
Université de Caen Département d'informatique

# Analyse et classification des empreintes digitales

Analyse et reconnaissance d'empreintes digitales

21 mars 2009

*Auteur :*
Jean-Nicolas des Pommare

*Encadrant :*
Youssef Chahir

# Table des matières

# Chapitre 1

# La reconnaissance d'empreintes digitales


De tous temps, les hommes ont cherché à mettre en place des moyens fiables pour s'assurer de l'identité des personnes avec lesquelles elles intéragissent. Ce besoin, qu'il soit justifié ou non, est aujourd'hui au centre de notre société. Que ce soit pour passer un examen, aller à un recrutement ou garder des enfants, il faut toujours pouvoir justifier de son identité, et donc avoir une confiance totale avec les outils que l'on utilise pour la vérifier.

Longtemps, le meilleur moyen de s'assurer que la personne que l'on a en face de soi est bien la bonne resta le partage d'un secret seulement connu des deux interlocuteurs ou d'un groupe sûr (comme l'utilisation d'un mot de passe par exemple). Une grande partie des méthodes mises au point depuis l'antiquité jusqu'à aujourd'hui a utilisé ce procédé. Au temps des romains, il y avait par exemple le chiffrement de César qui consistait en un simple décalage des lettres de l'alphabet. Pour comprendre les messages ainsi chiffrés, il fallait alors connaître le secret, c'est-à-dire savoir de combien décaler l'alphabet pour retrouver le message d'origine. Plus récemment, on peut citer l'exemple des machines à rotors, comme Enigma[1], qui permettait de chiffrer et déchiffrer les transmissions des allemands pendant la seconde guerre mondiale. Sans une telle machine (ici la clé qu'il convient de garder secrète et qui montre que l'on est bien une personne habilitée à lire le message), tout déchiffrage se révélait alors impossible. Cette façon de procéder reste aujourd'hui encore très présente dans nos vies, en particulier sur internet : pour pouvoir s'identifier sur un site, c'est-à-dire prouver que nous sommes bien la personne que nous prétendons être, il suffit souvent de rentrer un simple login (identifiant de compte/connexion) et un mot

[1] inventée par un ingénieur allemand du nom de Arthur Scherbius

de passe, qui n'est censé être connu que de nous et du site en question. Login et mot de passe qui transitent souvent en clair sur internet et qui peuvent donc se retrouver entre les mains de n'importe qui...

Le problème majeur de l'identification par secrets est la pérennité dudit secret. Les quelques méthodes citées, et les nombreuses autres inventées au fil du temps, ont toutes été percées plus ou moins facilement. Si les méthodes d'authenfication par clés privées/publiques sont aujourd'hui considérées comme sûres, il n'en reste pas moins qu'elles sont basées sur la préservation d'un secret et sur l'espoir que les clés privées ne seront jamais récupérées/trouvées. Si cet espoir est fondé pour des personnes qui ont des connaissances en informatique et qui savent sécuriser leurs communications, toute personne n'est pas à même d'empêcher des intrusions sur une machine, principalement parce qu'elle n'a aucune connaissance sur les éventuels risques.

Alphonse Bertillon[2] était un célèbre criminologue français qui fonda en 1870 le premier laboratoire de police scientifique pour l'identification de criminels. Pour se faire, il inventa l'anthropométrie judiciaire, technique qui consiste à mesurer les particularités dimensionnelles d'un homme, appliquée ici aux criminels pour avoir un meilleur moyen de les caractériser, les traits du visage seuls étant trop vagues pour authentifier formellement une personne. Ce système fut rapidement adopté dans tout l'Europe et se répendit même jusqu'aux Etats-Unis. D'où l'idée naissante de non plus identifier une personne par un secret, mais par des caractéristiques physiques qui lui sont propres. Aujourd'hui, on regroupe ces techniques sous la dénomination de *Biométrie*.

## 1.1 La biométrie

### 1.1.1 Qu'est-ce que la biométrie ?

Le mot *Biométrie* peut revêtir plusieurs significations. Il désigne généralement l'étude quantitative des êtres humains. Ce terme trouve ses origines dans le grec ancien : il est composé de *bios*, qui signifie *vie*, et *metron*, la *mesure*. Lorsqu'il sera fait mention de biométrie dans la suite de ce rapport, le terme sera utilisé dans un sens plus restrictif : la biométrie est une science portant sur l'identification des personnes en fonction de caractéristiques biologiques qui leurs sont propres. Plus précisément, il s'agit de l'étude de méthodes pour la reconnaissance d'être humains basée sur un ou plusieurs aspects physiques ou comportementaux uniques à l'individu.

Il existe deux principaux types d'analyses biométriques : l'analyse morphologique et l'analyse comportementale. L'analyse morphologique regroupe principalement l'étude des empreintes digitales, de l'iris, des veines, de la morphologie de la main ou encore du poids. Pour l'analyse comportementale, on trouve principalement la dynamique de la frappe sur le clavier ou la signature d'une personne. D'autres types d'analyse rentrent à la fois dans ces deux catégories, telle l'analyse de la voix, en partie caractérisée par les cordes vocales, mais également avec le ton donné et l'accent, et d'autres encore qui ne rentrent pas dans

[2] 24 avril 1853 - 13 février 1914

ces catégories, comme l'analyse de l'A.D.N..

Aujourd'hui, un système biométrique efficace est un système qui se doit d'utiliser plusieurs de ces techniques. D'abord parce que plus les mécanismes de sécurité sont nombreux et variés, plus il devient difficile de les contrefaire ou de les abuser. Mais également parce que les différentes techniques développées ne permettent pas nécessairement d'identifier à coup sûr une personne (la corpulence de deux personnes peut être très proche) ou parce qu'elles sont trop lourdes à gérer lorsqu'elles sont appliquées à de nombreuses personnes. On préférera par exemple l'utilisation d'un badge qui possède l'identifiant d'une personne pour vérifier la concordance de son iris avec l'empreinte présente dans une base de données plutôt que de devoir parcourir toute une base de donnée afin de vérifier si l'iris scanné est habilité ou non à faire une action.

Les contrôles biométriques sont d'ores et déjà d'actualité, et pas que dans des zones à accès restreints de grandes entreprises. Les nouveaux passeports qui nous sont délivrés contiennent de nombreuses données biométriques portant sur l'identification de la personne qui le possède, d'où leur nom de "passeport biométrique". Ainsi, l'allemagne fait équiper progressivement ses postes aux frontières de scanners pour visages empreintes digitales[3]. Ces scanners pourront comparer les données qu'ils relèveront avec les données présentes dans le passeport biométrique pour s'assurer de l'authenticité de la personne.

### 1.1.2 Le marché de la biométrie

Le marché de la biométrie est loin d'être marginal, il connaît d'ailleurs un engouement sans précédent (dû à l'arrivée d'un certain nombre de technologies à maturité). Les principaux marchés porteurs de la sécurité sont bien évidemment Internet et le commerce électronique, mais d'autres domaines arrivent avec des besoins réels. On peut par exemple citer le télétravail et la mise à disposition de données aux clients et fournisseurs. Là où il y a un risque pour les entreprises concernant l'accès à leurs systèmes d'informations, il existe un marché possible pour la biométrie.

L'arrivée massive des capteurs d'empreintes digitales, des logiciels de reconnaissance de visage pour l'authentification de session, la sécurisation de terminaux mobiles ou encore les contrôles aux cantines ne sont que quelques exemples des besoins nouveaux en matière de sécurité qui viennent s'ajouter aux marchés déjà existant tels que l'accès aux zones sensibles et aux salles d'informatique, aux systèmes pour l'ouverture de coffres-forts avec serrures électroniques, ou encore aux fichiers judiciaires. Une enquête publiée par Toshiba montra que 90% des cadres dirigeants et chefs d'entreprises européens stockent des données sensibles ou même confidentielles sur leurs outils de communication. Parmis ces 90%, 22% admettent avoir déjà perdu l'un de ces outils...

On peut constater avec le graphique présenté ci-dessous que le marché de la biométrie subit une croissante constante et conséquente ces dernières années. Il

[3]Bettina Reichmuth, "L'identification biométrique", ARTE Magazine,14 juin 07. Lien vers l'article

est aujourd'hui estimé à près de 4 milliards de dollars et croît d'1,5 milliards de dollars tous les ans. A lui seul, le secteur de la finance en représenterait le tiers. Enfin, les programmes d'envergure de la part des gourvernements et d'entreprises privées risquent de doper encore un peu plus ce marché déjà porteur.

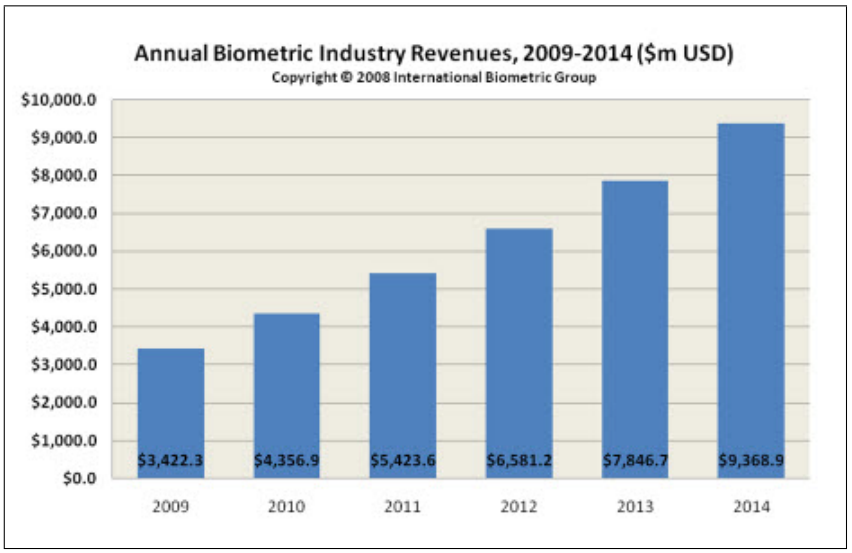



FIG. 1.1: Croissance estimée du marché de la biométrie en millards de dollars (étude réalisée par l'International Biometric Group)

Le grand gagnant de la biométrie est d'abord la reconnaissance d'empreintes digitales qui à elle seule représente près de 50% du marché.

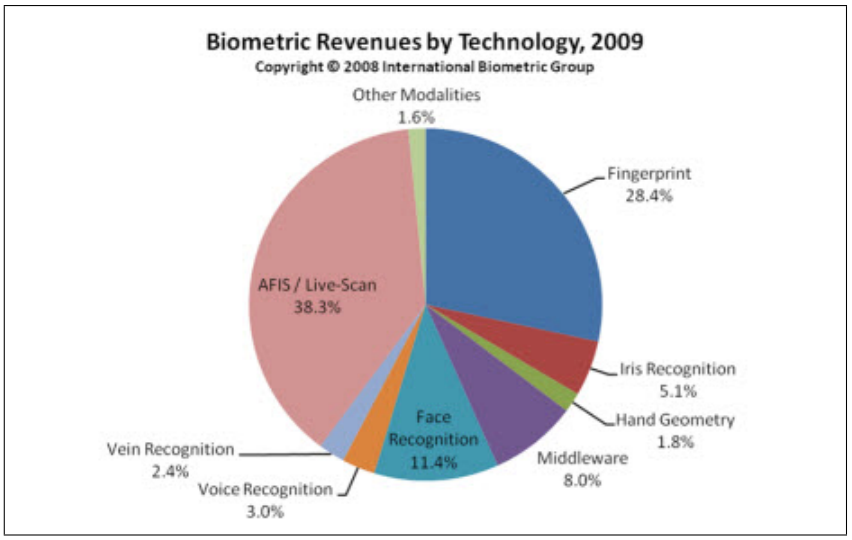



FIG. 1.2: Parts des technologies utilisées dans le secteur de la biométrie estimé par l'International Biometric Group

## 1.2 Empreintes digitales

### 1.2.1 Formation des empreintes

Les empreintes digitales sont composées d'un ensemble de crêtes discontinues. Elles se forment aux alentours de la treizième semaine de grossesse. De nombreux facteurs vont façonner ces crêtes, tel que la vitesse de croissance des doigts, l'alimentation du foetus ou encore la pression sanguine. C'est ce processus qui rend chaque empreinte unique. Même de vrais jumeaux auront des empreintes différentes, bien qu'il sera plus difficile de les distinguer.

