1.4.3. Le fichier signatures**

Le fichier signature correspond à l'information utile minimum contenue dans l'image qui est nécessaire à l'identification. Pour chaque minutie valide, le fichier contiendra les informations :

**Coordonnées des minuties** : Les positions (x, y) des minuties détectées dans l'empreinte digitale.

**Orientation des minuties** : L'angle ou la direction de chaque minutie (le bloc qui contient la minutie).

**Type de minuties** : bifurcation ou terminaison.

#### **1.4.4. Phase de Comparaison ou d'appariement**

La phase de comparaison ou d'appariement est une étape critique d'un système de reconnaissance des empreintes digitales. La phase d'appariement a pour tâche de mesurer le degré de similarité, c'est-à-dire le taux d'appariement, entre les deux signatures.

## Chapitre 2

# Prétraitement de l'image d'empreinte : partie pratique



## 2. Prétraitement de l'image d'empreinte : partie pratique

---

### 2.1.Introduction

Dans ce chapitre, nous allons présenter les résultats des algorithmes de prétraitement de l'image d'empreinte digitale développés au cours de ce travail.

### 2.2.Normalisation

La Figure 16 présente l'image de l'empreinte originale en niveau de gris et l'image après normalisation

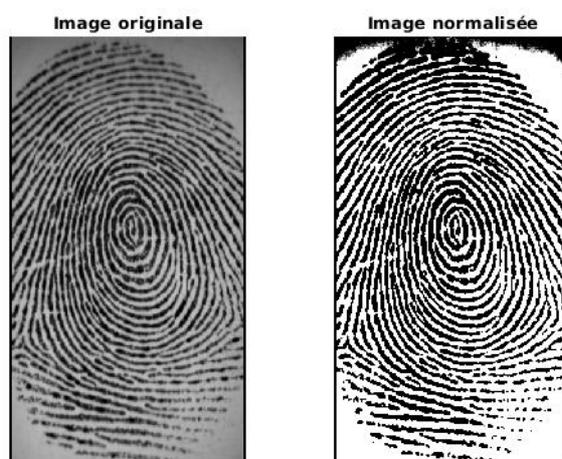


Figure 16: Résultat de la normalisation de l'image d'empreinte

### 2.3.Calcul de l'image de l'orientation

L'image d'orientation de l'image d'empreinte digitale est utilisée dans la partie de filtrage locale par filtre de Gabor. Elle est calculée en divisant l'image globale en blocs et appliquer l'algorithme discuté dans la partie théorique. La Figure 17 présente l'image de l'empreinte originale en niveau de gris et l'image de l'orientation calculée.

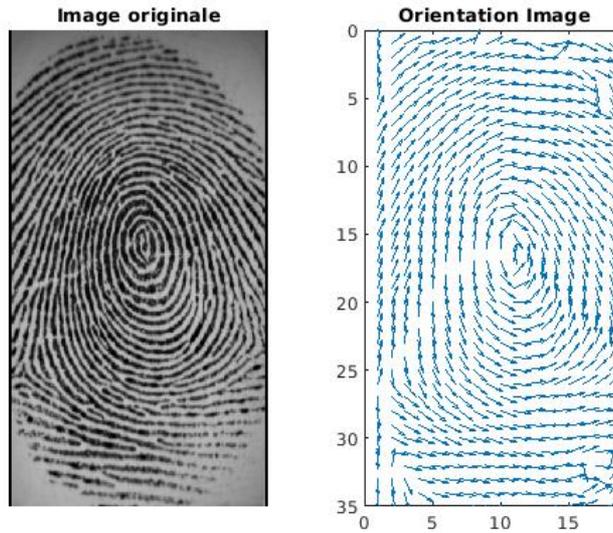


Figure 17: Calcul de l'image d'orientation de l'image d'empreinte

Pour montrer les détails du calcul de l'orientation, la Figure 18 présente comment l'algorithme calcule l'orientation dans chaque bloc. Les lignes rouges montrent l'orientation de chaque bloc dessinés au dessus de l'image originale en niveau de gris. L'image 19 présente un agrandissement (zoom) sur une partie de la figure.