L'intérêt pratique de ces crêtes est double :

- Elles permettent une meilleure accroche des doigts sur des objets pour pouvoir mieux les saisir.
- Elles amplifient les vibrations ressenties lorsque le doigt touche une surface irrégulière en envoyant plus de signaux aux terminaisons nerveuses impliquées dans la perception de la texture.

### 1.2.2 Utilisation des empreintes digitales

L'utilisation des empreintes ne date pas d'hier : il y a 5000 ans, on en retrouve déjà la trace sur des tablettes d'argile. Elles servaient alors de signature. Plus tard, les dignitaires chinois se mirent à déposer une trace de leur empreinte sur des sceaux en terre pour les documents officiels. Dès le physicen Rashid-al-Din Hamadani (1247-1318), on savait déjà que "L'expérience montre que pas deux individus ont des doigts exactement identiques". C'est en 1823 que Jan Evangelista Purkinje (1787-1869), physiologiste tchèque, publia le premier une thèse dans laquelle il étudiait neuf types différents d'empreintes digitales. Le docteur Henry Faulds (1843-1930), en 1880, discutait déjà de l'utilité des empreintes pour l'identification des personnes. Il proposait même une nouvelle méthode avec de l'encre d'imprimerie pour les enregistrer. Il fallut attendre Francis Galton (1822-1911) qui étudia pendant dix ans les empreintes digitales avant de publier un livre sobrement appelé *Fingerprints* dans lequel il établit l'unicité et la permanence des empreintes digitales. Il calcula ainsi qu'il y avait une chance sur 64 milliards que deux individus aient la même empreinte.

En 1891 fut mis en place le premier fichier d'empreintes en Argentine par Juan Vucetich, un dirigeant de la police qui fut également le premier à identifier un criminel à l'aide de ses empreintes en 1892. Plus près de nous, le fichier du FBI comportait en 1999 les empreintes de quelques 33 millions de criminels, et le fichier français en comportait 900 000 en 1998.

Aujourd'hui, les empreintes digitales sont principalement utilisées dans la police criminelle et la sécurité.

### 1.2.3 Intérêts de l'empreinte digitale

Les empreintes digitales ont des caractéristiques qui les rendent intéressantes à utiliser pour l'identification des individus. En voici un résumé :

- *Universalité* : Plus de 96% de la population mondiale en possède, ce qui permet d'avoir un moyen de caractérisation important pour tous les humains, indépendamment de leur origine.
- *Uniques* : Chaque personne a une empreinte qui lui est propre (voir section précédente concernant les recherches de Francis Galton).
- *Persistantes* : Les coupures et autres blessures au niveau du doigt n'altèrent pas l'empreinte (il faudrait brûler le doigt en profondeur pour cela).
- *Performantes* : Les traitements appliquables pour comparer deux empreintes ne sont pas trop lourds et peuvent être effectués dans des temps raisonnables.
- *Acquisition transparente* : L'acquisition n'est ni invasive (pas de piqûre), ni contraingnante pour l'utilisateur (juste le doigt à appliquer sur un capteur).

Deux types d'empreintes digitales peuvent être analysées :

- Les empreintes directes, qui laissent une marque visible, et qui sont utilisées principalement pour la sécurité.
- Les empreintes latentes, provoquées par la sueur, la saleté et autres résidus, qui elles sont laissées involontairement. Elles servent surtout pour confondre les criminels.

Devant l'intérêt croissant que portent les entreprises à la biométrie, en particulier vis-à-vis des technologies utilisant les empreintes digitales, l'augmentation des revenus de cette technologie et les propriétés intéressantes que l'empreinte digitale développe, il m'a semblé pertinant de travailler sur un sujet de projet d'année portant sur l'analyse et la comparaison d'empreintes digitales.

## 1.3 Principe de la reconnaissance d'empreintes digitales

Pour comprendre les procédés mis en place dans l'analyse et la reconnaissance d'empreintes digitales, il est utile de décomposer le travail à réaliser en trois parties :

On peut distinguer trois étapes essentielles à la comparaison d'empreintes digitales :

- *Le prétraitement*, qui consiste à améliorer la qualité d'une image donnée en entrée pour extraire le maximum de caractéristiques utiles de l'image exploitables en vue d'une future comparaison, tout en supprimant les erreurs induites avec les imprécisions du capteurs ou les défauts de l'empreinte.
- *L'extraction de caractéristiques*, qui utilise l'image améliorée et qui en ressort ses principales caractéristiques.

– *La Comparaison*, qui confronte les caractéristiques de deux empreintes pour déterminer si elles appartiennent ou non à la même personne. L'objectif à atteindre est de minimiser à la fois les faux positifs (deux empreintes de personnes différentes qui sont reconnues comme appartenant à une seule et même personne) et les faux négatifs (deux empreintes d'une même personne qui sont déterminées comme étant deux empreintes différentes)

Les trois chapitres suivant expliqueront dans le détail ces étapes de l'analyse et de la comparaison d'empreintes digitales, les choix techniques opérés et le développement de solutions pour tenter de répondre à ce problème.

# Chapitre 2

# Amélioration de l'image

Bien que les outils qui permettent la capture d'empreintes digitales soient en constante évolution, il arrive fréquemment qu'une image ne soit pas exploitable à la sortie d'un scanner. Or, la performance des algorithmes qui tentent d'extraire les caractéristiques propres à une empreinte digitale pour les comparer à celles d'autres empreintes dépend fortement de la qualité de l'image en entrée. Pour un système qui vise la sécurité de zones ou de données sensibles, on peut se permettre d'allouer des budgets conséquents dans l'achat de capteurs onéreux qui garantissent une grande précision dans l'acquisition de l'empreinte. Mais pour les systèmes les plus communs, et donc les plus économiques, il faut pallier les imprécisions du capteur par des traitements parfois lourds pour garantir une image d'une précision suffisante avec laquelle il sera possible de travailler.

Un second problème majeur intervient lors de l'acquisition de l'empreinte, indépendamment du capteur, ce qui le rend d'autant plus difficile à corriger. Bien que nous gardons nos empreintes durant toute notre vie, elles évoluent au fil des jours. L'un des principaux facteurs de changement concerne l'épiderme : selon le temps, l'humeur ou encore la fatigue, les pores sont plus ou moins apparents, les mains moites ou sèches, des coupures peuvent avoir été provoquées par des objets,...Qui plus est, la façon d'appuyer son doigt sur le capteur peut faire varier de beaucoup l'acquisition, en écrasant les crêtes. La position du doigt peut varier. Il faut encore ajouter qu'en fonction des ethnies, comme la population asiatique, la finesse de l'empreinte digitale varie suffisamment pour pouvoir poser problème, tout comme pour les enfants.

Les techniques usuelles d'amélioration d'image (en particulier les filtres linéaires) ne permettent pas de pouvoir préserver efficacement les contours et les courbes dans une image. C'est pourquoi il a fallu employer un autre type de filtrage : le filtrage contextuel qui préserve à la fois la courbure des crêtes de l'empreinte digitale tout en reconstruisant l'empreinte en comblant les microcoupures dûes à l'imprécision du capteur ou à une coupure sur l'empreinte elle-même.

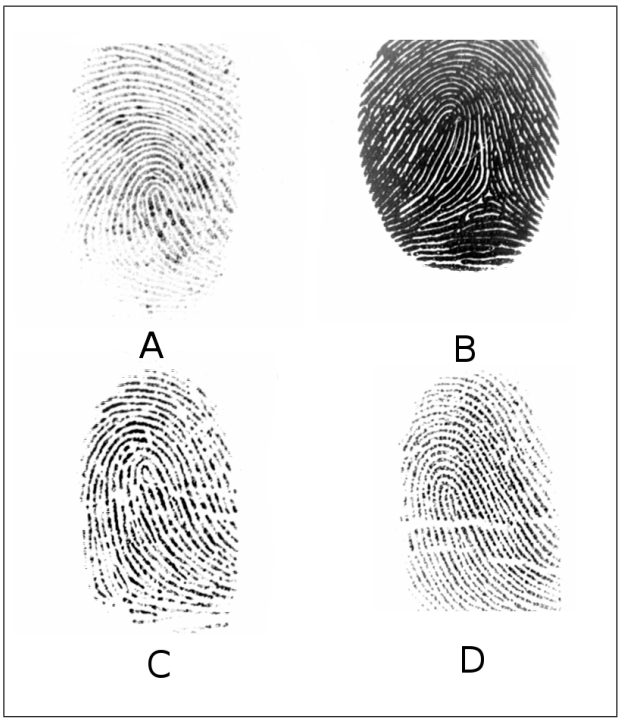



FIG. 2.1: Exemples d'acquisitions de mauvaise qualité : A) Contraste trop faible ; B) Empreinte trop humide ; C) Empreinte trop sèche D) Coupures dans l'empreinte

FIG. 2.2: Acquisitions d'une même empreinte avec un capteur "V300" de la société CrossMatch. On peut constater des différences flagrantes qui peuvent nous faire hésiter quant à la similitude entre ces empreintes.

## 2.1 Un point sur la capture de l'empreinte

Il est loin d'être facile de capturer une empreinte : en effet, la surface à capturer est de très faible dimension comparée au contenu de l'information qu'elle transporte. Le choix d'un capteur se fait donc en fonction de la population qu'il aura à analyser mais aussi des besoins de sécurité qu'il devra respecter.

Schématiquement, le travail du capteur consiste à trouver les lignes tracées par les crêtes de l'empreinte qui se trouvent en contact avec le capteur et les vallées qui ne le touchent pas. Il existe trois principaux types de capteurs :

- Capteur *Optique* : Il s'agit plus ou moins d'une caméra digitale. On applique le doigt sur une platine en plastique dur ou en quartz éclairée par une del et la caméra prend une photo. Ce type de capteur résiste bien aux fluctuations de températures mais est gêné par la luminosité ambiante et reste assez volumineux. Il est privilégié pour son coût assez faible et permet d'avoir des images assez nettes et précises ;

- Capteur *Silicium* : Il utilise l'un des quatre effets observables sur les semiconducteurs : l'effet piezo-électrique, l'effet capacitif, l'effet thermo-électrique ou l'effet photo-électrique. Sa taille et son coût sont assez réduits et il possède une durée de vide importante. Par contre, il est fragile aux décharges électrostatiques. Exemple de capteur silicium : les capteurs thermiques ;

- Capteur *Ultra Sonique* : La capture est possible grâce à l'envoi d'ultra sons dirigés très précisément vers des zones de l'empreinte. Le capteur calcul alors le temps que met l'onde pour faire un aller-retour. L'image est générée point par point. Ce capteur est très précis. De plus, il possède des avantages propres aux ultra-sons, c'est-à-dire que les ondes peuvent traverser certains matériaux comme le latex (utile pour éviter l'usurpation d'une identité en falsifiant les empreintes) ou la saleté qui peut gêner la bonne capture de l'empreinte. Ce type de capteur est par contre très onéreux et volumineux. Il conviendra plutôt à une population hétérogène.

N'oublions pas l'encre qui a été pendant très longtemps la seule solution pour relever les empreintes. Cette méthode est aujourd'hui assez obsolète de par l'obligation d'avoir un matériel adéquat pour les relever et du fait qu'il faille ensuite acquérir l'empreinte relévée avec un scanner, d'où une redondance dans les manipulations.

## 2.2 Technologies employées

L'étape de traitement d'image est une étape qui demande de nombreux calculs. J'ai donc opté pour une technologie C++. Puisqu'il s'agissait principalement de traitement d'image, le projet s'est vite orienté vers l'utilisation de la librairie open-source Pandore[1] développée au sein du Greyc[2], ce qui a permis d'éviter de redévelopper tout une série d'opérateurs de traitement d'image.

[1] Lien vers la librairie
[2] Groupe de Recherche en Informatique, Image, Automatique et Instrumentation de Caen

De plus, et bien que ce projet soit d'abord un projet visant une recherche de solution pour le problème posé et non pas une application finalisée, il a fallu fixer des contraintes quant à la durée des étapes de l'analyse et de la comparaison d'empreintes. C'est pourquoi j'ai décidé d'adopter les mêmes contraintes que pour la FVC2004[3], c'est-à-dire un temps maximal d'amélioration d'image de dix secondes et un temps de comparaison entre images maximal de cinq secondes.

## 2.3 Approche retenue pour l'amélioration de l'empreinte

Pendant les deux premiers mois, tout en travaillant avec la librairie Pandore sur la partie segmentation d'image, mon travail a principalement consisté à faire une recherche sur l'état de l'art en matière de reconnaissance d'empreintes digitales, et plus particulièrement dans les traitements visant à améliorer une image provenant de l'acquisition d'une empreinte. N'ayant que peu de temps pour travailler sur l'ensemble du projet, il n'était pas possible d'entreprendre une réflexion poussée sur une nouvelle méthode de traitement d'image. Il a donc fallu rechercher des techniques ayant déjà fait leurs preuves dans le domaine de l'amélioration d'empreintes et qui étaient réalisables dans le laps de temps donné pour le projet. Les deux points importants que nous voulions pouvoir trouver Monsieur Chahir et moi dans l'algorithme d'amélioration d'image résidaient dans l'utilisation d'une approche qui utiliserait à la fois l'orientation de l'empreinte (ici prise comme une texture) et la fréquence des crêtes dans l'image. Après de longues recherches, je me suis donc orienté vers un algorithme développé par une équipe de la *Michigan State University*[4].

## 2.4 Etapes de l'amélioration

Chaque étape de l'amélioration sera discutée et détaillée dans les parties suivantes, ce qui permettra de comprendre l'intérêt de tels traitements et l'application qu'il en a été faite dans le projet. En voici un résumé schématique :

Dans la suite de cette partie, j'utiliserai la même image témoin d'empreinte digitale tout au long des différents processus liés à l'amélioration d'une empreinte digitale afin de mieux percevoir les traitements qui y sont associés.

### 2.4.1 Segmentation et recadrage de l'image

La segmentation et le recadrage de l'empreinte représentent les premiers traitements à effectuer pour ne garder que la partie intéressante de l'image, c'est-à-dire l'empreinte en elle-même, et donc enlever le fond de l'image qui est tout autant bruité que pauvre en informations.

Pour mettre en place une telle méthode de segmentation, j'ai eu l'occasion de réfléchir à cette problématique durant un certain temps. La suite de cette

[3] La FVC (Fingerprint Verification Competition) est une compétition qui a lieu tous les deux ans et qui regroupe les grands industriels et les universités qui travaillent dans le domaine de l'analyse d'empreintes digitales Lien vers la FVC2004

[4] Pour plus de détails sur la publication, "*Fingerprint Image Enhancement : Algorithm and Performance Evaluation*" Lien vers la publication de Lin Hong, Yifei Wan et Anil Jain

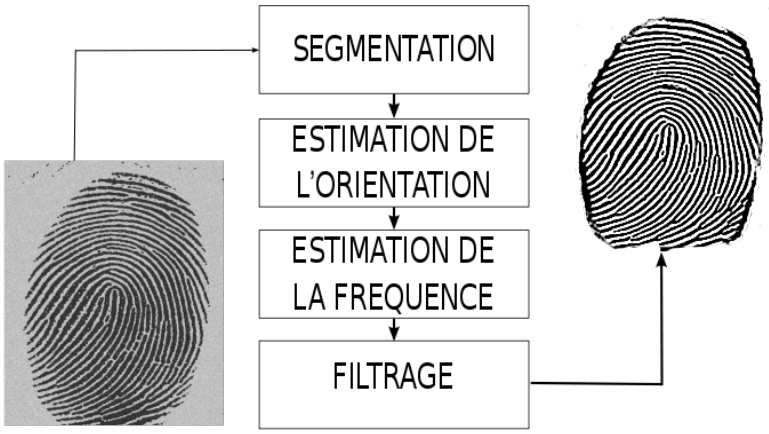



FIG. 2.3: Chaîne des traitements mis en jeu dans l'amélioration d'une image d'empreinte digitale

partie détaille cette méthode. Elle s'appuie largement sur la librairie Pandore en utilisant massivement ses opérateurs de traitement d'image. En voici un résumé :

- ETAPE 1 : Binarisation (voir 7) de l'image pour faire une première suppression du bruit dans l'image, de l'arrière-plan et pour ne garder que les crêtes et les quelques éventuels objets sur l'image ayant une intensité avoisinante à celle des crêtes.
- ETAPE 2 : Application d'une dilatation à l'image (voir 7) pour lier les crêtes entre elles et obtenir la forme générale de l'image.
- ETAPE 3 : Labellisation de l'image (voir 7), ce qui permet d'obtenir les différentes régions de l'image. L'une de ces régions doit notamment se détâcher des autres de par sa taille plus importante : il s'agit de l'empreinte.
- ETAPE 4 : Calcul de la plus grande région de l'image et suppression des autres régions pour ne garder que la forme de l'empreinte. A ce stade, les objets annexes à l'empreinte présents sur l'image d'entrée sont donc supprimés du masque (exception faite des objets adjacents à l'empreinte qui eux ont été liés à l'empreinte).
- ETAPE 5 : Calcul d'un contour grossier elliptique de la région, ce qui permet de couper dans le masque les objets adjacents à l'empreinte puisqu'ils sont d'une taille trop faible pour intervenir dans la modification de ce contour elliptique.
- ETAPE 6 : Utilisation du masque qui vient d'être créé pour supprimer toute l'information inutile sur l'image d'entrée. Il en ressort juste l'empreinte.

L'intérêt de cette technique n'est pas uniquement de permettre la segmentation de l'image, elle pourrait tout aussi bien être faite avec seulement des filtres morphologiques, voire une simple binarisation s'il n'y a pas d'autres objets dans l'image et que le fond est d'une couleur approximativement uniforme. Si cette technique est intéressante, c'est parce qu'elle permet en premier lieu de

supprimer les objets superflus pour la suite du procédé, comme le trait fait sur la capture de l'exemple ci-dessous qui aurait induit des erreurs. Mais surtout, grâce à l'étape 5, on a ainsi pu obtenir un masque de l'image qui va nous servir lors des deux points suivants :

- En retravaillant ce masque, on pourra avoir une zone d'intérêt de l'empreinte pour extraire ses caractéristiques (voir partie extraction de caractéristiques)
- En calculant le centre de gravité de ce masque, il sera alors possible de savoir si l'empreinte se situe au milieu de l'image et, si ce n'est pas le cas, on pourra la recentrer pour faciliter les traitements futurs, ce qui est actuellement dans mon implémentation de ma solution.

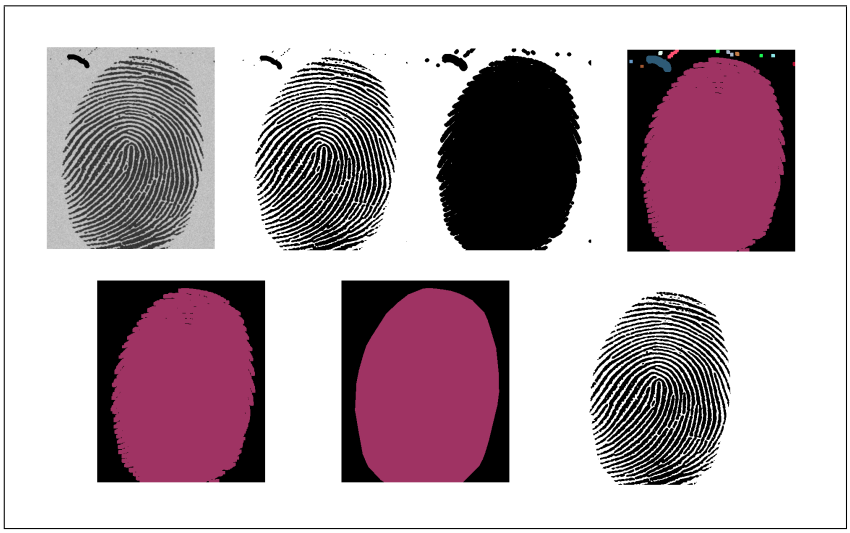


FIG. 2.4: Image d'entrée puis étapes 1 à 6 de la méthode de segmentation

### 2.4.2 Orientation de l'image

La deuxième partie de l'algorithme d'amélioration d'empreintes digitales s'appuie sur la publication du *Michigan State University* indiquée en 2.3. Dans cet algorithme, la première étape est le calcul de l'orientation de l'image. Ce calcul permet d'obtenir une allure générale de l'orientation des crêtes dans l'empreinte digitale. Cette donnée sera très utile pour la suite des traitements de cet algorithme.

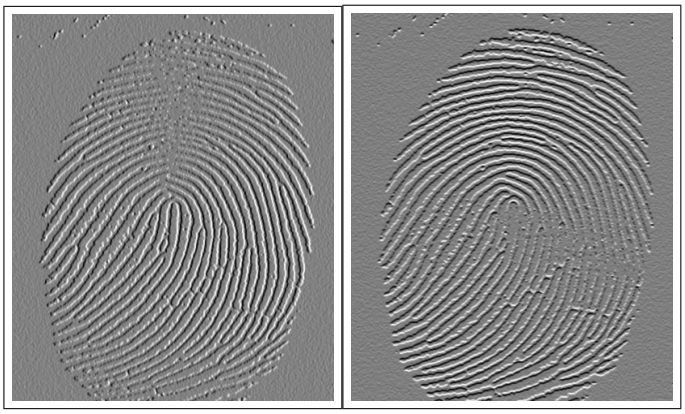
En premier lieu, il convient de calculer le gradient en x et en y de l'image d'entrée. Voici l'algorithme qui permet ce calcul :

L'image est ici considérée comme une matrice de pixels. Dans la suite de cette partie, la notation $\partial_x(i,j)$ fera référence au calcul du gradient en x. Quant à la notation $\partial_y(i,j)$, elle fera référence au calcul du gradient en y.

Une fois ce calcul effectué, on peut alors estimer l'orientation locale de l'image. Pour se faire, on va découper l'image en blocs d'une taille fixe $w*w$, où $w = dpi/50$, avec $dpi$ un paramètre donné en entrée de l'algorithme (après expérimentation, la valeur $w$ est en général optimale lorsqu'elle est comprise entre 15

```
for p.y = 1 to Image.Height() − 1 do
  for p.x = 1 to Image.Width() − 1 do
    deltaNS = Image[p.y + 1][p.x] − Image[p.y − 1][p.x]
    deltaEW = Image[p.y][p.x + 1] − Image[p.y][p.x − 1]
    deltaNWSE = Image[p.y + 1][p.x + 1] − Image[p.y − 1][p.x − 1]
    deltaNESW = Image[p.y − 1][p.x + 1] − Image[p.y + 1][p.x − 1]

    imdx[p.y][p.x] = deltaEW + ((deltaNWSE + deltaNESW)/2)
    imdy[p.y][p.x] = deltaNS + ((deltaNWSE − deltaNESW)/2)
  end for
end for
```



(a) $\partial_x(i,j)$ (b) $\partial_y(i,j)$

FIG. 2.5: Résultat du calcul du gradient en x et en y à partir de notre image témoin

et 19). Plus cette valeur sera faible, plus l'orientation sera locale, et plus elle sera forte, plus l'orientation reprendra l'orientation générale de l'image. On utilisera alors les équations suivantes pour estimer l'orientation locale de l'image :

$$\mathcal{V}_x(i,j) = \sum_{u=i-\frac{w}{2}}^{i+\frac{w}{2}} \sum_{v=j-\frac{w}{2}}^{j+\frac{w}{2}} 2\partial_x(u,v)\partial_y(u,v) \tag{2.1}$$

$$\mathcal{V}_y(i,j) = \sum_{u=i-\frac{w}{2}}^{i+\frac{w}{2}} \sum_{v=j-\frac{w}{2}}^{j+\frac{w}{2}} (\partial_x^2(u,v) - \partial_y^2(u,v)) \tag{2.2}$$

$$\mathcal{O}(i,j) = \frac{1}{2}\tan^{-1}(\frac{\mathcal{V}_x(i,j)}{\mathcal{V}_y(i,j)}) \tag{2.3}$$

où $\mathcal{O}(i,j)$ est l'estimation des moindres carrés[5] du bloc centré sur le pixel $(i,j)$. Mathématiquement, $\mathcal{O}(i,j)$ représente la direction orthogonale à la direc-

[5] La méthode des moindres carrés, indépendamment élaborée par Legendre en 1805 et Gauss en 1809, permet de comparer des données expérimentales, généralement entachées d'erreurs de mesure à un modèle mathématique censé décrire ces données.

tion dominante dans le spectre de Fourier du bloc $w * w$.