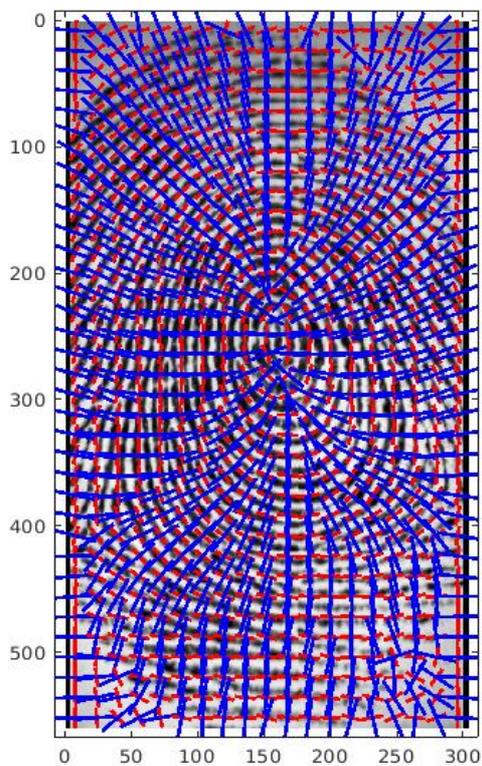


Figure 18: Détails du calcul de l'orientation de l'image d'empreinte

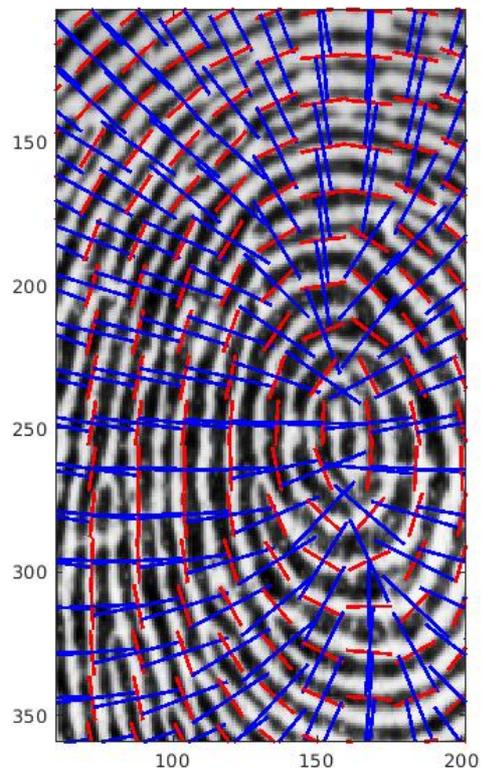


Figure 19: Agrandissement (zoom) sur l'image d'orientation

## 2.4. Calcul de l'image des fréquences

Cette étape consiste à calculer pour chaque bloc de l'image d'empreinte la fréquence de l'onde sinusoïdale représentant la forme des crêtes et vallées dans cette zone le long de la verticale à l'orientation locale.

Cette carte fréquentielle est utilisée dans la phase de filtrage vu que le filtre de Gabor est un filtre qui utilise des paramètres d'orientation et de phase ou de fréquence.

La Figure 20 représente la carte fréquentielle cote à cote avec l'image d'empreinte originale en niveaux de gris.