Une optimisation est proposée dans la publication. Je ne l'ai cependant pas implémentée, car la précision semblait suffisante lors de la génération de l'orientation de l'image avec les équations données ci-dessus. En effet, nous nous étions fixés comme point de départ d'utiliser en entrée des images d'assez bonne qualité, ce qui inhibe l'utilité d'une telle optimisation. Cette dernière part du constat que dans l'image, il y a une forte présence de bruit, de crêtes corrompues de coupures et autres incohérences qui induisent une imprécision dans le calcul de l'orientation. Comme l'orientation dans le voisinage d'un pixel d'une empreinte digitale varie normalement faiblement, il est proposé d'employer un filtre passe-bas[6] pour rectifier les incohérences du calcul de l'orientation. Il faut tout d'abord transformer l'image orientée en un champ de vecteurs[7] continus comme suit :

$$\Phi_x(i,j) = \cos(2\mathcal{O}(i,j)) \tag{2.4}$$

$$\Phi_y(i,j) = \sin(2\mathcal{O}(i,j)) \tag{2.5}$$

où $\Phi_x(i,j)$ et $\Phi_y(i,j)$ sont les composantes du champ de vecteurs. Avec ce champ résultant, on peut alors employer le filtre passe-bas suivant :

$$\Phi'_x(i,j) = \sum_{u=-w_\Phi/2}^{w_\Phi/2} \sum_{v=-w_\Phi/2}^{w_\Phi/2} W(u,v)\Phi_x(i-uw, j-vw) \tag{2.6}$$

$$\Phi'_y(i,j) = \sum_{u=-w_\Phi/2}^{w_\Phi/2} \sum_{v=-w_\Phi/2}^{w_\Phi/2} W(u,v)\Phi_y(i-uw, j-vw) \tag{2.7}$$

où $W$ est un filtre passe-bas à 2 dimensions et $w_\Phi * w_\Phi$ est la taille de ce filtre (La taille préconisée est de 5*5). Il ne reste alors plus qu'à calculer l'orientation locale en utilisant :

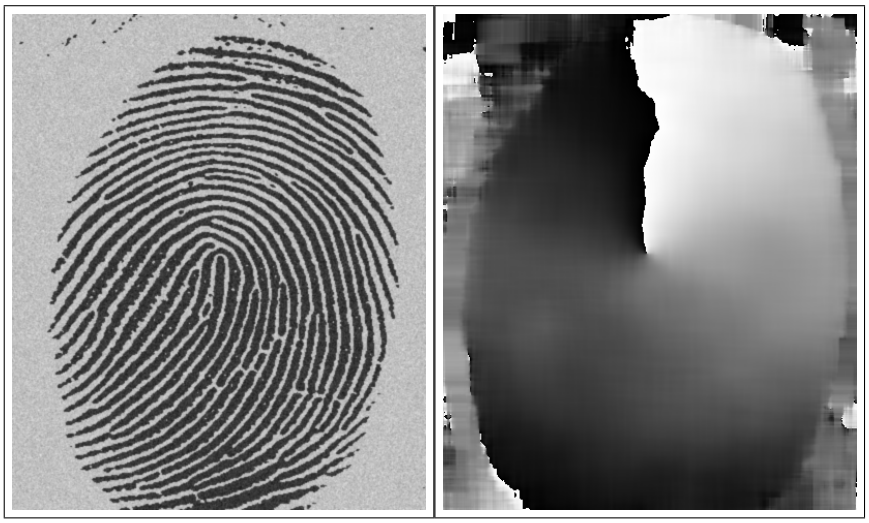
$$\mathcal{O}(i,j) = \frac{1}{2}\tan\left(\frac{\Phi'_y(i,j)}{\Phi'_x(i,j)}\right) \tag{2.8}$$

où $\mathcal{O}$ est le nouveau résultat du calcul de l'orientation de l'image.

Pour avoir un exemple de ce que donne le calcul de l'orientation d'une empreinte digitale sur notre image témoin (sans l'optimisation), se référer à la figure 2.4.2.

[6] Un filtre passe-bas est un filtre qui laisse passer les basses fréquences et qui atténue les hautes fréquences.

[7] En mathématiques, un champ de vecteurs ou champ vectoriel est une fonction qui associe un vecteur à chaque point d'un espace euclidien.



(a) Image d'origine

(b) Imagine générée à partir de l'orientation de $(a)$

FIG. 2.6: Résultat du calcul de l'orientation de l'image

### 2.4.3 Calcul de la fréquence médiane

L'algorithme pour le calcul de la fréquence médiane dans une empreinte part du principe que, dans un bloc de l'image (les mêmes blocs que lors du calcul de l'orientation de l'image), s'il n'y a pas de minuties ou de points singuliers qui apparaissent, alors les crêtes et les sillons peuvent être approximés par la forme d'une onde sinusoïdale dans une direction normale à l'orientation locale des crêtes (Cf figure 2.4.3).

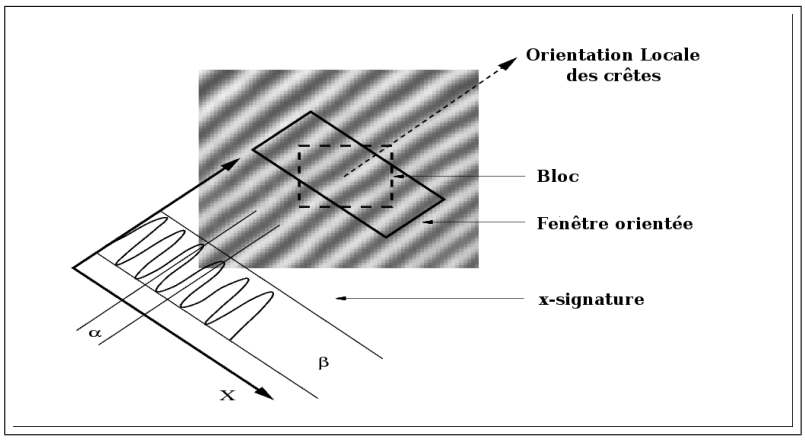



FIG. 2.7: Onde sinusoïdale approximant les crêtes d'un bloc en fonction de l'orientation de celles-ci

Cette partie s'appuie à la fois sur l'algorithme *Fingerprint Image Enhancement : Algorithm and Performance Evaluation* et sur le travail de Peter Kovesi sur ce même sujet.

Soient $\mathcal{G}$ l'image d'entrée et $\mathcal{O}$ l'orientation de cette image, alors l'algorithme pour le calcul de la fréquence médiane de l'empreinte est le suivant :

1. Diviser l'image en un nombre de blocs de taille $w * w$ (où $w$ est de même longueur que celle utilisée lors de l'étape précédente)

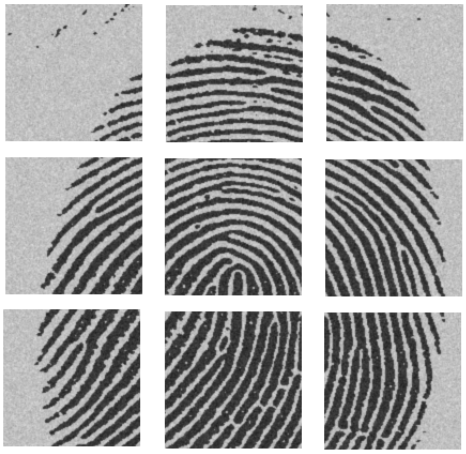


FIG. 2.8: Image divisée en blocs de taille équivalente

2. Orienter les blocs de telle façon que les crêtes soient aussi verticales que possible (on utilise alors l'orientation calculée pour chaque bloc afin d'estimer l'angle à appliquer à l'orientation de ce bloc).

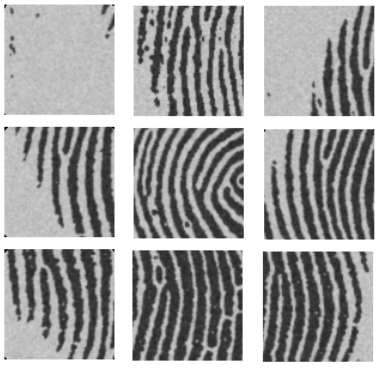


FIG. 2.9: Blocs réorientés pour que les crêtes se trouvent à la verticale

3. Pour chaque bloc, appliquer l'algorithme suivant :

```
Require: Un bloc de taille w * w
  colSumArray[bloc.Size()]; dilation[bloc.Size()]; meanColSumArray = 0;
  for i = 0 to bloc.Size() − 1 do
    colSumArray[i] = 0;
    for j = 0 to bloc.Size() − 1 do
      colSumArray[i]+ = bloc[i][j];
    end for
    meanColSumArray+ = colSumArray[i];
  end for
  meanColSumArray = meanColSumArray/bloc.Size();
  half = (bloc.Size() − 1)/2;
  for i = 0 to bloc.Size() − 1 do
    max = 0;
    for k = −half + i to k <= half + i do
      if k >= 0&&k < bloc.Size() then
        if colSumArray[k] > max then
          max = colSumArray[k];
        end if
      end if
    end for
    dilation[i] = max;
  end for
```

Il ne reste alors plus qu'à trouver les pics dans le tableau *colSumArray* pour déterminer la fréquence du bloc courant :

```
  for i = 0 to bloc.Size() − 1 do
    if dilation[i] == colSumArray[i]&&colSumArray[i] > meanColSumArray then
      Pic Trouvé en i !
    end if
  end for
```

On obtient alors pour chaque bloc une série de pics qui correspond aux vallées détectées dans l'empreinte digitale. On peut donc comparer ces pics aux pics de l'onde sinusoïdale que l'on avait avancé comme modèle. (Cf figure 2.4.3) pour une représentation des pics trouvés sur l'empreinte digitale témoin.

Pour terminer, il ne reste plus qu'à calculer la valeur moyenne de la fréquence des crêtes dans l'image : en effet, il a été trouvé expérimentalement qu'améliorer l'image avec une valeur moyenne des fréquences est meilleur qu'améliorer localement les blocs avec la fréquence trouvée pour chaque bloc. Si la fréquence d'un bloc est beaucoup plus importante ou faible que les autres blocs qui lui sont adjacents, on peut arriver lors de l'amélioration à des blocs qui ont des crêtes qui ne se prolongent pas de blocs en blocs.