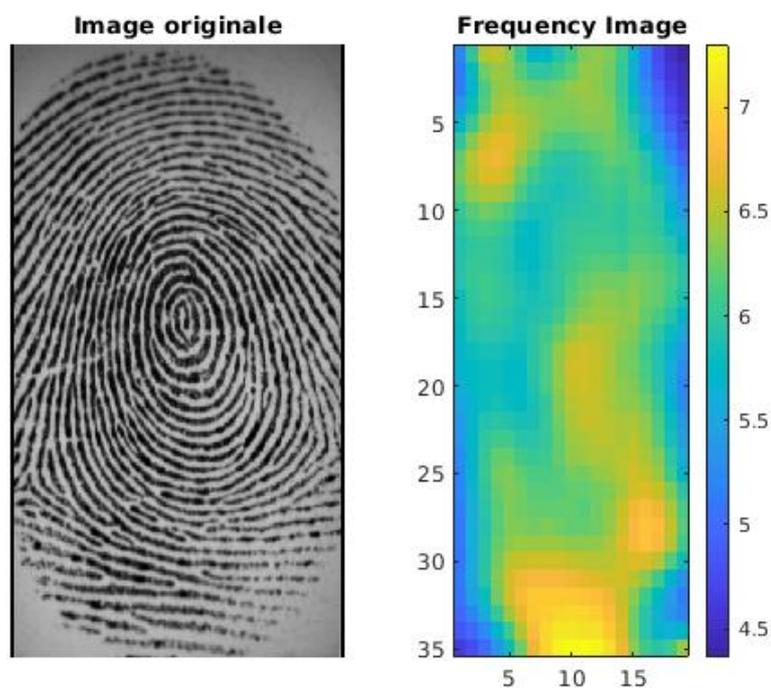


Figure 20: Image fréquentielle cote à cote avec l'image originale en niveaux de gris

## 2.5. Calcul du masque de l'image

Le calcul de masque de l'image consiste à étiqueter les pixels (en fait les bloc de pixels contenant le pixel en cours de traitement) en pixel de l'image ou non. L'algorithme décrit dans la partie théorique [11] n'a pas été implémenté ici. Par contre, nous avons utilisé deux algorithmes ; le premier est basé sur le calcul de la variance locale. Si la variance d'un bloc est supérieur à un seuil prédéfini, alors le bloc est marqué appartenant à l'image d'empreinte, sinon, il est marqué comme appartenant à l'arrière plan de l'image d'empreinte. Le deuxième algorithme est basé sur le calcul de l'énergie des blocs de l'image d'empreinte après un traitement par FFT [19].

La Figure 21 présente le masque calculé par les deux algorithmes cités, la partie utile de l'image est en blanc et la partie arrière plan est en noir.

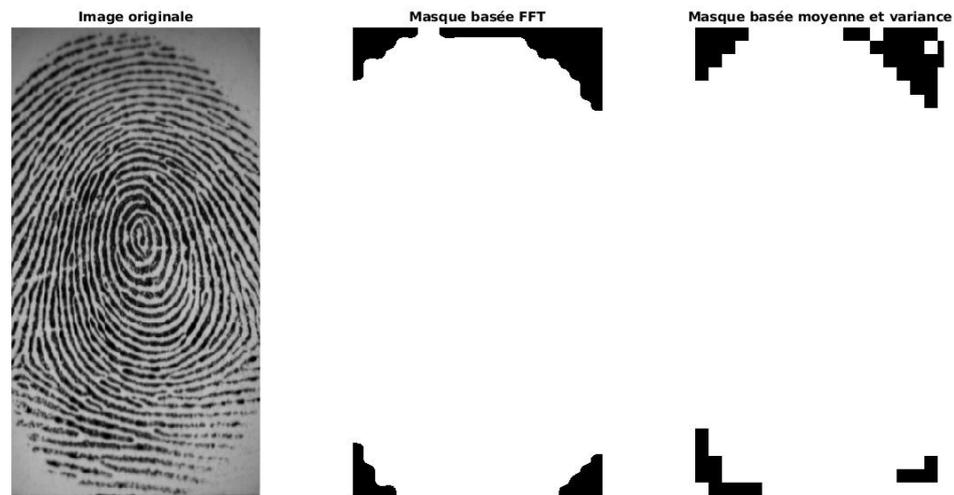


Figure 21: Calcul du masque de région utile de l'empreinte digitale

## 2.6. Filtrage de Gabor appliqué à l'image d'empreinte

L'étape finale de la phase de prétraitement de l'image d'empreinte digitale est le filtrage de Gabor. Il s'agit d'un filtre passe bande qui peut être accordé sur une fréquence et une orientation en plus d'un certain nombre de paramètres. Ces caractéristiques permet de conserver la structure des crêtes et vallées de l'empreinte et d'éliminer le bruit.