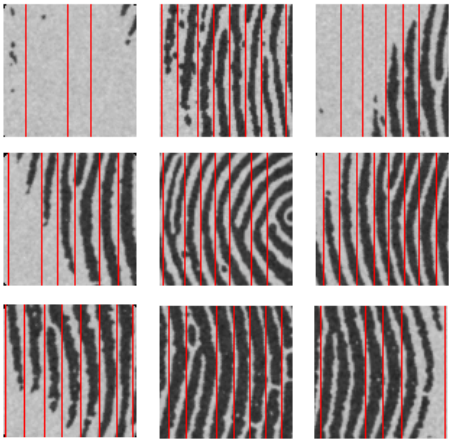


FIG. 2.10: Pics détectés dans les blocs

### 2.4.4 Génération des filtres de Gabor

L'un des filtres le plus utilisé est le filtre de Gabor. Ce filtre n'est qu'une fréquence pure modulée par une gaussienne[8], c'est-à-dire, un filtre passe bande avec une enveloppe gaussienne. Ce filtre est très répandu du fait de sa propriété de résolution optimale conjointe en fréquence et en temps. Les filtres de Gabor ont des propriétés de sélection à la fois sur la fréquence d'une image et à la fois sur son orientation. Il est donc tout à fait approprié d'utiliser des filtres de Gabor pour ce type d'amélioration.

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

- Une *fréquence*, déterminée grâce au calcul médian de la fréquence ;
- Une *orientation*, déterminée également grâce à l'orientation calculée précédemment ;
- Deux constantes $\delta_x$ et $\delta_y$ qui sont les constantes d'espace de l'enveloppe gaussienne sur les axes x et y.

L'intérêt d'un filtre de Gauss est donc de pouvoir n'optimiser qu'une certaine zone de l'image selon son orientation. Voici l'équation qui permet de calculer un tel filtre :

$$h(x, y : \phi, f) = exp\{-\frac{1}{2}\frac{(x\cos\phi)^2}{\delta_x^2} + \frac{(y\sin\phi)^2}{\delta_y^2}\}\cos(2\pi f x\cos\phi) \qquad (2.9)$$

où $\phi$ est l'orientation du filtre de Gabor, $f$ la fréquence et $\delta_x$ et $\delta_y$ les constantes d'espace.

[8] Une fonction gaussienne est une fonction en exponentielle de l'opposé du carré de l'abscisse. Elle a une forme caractéristique de courbe en cloche

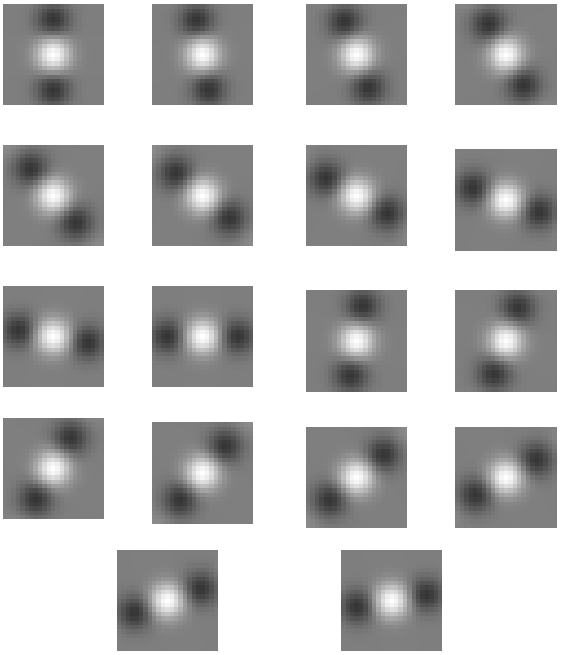


FIG. 2.11: Filtres de Gabor générés

### 2.4.5 Amélioration de l'image

Une fois les filtres de Gabor générés (au nombre de 18, un tous les 10 degrés), il ne reste plus qu'à les appliquer à l'image d'origine et à stocker ces 18 images filtrées résultantes (Cf figure 2.12).

L'opération finale de l'amélioration consiste à combiner entre elles les différentes images filtrées en fonction de l'angle calculé grâce à l'orientation de l'empreinte. La composition s'effectue simplement en reprenant la bonne image filtrée en fonction de $\mathcal{O}$, l'orientation des crêtes dans l'image.

Se référer à la figure 2.13 pour voir l'amélioration résultante d'une image.

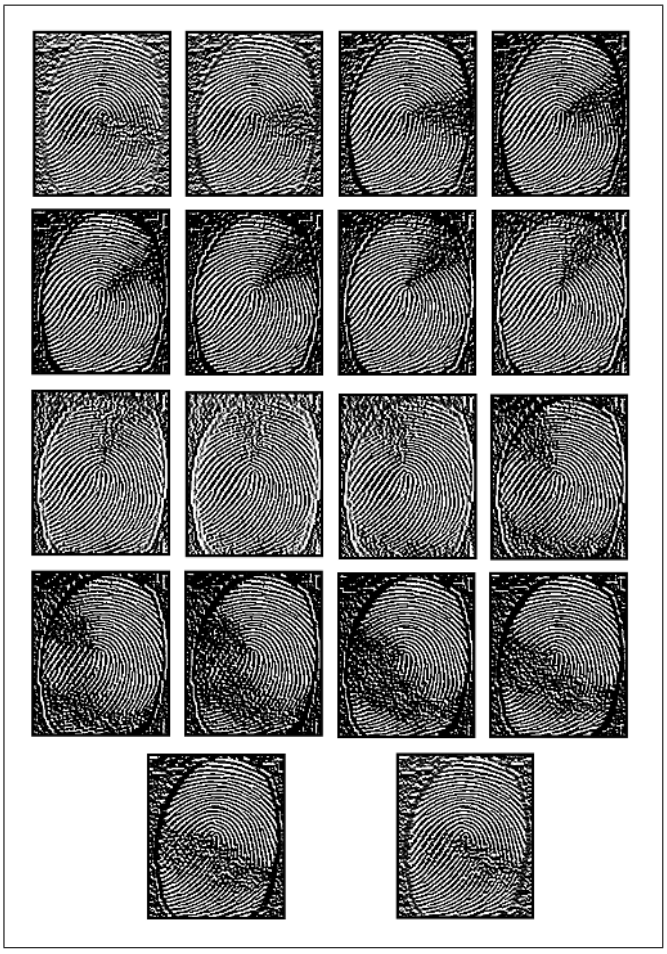


FIG. 2.12: Images filtrées générées

## 2.5 Squelettisation

La squelettisation est la dernière étape de cette partie. Elle n'est pas directement reliée aux autres processus car elle n'est pas indispensable dans le bon déroulement de l'améliorer. Si elle est ici utilisée, c'est pour pouvoir par la suite extraire plus facilement un certain type de caractéristiques.

L'étape de squelettisation consiste à amincir une forme de manière à ce qu'elle ne soit plus représentée que par un ensemble de segments irréductibles (Si on venait à supprimer ne serait-ce qu'un seul pixel sur un segment, alors soit on le raccourcirait, soit il s'en créerait deux). Cette opération se fait de manière itérative sur un objet. A chaque tour, on creuse plus profondément dans une forme jusqu'à ne plus pouvoir. La squelettisation permet de préserver la topoligie d'un objet ainsi que sa taille (Cf figure 2.14).

L'intérêt de squelettiser l'image améliorée est tout d'abord de gagner en temps de calculs : en effet, puisqu'il y aura moins de données à traiter, ce

FIG. 2.13: Notre empreinte témoin améliorée

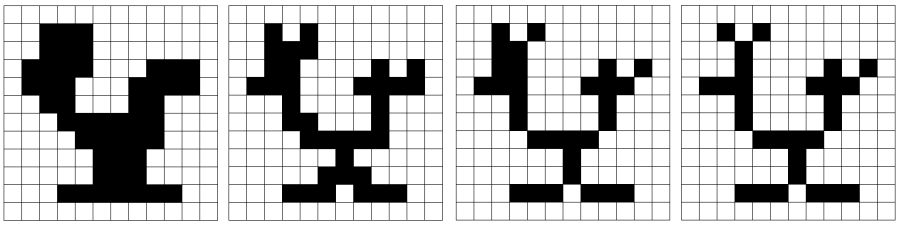


FIG. 2.14: Images filtrées générées

traitement ira plus vite. De plus, nous verrons dans la partie suivante l'avantage d'une telle technique pour l'extraction de caractéristiques. Se référer à la figure 2.15 pour voir le résultat d'une squelettisation sur l'empreinte témoin.

## 2.6 Conclusion

L'amélioration globale de l'image prend une dizaine de secondes. La majeure partie du temps est employée à la génération des filtres de Gabor et à leur application sur l'image.

Pour pouvoir comprendre l'apport de la méthode d'amélioration mise en place dans ce projet, il est intéressant de commencer en montrant un exemple comparatif de notre image témoin qui a simplement été binarisée et cette même image mais qui a subi les différents traitements expliqués dans les parties précédentes (Cf figure 2.16).

Cette comparaison introduit le sujet suivant qui est l'extraction de caractéristiques de l'image. On voit parfaitement sur l'image de gauche que les carac-

FIG. 2.15: Squelettisation de l'empreinte témoin

téristiques extraites ne sont pas exploitables. En effet, l'image comporte un tel nombre d'imprécisions qu'il n'est pas possible d'en extraire quelque chose.

Au contraire, l'image de droite qui utilise l'algorithme employé pour l'amélioration d'empreintes digitales montre la précision avec laquelle il trouve des caractéristiques.

Au final, la méthode semble répondre à la problématique initiale énoncée en y apportant une solution concrète.

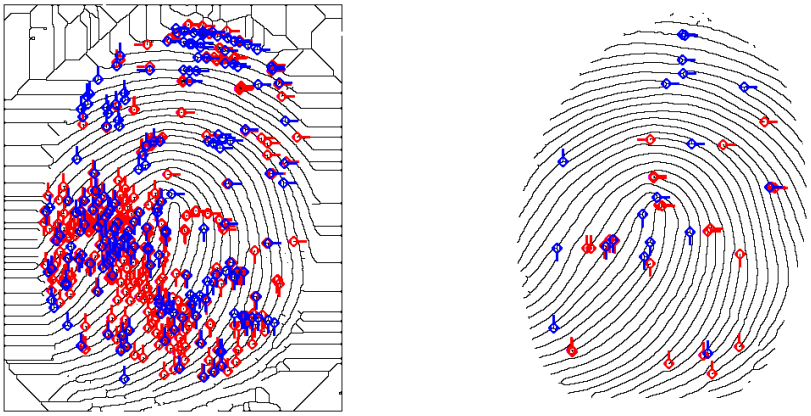


FIG. 2.16: Extraction de caractéristiques de l'image témoin.

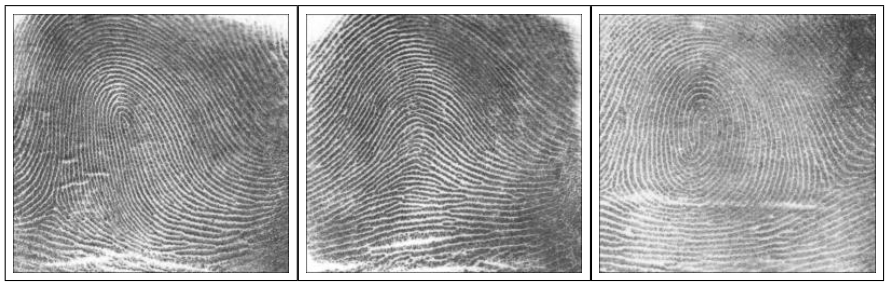
# Chapitre 3

# Extraction de caractéristiques

## 3.1 Les Minuties

Comme énoncé dans l'introduction, la comparaison d'empreintes digitales s'effectue grâce à l'analyse de caractéristiques propres à chacune d'elles qui permet, en les opposant, de trouver soit une concordance, soit une discordance. Il est par exemple possible de choisir la forme globale de l'empreinte comme caractéristique qui pemettrait la comparaison. Cependant, il n'est possible de regrouper les empreintes que dans un nombre restreint de catégories (Cf figure 3.1), car elles ont souvent la même allure générale, ce qui n'est pas suffisant pour un tel type de comparaison, encore moins lorsque l'on parle de comparer des milliers d'empreintes. La forme globale ne sera au mieux qu'une indication pour la comparaison, ou aura une tout autre utilité, comme lors de la classification des empreintes.