La Figure 22 montre le résultat de l'application du filtre de Gabor sur l'image d'empreinte après calcul de l'image d'orientations et de fréquences qui sont passées comme paramètres au filtre.

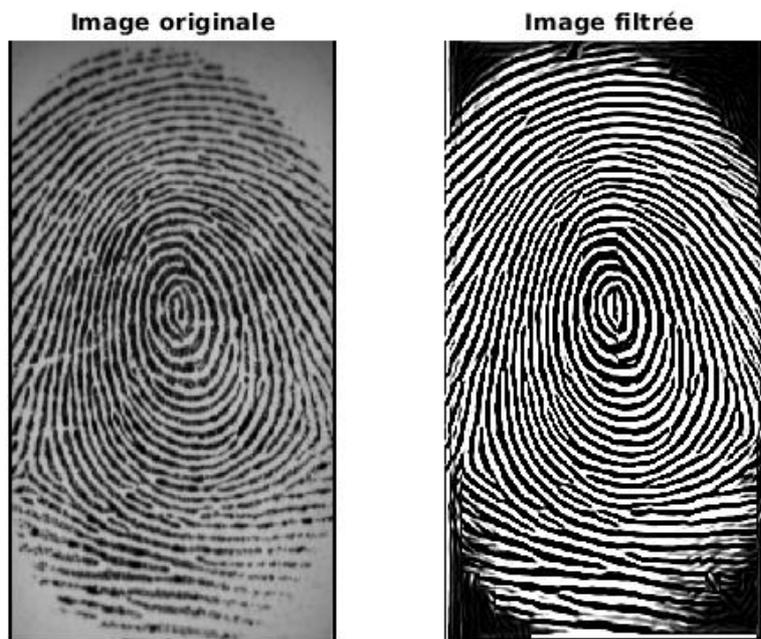


Figure 22: Résultat de l'application du filtre de Gabor sur l'image d'empreinte

## 2.7.Conclusion

Dans ce chapitre, nous avons présenté les résultats des différents algorithmes de prétraitement de l'image d'empreintes digitales depuis l'acquisition de l'image en niveaux de gris jusqu'à l'étape de filtrage. En effet, l'image d'empreinte digitale en niveaux de gris subit plusieurs traitements, à savoir la normalisation, le calcul de l'image d'orientation, le calcul de l'image des fréquences. Finalement, on utilise ces deux résultats pour effectuer le filtrage de Gabor qui permet une amélioration substantielle tant au niveau de bruit qu'au niveau de la clarté de la structure des vallées et crêtes.

Il est clair qu'il existe plusieurs techniques de prétraitement de l'image d'empreinte digitale qui diffèrent sur le but recherché ; à savoir la vitesse de traitement et les résultats obtenues.

Dans notre cas, nous avons travaillé sur la validation des algorithmes présentés dans le travail de Hong [11].

## **Conclusion Générale**

---

Dans ce travail, nous avons cherché à implémenter les algorithmes de prétraitement de l'image d'empreinte digitale. Il est nécessaire de préciser qu'il existe plusieurs techniques différentes tant sur la complexité des calculs que sur l'objectif final.

Les algorithmes développés dans ce travail sont issus principalement du travail de Hong [11], cependant dans le cas de calcul du masque d'image, nous avons utilisé d'autres algorithmes vu le rapport qualité/simplicité qu'ils présentent.

Pour chaque étape de prétraitement, nous avons donné le résultat sous forme de figure avec la figure originale côte à côte pour montrer l'effet du prétraitement.

Nous pensons que les algorithmes développés dans ce travail présentent des résultats satisfaisant en comparaison à d'autre plus complexes.

Comme perspective, nous pouvons envisager l'ajout des mesures de qualité à chaque étape pour comparer les différents algorithmes.

## Références bibliographiques

---

- [1] A. K. Jain, A. Ross, et S. Prabhakar, « An introduction to biometric recognition », *IEEE Trans. Circuits Syst. Video Technol.*, vol. 14, n° 1, p. 4-20, 2004, doi: 10.1109/TCSVT.2003.818349.
- [2] J. Wayman, « Fundamentals of Biometric Authentication Technologies. », *Int J Image Graph.*, vol. 1, p. 93-113, janv. 2001, doi: 10.1142/S0219467801000086.
- [3] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, et A. K. Jain, « FVC2002: Second Fingerprint Verification Competition », in *2002 International Conference on Pattern Recognition*, 2002, p. 811-814 vol.3. doi: 10.1109/ICPR.2002.1048144.
- [4] D. R. V. Bharathi, G. P. Jain, G. Hariharan, P. D. Ramkumar, et S. K. Sahoo, « Gabor filter design for fingerprint application using matlab and verilog HDL », *Int. J. Eng. Technol.*, vol. 5, n° 2, p. 1386-1391, 2013.
- [5] N. Galy, « Etude d'un système complet de reconnaissance d'empreintes digitales pour un capteur microsystème à balayage », Theses, Institut National Polytechnique de Grenoble - INPG, 2005. [En ligne]. Disponible sur: <https://theses.hal.science/tel-00009742>
- [6] N. Yager et A. Amin, « Fingerprint verification based on minutiae features: a review », *Pattern Anal. Appl.*, vol. 7, n° 1, p. 94-113, avr. 2004, doi: 10.1007/s10044-003-0201-2.
- [7] B. G. Sherlock, D. M. Monro, et K. Millard, « Fingerprint enhancement by directional Fourier filtering », *IEE Proc. - Vis. Image Signal Process.*, vol. 141, n° 2, p. 87-94(7), avr. 1994.
- [8] T. Kamei et M. Mizoguchi, « Image filter design for fingerprint enhancement », in *Proceedings of International Symposium on Computer Vision - ISCV*, 1995, p. 109-114. doi: 10.1109/ISCV.1995.476986.
- [9] P. J. Grottier, « PCASYS-a pattern-level classification automation system for fingerprints », 2017.
- [10] A. J. Willis et L. Myers, « A cost-effective fingerprint recognition system for use with low-quality prints and damaged fingertips », *Pattern Recognit.*, vol. 34, n° 2, p. 255-270, 2001, doi: [https://doi.org/10.1016/S0031-3203\(00\)00003-0](https://doi.org/10.1016/S0031-3203(00)00003-0).
- [11] L. Hong, Y. Wan, et A. Jain, « Fingerprint image enhancement: algorithm and performance evaluation », *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 20, n° 8, p. 777-789, 1998, doi: 10.1109/34.709565.
- [12] E. Saatci et V. Tavsanoğlu, « Fingerprint image enhancement using CNN Gabor-Type filters », in *Proceedings of the 2002 7th IEEE International Workshop on Cellular Neural Networks and Their Applications*, 2002, p. 377-382. doi: 10.1109/CNNA.2002.1035073.
- [13] B.-G. Kim, H.-J. Kim, et D.-J. Park, « New enhancement algorithm for fingerprint images », in *2002 International Conference on Pattern Recognition*, 2002, p. 879-882 vol.3. doi: 10.1109/ICPR.2002.1048169.
- [14] W.-P. Zhang, Q.-R. Wang, et Y. Y. Tang, « A wavelet-based method for fingerprint image enhancement », in *Proceedings. International Conference on Machine Learning and Cybernetics*, 2002, p. 1973-1977 vol.4. doi: 10.1109/ICMLC.2002.1175382.
- [15] C.-T. Hsieh, E. Lai, et Y.-C. Wang, « An effective algorithm for fingerprint image enhancement based on wavelet transform », *Pattern Recognit.*, vol. 36, n° 2, p. 303-312, 2003, doi: [https://doi.org/10.1016/S0031-3203\(02\)00032-8](https://doi.org/10.1016/S0031-3203(02)00032-8).
- [16] A. R. Rao, *A Taxonomy for Texture Description and Identification*. in Springer Series in Perception Engineering. New York, NY: Springer US, 1990. doi: 10.1007/978-1-4613-9777-9.