La problématique de cette partie était donc de trouver un moyen de comparer deux empreintes digitales qui soit suffisamment robuste pour permettre par la suite d'effectuer une comparaison entre deux acquisitions très proches (Acquisitions proches est ici au sens ou la même empreinte est acquise dans les mêmes conditions, c'est-à-dire sans trop d'altérations dûes à la moiteur ou la sécheresse des mains, sans translation, sans rotation, ...).



(a) Boucle à gauche (b) Arche (c) Tourbillon

FIG. 3.1: Types les plus primaires que l'on peut rencontrer en analysant des empreintes digitales.

Après des recherches poussées sur le sujet, un type de caractéristiques a été particulièrement mis en avant. Il a finalement été retenu pour la méthode d'extraction de caractéristiques. Cette méthode, c'est l'étude des *minuties* propres à l'empreinte.

Une minutie est définie comme étant un point caractéristique de l'une ou de plusieurs crêtes de l'empreinte. Une minutie se situe sur le changement de continuité d'une crête. En voici une liste qui détaille leur signification (Cf figure 3.1) :

- *Fin de crête* : Une crête se termine abruptement ;
- *Bifurcation* : Une crête se divise en deux crêtes distinctes ;
- *Petites crêtes ou île* : Une crête qui ne s'étend que sur une très courte distance ;
- *Enclos* : Une crête simple qui bifurque avant de se réunir juste après pour continuer en crête simple ;
- Une minuties peut également correspondre à d'autres petits détails de l'empreinte. Certains algorithmes prennent par exemple en compte la distance entre les pores de la peau ;
- Il existe encore d'autres types de minuties tels que les deltas, les crêtes en forme de y ou encore les demi-tours.

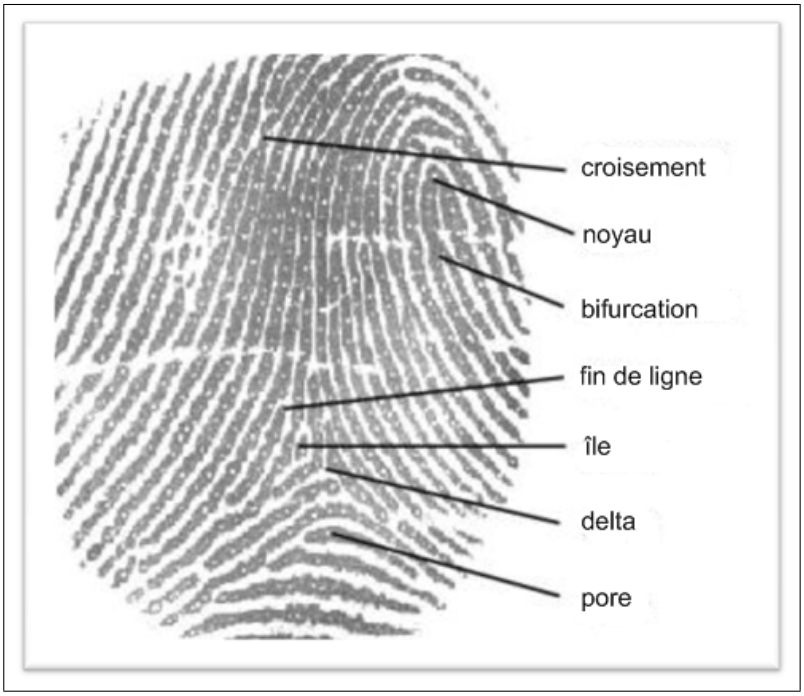



FIG. 3.2: Exemple de minuties que l'on peut retrouver sur une même empreinte

Si ce choix a été priviligié à un autre, c'est pour plusieurs raisons. Tout d'abord, l'étude des minuties est l'une des techniques les plus utilisées dans l'analyse et la comparaison d'empreintes digitales. Leur extraction est relative-

ment facilitée lorsqu'un prétraitement efficace est effectué en amont. Ensuite, le temps d'exécution pour leur comparaison se révèle assez limité. Enfin, le temps de développement rapide d'une méthode d'extraction de minuties n'est pas à négliger.

Remarque : en France, deux empreintes digitales sont considérées comme équivalentes lorsque l'on trouve au moins douze minuties concordantes. Reste à définir ce qu'est la concordance de minuties (Pour cela, voir partie 4).

## 3.2 Reconnaissance des Minuties

Une fois l'image de l'empreinte acquise améliorée, on se retrouve avec un squelette d'empreinte digitale parfaitement exploitable. C'est sur ce squelette que l'on va devoir travailler pour rechercher les minuties qui permettront de caractériser l'empreinte.

L'algorithme d'extraction de caractéristiques mis en place prend en entrée une empreinte squelettisée et en ressort une liste de minuties. Soit $M = m_0, m_1, .., m_n$ la liste de minuties correspondantes, où $m_i = (x, y, theta, type)$, avec $x$ et $y$ la position de la minutie dans l'image, $theta$ son orientation par rapport aux crêtes qui l'entourent (on utilisera ici l'orientation $\mathcal{O}(i, j)$ calculée dans la partie amélioration d'image) et $type$, le type de la minutie (bifurcation, fin de ligne, ...). J'ai choisi de me concentrer exclusivement sur l'étude de deux types de minuties, à savoir les fins de crêtes et les bifurcations, car elles se trouvent en plus grand nombre dans les empreintes et leur extraction est plus facile que pour d'autres types de minuties. Il n'est cependant pas impossible d'inclure par la suite de nouveaux types de minuties dans les algorithmes de détection de minuties utilisés dans cette partie.

### 3.2.1 Choix de la zone d'intérêt pour l'extraction des minuties

L'image en entrée a beau être améliorée, il n'en reste pas moins que toute la zone d'image n'admet pas que des informations utiles à l'extraction des caractéristiques. Pire, si on prend en compte toute la zone de l'image, on risque d'extraire des caractéristiques qui fausseraient par la suite la comparaison. En effet, selon l'inclinaison du pouce sur le capteur, la zone acquise de l'empreinte ne sera pas la même. Lors d'une acquisition, on ne peut obtenir qu'une empreinte partielle, il faut donc prendre soin à ne pas s'intéresser aux informations incomplètes.

Comme l'empreinte est recentrée lors de l'étape d'amélioration, on peut considérer que l'information la plus pertinante se trouve dans la zone centrale de l'image. Il sera alors possible de réemployer le masque de l'image précédemment calculé durant l'étape d'amélioration. Pour ce faire, sachant que le masque reprend la forme globale de l'empreinte, il suffit d'en diminuer la taille de manière à écarter la fin des crêtes du bord de l'acquisition. Ainsi, on évitera d'englober

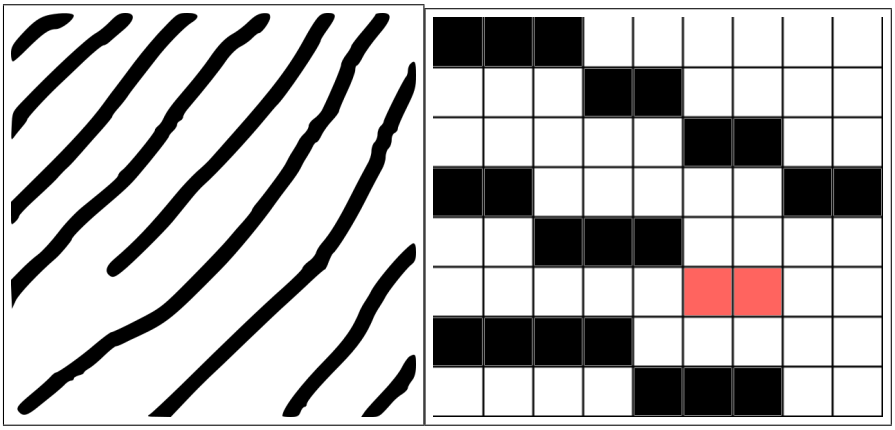
les fins de crêtes dûes à l'acquisition partielle de l'empreinte lors de l'extraction des caractéristiques. Si un pixel de l'empreinte est à l'intérieur du masque, alors on l'analysera pour déterminer s'il appartient aux types de minuties précités, sinon au l'ignorera (Cf figure 3.2.1).

FIG. 3.3: Utilisation du masque pour ne travailler que sur une partie intéressante de l'image

### 3.2.2 Extraction des fins de crête

Le premier type de minuties à extraire est la fin de crête (Cf figure 3.2.3). Cette extraction est réalisée d'une manière relativement simple, dont voici un résumé :

Pour trouver une fin de crête, il faut créer un filtre de taille 3∗3 et l'appliquer sur toute l'image en fonction du masque. Le filtre ne fait rien d'autre que calculer le nombre de cases blanches consécutives au voisinage immédiat du pixel central, c'est-à-dire qu'il est en mesure de déterminer le nombre de crêtes autour du pixel central.



(a) Schéma représentant une fin de crête (b) Représentation d'une fin de crête sur un squelette d'empreinte digitale

FIG. 3.4: Deux représentations d'une fin de crête.

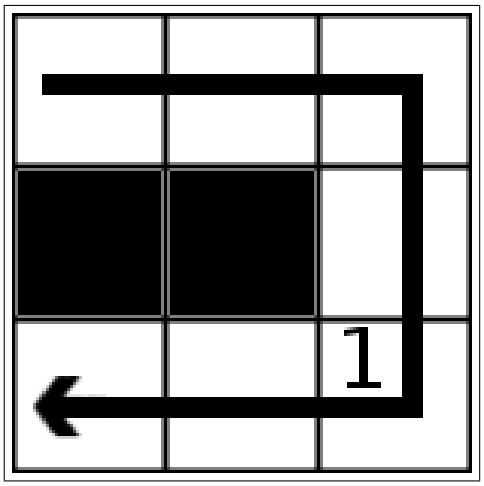


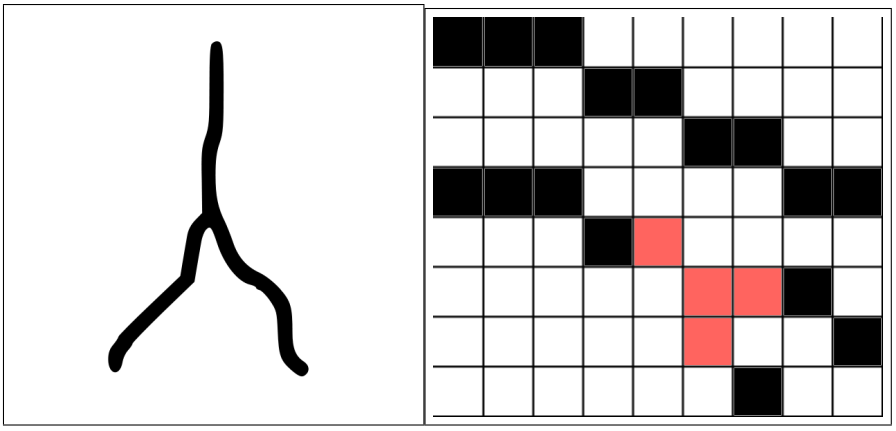

FIG. 3.5: Exemple d'application du filtre généré : comme il ne trouve ici qu'une seule zone blanche, il n'y a donc qu'une seule crête, c'est pourquoi nous sommes en présence d'une fin de crête

### 3.2.3 Extraction des bifurcations

Il s'agit du second type de minuties à extraire dans une image. Une bifurcation est déterminée par la présence de trois crtes dans le voisinage immédiat d'un pixel (taille du filtre de 3∗3). Le procédé d'extraction reprend alors le même principe que pour l'extraction des fins de crêtes, mais y rajoute une condition supplémentaire déterminée après une première série d'expérimentations.

Lors du parcours du voisinage immédiat, il se peut que l'on détecte une fin de crête alors qu'il s'agit en réalité d'un problème lié à l'amélioration. Il a donc fallu y appliquer un correctif. Ce problème se résume par la présence d'un

pixel perturbateur au voisinage immédiat de l'image. Pour corriger ce problème, après avoir décelé une bifurcation dans le voisinage immédiat, il suffit de faire de même avec cette fois-ci un filtre de taille 5*5 pour déterminer si l'on se trouve devant une vraie bifurcation ou non (Cf figure 3.7).