- [17] A. K. Jain et F. Farrokhnia, « Unsupervised texture segmentation using Gabor filters », *Pattern Recognit.*, vol. 24, n° 12, p. 1167-1186, 1991, doi: [https://doi.org/10.1016/0031-3203\(91\)90143-S](https://doi.org/10.1016/0031-3203(91)90143-S).
- [18] V. K. Alilou, « FingerPrint Matching: A simple approach », 3 septembre 2023. <https://fr.mathworks.com/matlabcentral/fileexchange/44369-fingerprint-matching-a-simple-approach> (consulté le 3 septembre 2023).
- [19] S. Chikkerur, V. Govindaraju, et A. Cartwright, *Fingerprint Image Enhancement Using STFT Analysis*, vol. 3687. 2005, p. 29. doi: 10.1007/11552499\_3.

## Amélioration de l'image des empreintes digitales en vue de leur reconnaissance

---

**Résumé :** Le présent mémoire présente l'étude et l'implémentation de quelques algorithmes de prétraitement de l'image d'empreinte digitale. Les algorithmes de prétraitements ont pour objectif l'amélioration de l'image d'empreinte en réduisant le bruit et à rendre les caractéristiques de l'empreinte digitale plus distinctes pour faciliter leur analyse et leur correspondance (appariement). Nous avons implémenté les algorithmes présentés par Hong [11]. Les résultats obtenus montrent un rapport qualité/complexité excellent par rapport à d'autres algorithmes plus complexes. Les programmes sont développés sous Matlab et les résultats sont présentés sous forme de figures.

---

Mots-clés : Amélioration image empreinte, filtre de Gabor, prétraitement de l'image d'empreinte, image d'orientation, masque d'image d'empreinte

---

### Enhancement of fingerprint image for their recognition

---

**Abstract :** This works presents the study and implementation of several fingerprint image preprocessing algorithms. Preprocessing algorithms aim to improve the fingerprint image by reducing noise and enhancing the distinctiveness of fingerprint features to facilitate their analysis and matching. We implemented the algorithms presented by Hong [11]. The results obtained demonstrate an excellent quality-to-complexity ratio compared to other more complex algorithms. The programs are developed in Matlab, and the results are presented in the form of figures.

---

Keywords : Fingerprint image enhancement, Gabor filter, Fingerprint image preprocessing, Orientation image, Fingerprint image mask.

---

### تحسين صورة بصمات الأصابع للتعرف عليها

---

**ملخص :** تقدم هذه الأطروحة دراسة وتنفيذ بعض خوارزميات المعالجة المسبقة لصور بصمات الأصابع. تهدف خوارزميات المعالجة المسبقة إلى تحسين صورة بصمة الإصبع عن طريق تقليل الضوضاء وجعل خصائص بصمة الإصبع أكثر تميزاً لتسهيل تحليلها ومطابقتها. قمنا بتنفيذ الخوارزميات التي قدمها هونغ [11]. تظهر النتائج التي تم الحصول عليها نسبة جودة/تعقيد ممتازة مقارنة بالخوارزميات الأخرى الأكثر تعقيداً. يتم تطوير البرامج في برنامج MATLAB وتعرض النتائج كأشكال.

---

كلمات مفتاح : تحسين صورة بصمة الإصبع، مرشح جابور، المعالجة المسبقة لصورة بصمة الإصبع، صورة الاتجاه، قناع صورة بصمة الإصبع.