(a) Schéma représentant la bifurcation d'une crête

(b) Représentation d'une bifurcation sur un squelette d'empreinte digitale

FIG. 3.6: Deux représentations de bifurcations.

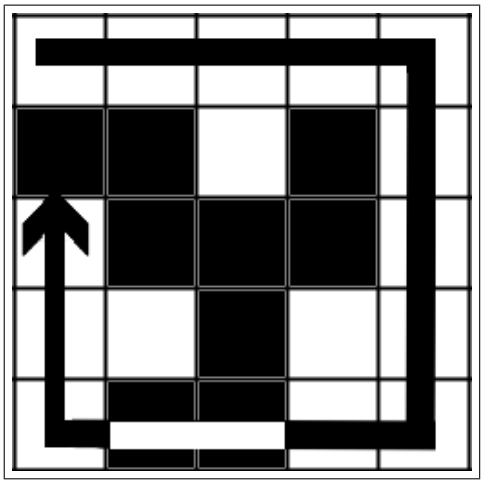


FIG. 3.7: Exemple d'application du filtre généré : le filtre trouve une bifurcation au voisinage immédiat du pixel central, mais après analyse du voisinage avec un filtre 5*5, on se rend compte qu'il s'agit d'un cas d'erreur et il n'est donc pas pris en compte.

### 3.2.4 Conclusion

En conclusion, la méthode d'extraction de caractéristiques permet de trouver un nombre suffisant de minuties pour permettre une comparaison pas la suite et elle répond donc bien à la problématique initiale. Cependant, il est à noter que cette méthode dépend entièrement de l'amélioration d'image réalisée avant. Plus l'amélioration sera de bonne qualité, plus cette méthode sera performante.

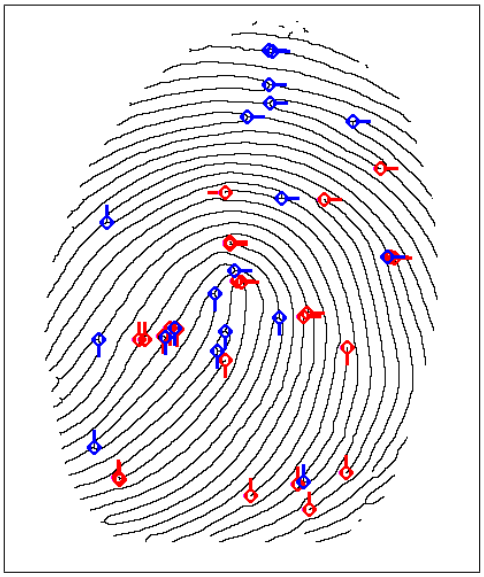


FIG. 3.8: Extraction des caractéristiques de notre empreinte témoin.

# Chapitre 4

# Comparaison

La comparaison des minuties une fois extraites est une partie essentielle de l'analyse de l'empreinte digitale. Elle a donc été sujette à plusieurs expérimentations pour tenter d'offrir une solution aussi souple et robuste que possible. Le principe général de la comparaison est de retrouver d'une empreinte à l'autre les mêmes minuties. Pourtant, nous pourrons voir dans la suite de cette partie qu'en fonction de l'approche, les résultats peuvent être radicalement différents.

Dans cette partie, l'objectif fixé était assez sommaire : il fallait surtout réussir à mettre en place une méthode de comparaison qui puisse arriver à trouver une corrélation entre deux empreintes très proches.

## 4.1 Méthode naïve de concordance

C'est la méthode la plus facile à mettre en oeuvre pour une première comparaison. Elle a été étudiée et testée pour répondre au besoin énoncé pour ce projet d'année : offrir une méthode de comparaison simple entre les empreintes qui ne seraient pas sujettes aux translations ou rotations. Elle repose donc également sur un principe simple : la superposition des empreintes (Cf figure 4.1). Grâce au centrage de l'acquisition de l'empreinte, on peut émettre l'hypothèse forte que l'on va pouvoir retrouver les mêmes minuties à la même place, modulo une certaine distance et un certain angle entre elles.

Pour ce faire, on utilise un algorithme très simple qui prend en paramètre une *distance* et un angle maximals pour chercher une concordance entre deux minuties. Le principe est de faire passer une fenêtre sur la première empreinte, et pour chacune des minuties extraites dans la partie 3, on cherche une correspondance dans cette fenêtre de grandeur *distance*. Si on trouve une autre minutie, on vérifie qu'elle est bien du même type que la minutie initiale et que l'angle entre les deux est le même, modulo l'approximation donnée en entrée (Cf figure 4.1).

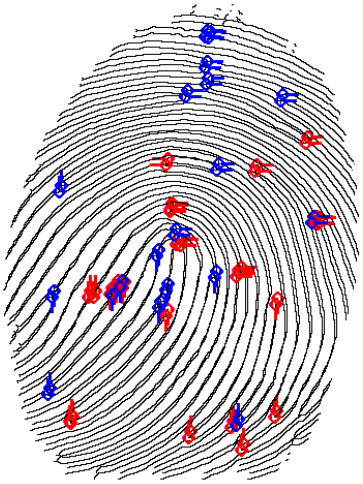


FIG. 4.1: Superposition de deux empreintes pour tenter de trouver une concordance entre elles

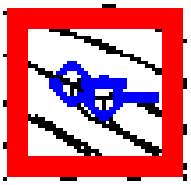


FIG. 4.2: Concordance au niveau local

### 4.1.1 Analyse de la méthode

Cette méthode est intéressante pour voir si les traitements appliqués aux chapitres précédents sont pertinants. En effet, deux minuties présentes au même endroit, ayant le même type ainsi que le même angle seront reconnues comme étant identiques. Ainsi, en comparant deux fois la même empreinte, on trouve un taux de concordance de l'ordre de 100% entre les deux images.

Pourtant, une fois testée en situation réelle (pas avec un simple cas d'école), je me suis rapidement rendu compte que cette méthode était inapliquable dès lors que l'on souhaitait entreprendre une véritable comparaison entre deux acquisitions différentes de la même empreinte. Comme expliqué dans l'introduction de la partie amélioration, de nombreux facteurs jouent sur l'acquisition, et on ne comparera jamais deux empreintes strictement identiques. Selon l'inclinaison du doigt ou une orientation légèrement différente, les résultats s'écroulent rapidement pour ne pas dépasser les 5 à 10% de concordance, ce qui est bien trop peu pour une authentification. La seule possibilité pour accroître artificiellement le résultat serait d'augmenter la taille de la fenêtre ou encore le décalage au niveau de l'angle. C'est pourquoi il m'a semblé nécessaire de mettre en place une nouvelle méthode de comparaison afin de palier aux trop nombreux défauts de celle-ci.

## 4.2 Méthode de concordance de graphes

Pour pouvoir mettre en place un algorithme de comparaison plus efficace, il a fallu réfléchir aux problèmes de la méthode employée ci-dessus. La concordance entre minuties n'est pas inintéressante, il s'agit principalement d'un problème de translataion ou de rotation de l'image. Dès lors, on se retrouve devant un problème de correspondance entre les deux empreintes. Il faut réussir à les superposer au mieux. Si cela peut s'avérer possible entre deux images d'empreintes dont l'une aurait reçu une transformation linéaire (translation, rotation), comment faire entre deux acquisitions résolument différentes de la même image ?

(a) Pemière acquisition d'empreinte

(b) Deuxième acquisitions d'une même empreinte

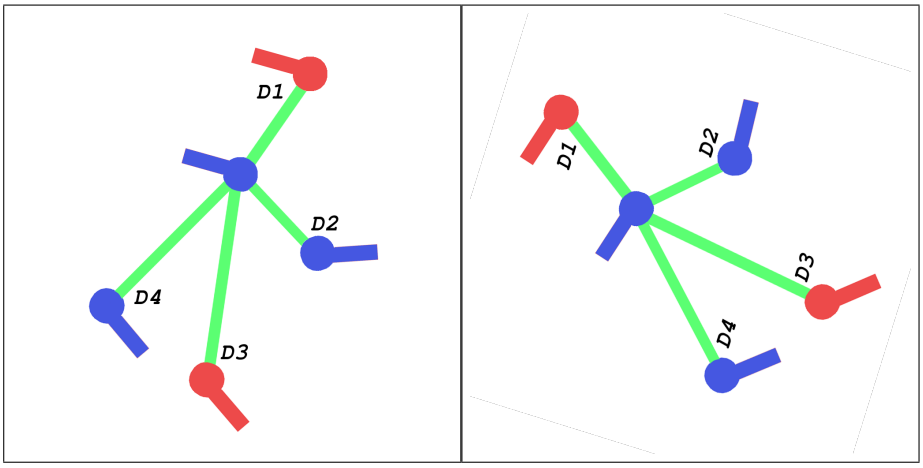
FIG. 4.3: Deux acquisition radicalement différentes qui ne peuvent pas répondre à un problème simple de superposition

On voit donc que la résolution de ce problème est plus complexe qu'un simple nouveau traitement d'image. Il faut réussir à s'abstraire de la position absolue des minuties dans l'empreinte qui ne permettent pas de mettre en place une méthode de concordance efficace.

L'idée nouvelle mise en place dans cette partie est donc de travailler au niveau des minuties avec des positions relatives et non plus absolues. Pour ce faire, on doit mettre de côté le fait que la minutie ait une position déterminée sur l'empreinte en $x, y$. Voyons les choses autrement : chaque minutie a une certaine distance avec les autres ainsi qu'une certaine différence d'angle. Quelle que soit la transformation linéaire qui est faite à l'image, une minutie aura toujours la même distance ainsi que le même angle relativement à une autre (Cf figure 4.2). C'est sur ce postulat de base que j'ai été amené à travailler pour proposer une nouvelle approche de comparaison d'empreinte.

Comme la figure 4.4 le laisse à supposer, une minutie ne se définit donc plus que par son type. Pour le reste, c'est en se référant aux autres minuties

de l'empreinte que l'on va pouvoir préciser la forme d'un ensemble de minuties adjacentes qui servira alors à donner une idée de la ressemblance entre plusieurs minuties. Le principe est donc de former un graphe entre toutes les minuties de l'empreinte, valué à la fois par leur distance respective et par leur différence d'orientation (CF figure 4.2).




(a) Mise en relation des minuties avoisinantes (b) La même relation, mais qui a subi une rotation. On doit pouvoir dire qu'il s'agit bien du même graphe

FIG. 4.4: Création d'un lien entre une minutie et les autres minuties qui l'entourent. Ce graphe pourra alors être comparé à un autre graphe de minuties pour déterminer si deux minuties sont équivalentes ou non.

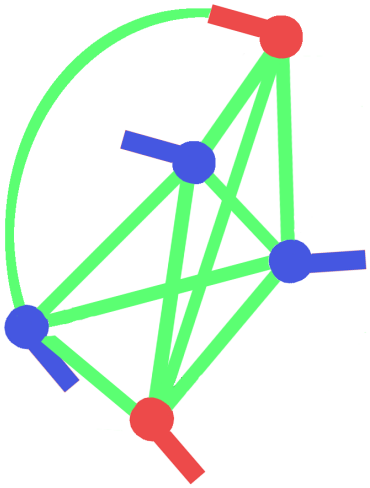


FIG. 4.5: Création du graphe complet entre les différentes minuties

### 4.2.1 Comparaison de deux minuties

Pour pouvoir comparer deux minuties, il faut au préalable calculer et stocker les distances qui les séparent ainsi que la différence entre leurs angles respectifs, cela afin d'évinter un trop nombreux calculs. Une fois cette étape achévée, il va falloir comparer chaque minutie d'une première image à toutes les autres de l'image deux (en s'arrêtant en cas de concordance pour éviter un nombre trop élevé de calculs inutiles). A noter qu'il est préférable de prendre un ordre de comparaison entre les images de sorte que l'on compare toujours l'image qui a le moins de minuties avec celle qui en a le plus, ou l'inverse, pour éviter une trop grande différence dans la taille des graphes. Pour ma part, j'ai décidé de travailler en prenant comme première image celle qui a le moins de minuties.

Voici un algorithme qui permet la comparaison de deux minuties $minutie1$ et $minutie2$ une fois la première étape de calculs réalisée :

---

$compteur = 0$;
**for** $Minutie\ min1 : minutie1.getOthersMinutiesValue()$ **do**
  **for** $Minutie\ min1 : minutie2.getOthersMinutiesValue()$ **do**
    **if** $min1.getType() == min2.getType()\&\&abs(min1.getAngle() - min2.getAngle()) < 10\&\&abs(min1.getDist() - min2.getDist()) < 20$ **then**
      $compteur++$;
      $break$;
    **end if**
  **end for**
**end for**
$RETURN\ compteur$

---

Il ne reste plus qu'à déterminer un seuil d'équivalence entre deux minuties selon leur proximité. Après expérimentations, j'en suis arrivé à la conclusion qu'il était nécessaire qu'il y ait au moins les 3/4 des minuties adjacentes à une minuties de l'empreinte qui doivent être concordantes pour pouvoir affirmer qu'il s'agit bien de la même. Toutes les minuties ne peuvent pas être répérables d'une acquisition à l'autre, mais dans la globalité, on retrouve un nombre de minuties avoisinant.

### 4.2.2 Déterminer l'égalite de deux empreintes

La dernière étape de la comparaison consiste en le calcul d'un coefficiant qui sanctionnera la ressemblence des deux empreintes. Ce coefficient correspond simplement au nombre de concordances trouvées sur le minimum de minuties entre les deux empreintes. Plus ce coefficiant sera élevé, plus il indiquera une forte présomption d'égalité entre deux empreintes.

En moyenne, selon cette méthode, on constate sur des images bien prétraitées que des empreintes équivalentes ont des taux de ressemblance assez élevés (de l'ordre de 70 à 80%) quand deux empreintes différentes n'ont qu'un taux assez faible de ressemblance (entre 10 à 30%).

### 4.2.3 Optimisation

Avec l'algorithme précédent, on va devoir parcourir toutes les minuties d'une première image et vérifier si elles sont contenues dans la seconde. Cependant, rien n'empêche que l'on puisse trouver plusieurs fois une concordance avec la même minutie de l'empreinte deux entre deux minuties de la première empreinte.

Lorsque l'on teste l'algorithme, on se rend compte que pour les empreintes dont les minuties ont pu être bien extraites, cette question ne se pose pas vraiment, car il n'exite pas ou peu de minuties qui ont la même forme de graphe. Le problème vient du fait que l'algorithme d'amélioration d'image n'est pas fait pour améliorer des images de trop mauvaise qualité, d'où lors d'extractions de caractéristiques sur ces images un trop grand nombre de fausses minuties qui sont extraites, ce qui tend à augmenter la liste des minuties concordantes lors de la vérification entre les graphes.

Pour résoudre en partie ce problème, on peut mettre en place une étape supplémentaire dans le calcul de la concordance entre deux minuties. Plutôt que de s'arrêter à la première concordance trouvée entre une minutie d'une image1 et une autre d'une image2, on va calculer toutes les concordances qui existent entre les minuties. Une fois cette tâche accomplie, il convient de réaliser un algorithme d'attribution de minuties pour optimiser le nombre de minuties concordantes.

Au final, cette solution n'est pas optimale, car si elle permet d'éviter la réutilisation d'une même minutie sur plusieurs concordances, elle n'est surtout là que pour pallier aux manques de la méthode d'amélioration sur les images de mauvaise qualité.

### 4.2.4 Analyse de la méthode

La méthode de comparaison est satisfaisante comparée aux besoin initiaux énoncés. En effet, elle permet non seulement de pouvoir comparer deux empreintes d'acquisition différentes avec un taux de réussite acceptable (voir partie Résultats), mais elle est également assez flexible et permet la comparaison d'empreintes ayant subi des translations ou des rotations.

Pour être plus efficace, cette méthode pourrait prendre en compte l'identification du type de l'empreinte (arche, boucle, tourbillon, ...) afin de pouvoir éviter des comparaisons qui n'auraient pas lieu d'être entre des empreintes qui n'auraient pas la même forme.

Un problème majeur de cette solution est qu'elle repose entièrement sur la forme globale du graphe ainsi créé. Si une empreinte venait n'être acquise que partiellement, alors tout une partie du graphe serait manquante et le risque serait alors grand de ne pas trouver suffisamment de concordances pour dire qu'il s'agit bien de la même minutie.

Enfin, un deuxième problème vient du fait que cette solution dépend lourdement du nombre de minuties : plus la taille des listes augmentera, et plus l'algorithme sera long en temps de calculs, ce qui n'est pas gênant ici mais qui le serait plus dans un cas d'utilisation réelle ou un délai d'attente raisonnable

doit être tenu et qui retreint donc le temps alloué aux calculs.

# Chapitre 5

# Résultats

Dans cette section seront discutés les résultats globaux associés à toute la méthode d'analyse et de comparaison d'empreintes réalisée cette année. Pour ce faire, j'ai repris des cas précis de jeux de tests de la FVC pour pouvoir en tirer mes propres conclusions.

A partir d'une série d'une trentaine d'acquisitions de mêmes empreintes et d'empreintes différentes, j'ai pu me faire une idée des avantages et inconvénients des méthodes réalisées.

## 5.1 Partie Amélioration d'empreinte

L'algorithme d'amélioration d'image que j'ai pu développer cette année permet l'amélioration et l'optimisation d'une empreinte pour l'extraction de caractéristiques. Le but était de permettre l'optimisation d'une empreinte en bonne état après acquisition. Cette étape est remplie. Les micro-coupures des empreintes sont réparées et les minuties n'excèdent pas 100 sur une image de bonne qualité. Cependant, l'algorithme mis en place se révèle insuffisant pour une amélioration d'image de moins bonne qualité, en arrivant pas à combler tous les trous de l'empreintes.

## 5.2 Partie Extraction de caractéristiques

Il est difficile d'estimer la réussite ou non de l'algorithme d'extraction de caractéristiques. En effet, celui-ci se repose entièrement sur la partie amélioration d'image. Il a toujours décelé les minuties importantes de l'images, en particulier les bifurcations qui sont rarement de fausses minuties et sur lesquelles on peu donc plus compter.

Du fait de la faiblesse de l'algorithme d'amélioration d'empreintes sur les images de mauvaise qualité, l'extraction est inefficace en générant trop de minuties. Cependant, comme le postulat de base était d'avoir des empreintes de bonne qualité, l'extraction se révèle suffisante.

## 5.3 Partie Comparaison

L'étape de comparaison est une réussite comparé aux objectifs énoncés à la base. L'algorithme mis en place est capable de déterminer la proximité entre deux empreintes, quand bien même elles auraient pu subir des transformations linéaires.

Reste deux problèmes sur lesquels je n'ai pas une l'occasion de me pencher cette année et qui mériteraient une meilleure attention :

- Les transformations non-linéaires d'une empreinte : Lorsque le doigt est plus ou moins appuyé sur le capteur ;
- Les empreintes partielles : lorsque le doigt n'est appuyé que partiellement.

# Chapitre 6

# Conclusion

Ce projet m'a permis de découvrir une nouvelle discipline, à savoir la reconnaissance d'empreintes digitales, et plus généralement la biométrie, tout en renforçant mes connaissance sur le traitement d'images et la programmation, notamment le C++.

Au travers de l'étude des résultats, il est assez facile d'arriver à se rendre compte de la problématique importante de l'analyse et de la comparaison d'empreintes digitales. Encore aujourd'hui, il est assez difficile d'obtenir des algorithmes qui répondent à plusieurs problèmes simultanément, comme pour la comparaison d'empreintes ou l'étude d'un graphe des minuties qui n'est pas entièrement compatible avec la comparaison d'empreintes partielles, ou les problèmes de l'amélioration d'image où l'on doit réussir à améliorer à la fois les captures d'empreintes trop sèches, trop humides, mal cadrées, ...De plus, la partie extraction de caractéristiques a elle aussi son lot de problèmes, à savoir comment déterminer si une minutie se révèle être ou non un faux positif. Il s'agit donc là d'avoir une vraie réflexion de fond sur le problème et de fournir un travail assez conséquent pour pouvoir prétendre à tous les gages de sécurité en matière de faux positifs ou de faux négatifs.

Pour ce qui est des objectifs initiaux liés au projet, je pense qu'ils sont entièrement remplis, avec une solution apportée qui répond à chaque problématique posée. Le temps a manqué pour améliorer certaines parties du projet ou pour implémenter des algorithmes plus poussés, notamment en ce qui concerne la partie amélioration d'image, qui joue un rôle crucial dans le reste du procédé.

Au final, j'ai trouvé ce projet particulièrement intéressant puisqu'il m'a laissé la possibilité de monter en compétences sur de nouveaux sujets avec mes propres moyens en me documentant .

# Chapitre 7

# Glossaire

Binarisation :

La binarisation est un opérateur de traitement d'image qui permet de produire à partir d'une image en niveaux de gris ou en couleurs deux classes de pixels, en général noirs et blancs pour représenter cette même image. L'une des techniques les plus courantes est la binarisation par seuillage : tous les pixels sous un certains seuil seront transformés en pixels noirs tandis que les autres deviendront blancs (Cf figure 7).

(a) Image originale (b) Image binarisée

Fig. 7.1: Binarisation d'un dessin

Opérateurs Morphologiques :

Les deux principaux opérateurs de la morphologie mathématique sont la dilatation et l'érosion. La dilatation permet d'augmenter les zones noires de l'images tandis que l'érosion les diminuent.

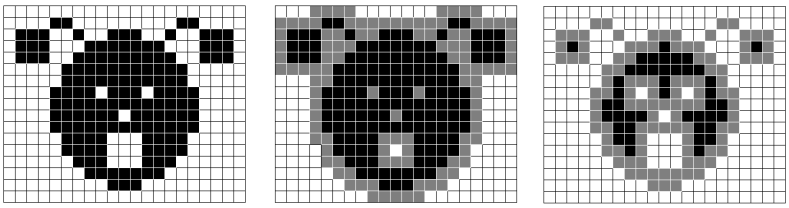


FIG. 7.2: Image source ; Dilatation par un carré 3*3, Erosion par un carré 3*3

LABELLISATION : La labellisation d'une image est un opérateur de traitement d'image qui marque des ensembles de pixels connexes d'une même valeur de niveaux de gris d'un identifiant différent des autres régions de pixels connexes. On obtient donc une cartographie des régions d'une image grâce à une labellisation.

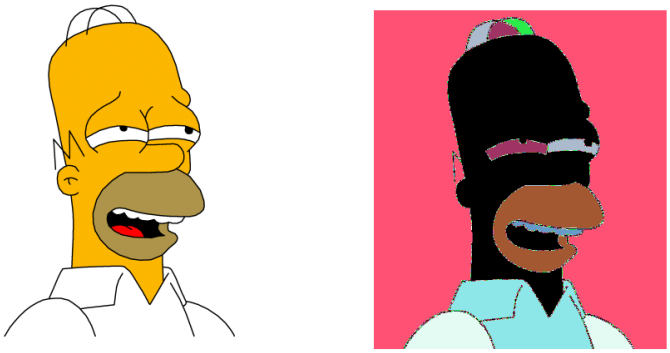


FIG. 7.3: Exemple de labellisation

# Chapitre 8

# Bibliographie

http ://fr.wikipedia.org/
http ://www.biometrie-online.net
http ://www.biometricgroup.com/
http ://www.europeanbiometrics.info/
http ://www.didier-pol.net/1poli-sc.htm
Handbook of Fingerprint Recognition - D. Maltoni, D. Maio, A.K. Jain, S. Prabhakar
Algorithms for Image Processing and Computer Vision - J.R. Parker
http ://www.cse.msu.edu/
http ://www.csse.uwa.edu.au/